

Resource Center

Documentação



1. Blockbit XDR - Guia do Administrador	5
1.1 XDR - Introdução	6
1.2 XDR - Requisitos mínimos	8
1.3 XDR - Arquitetura	9
1.4 XDR - API	11
1.4.1 XDR - API - Atualização dos agentes	14
1.4.2 XDR - API - Configuração	16
1.4.3 XDR - API - Desativação de agente	22
1.4.4 XDR - API - Role Based Access Control	23
1.4.4.1 XDR - API - Referência RBAC	24
1.5 XDR - Dados coletados	29
1.6 XDR - Agentes	31
1.6.1 XDR - Agentes - Comunicação via proxy web	33
1.6.2 XDR - Agentes - Instalando o Agente nos endpoints	35
1.7 XDR - Sistema de buscas	38
1.8 XDR - Primeiro acesso	40
1.9 XDR - Dashboard	42
1.9.1 XDR - Dashboard - Gráficos	43
1.9.2 XDR - Dashboard - Mitre ATT&CK	44
1.9.3 XDR - Dashboard - Overview	45
1.9.4 XDR - Dashboard - Técnicas	46
1.10 XDR - Security Events	47
1.10.1 XDR - Security Events - Hits	49
1.10.2 XDR - Security Events - Lista de eventos	50
1.10.3 XDR - Security Events - Notificações	51
1.10.4 XDR - Security Events - Ransomware Events	52
1.11 XDR - Custom Dashboards	58
1.11.1 XDR - Custom Dashboards - Create Dashboard	59
1.11.2 XDR - Custom Dashboards - Create Visualization	61
1.11.2.1 XDR - Custom Dashboards - How to - Criar visualização	62
1.11.2.2 XDR - Custom Dashboards - Visualizações	64
1.12 XDR - Reports	66
1.13 XDR - Endpoint Control Center	67
1.13.1 XDR - Endpoint Control Center - Criar política	69
1.14 XDR - Endpoints Summary	75
1.14.1 XDR - Endpoints Summary - Configurações	77
1.14.2 XDR - Endpoints Summary - Summary Panel	89
1.15 XDR - Endpoint Groups & Sub-Groups	95
1.15.1 XDR - Endpoint Groups - Inheritance	99
1.15.2 XDR - Endpoint Groups - View details	102
1.15.3 XDR - Endpoints Groups - Active Response	105
1.16 XDR - Users	107
1.16.1 XDR - Security - Roles	108
1.16.1.1 XDR - Security - Create role	110
1.16.2 XDR - Security - Users	113
1.16.2.1 XDR - Security - Create User	115
1.16.3 XDR - Security - Permissions	116
1.16.4 XDR - Security - Multi Factor Authentication	118
1.17 XDR - Indices	119
1.17.1 XDR - Indices - Indices	120
1.17.1.1 XDR - Indices - Indices - Create index	122
1.17.2 XDR - Indices - Settings	125
1.17.3 XDR - Indices - State Management Policies	126
1.17.3.1 XDR - Indices - State Management Policies - JSON editor	127
1.17.3.2 XDR - Indices - State Management Policies - Visual editor	128
1.18 XDR - Audit	131
1.18.1 XDR - Audit - Overview	132
1.18.2 XDR - Audit - Settings	135
1.19 XDR - Quarantine	137
1.20 XDR - Configuration Assessment	139
1.21 XDR - Malware Detection	141
1.22 XDR - File Integrity Monitoring	143
1.23 XDR - Secure Internet Gateway	146
1.23.1 XDR - Secure Internet Gateway - Groups	151
1.23.1.1 XDR - Secure Internet Gateway - Groups - Adlists	152
1.23.1.2 XDR - Secure Internet Gateway - Groups - Clients	154
1.23.1.3 XDR - Secure Internet Gateway - Groups - Domains	155
1.23.2 XDR - Secure Internet Gateway - Local DNS	158
1.23.3 XDR - Secure Internet Gateway - Query Log	160
1.23.3.1 XDR - Secure Internet Gateway - Query Log - Long Term Data	161
1.24 XDR - Threat Hunting	164
1.25 XDR - Threat Monitor - CTI	166
1.25.1 XDR - Threat Monitor - CTI - Dashboard	167
1.25.1.1 XDR - Threat Monitor - CTI - Dashboard - Ações	169
1.25.2 XDR - Threat Monitor - CTI - Analyses	173
1.25.3 XDR - Threat Monitor - CTI - Cases	176
1.25.4 XDR - Threat Monitor - CTI - Observations	178
1.25.5 XDR - Threat Monitor - CTI - Threats	180
1.25.6 XDR - Threat Monitor - CTI - Arsenal	181

1.25.7 XDR - Threat Monitor - CTI - Techniques	184
1.25.8 XDR - Threat Monitor - CTI - Entities	185
1.25.9 XDR - Threat Monitor - CTI - Locations	187
1.25.10 XDR - Threat Monitor - CTI - Events	188
1.25.11 XDR - Threat Monitor - CTI - Data	190
1.25.12 XDR - Threat Monitor - CTI - Trash	193
1.25.13 XDR - Threat Monitor - CTI - Settings	194
1.26 XDR - Vulnerability detection	199
1.26.1 XDR - Vulnerability detection - Inventory	200
1.27 XDR - MITRE ATT&CK	201
1.27.1 XDR - MITRE ATT&CK - Dashboard	202
1.27.2 XDR - MITRE ATT&CK - Framework	203
1.27.3 XDR - MITRE ATT&CK - Intelligence	206
1.28 XDR - Malware Sandboxing	208
1.29 XDR - Security Operations	209
1.29.1 XDR - Security Operations - GDPR	211
1.29.2 XDR - Security Operations - HIPAA	212
1.29.3 XDR - Security Operations - LGPD	213
1.29.4 XDR - Security Operations - NIST 800-53	214
1.29.5 XDR - Security Operations - PCI DDS	215
1.29.6 XDR - Security Operations - TSC	216
1.30 XDR - Cloud Security	217
1.30.1 XDR - Cloud Security - Amazon Web Services	218
1.30.2 XDR - Cloud Security - Azure/Microsoft 365	219
1.30.3 XDR - Cloud Security - Docker	220
1.30.4 XDR - Cloud Security - GitHub	221
1.30.5 XDR - Cloud Security - Google Cloud	222
1.31 XDR - Downloads	223
2. Blockbit ATP Sandbox - Guia do Administrador	224
2.1 Blockbit ATP Sandbox - Introdução e Login	225
2.2 Blockbit ATP Sandbox - Seções	227
2.2.1 Blockbit ATP Sandbox - Dashboard	228
2.2.2 Blockbit ATP Sandbox - Analysis	229
2.2.2.1 Blockbit ATP Sandbox - Overview	231
2.2.2.2 Blockbit ATP Sandbox - Static	233
2.2.2.3 Blockbit ATP Sandbox - Behavior	234
2.2.2.4 Blockbit ATP Sandbox - Network	237
2.2.2.5 Blockbit ATP Sandbox - Screenshot	238
2.2.2.6 Blockbit ATP Sandbox - Report	239

Blockbit XDR - Guia do Administrador

O Blockbit XDR (eXtended Detection and Response) é uma solução baseada em cloud que utiliza aprendizado de máquina para detectar, priorizar e responder ameaças. Ela utiliza dados de diversos endpoints e, com Inteligência Artificial baseada no standard Mitre ATT&CK, oferece a rota mais curta entre detecção e resposta.

Versão da documentação	Lançamento
1.0.0	02/04/2024
1.0.1	15/10/2024
1.0.2	18/12/2024

XDR - Introdução

O Blockbit XDR (eXtended Detection and Response) é uma solução que congrega diversas tecnologias para detectar, priorizar e responder ameaças.

A tecnologia XDR (eXtended Detection and Response) coleta dados de diversos pontos de rede como servidores, e-mail, ambientes de nuvem e endpoints. Esses dados são analisados e contextualizados, permitindo detectar ameaças. Com essas informações, é possível descobrir o escopo e impacto das ameaças, como elas entraram no sistema e o que pode ser afetado. Essas ameaças são, por sua vez, analisadas, contextualizadas e priorizadas para que possam ser tratadas de acordo com o seu nível de risco.

O Blockbit XDR (eXtended Detection & Response) é uma solução avançada de cibersegurança, projetada para oferecer visibilidade, proteção e resposta abrangentes a ameaças em múltiplos vetores, incluindo endpoints, redes, e-mails e ambientes em nuvem.

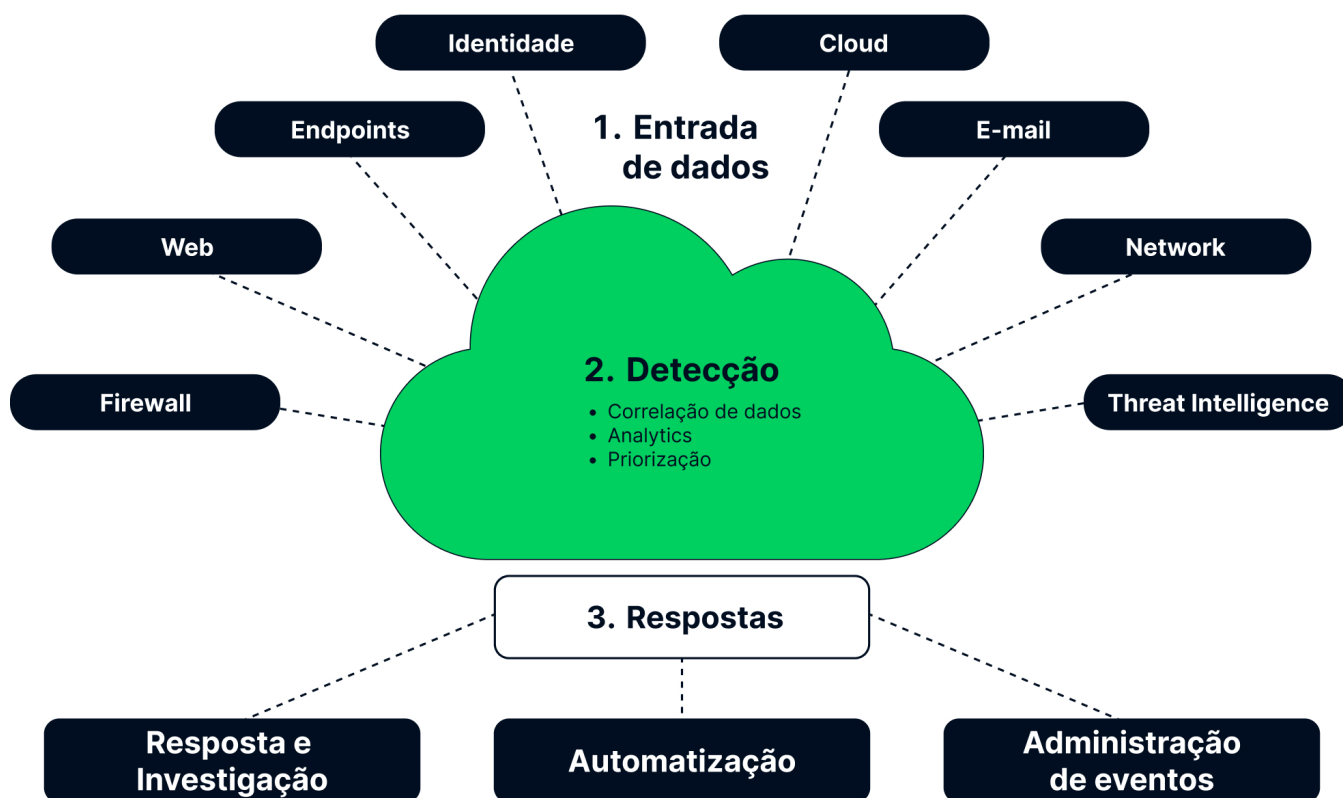
Combinando os recursos de EPP (Endpoint Protection Platform) e EDR (Endpoint Detection and Response), o Blockbit XDR garante uma abordagem completa para a prevenção, detecção e resposta a incidentes cibernéticos.

A solução coleta, analisa e contextualiza dados provenientes de diferentes pontos da rede, permitindo identificar ameaças conhecidas e desconhecidas. Com isso, é possível determinar o escopo e impacto das ameaças, compreender suas origens e os ativos potencialmente comprometidos.

Os recursos de EPP garantem a proteção proativa dos endpoints, bloqueando malware, ataques zero-day e outras ameaças avançadas antes que possam causar danos. Já as funcionalidades de EDR fornecem monitoramento contínuo, análise de comportamento e resposta a incidentes, possibilitando a detecção de atividades suspeitas, investigação forense e contenção automatizada de ameaças.

O Blockbit XDR permite que ações de remediação sejam aplicadas simultaneamente em múltiplos sistemas e eventos, acelerando o processo de mitigação e reduzindo o impacto de ataques coordenados. Essa abordagem garante uma resposta rápida e eficiente, minimizando riscos e evitando a propagação de ameaças em ambientes corporativos.

Como o **Blockbit XDR** funciona:



O Blockbit XDR possui mecanismos avançados de reversão de alterações maliciosas, permitindo a restauração do sistema ao estado anterior ao ataque. A solução realiza backups regulares e mantém registros detalhados de modificações, garantindo resiliência contra ransomware, exclusões acidentais e alterações não autorizadas.

Reversão de Alterações no Sistema

O Blockbit XDR é capaz de desfazer qualquer modificação realizada por um ataque, restaurando configurações do sistema, edições de registro e permissões de arquivos comprometidos.

Recuperação de Arquivos e Dados Criptografados

Para sistemas Windows, a solução pode reverter eventos destrutivos, restaurando arquivos excluídos ou criptografados por ransomware através do console de administração central.

Isolamento e Contenção de Dispositivos na Rede

O Blockbit XDR pode colocar um dispositivo em quarentena, restringindo sua comunicação com a rede para evitar a propagação de ameaças.

Também permite configurar políticas automáticas para isolar máquinas comprometidas (Host Isolation), impedindo que ataques avancem dentro da organização.

Esses recursos garantem resposta rápida, mitigação eficaz e continuidade operacional, minimizando o impacto de ataques cibernéticos.

XDR - Requisitos mínimos

- **Sistemas operacionais suportados**

- a. Windows
 - i. Windows Server 2008 (todas as versões), 2011, 2012, 2012 R2, 2016, 2019, 2022, 2025 e superiores;
 - ii. Windows versão 7 (todas as versões), 8.1, 10, 11 e superiores;
- b. macOS (amd/arm)
 - i. Big Sur, Monterey, Ventura, Sonoma, Sequoia e superiores;
- c. Linux
 - i. Ubuntu, Debian, Raspbian, Fedora, CentOS, Red Hat Enterprise Linux (RHEL), Rocky Linux, AlmaLinux, SUSE Linux Enterprise ou OpenSUSE;
 - ii. Nuvens públicas, como AWS Linux, Oracle Linux, Azure Linux ou Google Cloud Ubuntu Pro;
- d. Solaris
- e. HP-UX
- f. AIX.

- **Tamanho do agente:** entre 50 e 100 MB;

- **Requisito de memória:** entre 10 e 50 MB;

- **Requisito de disco:** entre 50 e 100 MB;

- **Requisito de rede:** 10 KB/sec;

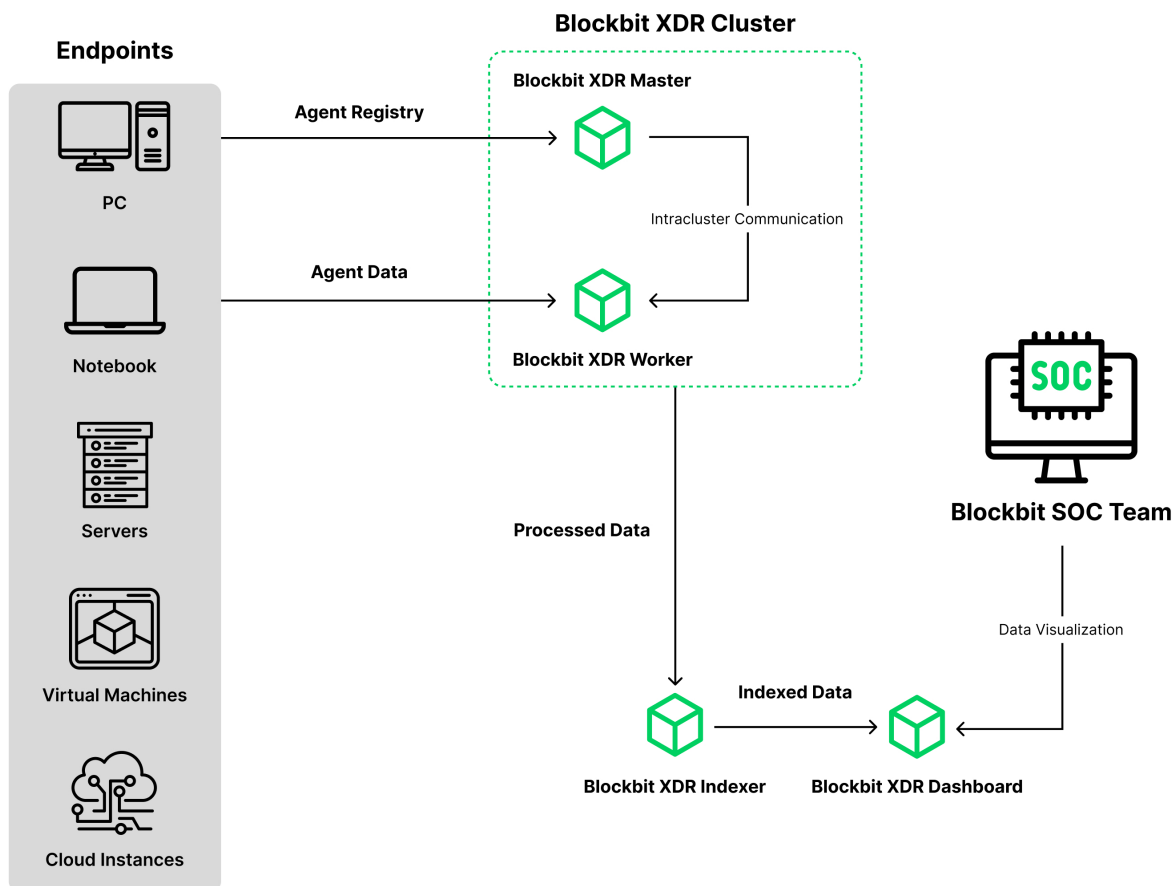
- **Requisito para conectividade entre agentes:** Portas **1514/TCP** e **1515/TCP** abertas para a Internet.

Todos os sistemas operacionais mencionados acima são suportados em instalações nativas em hardware físico, em ambientes de virtualização on-premises, como VMware, KVM entre outras, além de infraestruturas em nuvens públicas e privadas como AWS, Azure,, Google, Oracle entre outras, garantindo flexibilidade e compatibilidade para diversas arquiteturas de TI.

XDR - Arquitetura

A arquitetura do **Blockbit XDR** usa uma abordagem escalável e modular implantada em um ambiente **Kubernetes**. Isso facilita a orquestração dos componentes de maneira distribuída, permitindo alta disponibilidade, escalabilidade e flexibilidade.

Componentes



1. Blockbit XDR Console de Administração e Dashboards:

A console de administração e os dashboards do Blockbit XDR são disponibilizados por meio da nuvem da Blockbit, que é gerenciada, monitorada e continuamente atualizada pela empresa para garantir alta disponibilidade e segurança.

A console de administração é acessível via navegador web, permitindo um acesso unificado ou distribuído a partir de qualquer dispositivo conectado à internet, sem a necessidade de instalação de software adicional. Essa interface centralizada recebe dados indexados pelo Indexer, proporcionando visualização detalhada por meio de gráficos dinâmicos, alertas em tempo real e painéis personalizáveis.

O Blockbit XDR adota uma arquitetura de administração centralizada, permitindo a aplicação de políticas de segurança unificadas, escaláveis de forma simples e ágil, abrangendo desde ambientes com dezenas até milhões de endpoints. Através de um único console de gerenciamento, os administradores podem configurar, monitorar e responder a incidentes de forma eficiente, assegurando a padronização das políticas de segurança, a conformidade com normas regulatórias e a orquestração inteligente dos agentes distribuídos na rede.

A solução utiliza Kubernetes para garantir escalabilidade e disponibilidade contínua da interface, mesmo em cenários de alta demanda, assegurando uma experiência fluida e responsiva para todos os usuários.

2. Endpoints:

PCs, Notebooks, Servidores, Máquinas Virtuais e Instâncias na Nuvem: pontos de origem onde os agentes do Blockbit XDR são instalados, com a função de coletar dados de segurança, como logs, eventos e atividades suspeitas, diretamente dos dispositivos monitorados. Para mais informações, consulte [Agentes](#).

Registro dos Agentes: Cada endpoint registra seus agentes no cluster central do Blockbit XDR. Esses agentes são configurados para enviar dados de segurança para processamento.

Dados dos Agentes: Após o registro, os agentes transmitem os dados coletados para o cluster para processamento e análise.

3. Blockbit XDR Cluster:

Blockbit XDR Master: componente central do cluster, responsável pela comunicação dentro do cluster, gerenciamento de cargas de trabalho e coordenação dos diferentes serviços distribuídos pelo Kubernetes.

Blockbit XDR Worker: realiza a coleta, processamento inicial e envio de dados para outros componentes do sistema.

No **Blockbit XDR Cluster**, tanto os Workers quanto os Indexers podem ser dimensionados conforme a necessidade, permitindo a existência de um ou mais desses componentes. Essa flexibilidade possibilita a distribuição dos serviços entre diferentes sites, locais ou regiões geográficas, assegurando balanceamento de carga e conformidade com políticas específicas dos endpoints.

A console de administração suporta uma implementação baseada em estrutura organizacional sem restrições quanto ao número de sites, locais ou departamentos, permitindo a segmentação granular e a aplicação de políticas com herança em qualquer nível, incluindo configurações específicas para diferentes ambientes.

4. Blockbit XDR Logger e Indexer:

O **Blockbit XDR Logger e Indexer** é responsável por receber e indexar os dados processados do Worker, garantindo um armazenamento seguro e estruturado das informações coletadas. Para proteger a integridade e a confidencialidade dos dados, o Blockbit XDR utiliza criptografia AES-256 para armazenar logs, alertas e eventos de segurança na nuvem da Blockbit.

O acesso às informações é rigorosamente controlado por meio de Role-Based Access Control (RBAC), permitindo que apenas usuários autorizados consultem dados sensíveis. Além disso, o tempo e a capacidade de armazenamento dos registros, incluindo logs processados e não processados, eventos, auditorias e relatórios, são configurados de acordo com os termos estabelecidos no licenciamento e/ou contrato. Essa definição assegura a retenção adequada das informações, garantindo conformidade com as exigências operacionais e regulatórias da organização.

5. Security Operations Center (SOC):

A equipe de SOC utiliza o Dashboard para análise e tomada de decisão, visualizando dados de segurança processados e organizados para identificar ameaças e responder a incidentes em tempo real.

Kubernetes na Arquitetura do Blockbit XDR:

Orquestração e Gestão de Contêineres: Cada componente do Blockbit XDR (Master, Workers, Indexer, Dashboard) pode ser empacotado como um contêiner e orquestrado pelo Kubernetes, facilitando o escalonamento automático, reinicialização em caso de falha e balanceamento de carga entre diferentes nós, em datacenters distribuídos em todos Brasil, na nuvem da Blockbit.

Alta Disponibilidade: O Kubernetes permite implantações com múltiplas réplicas dos serviços, podendo ser executadas para garantir a resiliência do sistema.

Gerenciamento de Configuração: O Kubernetes gerencia dinamicamente as configurações de cada componente do Blockbit XDR, permitindo ajustes conforme a necessidade, sem downtime.

XDR - API

A API do Blockbit XDR é uma RESTful API que permite a interação do Blockbit XDR Manager com qualquer script ou programa capaz de fazer requisições.

Autenticação

A API do Blockbit XDR requer autenticação. Toda chamada precisa incluir um JSON Web Token (JWT). O JWT é um padrão aberto (RFC 7519) que permite a transmissão segura de informações como um objeto JSON.

Para obter um token JWT, chame basicAuth para POST /security/user/authenticate.

Tokens JWT tem uma validade padrão de 900 segundos. Para mudar, chame PUT /security/config. Tokens anteriores à mudança são revogados automaticamente.

Login com usuário e senha:

```
curl -u <USER>:<PASSWORD> -k -X POST "https://<HOST_IP>:55000/security/user/authenticate"
```

Use o token da resposta anterior para qualquer requisição no endpoint:

```
curl -k -X <METHOD> "https://<HOST_IP>:55000/<ENDPOINT>" -H "Authorization: Bearer <YOUR_JWT_TOKEN>"
```

Acesso

Para acessar a API:

Se o SSL (HTTPS) estiver habilitado e a API estiver utilizando o certificado autoassinado, você precisa adicionar o parâmetro -k para evitar verificação da comunicação do servidor.

1 - Use o seguinte comando enviar uma requisição de autenticação de usuário via POST:

Troque os valores <BLOCKBITXDR_API_USER> e <BLOCKBITXDR_API_PASSWORD> para as suas credenciais.

Substitua a variável TOKEN pela resposta JWT.

```
TOKEN=$(curl -u <BLOCKBITXDR_API_USER>:<BLOCKBITXDR_API_PASSWORD> -k -X POST "https://localhost:55000/security/user/authenticate?raw=true")
```

2 - Verifique se o TOKEN foi gerado.

A resposta deve ser algo assim:

```
eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJ3YXp1aCIsImF1ZCI6IldhenVoIEFQSSBSRVNUIiwibmJmIjoxNzA3ODk4NTEzLCJleHAiOjE3Mjc4NDk0MTM5InN1YiI6IndhenVoIiwicnVuc2FzIjpmYWxzZSwicmJhY19yb2xlcYI6WzFkLCJyYmFjX21vZGU0IjE3Mjc4NDk0MTM5LmF1ZCJ3dV3SnT0C-PV2oGZGcyH3GpStS0u161UHHT7w6eUm_REOP_g8SqqIJDDW0gCcQNJTEECortIuI4zj7nybNhACRlBrDBZoG4Re4HXEpAchyFQXwq0SsZ3HHSj7eJinBF0pJDG0D8d1_LkcoxaX3FpxpsCZ4xzJ492CpnVZLT8qI4
```

3 - Envie uma requisição:

```
curl -k -X GET "https://localhost:55000/" -H "Authorization: Bearer $TOKEN"
```

A resposta deve ser assim:

```
{
  "data": {
    "title": "Blockbit XDR API REST",
    "api_version": "4.7.4",
    "revision": 40717,
    "license_name": "GPL 2.0",
    "license_url": "https://github.com/blockbitxdr/blockbitxdr/blob/master/LICENSE",
    "hostname": "blockbitxdr-master",
    "timestamp": "2024-05-14T21:34:15Z"},
  "error": 0
}
```

Depois de entrar, você pode acessar qualquer endpoint utilizando a estrutura abaixo:

Troque <METHOD> pelo método desejado e <ENDPOINT> pelo endpoint desejado.

```
curl -k -X <METHOD> "https://localhost:55000/<ENDPOINT>" -H "Authorization: Bearer $TOKEN"
```

Requisições e respostas

A API do XDR Blockbit tem três componentes principais: o método de requisição (GET, POST, PUT, ou DELETE), a URL que especifica o endpoint e o header de autorização com o JWT.

Exemplo cURL:

```
curl -k -X GET "https://localhost:55000/agents/summary/os?pretty=true" -H "Authorization: Bearer $TOKEN"
```

O comando cURL para cada requisição tem os seguintes campos:

Campo	Descrição
-X GET/POST/PUT/DELETE	Especifica o método da requisição.
http://<BLOCKBITXDR_MANAGER_IP>:55000/<ENDPOINT> https://<BLOCKBITXDR_MANAGER_IP>:55000/<ENDPOINT>	Especifica as URLs dos endpoints.
-H "Authorization: Bearer <YOUR_JWT_TOKEN>"	Especifica a autorização JWT
-k	Suprime erros de SSL

As respostas tem a seguinte estrutura:

Campo	Subcampos	Descrição
data	affected_items	Lista os itens afetados.
	total_affected_items	Mostra o total de itens afetados.
	failed_items	Lista os itens que falharam.
	total_failed_items	Mostra o total de itens que falharam.
message		Descrição do resultado
error		Descrição do erro.

A API pode dar as seguintes respostas

Resposta	Descrição
200	Tudo certo.
400	Bad request. Requisição não aceita por algum erro.

401	Unauthorized. Requisição sem chave de API válida.
402	Request failed. A requisição falhou, mesmo com parâmetros válidos.
403	Forbidden. A chave API não tem permissão para realizar a requisição.
404	Not found. O recurso para a requisição não existe.
409	Conflict. A requisição entra em conflito com outra.
429	Too many requests. Mais requisições que a capacidade da API.
500, 502, 503 e 504	Server error. Erro no servidor Blockbit XDR.

Exemplo de resposta:

```
{
  "data": {
    "affected_items": [
      "master-node",
      "worker1"
    ],
    "total_affected_items": 2,
    "failed_items": [],
    "total_failed_items": 0
  },
  "message": "Restart request sent to all specified nodes",
  "error": 0
}
```

XDR - API - Atualização dos agentes

A atualização do agente do Blockbit XDR nos endpoints ocorre de forma transparente e automatizada, garantindo zero impacto no desempenho ou na operação dos dispositivos protegidos. O processo é otimizado para evitar interrupções, assegurando a continuidade das atividades dos usuários.

Para realizar a atualização do agente, siga os passos abaixo:

1 - Verificar a versão atual dos agentes

Antes de atualizar, verifique quais agentes estão desatualizados. Você pode fazer isso via API ou interface do Blockbit XDR.

API

Para listar os agentes desatualizados por API, execute o seguinte comando:

```
bash curl -k -X GET "https://<BLOCKBIT_XDR_MANAGER_IP>:55000/agents/outdated" -H "Authorization: Bearer <YOUR_JWT_TOKEN>"
```

Substitua <BLOCKBIT_XDR_MANAGER_IP> pelo IP do seu manager.

Substitua <YOUR_JWT_TOKEN> pelo seu token JWT.

2. Atualizar os agentes manualmente

Para atualizar um agente específico, use o seguinte comando:

```
bash curl -k -X PUT "https://<BLOCKBIT_XDR_MANAGER_IP>:55000/agents/upgrade" -H "Authorization: Bearer <YOUR_JWT_TOKEN>"
```

Para atualizar todos os agentes, use o seguinte comando:

```
bash curl -k -X PUT "https://<BLOCKBIT_XDR_MANAGER_IP>:55000/agents/upgrade_custom" -H "Authorization: Bearer <YOUR_JWT_TOKEN>"
```

3 - Atualizar os agentes em grupo

Para atualizar agentes de um grupo específico, use o seguinte comando

```
bash curl -k -X PUT "https://<BLOCKBIT_XDR_MANAGER_IP>:55000/agents/group/<GROUP_ID>/upgrade" -H "Authorization: Bearer <YOUR_JWT_TOKEN>"
```

Substitua <GROUP_ID> pelo ID do grupo que deseja atualizar.

4 - Reiniciar os agentes

Após atualizar, reinicie os agentes:

```
bash curl -k -X PUT "https://<BLOCKBIT_XDR_MANAGER_IP>:55000/agents/restart" -H "Authorization: Bearer <YOUR_JWT_TOKEN>"
```

5 - Verificar se a atualização foi bem-sucedida

Para mostrar a versão do agente em execução, use o comando

```
bash curl -k -X GET "https://<BLOCKBIT_XDR_MANAGER_IP>:55000/agents/summary/os" -H "Authorization: Bearer <YOUR_JWT_TOKEN>"
```

XDR - API - Configuração

A API do XDR pode ser configurada no servidor Blockbit XDR. Por definição, todas as opções estão comentadas. Para aplicar uma configuração, descomente e edite.

Ao rodar a API do XDR em cluster, toda configuração feita no nó mestre precisa ser replicada **manualmente** nos outros nós.

```
host: ['0.0.0.0', '::']
port: 55000

drop_privileges: yes
experimental_features: no
max_upload_size: 10485760

intervals:
  request_timeout: 10

https:
  enabled: yes
  key: "server.key"
  cert: "server.crt"
  use_ca: False
  ca: "ca.crt"
  ssl_protocol: "auto"
  ssl_ciphers: ""

logs:
  level: "info"
  format: "plain"
  max_size:
    enabled: false

cors:
  enabled: no
  source_route: ""
  expose_headers: ""
  allow_headers: ""
  allow_credentials: no

access:
  max_login_attempts: 50
  block_time: 300
  max_request_per_minute: 300

upload_configuration:
  remote_commands:
    localfile:
      allow: yes
      exceptions: []
    wodle_command:
      allow: yes
      exceptions: []
  limits:
    eps:
      allow: yes
  agents:
    allow_higher_versions:
      allow: yes
  indexer:
    allow: yes
  integrations:
    virustotal:
      public_key:
        allow: yes
        minimum_quota: 240
```

Após configurar, reinicie a API com o seguinte comando:

```
systemctl restart blockbit-xdr-manager
```

Opções de configuração

host

Valores permitidos	Valor padrão	Descrição
Uma lista de IPs ou hostnames válidos	['0.0.0.0', '::']	/Endereços de IP ou hostnames onde a API do XDR está rodando.

port

Valores permitidos	Valor padrão	Descrição
Entre 1 e 65535	55000	Porta onde a API do XDR irá ouvir.

drop_privileges

Valores permitidos	Valor padrão	Descrição
sim, verdadeiro, não, falso	verdadeiro	Executar o processo blockbit-xdr-api como o usuário.

experimental_features

Valores permitidos	Valor padrão	Descrição
sim, verdadeiro, não, falso	falso	Habilitar recursos em desenvolvimento.

max_upload_size

Valores permitidos	Valor padrão	Descrição
Qualquer número inteiro positivo	10485760	Definir o tamanho máximo do corpo que a API pode aceitar, em bytes (0 -> ilimitado).

intervals

Subcampo	Valores permitidos	Valor padrão	Descrição
request_timeout	Qualquer número inteiro positivo	10	Definir o tempo máximo de resposta (em segundos) para cada solicitação da API.

https

Subcampos	Valores permitidos	Valor padrão	Descrição
enabled	sim, verdadeiro, não, falso	verdadeiro	Habilitar ou desabilitar SSL (https) na API do servidor Blockbit XDR.
key	Qualquer string de texto	server.key	Nome da chave privada.
cert	Qualquer string de texto	server.crt	Nome do certificado.
use_ca	sim, verdadeiro, não, falso	falso	Se deve ou não usar um certificado de uma Autoridade Certificadora.
ca	Qualquer string de texto	ca.crt	Nome do certificado da Autoridade Certificadora (CA).
ssl_protocol	TLS, TLSv1, TLSv1.1, TLSv1.2, auto	auto	Protocolo SSL a ser permitido. Seu valor não diferencia maiúsculas de minúsculas.
ssl_ciphers	Qualquer string de texto	Nenhum	Cifras SSL a serem permitidas. Seu valor não diferencia maiúsculas de minúsculas.

logs

Subcampos	Valores permitidos	Valor padrão	Descrição
level	desativado, informação, aviso, erro, depuração, depuração2 (cada nível inclui o nível anterior)	informação	Definir o nível de verbosidade dos logs da API do servidor Blockbit XDR.
format	simples, json ou ambos (simples,json)	simples	Definir o formato dos logs da API do servidor Blockbit XDR.

max_size

Subcampos	Valores permitidos	Valor padrão	Descrição
enabled	sim, verdadeiro, não, falso	falso	Alternar entre rotação de logs da API Blockbit XDR baseada em tempo e em tamanho. Habilitar esta opção desativa a rotação baseada em tempo, habilitando a rotação baseada em tamanho de arquivo.
size	Qualquer número positivo seguido por uma unidade válida. K/k para kilobytes, M/m para megabytes.	1M	Definir o tamanho máximo do arquivo para não acionar a rotação de logs baseada em tamanho. Valores menores que 1 M são considerados como 1 M.size

cors

Subcampos	Valores permitidos	Valor padrão	Descrição
enabled	sim, verdadeiro, não, falso	falso	Habilitar ou desabilitar o uso de CORS na API do servidor Blockbit XDR.
source_route	Qualquer string de texto	*	Fontes para as quais os recursos estarão disponíveis. Por exemplo http://client.example.org .
expose_headers	Qualquer string de texto	*	Quais cabeçalhos podem ser expostos como parte da resposta.
allow_headers	Qualquer string de texto	*	Quais cabeçalhos HTTP podem ser usados durante a solicitação real.
allow_credentials	sim, verdadeiro, não, falso	falso	Informar aos navegadores se devem expor a resposta ao JavaScript frontend ou não.

access

Subcampos	Valores permitidos	Valor padrão	Descrição
max_login_attempts	Qualquer número inteiro positivo	50	Definir um número máximo de tentativas de login durante um número especificado de segundos de block_time.
block_time	Qualquer número inteiro positivo	300	Período de tempo estabelecido (em segundos) para tentar solicitações de login. Se o número estabelecido de solicitações (max_login_attempts) for excedido dentro desse limite de tempo, o endereço IP é bloqueado até o final do período de block_time.
max_request_per_minute	Qualquer número inteiro positivo	300	O número máximo de solicitações permitidas por minuto. Aplica-se a todos os endpoints da API do servidor Blockbit XDR, exceto para solicitações de autenticação. Atingir esse limite em menos de um minuto bloqueia todas as solicitações recebidas de qualquer usuário pelo tempo restante. Um valor de 0 desativa esse recurso. Para solicitações POST /events, o valor efetivo é 30 para valores maiores que 30.

upload_configuration

remote_commands (localfile e wodle "command")

Subcampos	Valores permitidos	Valor padrão	Descrição
allow	sim, verdadeiro, não, falso	verdadeiro	Permitir upload de configurações com comandos remotos através da API do servidor Blockbit XDR. Definir esta opção como falso impede o upload de arquivos ossec.conf que contêm a opção wodle "command" ou a opção <command> dentro da tag localfile.
exceptions	lista de comandos	[]	Definir uma lista de comandos permitidos para upload através da API. Essas exceções sempre podem ser carregadas independentemente da configuração allow.

limits

eps

Subcampo	Valores permitidos	Valor padrão	Descrição
allow	sim, verdadeiro, não, falso	verdadeiro	Permitir upload de configurações com limites de EPS modificados através da API do servidor Blockbit XDR. Definir esta opção como falso impede o upload de arquivos ossec.conf se a seção <limits><eps> dentro da tag global tiver sido alterada.

agents

allow_higher_versions

Subcampo	Valores permitidos	Valor padrão	Descrição
allow	sim, verdadeiro, não, falso	verdadeiro	Permitir upload de configurações que aceitam versões superiores de agentes através da API do servidor Blockbit XDR. Definir esta opção como falso impede o upload de arquivos ossec.conf que contenham a seção <allow_higher_versions> com o valor sim dentro das tags auth ou remote.

indexer

Subcampo	Valores permitidos	Valor padrão	Descrição
allow	sim, verdadeiro, não, falso	verdadeiro	Permite upload de uma seção de configuração do indexador atualizada através da API do servidor Blockbit XDR. Definir esta opção como falso impede a atualização da configuração do indexador ao carregar ossec.conf.

integrations

virustotal (public_key)

Subcampos	Valores permitidos	Valor padrão	Descrição
allow	sim, verdadeiro, não, falso	verdadeiro	Permite upload de uma seção de configuração de integração do VirusTotal atualizada usando uma chave de API pública através da API do servidor Blockbit XDR. Definir esta opção como falso impede a atualização da configuração de integrações do VirusTotal ao carregar ossec.conf.
minimum_quota	Qualquer número inteiro positivo	240	Valor mínimo de cota para a chave de API pública do VirusTotal.

Configuração de segurança da API do servidor Blockbit XDR

Você pode consultar e modificar a configuração de segurança, incluindo as configurações **auth_token_exp_timeout** e **rbac_mode**, exclusivamente através dos endpoints da API do servidor Blockbit XDR:

GET /security/config,

PUT /security/config

DELETE /security/config.

O **auth_token_exp_timeout** define a duração em segundos antes de um token de autenticação expirar e exigir renovação.

O **rbac_mode** determina o comportamento geral do sistema de Controle de Acesso Baseado em Funções, que pode ser configurado para permitir ou restringir amplamente o acesso a recursos e endpoints com base em funções e permissões de usuário.

A configuração é aplicada a cada API do servidor Blockbit XDR em um cluster, se aplicável.

```
auth_token_exp_timeout: 900 rbac_mode: white
```

A alteração da configuração de segurança revoga todos os JWTs. Você precisará fazer login e obter um novo token após a alteração.

Opções de configuração de segurança

auth_token_exp_timeout

Valores permitidos	Valor padrão	Descrição
Qualquer número inteiro positivo	900	Definir quantos segundos são necessários para que os tokens JWT expirem.
Qualquer número inteiro positivo	240	Valor mínimo de cota para a chave de API pública do VirusTotal.

rbac_mode

Valores permitidos	Valor padrão	Descrição
black, white	white	Definir o comportamento do RBAC. Por padrão, tudo é permitido no modo black enquanto tudo é negado no modo white. Escolha o rbac_mode que melhor se adapte à infraestrutura RBAC desejada. No modo black, é muito fácil negar alguns pares de ação-recurso específicos com apenas algumas políticas, enquanto o modo white é mais seguro e requer construção do zero.

Endpoints de configuração

A API do servidor Blockbit XDR possui vários endpoints que permitem consultar sua configuração atual.

Obter configuração

GET /manager/api/config: Obtenha a configuração completa da API do servidor Blockbit XDR local.

GET /cluster/api/config: Obtenha a configuração completa da API do servidor Blockbit XDR de todos (ou de uma lista) dos nós do cluster.

GET /security/config: Obtenha a configuração de segurança atual.

Modificar configuração

PUT /security/config: Modifique a configuração de segurança.

Restaurar configuração

DELETE /security/config: Restaure a configuração de segurança padrão.

Certificado SSL

Este processo é feito automaticamente quando a API do servidor Blockbit XDR é executada pela primeira vez.

O certificado SSL garante comunicação segura entre a API do servidor Blockbit XDR e seus clientes.

Para gerar novos certificados para a API do servidor Blockbit XDR:

Gere a chave e a solicitação de certificado (o pacote openssl é necessário):

```
cd /var/ossec/api/configuration/ssl openssl req -newkey rsa:2048 -new -nodes -x509 -days 365 -keyout server.key -out server.crt
```

Por padrão, a senha da chave deve ser inserida toda vez que o servidor for executado. Se a chave foi gerada pela API do servidor Blockbit XDR ou pelo comando acima, ela não terá uma senha.

(Opcional) Proteja a chave com uma senha:

```
ssh-keygen -p -f server.key
```

Você será solicitado a inserir e confirmar a nova senha.

XDR - API - Desativação de agente

Para desativar um agente via API, utilize os seguintes comandos:

- **Para desconectar um agente temporariamente:**

```
bash curl -X PUT "https://<XDR_MANAGER_IP>:55000/agents/<AGENT_ID>/restart" \ -H "Authorization: Bearer <YOUR_JWT_TOKEN>"
```

O agente irá reiniciar e parar de comunicar com **XDR Manager** temporariamente.

- **Para forçar a reconexão do agente:**

```
bash curl -X PUT "https://<XDR_MANAGER_IP>:55000/agents/reconnect" \ -H "Authorization: Bearer <YOUR_JWT_TOKEN>"
```

XDR - API - Role Based Access Control

A API do Blockbit XDR oferece o Role Based Access Control, ou RBAC (Controle de Acesso Baseado em Função). Ele permite o controle do acesso a endpoints e recursos baseado em privilégios de usuários.

Para mais informações, vá em [Security](#).

Políticas de RBAC

As políticas controlam as permissões da API usando três elementos: ações, recursos e efeito.

- **Ações** representam uma hierarquia de ações que um usuário pode realizar.

Exemplo: reiniciar agente.

```
agent:restart
```

- **Recursos** são qualquer entidade sujeita a uma ação. O conjunto de recursos é dinâmico, mas os tipos são estáticos.

```
agent:id:001 node:id:*
```

- **Efeito:** pode ser apenas "permitir" ou "negar".

Modos de RBAC

Na API do Blockbit XDR, há dois modos de RBAC: lista negra e lista branca. Esses modos irão definir como serão tratadas as ações dos usuários e as responsabilidades do administrador.

Lista negra (black): permite todas as ações por padrão. O administrador define quais ações vão ser proibidas.

Lista branca (white): proíbe todas as ações por padrão. O administrador define quais ações vão ser permitidas.

XDR - API - Referência RBAC

Nesta página, podem ser encontradas ações, recursos e efeitos de políticas RBAC na API do Blockbit XDR.

Recurso	Descrição	Exemplo
agent:group	Referência a agentes via nome do grupo.	agent:group:web
agent:id	Referência a agentes via ID do agente.	agent:id:001
group:id	Referência a grupos de agentes via ID do grupo.	group:id:default
node:id	Referência ao nó do cluster via ID do nó.	node:id:worker1
decoder:file	Referência ao arquivo de decodificador via nome do arquivo.	decoder:file:0005-blockbit_xdr_decoder.xml
list:file	Referência ao arquivo de lista via nome do arquivo.	list:file:audit-keys
rule:file	Referência ao arquivo de regras via nome do arquivo.	rule:file:0610-win-ms_logs_rules.xml
policy:id	Referência à política de segurança via ID.	policy:id:1
role:id	Referência ao papel de segurança via ID.	role:id:1
rule:id	Referência à regra de segurança via ID.	rule:id:1
user:id	Referência ao usuário de segurança via ID.	user:id:1

Ações

Em cada ação, os endpoints afetados são especificados junto com os recursos necessários, seguindo esta estrutura: <Método> <Endpoint> (<Recurso>).

active_response

O endpoint /active-response da API permite aos usuários interagir com o módulo de Resposta Ativa.

active_response:command

PUT /active-response (agent:id, agent:group)

agent

O endpoint /agents da API permite aos usuários registrar e gerenciar agentes no servidor .

agent:create

POST /agents (:)
POST /agents/insert (:)
POST /agents/insert/quick (:)

agent:delete

DELETE /agents (agent:id, agent:group)

agent:modify_group

DELETE /agents/group (agent:id, agent:group)
DELETE /agents/{agent_id}/group (agent:id, agent:group)
DELETE /agents/{agent_id}/group/{group_id} (agent:id, agent:group)
PUT /agents/group (agent:id, agent:group)
PUT /agents/{agent_id}/group/{group_id} (agent:id, agent:group)

agent:read

GET /agents (agent:id, agent:group)
GET /agents/outdated (agent:id, agent:group)
GET /agents/stats/distinct (agent:id, agent:group)
GET /agents/summary/os (agent:id, agent:group)
GET /agents/summary/status (agent:id, agent:group)
GET /agents/{agent_id}/config/{component}/{configuration} (agent:id, agent:group)
GET /agents/{agent_id}/daemons/stats (agent:id, agent:group)
GET /agents/{agent_id}/key (agent:id, agent:group)
GET /agents/no_group (agent:id, agent:group)
GET /groups/{group_id}/agents (agent:id, agent:group)
GET /agents/{agent_id}/stats/{component} (agent:id, agent:group)
GET /overview/agents (agent:id, agent:group)

agent:reconnect

PUT /agents/reconnect (agent:id, agent:group)

agent:restart

PUT /agents/group/{group_id}/restart (agent:id, agent:group)
 PUT /agents/node/{node_id}/restart (agent:id, agent:group)
 PUT /agents/restart (agent:id, agent:group)
 PUT /agents/{agent_id}/restart (agent:id, agent:group)

agent:upgrade

GET /agents/upgrade_result (agent:id, agent:group)
 PUT /agents/upgrade (agent:id, agent:group)
 PUT /agents/upgrade_custom (agent:id, agent:group)

cluster

O endpoint /cluster da API permite aos usuários gerenciar a configuração e a integridade do nó mestre e dos nós de trabalho no cluster.

cluster:read_api_config

GET /cluster/api/config (node:id)

cluster:read

GET /cluster/configuration/validation (node:id)
 GET /cluster/healthcheck (node:id)
 GET /cluster/local/config (node:id)
 GET /cluster/local/info (node:id)
 GET /cluster/nodes (node:id)
 GET /cluster/{node_id}/configuration (node:id)
 GET /cluster/{node_id}/configuration/{component}/{configuration} (node:id)
 GET /cluster/{node_id}/daemons/stats (node:id)
 GET /cluster/{node_id}/info (node:id)
 GET /cluster/{node_id}/logs (node:id)
 GET /cluster/{node_id}/logs/summary (node:id)
 GET /cluster/{node_id}/stats (node:id)
 GET /cluster/{node_id}/stats/hourly (node:id)
 GET /cluster/{node_id}/stats/weekly (node:id)
 GET /cluster/{node_id}/status (node:id)
 PUT /agents/node/{node_id}/restart (node:id)
 PUT /cluster/restart (node:id)
 GET /cluster/ruleset/synchronization (node:id)

cluster:restart

PUT /cluster/restart (node:id)

cluster:status

GET /cluster/status (:)

cluster:update_config

PUT /cluster/{node_id}/configuration (node:id)

decoders

O endpoint /decoder da API permite aos usuários gerenciar e recuperar informações sobre os decodificadores incluídos no servidor.

decoders:read

GET /decoders (decoder:file)
 GET /decoders/files (decoder:file)
 GET /decoders/files/{filename} (decoder:file)
 GET /decoders/parents (decoder:file)

decoders:update

PUT /decoders/files/{filename} (:)

decoders:delete

PUT /decoders/files/{filename} (:)
 DELETE /decoders/files/{filename} (decoder:file)

Event

O endpoint /event da API permite aos usuários ingerir eventos de segurança para o mecanismo de análise.

event:ingest

POST /events (:)

Group

O endpoint /groups da API permite aos usuários agrupar agentes em subconjuntos distintos para configurações centralizadas.

group:create

POST /groups (:)

group:delete

DELETE /groups (group:id)

group:modify_assignments

```
DELETE /agents/group (group:id)
DELETE /agents/{agent_id}/group (group:id)
DELETE /agents/{agent_id}/group/{group_id} (group:id)
PUT /agents/group (group:id)
PUT /agents/{agent_id}/group/{group_id} (group:id)
```

group:read

```
GET /groups (group:id)
GET /groups/{group_id}/agents (group:id)
GET /groups/{group_id}/configuration (group:id)
GET /groups/{group_id}/files (group:id)
GET /groups/{group_id}/files/{file_name} (group:id)
GET /overview/agents (group:id)
```

group:update_config

```
PUT /groups/{group_id}/configuration (group:id)
```

Lists

O endpoint /lists da API permite aos usuários recuperar e gerenciar as listas CDB que são usadas para verificar arquivos maliciosos nos agentes.

lists:read

```
GET /lists (list:file)
GET /lists/files (list:file)
GET /lists/files/{filename} (list:file)
```

lists:update

```
PUT /lists/files/{filename} (:)
```

lists:delete

```
DELETE /lists/files/{filename} (list:file)
PUT /lists/files/{filename} (:)
```

Logtest

O endpoint /logtest da API permite aos usuários testar e verificar novas regras e decodificadores contra exemplos de logs fornecidos no mecanismo de análise.

logtest:run

```
PUT /logtest (:)
DELETE /logtest/sessions/{token} (:)
```

Manager

O endpoint /manager da API permite aos usuários gerenciar e coletar informações relevantes do gerenciador.

manager:read_api_config

```
GET /manager/api/config (:) 
```

manager:read

```
GET /manager/configuration (:)
GET /manager/configuration/validation (:)
GET /manager/configuration/{component}/{configuration} (:)
GET /manager/daemons/stats (:)
GET /manager/info (:)
GET /manager/logs (:)
GET /manager/logs/summary (:)
GET /manager/stats (:)
GET /manager/stats/analysisid (:)
GET /manager/stats/hourly (:)
GET /manager/stats/remoted (:)
GET /manager/stats/weekly (:)
GET /manager/status (:)
PUT /manager/restart (:) 
```

manager:restart

```
PUT /manager/restart (:) 
```

manager:update_config

```
PUT /manager/configuration (:) 
```

MITRE

O endpoint /mitre da API permite aos usuários recuperar uma visão geral das táticas e técnicas correspondentes do banco de dados MITRE ATT&CK.

mitre:read

GET /mitre/metadata (:)
GET /mitre/tactics (:)
GET /mitre/techniques (:)
GET /mitre/groups (:)
GET /mitre/mitigations (:)
GET /mitre/software (:)
GET /mitre/references (:)

Rootcheck

O endpoint /rootcheck da API permite aos usuários interagir com o módulo rootcheck e recuperar resultados das varreduras nos agentes.

rootcheck:clear

DELETE /rootcheck/{agent_id} (agent:id, agent:group)
DELETE /experimental/rootcheck (agent:id, agent:group)

rootcheck:read

GET /rootcheck/{agent_id} (agent:id, agent:group)
GET /rootcheck/{agent_id}/last_scan (agent:id, agent:group)

rootcheck:run

PUT /rootcheck (agent:id, agent:group)

Rules

O endpoint /rules da API permite aos usuários gerenciar e recuperar informações sobre as regras usadas para analisar eventos recebidos e gerar alertas.

rules:read

GET /rules (rule:file)

GET /rules/files (rule:file)

GET /rules/files/{filename} (rule:file)

GET /rules/groups (rule:file)

GET /rules/requirement/{requirement} (rule:file)

rules:update

PUT /rules/files/{filename} (:)

rules:delete

PUT /rules/files/{filename} (:)
DELETE /rules/files/{filename} (rule:file)

SCA

O endpoint /sca da API permite aos usuários interagir com o módulo SCA e coletar os resultados relevantes das varreduras SCA dos agentes.

sca:read

GET /sca/{agent_id} (agent:id, agent:group)

GET /sca/{agent_id}/checks/{policy_id} (agent:id, agent:group)

Security

O endpoint /security da API permite que os administradores gerenciem aspectos relacionados à segurança no ambiente.

security:create_user

POST /security/users (:)

security:create

POST /security/policies (:)
POST /security/roles (:)
POST /security/rules (:)

security:delete

DELETE /security/policies (policy:id)
DELETE /security/roles (role:id)
DELETE /security/roles/{role_id}/policies (role:id, policy:id)
DELETE /security/roles/{role_id}/rules (role:id, rule:id)
DELETE /security/rules (rule:id)
DELETE /security/users (user:id)
DELETE /security/users/{user_id}/roles (user:id, role:id)

security:edit_run_as

PUT /security/users/{user_id}/run_as (:)

security:read_config

GET /security/config (:)

security:read

GET /security/policies (policy:id)
GET /security/roles (role:id)
GET /security/rules (rule:id)
GET /security/users (user:id)

security:revoke

PUT /security/user/revoke (:)

security:update_config

DELETE /security/config (:)
PUT /security/config (:)

security:update

POST /security/roles/{role_id}/policies (role:id, policy:id)
POST /security/roles/{role_id}/rules (role:id, rule:id)
POST /security/users/{user_id}/roles (user:id, role:id)
PUT /security/policies/{policy_id} (policy:id)
PUT /security/roles/{role_id} (role:id)
PUT /security/rules/{rule_id} (rule:id)
PUT /security/users/{user_id} (user:id)

Monitoramento de integridade de arquivos

O endpoint /syscheck da API permite aos usuários interagir com o módulo de Monitoramento de Integridade de Arquivos, realizando varreduras de rotina e recuperando os resultados do syscheck.

syscheck:clear

DELETE /experimental/syscheck (agent:id, agent:group)
DELETE /syscheck/{agent_id} (agent:id, agent:group)

syscheck:read

GET /syscheck/{agent_id} (agent:id, agent:group)
GET /syscheck/{agent_id}/last_scan (agent:id, agent:group)

syscheck:run

PUT /syscheck (agent:id, agent:group)

Syscollector

O endpoint /syscollector da API permite aos usuários coletar informações do sistema de endpoints monitorados e enviá-las para o servidor.

syscollector:read

GET /experimental/syscollector/hardware (agent:id, agent:group)
GET /experimental/syscollector/hotfixes (agent:id, agent:group)
GET /experimental/syscollector/netaddr (agent:id, agent:group)
GET /experimental/syscollector/netiface (agent:id, agent:group)
GET /experimental/syscollector/netproto (agent:id, agent:group)
GET /experimental/syscollector/os (agent:id, agent:group)
GET /experimental/syscollector/packages (agent:id, agent:group)
GET /experimental/syscollector/ports (agent:id, agent:group)
GET /experimental/syscollector/processes (agent:id, agent:group)

GET /syscollector/{agent_id}/hardware (agent:id, agent:group)
GET /syscollector/{agent_id}/hotfixes (agent:id, agent:group)
GET /syscollector/{agent_id}/netaddr (agent:id, agent:group)
GET /syscollector/{agent_id}/netiface (agent:id, agent:group)
GET /syscollector/{agent_id}/netproto (agent:id, agent:group)
GET /syscollector/{agent_id}/os (agent:id, agent:group)
GET /syscollector/{agent_id}/packages (agent:id, agent:group)
GET /syscollector/{agent_id}/ports (agent:id, agent:group)
GET /syscollector/{agent_id}/processes (agent:id, agent:group)

Tasks

O endpoint /tasks da API permite aos usuários obter informações de status sobre as tarefas realizadas pelo manager.

task:status

GET /tasks/status (:)

XDR - Dados coletados

O **Blockbit XDR** garante a proteção dos dados dos dispositivos gerenciados por meio de **criptografia robusta**, tanto em repouso quanto durante a transmissão. Todas as informações são processadas e correlacionadas automaticamente, resultando na geração de logs e alertas em tempo real, assegurando integridade, confidencialidade e detecção proativa de ameaças.

1. Criptografia em repouso (armazenamento)

- O **Blockbit XDR** utiliza **criptografia para armazenar dados coletados dos endpoints e eventos de segurança na nuvem da Blockbit**.
- Os logs, alertas e dados sensíveis são armazenados na nuvem da Blockbit com **criptografia AES-256**.
- O acesso às informações é restrito por meio de **Role-Based Access Control (RBAC)**. Apenas usuários autorizados podem visualizar dados sensíveis.
- O período e/ou a capacidade de armazenamento dos dados, incluindo logs (processados e não processados), eventos, auditorias e relatórios, são configurados de acordo com os termos estabelecidos no licenciamento e/ou contrato. Essa definição garante a retenção adequada das informações, conforme as necessidades operacionais e os requisitos de conformidade da organização.

2. Criptografia em trânsito (transmissão)

- Todas as comunicações entre agentes e o console do **Blockbit XDR** são protegidas utilizando **TLS 1.3 ou superior**.
- A API do **Blockbit XDR** exige comunicação segura via **HTTPS (SSL/TLS)** para todas as interações com o console e agentes.
- O tráfego entre componentes internos, como agentes e o **Blockbit XDR Manager**, também segue protocolos seguros, impedindo a interceptação de dados.

3. Conformidade

- O **Blockbit XDR** segue boas práticas de segurança compatíveis com **LGPD, GDPR, PCI DSS, ISO 27001 e NIST**.

Para permitir a operação, o Blockbit XDR coleta os seguintes dados:

Dado	Descrição
@timestamp	Data e hora do evento.
GeoLocation.country_name	Nome do país de origem do evento.
GeoLocation.location	Coordenadas da origem do evento.
GeoLocation.region_name	Nome da divisão subnacional de origem do evento.
_index	Nome do índice onde os dados foram armazenados.
agent.id	Identificação única do agente que coletou ou gerou o evento.
agent.name	Nome do do agente que coletou ou gerou o evento.
cluster.name	Nome do cluster onde o agente está.
cluster.node	Localização do evento dentro do cluster.
data.id	Identificação do dado processado.
data.protocol	Protocolo do evento.
data.srcip	IP de origem do evento.
data.url	URL do recurso envolvido no evento.
decoder.name	Nome do decodificador que interpreta os dados recebidos.
full_log	Registro do evento em log.
id	Identificador do evento.
input.type	Tipo de entrada do evento.
location	Localização do evento.
manager.name	Nome do sistema que supervisiona os agentes.

rule.description	Descrição da regra acionada ao gerar o evento.
rule.firedtimes	Quantas vezes a regra citada foi acionada.
rule.gdpr	Indicador de conformidade da regra com o GDPR.
rule.groups	Rule Group (Grupo de Regras) é um agrupamento lógico de regras que compartilham um mesmo propósito ou categoria de detecção. Esse conceito facilita a organização e aplicação das regras dentro do mecanismo de análise de eventos.
rule.id	Rule ID (ID da Regra) é um identificador numérico exclusivo atribuído a uma regra de detecção dentro do sistema de análise de logs. Essas regras são responsáveis por correlacionar eventos, detectar anomalias e gerar alertas de segurança.
rule.level	Nível de severidade associado à regra
rule.mail	Indica se a regra envia modificações por e-mail.
rule.nist_800_53	Indicador de conformidade da regra com o NIST SP 800-53.
rule.pci_dss	Indicador de conformidade da regra com o PCI-DSS
rule.tsc	Indicador de conformidade da regra com o TSC.

Qual a diferença entre Rule ID e Rule Group?

Feature	Rule ID	Rule Group
O que é?	Identificador único de uma regra específica.	Conjunto de regras agrupadas por um tema comum.
Como funciona?	Cada evento pode corresponder a um Rule ID específico.	Um Rule Group pode conter múltiplos Rule IDs relacionados.
Exemplo	Rule ID 100010 para falhas SSH.	Rule Group "ssh_bruteforce" contendo regras de falha e força bruta.
Uso	Para filtrar eventos específicos.	Para visualizar eventos correlacionados.

Como um Rule Group funciona?

- Cada **Rule Group** contém um conjunto de **Rule IDs** que compartilham um contexto comum.
- Essas regras podem analisar logs de **diferentes fontes**, como sistemas operacionais, redes e aplicações.
- O Rule Group ajuda na **organização das regras**, permitindo identificar padrões específicos e categorizar ataques.
- Os Rule Groups facilitam a correlação de múltiplos eventos, melhorando a detecção de ameaças

Exemplo de Rule Groups disponíveis no Blockbit XDR:

- **Windows rules (windows_rules.xml)** – Regras para eventos do Windows.
- **Linux rules (pam_rules.xml, sshd_rules.xml)** – Regras para autenticação e acesso SSH.
- **Web Attack rules (web_rules.xml)** – Regras para detectar ataques a servidores web.
- **MITRE ATT&CK rules (mitre_rules.xml)** – Regras mapeadas com a matriz MITRE ATT&CK.

Com o Blockbit XDR é possível criar rules e rule groups personalizados são úteis para detecção de ataques específicos na sua infraestrutura.

XDR - Agentes

No Blockbit XDR, a peça central é o Agente.

O agente é um serviço do XDR instalado num endpoint (PC, notebook, máquina virtual, instância de nuvem). Ele vai proteger o endpoint e responder ameaças.

Combinando os recursos de EPP (Endpoint Protection Platform) e EDR (Endpoint Detection and Response), o Blockbit XDR garante uma abordagem completa para a prevenção, detecção e resposta a incidentes cibernéticos.

Análise de Processos em Tempo Real

Antes de enviar um alerta ao console de administração, o agente examina as informações do processo localmente, avaliando comportamento, assinaturas e características do executável.

Se um processo for identificado como potencialmente malicioso, o agente pode realizar ações automáticas de remediação, como bloquear, encerrar o processo ou isolar o endpoint, reduzindo o tempo de detecção e mitigação do ataque.

Inteligência Artificial e Aprendizado Automático na Análise de Arquivos

O agente utiliza inteligência artificial e aprendizado de máquina para analisar arquivos antes da execução, prevenindo ameaças conhecidas e desconhecidas (Zero-Day).

Durante a execução de um arquivo, o agente monitora seu comportamento em tempo real, detectando anomalias, tentativas de exploração e movimentação lateral.

Caso um arquivo apresente um comportamento suspeito, o agente pode impedir sua execução, enviá-lo à quarentena ou aplicar medidas corretivas automaticamente.

Com essa abordagem proativa e inteligente, o Blockbit XDR garante detecção avançada, resposta rápida e redução do tempo de mitigação de ataques, fornecendo proteção robusta para endpoints em qualquer ambiente.

Proteção Anti-Tamper do Blockbit XDR

O Blockbit XDR possui uma robusta proteção anti-tamper, impedindo que usuários não autorizados ou ameaças tentem desativar, modificar ou remover o agente de segurança, garantindo a integridade do sistema e a continuidade da proteção.

1. Proteção de Arquivos, Processos e Serviços

Impede modificação, exclusão ou encerramento dos serviços do Blockbit XDR, bloqueando ações maliciosas de ransomwares, rootkits e outras ameaças avançadas.

Garante que mesmo um usuário com credenciais de administrador local não consiga desativar ou remover o agente, reforçando a segurança contra ataques internos e externos.

2. Restrições Rígidas de Permissão

Somente administradores devidamente autorizados podem realizar alterações nas configurações ou desinstalar o agente.

O agente do Blockbit XDR impede manipulações indevidas por meio de controles internos reforçados e proteção contra modificações não autorizadas no registro do sistema.

3. Execução em Nível de Kernel para Máxima Proteção (Windows)

O agente do Windows é executado diretamente no espaço do kernel, garantindo o mais alto nível de proteção contra manipulações (anti-tamper).

Atua no nível do driver do sistema operacional, assegurando prioridade sobre processos comuns e bloqueando tentativas de comprometimento por parte de malwares e ataques avançados.

Monitoramento contínuo do estado do agente, com mecanismos de autorreparação, que restauram automaticamente qualquer tentativa de interrupção dos serviços essenciais do Blockbit XDR.

Um agente só pode ser desinstalado ou modificado com usuário, senha e MFA de um administrador do XDR.

Na lista, cada agente corresponde a um endpoint.

A forma de selecionar um agente é padronizada no Blockbit XDR.

Para selecionar um agente, clique em  **Explore agent** ().

Um modal com a lista de agentes irá abrir.

Explore agent

Search						
ID ↑	Name		Group	Version	Operating system	Status
001	b	o	default	v1.0.0	 CentOS Linux 7.9	● active ⓘ
003	x	a	default	v1.0.0	 Microsoft Windows	● active ⓘ
004	f		default	v1.0.0	 Microsoft Windows Server 2019 Standard	● active ⓘ
006	l		default	v1.0.0	 Microsoft Windows 10 Pro	● disconnected ⓘ
007	l		default	v1.0.0	 Microsoft Windows 10 Pro	● active ⓘ
009	q		default	v1.0.0	 Ubuntu	● active ⓘ

Para procurar um agente específico, use a barra de pesquisa (**Search**).

Clique no agente para selecioná-lo.

Para cada agente, há as seguintes características.

O **Id** é o número identificador do agente.

Name é o nome do agente.

IP address é o endereço IP do agente.

Operating system é o sistema operacional do agente.

Version é a versão do agente.

Status é o status do agente. São dois status: ativo (**active**) e desconectado (**disconnected**).

XDR - Agentes - Comunicação via proxy web

Para configurar o agente do **Blockbit XDR** para comunicar-se com o **Manager/Workers** via **proxy web**, siga os seguintes passos:

1. Configure o Agente para uso de Proxy

O arquivo de configuração do agente está localizado em:

Linux: blockbitxdretc.conf

Windows: blockbitxdr/ossec.conf

Antes de modificar o arquivo no Windows, utilize este comando para pausar o agente.

```
net stop "Blockbit XDR"
```

Na seção <remote>, adicione a seguinte configuração:

```
<remote>
  <proxy>
    <enabled>yes</enabled>
    <host>proxy.example.com</host>
    <port>8080</port>
    <username>usuario_proxy</username>
    <password>senha_proxy</password>
  </proxy>
</remote>
```

Após modificar o arquivo no Windows, utilize este comando para reiniciar o agente.

```
net start "Blockbit XDR"
```

2. Reinicie o Agente para Aplicar as Configurações

Após modificar o arquivo de configuração, reinicie o serviço do agente:

- Sistema com systemctl:

```
systemctl restart blockbit-xdr-agent
```

- Sistema sem systemctl:

```
/var/ossec/bin/ossec-control restart
```

3. Verifique o Status da Comunicação

Para garantir que o agente está se comunicando corretamente com o **Manager/Workers** através do proxy, utilize o seguinte comando:

```
tail -f /var/ossec/logs/ossec.log
```

Para verificar o status no Windows, utilize este comando:

```
Get-Content "C:\Program Files (x86)\blockbit-xdr\ossec.log" -Wait
```

XDR - Agentes - Instalando o Agente nos endpoints

O **Blockbit XDR Agent** pode ser instalado manualmente nos endpoints (Windows, Linux e macOS) para garantir a **proteção, monitoramento e resposta a ameaças em tempo real**. Durante a instalação, é possível **especificar o grupo ao qual o endpoint será atribuído** utilizando o parâmetro **BBXDR_AGENT_GROUP**.

Instalação no Windows

Abra o PowerShell como Administrador

1. Pressione `Win + X` e selecione **PowerShell (Admin)** ou **Terminal do Windows (Admin)**.
2. Navegue até o diretório onde o instalador foi salvo:

```
powershell
cd "C:\Caminho\para\o\arquivo"
```

Instale o agente e defina o grupo do endpoint

No PowerShell, execute o seguinte comando:

```
powershell
.\blockbit-xdr-agent-1.0.0-1.msi /q BBXDR_MANAGER='xdr-nome do cliente.blockbit.com'
BBXDR_REGISTRATION_PASSWORD='XXXX' BBXDR_REGISTRATION_SERVER='xdr-nome do cliente.blockbit.com'
BBXDR_AGENT_GROUP='default' BBXDR_AGENT_NAME=$ENV:COMPUTERNAME
```

Inicie o Agente

Após instalar, inicie o agente manualmente:

```
powershell
net start "Blockbit XDR"
```

O agente está ativo e no grupo configurado.

A instalação do Blockbit XDR Agent também pode ser realizada de forma automatizada e em massa, utilizando scripts via PowerShell, GPO (Group Policy Object) no Active Directory, SCCM (System Center Configuration Manager) ou ferramentas de gerenciamento de endpoint, permitindo a distribuição remota para múltiplos dispositivos simultaneamente, garantindo agilidade e padronização na implantação

Instalação no Linux

O [agente](#) pode ser instalado em distribuições **Ubuntu e CentOS** usando os pacotes `.deb` e `.rpm`

Acesse o terminal e localize o diretório de instalação:

```
bash
cd /caminho/para/o/arquivo
```

Execute o instalador conforme a distribuição:

Ubuntu/Debian:

```
bash
BBXDR_MANAGER="xdr-bb.nome do cliente.com" BBXDR_REGISTRATION_PASSWORD="XXXX" BBXDR_REGISTRATION_SERVER="xdr-nome do cliente.blockbit.com" BBXDR_AGENT_GROUP="default" BBXDR_AGENT_NAME='MACHINE_NAME_Linux' dpkg -i bbxdr-agent_1.0.0-1_amd64.deb
```

CentOS/RHEL:

```
bash
BBXDR_MANAGER="xdr-nome do cliente.blockbit.com" BBXDR_REGISTRATION_PASSWORD="XXXX" BBXDR_REGISTRATION_SERVER="
xdr-nome do cliente.blockbit.com" BBXDR_AGENT_GROUP="default" BBXDR_AGENT_NAME='default' BBXDR_AGENT_NAME="
MACHINE_NAME_Linux' rpm -ihv bbxdr-agent-1.0.0-1.x86_64.rpm
```

Ative e inicie o agente

```
bash
systemctl daemon-reload
systemctl enable bbxdr-agent
systemctl start bbxdr-agent
systemctl status bbxdr-agent
```

O agente está ativo e no grupo configurado.

Instalação no macOS

Crie o Arquivo de Configuração

Abra o terminal e execute:

```
bash
cat <<EOF >/tmp/bbxdr_envs
BBXDR_MANAGER="xdr-nome do cliente.blockbit.com"
BBXDR_REGISTRATION_PASSWORD="XXXX"
BBXDR_REGISTRATION_SERVER="xdr-nome do cliente.blockbit.com"
BBXDR_AGENT_GROUP="default"
BBXDR_AGENT_NAME="MACHINE_NAME_macOs"
EOF
```

Execute o instalador

```
bash
sudo installer -pkg ./bbxdr-agent-1.0.0-1.arm64.pkg -target /
```

O agente está ativo e no grupo configurado.

Desinstalação do Agente Blockbit XDR

Para garantir a segurança e o controle total do ambiente, o processo de desinstalação do agente do Blockbit XDR exige a autenticação com credenciais de administrador da plataforma, além da validação em dois fatores (MFA - Multi-Factor Authentication).

Essa verificação dupla assegura que apenas usuários devidamente autorizados possam remover o agente, impedindo tentativas de desativação por usuários não autorizados ou por ameaças que visem comprometer a proteção do endpoint.



Log in to Blockbit XDR



Username



Password



MFA Code

Log in



XDR - Sistema de buscas

No Blockbit XDR, o sistema de buscas é padronizado.

Em **Search**, você pode procurar por elementos específicos. Você pode montar queries simplificadas usando o [Dashboard Query Language](#).

Em **+Add filter**, você pode adicionar filtros à pesquisa.

EDIT FILTER

Edit as Query DSL

Field

Operator

Select a field first

Waiting

☒ Create custom label?

Cancel

Save

Em **Field**, você pode selecionar os campo que serão pesquisados.

Em **Operator**, x

Ao clicar em **create custom label?**, você pode criar um nome específico para a query.

Em **Edit as Query DSL**, você pode criar uma query via DSL.

Clique em salvar () para salvar a query.

Ao clicar no calendário (), um modal irá abrir e você poderá selecionar um intervalo de tempo para verificar os eventos de segurança.

Em **quick select**, você poderá selecionar rapidamente um intervalo de tempo. Você pode determinar se o intervalo vale para os últimos (**Last**) ou próximos (**Next**) momentos, a quantidade e a duração do intervalo. Para aplicar, clique em **Apply**.

Quick select

< >

Last

24

hours

Apply

Last

Next

Em **Commonly used**, você poderá usar um intervalo pré-programado (ex: últimos 15 minutos).

Commonly used

Today

Last 24 hours

This week

Last 7 days

Last 15 minutes

Last 30 days

Last 30 minutes

Last 90 days

Last 1 hour

Last 1 year

Em **Recently used date ranges**, você poderá reutilizar um intervalo de tempo.

Recently used date ranges

Aug 7, 2024 @ 10:30:30.820 to Aug 7, 2024 @ 10:30:30.840

Aug 7, 2024 @ 10:30:30.000 to Aug 7, 2024 @ 10:30:31.000

Aug 7, 2024 @ 10:30:30.543 to Aug 7, 2024 @ 10:30:30.658

Aug 7, 2024 @ 10:30:30.000 to Aug 7, 2024 @ 10:31:00.000

Aug 7, 2024 @ 10:30:00.000 to Aug 7, 2024 @ 11:00:00.000

Last 6 days

Em **Refresh every**, você poderá configurar a atualização automática da página. Você pode determinar a quantidade e a duração do intervalo. Para aplicar, clique em **Start**.

Refresh every

0

seconds

▶

Start

Ao clicar no campo de tempo, você poderá selecionar três formas de intervalo:
Absoluto (**Absolute**): uma data e horário específico (Ex: 15h37 de 15 de outubro de 2023).

Absolute

Relative

Now

<August 2024>

SU

MO

TU

WE

TH

FR

SA

28

29

30

31

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

08:00

08:30

09:00

09:30

10:00

10:30

11:00

11:30

12:00

End date

Aug 8, 2024 @ 10:55:07.878

Relativo (**Relative**): um intervalo de tempo relativo ao momento presente (ex: 2 minutos atrás).

Absolute

Relative

Now

2

Minutes ago

Round to the minute

End date

Aug 8, 2024 @ 10:55:24.901

Agora (**Now**): ao configurar o intervalo para "now", toda atualização vai ser feita relativa ao momento presente.

Para atualizar a página, clique em **Refresh**.

XDR - Primeiro acesso

O **Blockbit XDR** oferece um acesso seguro e flexível para administradores e usuários autorizados, garantindo proteção reforçada através de múltiplos métodos de autenticação.

Ao acessar a plataforma, o usuário será direcionado para a tela de login, onde poderá autenticar-se utilizando uma das seguintes opções:

- **Usuário Local + MFA:** Utiliza credenciais cadastradas diretamente no Blockbit XDR, exigindo nome de usuário, senha e um token de autenticação multifator (MFA).
- **SSO via LDAP + MFA:** Permite a autenticação integrada com um servidor LDAP corporativo, adicionando uma camada extra de segurança com MFA.
- **Autenticação via SAML (Single Sign-On):** Integra-se com provedores de identidade compatíveis com o protocolo **SAML (versão 2.0 ou superiores)**, como Microsoft Active Directory Federation Services (ADFS), Azure AD, Google Workspace, entre outros, permitindo o login único com credenciais corporativas.

Para realizar o login, o usuário deve inserir suas credenciais no formulário e, se configurado, fornecer o token MFA. Alternativamente, é possível utilizar a opção **"Log in with single sign-on"**, que direciona para o fluxo de autenticação via SAML.

Essa abordagem garante maior segurança e conformidade com políticas corporativas, facilitando o gerenciamento de acessos e protegendo contra acessos não autorizados.



Ao acessar o Blockbit XDR pela primeira vez, você terá que aceitar os termos e condições:

Terms of Service

CONTRATO DE LICENÇA PARA USUÁRIO FINAL

Este instrumento particular é um acordo legal entre a BLOCKBIT TECNOLOGIA LTDA., sociedade com sede na Rua Alexandre Dumas, 1711, Birmann 11, Térreo, Loja 2, Chácara Santo Antônio, São Paulo/SP, CEP: 04717-911, inscrita no CNPJ/MF sob o nº 02.423.535/0001-09, doravante denominada apenas "BLOCKBIT", e V.Sa. (pessoa física ou jurídica), doravante designada de "CONTRATANTE", que têm, entre si, justo e acertado o presente contrato, que se regerá pelas condições e cláusulas seguintes:

LICENCIAMENTO:

1) O presente instrumento tem por objeto o licenciamento do direito de uso dos módulos de software não personalizado que integram a PLATAFORMA BLOCKBIT UTM, BLOCKBIT SMX, BLOCKBIT BBX, BLOCKBIT NGFW, BLOCKBIT SD-WAN, BLOCKBIT XDR E/OU BLOCKBIT SIEM (doravante denominada apenas "Produtos BLOCKBIT"), assim como das respectivas atualizações. A utilização destes módulos de software deverá obedecer estritamente o quanto contido neste instrumento, bem como na(s) documentação(ões) técnica(s) que o(s) acompanha(m).

Accept

Accept

Clique em Accept () para aceitar.

XDR - Dashboard

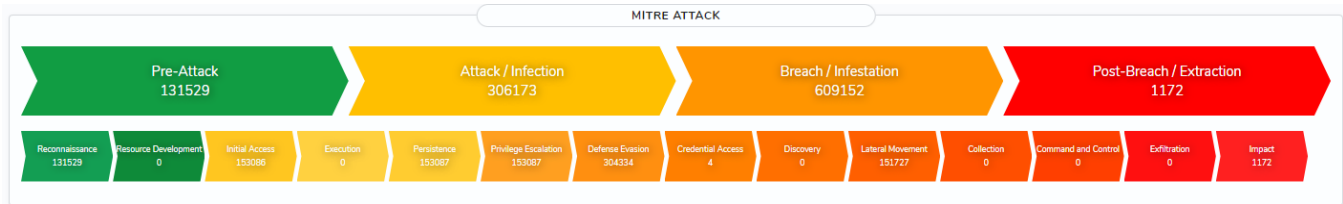
O Dashboard do Blockbit XDR oferece uma interface intuitiva e centralizada, proporcionando uma visão abrangente da segurança do ambiente em tempo real. Com gráficos interativos, painéis personalizáveis e alertas priorizados, os administradores podem monitorar eventos críticos, analisar ameaças e tomar decisões rápidas. O fluxo de trabalho estruturado permite uma resposta ágil a incidentes, incluindo ações automatizadas para mitigação de riscos, facilitando a investigação e garantindo uma gestão eficiente da segurança cibernética.

Este é o principal espaço do Blockbit XDR. Por aqui, você pode conferir e controlar as ameaças e conferir o status do sistema.

Overview

Nesta seção, são apresentadas informações gerais sobre ameaças em curso. Para mais informações, vá em [Overview](#).

Mitre ATT&CK



O MITRE ATT&CK é uma base de conhecimento que organiza e descreve **táticas** (o porquê de um ataque) e **técnicas** (o como um ataque é executado) utilizadas por adversários em ambientes reais. Essa estrutura serve como fundamento para a inteligência e correlação de eventos no Blockbit XDR, guiando a forma como as ameaças são identificadas, classificadas e investigadas.

Com base nesse modelo, o Blockbit XDR permite a construção de uma linha do tempo detalhada do incidente, correlacionando eventos e revelando a trajetória completa da ameaça dentro do ambiente monitorado. Isso possibilita a detecção de padrões comportamentais, a identificação precisa dos vetores de intrusão e a resposta rápida a ataques complexos e persistentes, fortalecendo significativamente a capacidade de defesa da organização.

Cada tática ou técnica tem um remédio específico e o Blockbit XDR tem uma [base de referências](#) que pode ser consultada.

Para mais informações, acesse [Mitre ATT&CK](#).

Gráficos

O Blockbit XDR apresenta representações visuais da severidade dos ataques. Para mais informações, vá em [Gráficos](#).

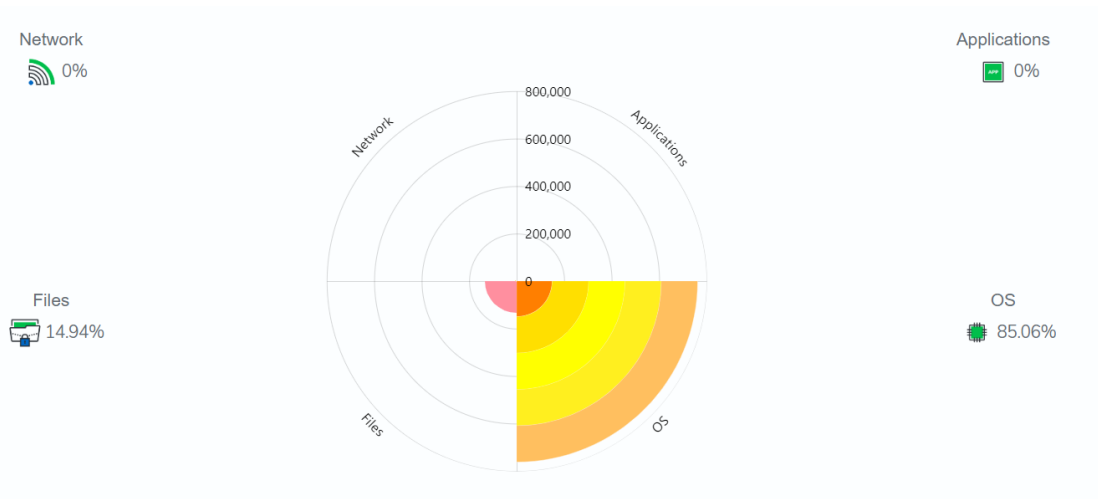
Técnicas

Aqui são elencadas as principais técnicas de ataques e os eventos vinculados. Um ataque pode usar mais de uma técnica simultaneamente. Para mais informações, vá em [Técnicas](#).

Todos os botões são clicáveis, redirecionando para a página Security Events com o filtro correspondente, facilitando a investigação das ameaças.

XDR - Dashboard - Gráficos

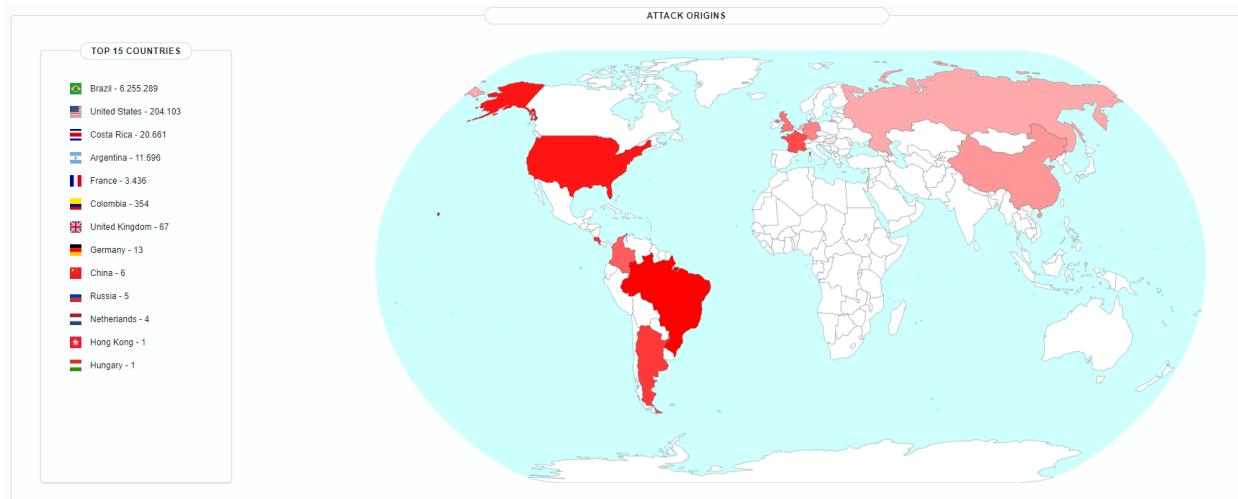
O Blockbit XDR apresenta dois gráficos divididos em 4 seções. Cada seção tem 1/4 de um círculo, onde cada faixa ataques divididos por severidade. Quanto mais ao centro, mais severo.



São mostradas as vias de entrada dos ataques.

- **Network:** rede
- **Files:** arquivo
- **Application:** aplicação
- **Operating System:** sistema operacional

Mapa-mundi



São mostrados os lugares de origem dos ataques. Os países em vermelho originaram ataques.

À esquerda, há um ranking dos 15 países que mais originaram ataques. Para ver o nome do país, passe o mouse sobre ele. Para dar zoom, use a roda do mouse.

XDR - Dashboard - Mitre ATT&CK

O Mitre ATT&CK é uma base de técnicas e padrões de ataque. Cada técnica tem um remédio específico.

Há dois conceitos:

Técnica: como o atacante entra num sistema.

Tática: Por que o atacante entra num sistema.

Para mais informações, visite [Mitre ATT&CK](#).

No Dashboard, os ataques são classificados de acordo com a severidade e divididos em 4 níveis categorias, que são divididas em 14 subníveis.

Pre-attack: preparo do ataque

Severidade	Baixa
Reconnaissance	Coleta de informações.
Resource development	Estabelecimento de recursos para ataques futuros.
Initial access	Tentativa de invasão de rede.
Execution	Tentativa de rodar código malicioso.

Attack/Infection: Tentativas de ataque

Severidade	Média
Persistence	Tentativa de manter o ataque.
Privilege escalation	Tentativa de ganhar permissões de nível maior.
Defense evasion	Tentativa de evitar defesas e passar despercebido.

Breach/Infestation: Violação

Severidade	Alta
Credential access	Tentativa de roubar nomes e senhas.
Discovery	Exploração de ambiente
Lateral movement	Tentativa de se mover pelo ambiente.
Collection	Tentativa de coleta de dados.

Post-breach/Extraction: Impacto

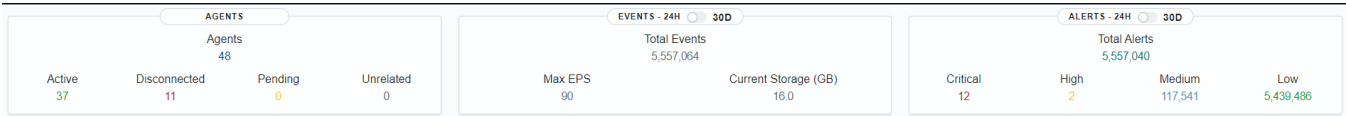
Severidade	Crítica
Command and control	Tentativa de comunicação com sistemas comprometidos para controlá-los.
Exfiltration	Tentativa de roubo de dados.
Impact	Tentativa de manipular, interromper ou destruir um sistema ou seus dados.

Para informações mais aprofundadas sobre o Mitre ATT&CK, visite attack.mitre.org.

XDR - Dashboard - Overview

Overview

O Blockbit XDR oferece um sistema de correlação automática de alertas, permitindo que eventos relacionados ao mesmo ataque sejam agrupados e analisados de forma eficiente. Esse recurso reduz o tempo de resposta e melhora a detecção de ameaças complexas, garantindo uma visão unificada do incidente.



Agents

O agente é um serviço do XDR instalado num endpoint (PC, notebook, máquina virtual, instância de nuvem). Ele vai proteger o endpoint e responder ameaças.

Ao clicar no número de agentes, você irá para a lista deles. Para mais informações, acesse [Agentes](#).

Active: ativos;

Disconnected: desconectados;

Pending: em processo de conexão;

Unrelated: registrados, mas não conectados.

Events

Número de eventos no período. No switch, você pode escolher entre 24 horas ou 30 dias.

Total events: número de eventos no período selecionado;

Max EPS: eventos por segundo. O intervalo de é de 60 segundos;

Current Storage: total de logs de eventos salvos.

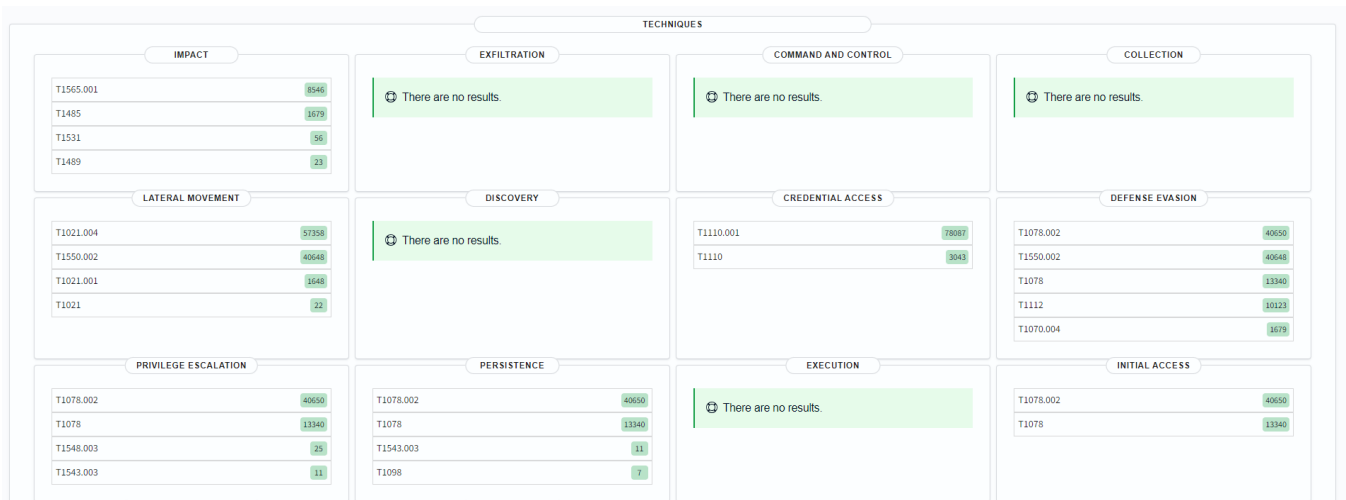
Total alerts

- O painel exibe o total de alertas detectados, permitindo a visualização e o monitoramento de ameaças ao longo do tempo, com opções para análise nos últimos 24 horas ou 30 dias.
- Os **alertas** são classificados automaticamente em níveis de severidade:
 - Critical (crítico)** – Ameaças de alto risco que exigem atenção imediata.
 - High (alto)** – Ataques em potencial que precisam ser analisados.
 - Medium (médio)** – Atividades suspeitas que requerem monitoramento.
 - Low (baixo)** – Eventos de menor impacto, mas que podem indicar padrões maliciosos.

Todos os botões são clicáveis, redirecionando para a página Security Events com o filtro correspondente, facilitando a investigação das ameaças.

XDR - Dashboard - Técnicas

Aqui são elencadas as principais técnicas de ataques e os eventos vinculados. Um ataque pode usar mais de uma técnica simultaneamente.



As técnicas são organizadas por severidade decrescente e agrupam táticas associadas.

Ao passar o mouse sobre qualquer tática, aparecerá um modal com mais informações.

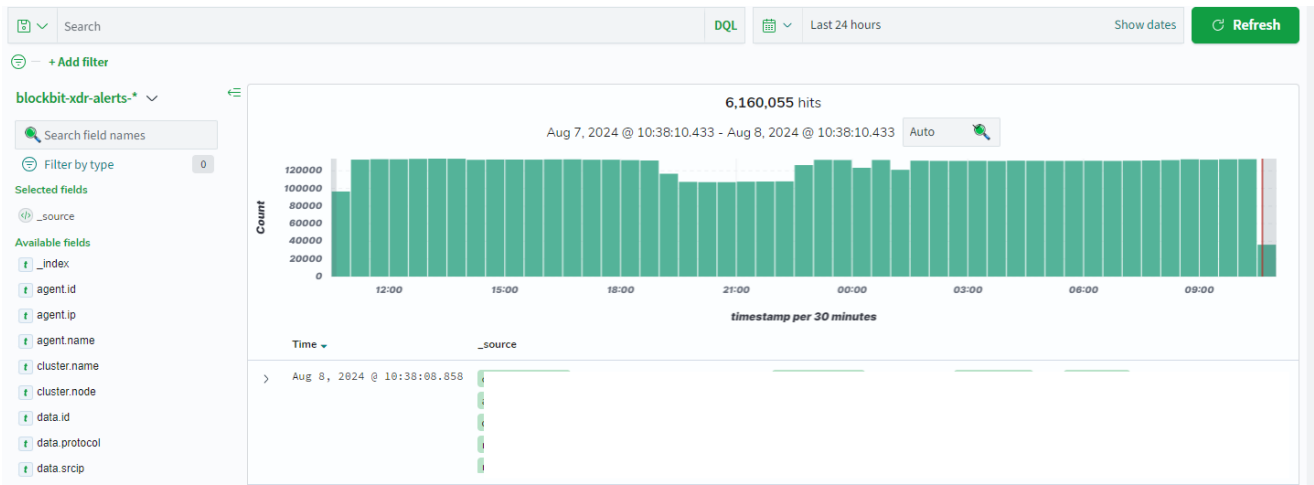
Ao clicar, você será direcionado à página [Security events](#) com informações de ataques utilizando a tática selecionada.

São mostradas apenas táticas associadas a eventos.

XDR - Security Events

Esta página fornece uma visão detalhada de todos os eventos de segurança registrados pelo Blockbit XDR, permitindo uma análise aprofundada e facilitando a investigação de incidentes em tempo real.

Quando uma ameaça é detectada, o usuário do agente recebe uma notificação detalhada, informando a ação tomada e os detalhes do evento ocorrido. Isso garante transparência e rápida resposta a incidentes, permitindo que os administradores visualizem e gerenciem eventos críticos com eficiência.



Busca e Filtragem de Eventos

- A barra de pesquisa permite buscar eventos específicos com base em critérios definidos pelo usuário.
- É possível criar filtros personalizados a partir de uma pesquisa já executada, facilitando a segmentação e análise recorrente de eventos semelhantes.
- Para mais informações, confira a sessão [Sistema de buscas](#).

Gráfico de Hits

- O gráfico de hits exibe a quantidade de eventos registrados em um período de tempo selecionado, permitindo identificação rápida de picos de atividade suspeita.
- Os eventos podem ser filtrados por período para facilitar a análise de comportamentos anômalos ao longo do tempo.
- Para mais informações, confira a sessão [Hits](#).

Lista de Eventos

- Abaixo do gráfico, encontra-se a lista detalhada dos eventos registrados, incluindo informações sobre a origem, tipo de ameaça e ação tomada.
- Ao selecionar um evento específico, o administrador pode visualizar todos os eventos associados a ele, permitindo uma investigação aprofundada do incidente.
- Para mais informações, confira a sessão [Lista de eventos](#).

Análise Forense e Linha do Tempo do Ataque

- O sistema possibilita a visualização de todos os processos anteriores ao evento em uma linha do tempo detalhada, permitindo a reconstrução do ataque e a análise forense do incidente.
- Isso possibilita identificar o ponto de entrada da ameaça, sua progressão no ambiente e as ações realizadas pelo atacante.

Correlação e Associação de Objetos

- O Blockbit XDR permite identificar todos os objetos relacionados a uma detecção específica, como arquivos modificados, processos iniciados, conexões de rede estabelecidas e chaves de registro alteradas.
- Essa funcionalidade auxilia na correlação de eventos e na identificação de padrões de ataque, facilitando a mitigação de ameaças e aprimorando as estratégias de defesa.

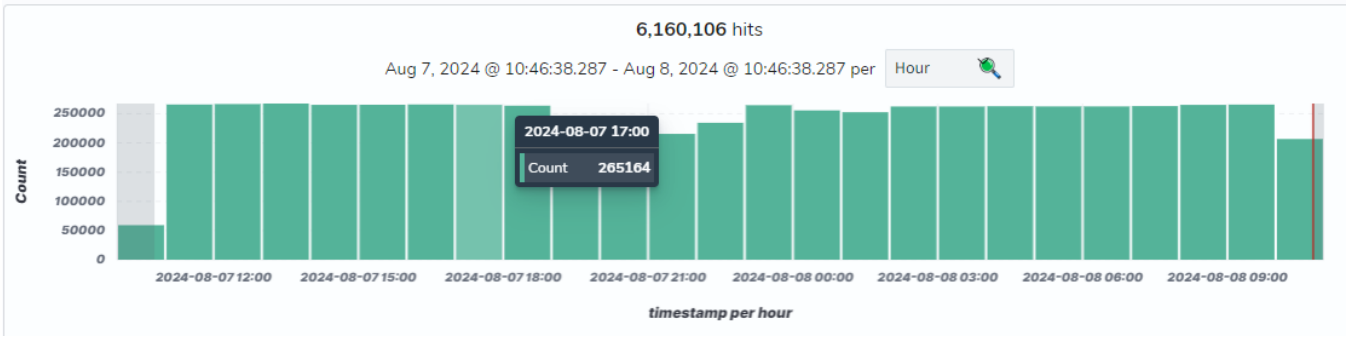
Remediação e Mitigação

- O Blockbit XDR pode marcar um grupo completo de eventos ou eventos isolados como ameaça e iniciar ações de resposta e mitigação, incluindo **Playbooks**.
- Um **Playbook** é uma sequência estruturada de ações que são executadas automaticamente ou sob aprovação do analista, com o objetivo de detectar, analisar, conter e mitigar ameaças. Esses conjuntos de ações são baseados em regras predefinidas e fluxos de decisão, permitindo que o sistema tome medidas proativas diante de eventos suspeitos ou ataques cibernéticos.

- Além das ações manuais, o Blockbit XDR permite a criação de **Playbooks automatizados**, possibilitando uma resposta imediata a eventos ou ataques com base em comportamentos maliciosos. Esses **Playbooks** são altamente personalizáveis, permitindo a adaptação das respostas às necessidades específicas de cada ambiente, garantindo maior eficiência e automação na mitigação de ameaças.

XDR - Security Events - Hits

O gráfico de hits mostra quantos eventos de segurança (hits) ocorreram no intervalo de tempo selecionado.



Ao passar o mouse sobre uma coluna, será mostrado o intervalo de tempo selecionado e o número de hits.

Ao clicar numa coluna, o intervalo selecionado é dividido.

A divisão de intervalos é a seguinte: Ano - Mês - Semana - Dia - Hora - Minuto - Segundo - Milissegundo.

XDR - Security Events - Lista de eventos

Abaixo do gráfico, estão listados os eventos.

>	Aug 7, 2024 @ 21:41:43.558
>	Aug 7, 2024 @ 21:41:43.558
>	Aug 7, 2024 @ 21:41:43.558  

Ao clicar num evento, você tem acesso a todas as informações dele como tabela ou JSON. Para mais informações, visite [Dados Coletados](#).

XDR - Security Events - Notificações

No Endpoint, quando uma ameaça for detectada, irá aparecer uma notificação para o usuário do agente onde o evento foi detectado.

Esta notificação irá descrever a ação tomada pelo Blockbit XDR, apresentar uma mensagem com a ação que usuário deve tomar.

No botão **Mais informações**, o usuário pode acessar informações detalhadas sobre a ameaça.

O botão **Fechar** fecha a notificação.



XDR - Security Events - Ransomware Events

Guia do Administrador do Blockbit XDR: Detecção, Correlação e Resposta a Incidentes de Ransomware

1. Introdução

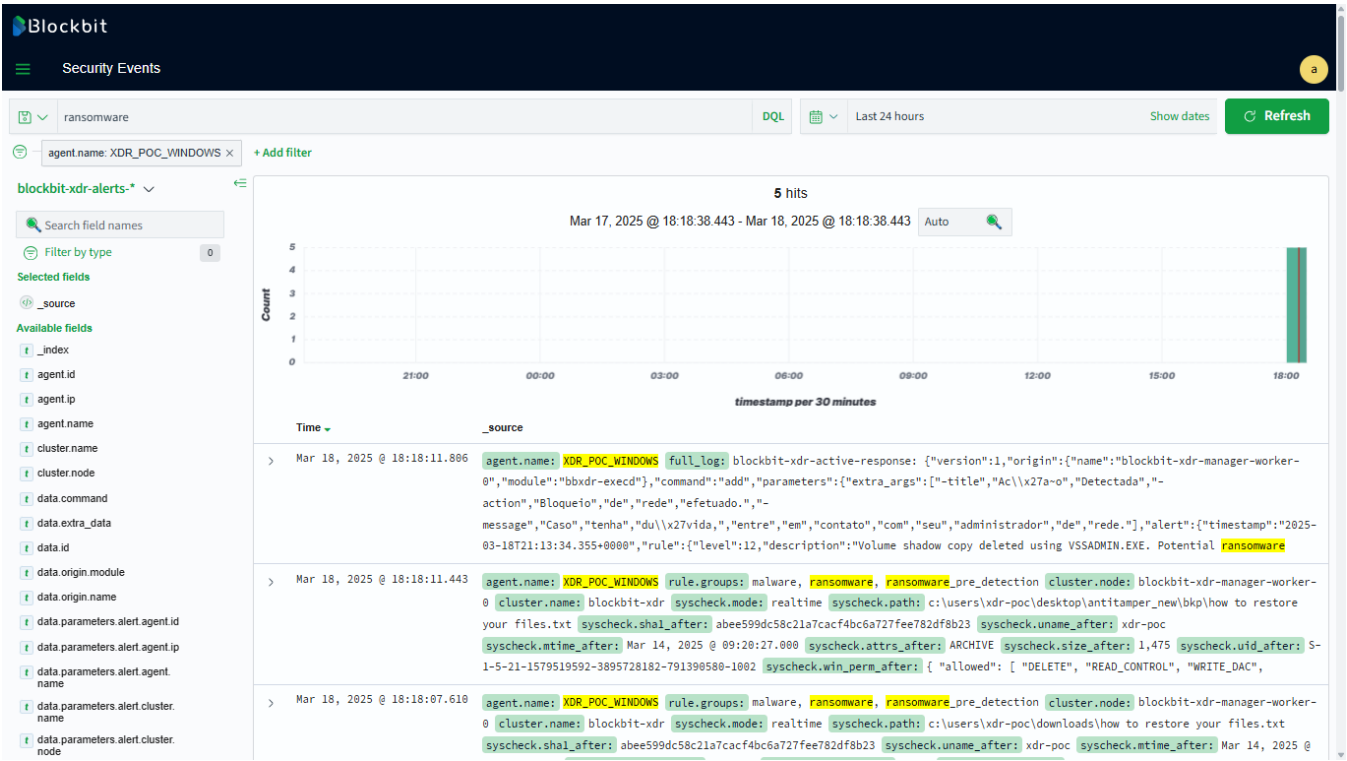
O Blockbit XDR é uma solução avançada de segurança que permite a detecção, correlação e resposta a incidentes de ransomware utilizando múltiplos vetores de análise e resposta automatizada. Este guia visa orientar o administrador na investigação e mitigação de ataques, utilizando a filtragem por rule.group e aplicando ações de contenção e recuperação.

2. Identificação de Eventos Relacionados a Ransomware

2.1 Aplicação de Filtros

Para iniciar a análise de um possível ataque de ransomware, utilize o filtro rule.group="ransomware" no painel de eventos do Blockbit XDR:

Acesse a interface de Security Events.
No campo de busca, insira "ransomware" ou utilize o filtro rule.group=ransomware.
Visualize os eventos relacionados à detecção de ransomware no ambiente.



Logs do início do incidente

Blockbit

Security Events

1742332414.833241546

data.sca.check.compliance.tsc	input.type	log
data.sca.check.description	location	EventChannel
data.sca.check.id	manager.name	blockbit-xdr-manager-worker-0
data.sca.check.rationale	rule.description	Volume shadow copy deleted using VSSADMIN.EXE. Potential ransomware activity detected.
data.sca.check.reason	rule.firedtimes	1
data.sca.check.references	rule.groups	malware, ransomware, ransomware_pre_detection
data.sca.check.registry	rule.id	100616
data.sca.check.remediation	rule.level	12
data.sca.check.result	rule.mail	true
data.sca.check.title	rule.mitre.id	T1490, T1059.003
data.sca.description	rule.mitre.tactic	Impact, Execution
data.sca.failed	rule.mitre.technique	Inhibit System Recovery, Windows Command Shell
data.sca.file	timestamp	Mar 18, 2025 @ 18:13:34.355
data.sca.invalid		
data.sca.passed		
data.sca.policy		
data.sca.policy_id		
data.sca.scan_id		
data.sca.score		
data.sca.total_checks		
data.sca.type		
data.scrip		
data.status		
data.url		
data.version		
data.win.eventdata.authenticationPackageName		

Exibe um alerta de pré-deteção de ransomware.

Blockbit

Security Events

Search

agent.name: XDR_POC_WINDOWS rule.groups: ransomware + Add filter

blockbit-xdr-alerts.*

Search field names

Filter by type

Selected fields

Available fields

Popular

rule.groups

_index

agent.id

agent.ip

agent.name

cluster.name

cluster.node

data.command

data.extra_data

data.id

data.origin.module

data.origin.name

data.parameters.alert.agent.id

data.parameters.alert.agent.name

data.parameters.alert.inhibitor

5 hits

Mar 17, 2025 @ 18:24:27.860 - Mar 18, 2025 @ 18:24:27.860 Auto

Count

timestamp per 30 minutes

Time

_source

Mar 18, 2025 @ 18:20:10.845

agent.name: XDR_POC_WINDOWS rule.groups: ransomware, ransomware_rollback cluster.name: blockbit-xdr-manager-worker-0 cluster.node: blockbit-xdr-manager-worker-0 data.rollback_status: File restore completed for DESKTOP-3FAA43M at 03/14/2025 09:26:48 rule.firedtimes: 1 rule.mail: false rule.level: 5 rule.description: BBXDR_Ransomware_Protection: Files restored successfully. rule.id: 100800 location: active-response/active-responses.log decoder.name: BBXDR_Ransomware id: 1742332810.833241546 full_log: BBXDR_Ransomware_Protection: File

Mar 18, 2025 @ 18:18:11.443

agent.name: XDR_POC_WINDOWS rule.groups: malware, ransomware, ransomware_pre_detection cluster.name: blockbit-xdr-manager-worker-0 cluster.node: blockbit-xdr-manager-worker-0 data.rollback_status: File restore completed for DESKTOP-3FAA43M at 03/14/2025 09:26:48 rule.firedtimes: 1 rule.mail: false rule.level: 5 rule.description: BBXDR_Ransomware_Protection: Files restored successfully. rule.id: 100800 location: active-response/active-responses.log decoder.name: BBXDR_Ransomware id: 1742332810.833241546 full_log: BBXDR_Ransomware_Protection: File

Mar 18, 2025 @ 18:18:07.610

agent.name: XDR_POC_WINDOWS rule.groups: malware, ransomware, ransomware_pre_detection cluster.name: blockbit-xdr-manager-worker-0 cluster.node: blockbit-xdr-manager-worker-0 data.rollback_status: File restore completed for DESKTOP-3FAA43M at 03/14/2025 09:26:48 rule.firedtimes: 1 rule.mail: false rule.level: 5 rule.description: BBXDR_Ransomware_Protection: Files restored successfully. rule.id: 100800 location: active-response/active-responses.log decoder.name: BBXDR_Ransomware id: 1742332810.833241546 full_log: BBXDR_Ransomware_Protection: File

Aplicação do filtro rule.group="ransomware".

3. Correlação de Eventos

Após identificar os eventos suspeitos, analise os logs detalhados para correlacionar atividades maliciosas.

3.1 Análise dos Logs

Identifique os alertas associados a ransomware e malware.
Verifique a origem do evento (agent.name, agent.ip, cluster.node).
Análise logs que indicam atividades suspeitas, como:
Criação e exclusão massiva de arquivos.
Execução de comandos suspeitos (exemplo: VSSADMIN.EXE deletando shadow copies).
Processos desconhecidos realizando modificações na estrutura do sistema.

Blockbit

Security Events

data.parameters.alert.rule.mitre.tactic

data.parameters.alert.rule.mitre.technique

data.parameters.alert.rule.nist_800_53

data.parameters.alert.rule.pci_dss

data.parameters.alert.rule.tsc

data.parameters.alert.timestamp

data.parameters.extra_args

data.parameters.program

data.protocol

data.rollback_status

data.sca.check.command

data.sca.check.compliance.cis

data.sca.check.compliance.cis_csc

data.sca.check.compliance.gdpr_IV

data.sca.check.compliance.gpg_13

data.sca.check.compliance.gpg13

data.sca.check.compliance.hipaa

data.sca.check.compliance.nist_800_53

data.sca.check.compliance.pci_dss

data.sca.check.compliance.tsc

data.sca.check.description

data.sca.check.id

data.sca.check.rationale

data.sca.check.reason

data.win.system.threadID

data.win.system.version

decoder.name

full_log

id

input.type

location

manager.name

rule.description

rule.firedtimes

rule.frequency

rule.groups

rule.id

rule.level

rule.mail

timestamp

2596

5

windows_eventchannel

>

1742332675.814518123

log

EventChannel

blockbit-xdr-manager-worker-0

Ransomware activity detected.

1

2

ransomware, ransomware_detection

100628

12

true

Mar 18, 2025 @ 18:17:55.295

Logs confirmando o ataque.

4. Respostas Automáticas e Ações Mitigatórias

O Blockbit XDR permite marcar um grupo completo de eventos ou eventos isolados como ameaça e iniciar ações de resposta e mitigação.

4.1 Isolamento da Máquina na Rede

Caso o Blockbit XDR detecte um ataque de ransomware em andamento:

- 1. Interrompe os processos relacionado ao ataque.
- 2. Isola o endpoint para impedir a propagação do malware.
- 3. Isola o arquivo suspeito.
- 4. Restaura os arquivos excluídos ou criptografados ao estado anterior ao ataque.
- 5. Por fim, reverte os eventos de dados ao estado seguro.

Blockbit

Security Events

2

_index

agent.id

agent.ip

agent.name

cluster.name

cluster.node

data.command

data.extra_data

data.id

data.origin.module

data.origin.name

data.parameters.alert.agent.id

data.parameters.alert.agent.name

data.parameters.alert.cluster.name

data.parameters.alert.cluster.node

data.parameters.alert.data.win.eventdata.commandLine

data.parameters.alert.data.win.eventdata.company

data.parameters.alert.data.win.eventdata.currentDirectory

data.parameters.alert.data.win.eventdata.description

data.parameters.alert.data.win.eventdata.fileVersion

data.parameters.alert.data.win.eventdata.hashes

data.parameters.alert.data.win.eventdata.image

Time

_source

Mar 18, 2025 @ 18:20:10.845

agent.name: XDR_POC_WINDOWS

rule.groups: ransomware, ransomware_rollback

cluster.node: blockbit-xdr-manager-worker-0

cluster.name: blockbit-xdr

input.type: log

agent.ip: 192.168.66.103

agent.id: 406

manager.name: blockbit-xdr-manager-worker-0

data.rollback_status: File restore completed for DESKTOP-3FAA43M at 03/14/2025 09:26:48

rule.firedtimes: 1

rule.mail: false

rule.level: 5

rule.description: BBXDR_Ransomware_Protection: Files restored successfully.

rule.id: 100000

location: active-response(active-responses.log

decoder.name: BBXDR_Ransomware

id: 1742332810.833241546

full_log: BBXDR_Ransomware_Protection: File

Mar 18, 2025 @ 18:18:11.443

agent.name: XDR_POC_WINDOWS

rule.groups: malware, ransomware, ransomware_pre_detection

cluster.node: blockbit-xdr-manager-worker-0

cluster.name: blockbit-xdr

syscheck.mode: realtime

syscheck.path: c:\users\xdr-poc\desktop\antitamper_new\bkp\how to restore your files.txt

syscheck.shal_after: abee599dc58c21a7cacf4bc6a727fee782df8b23

syscheck.uname_after: xdr-poc

syscheck.mtime_after: Mar 14, 2025 @ 09:20:27.000

syscheck.attrs_after: ARCHIVE

syscheck.size_after: 1,475

syscheck.uid_after: S-1-5-21-1579519592-3895728182-791390580-1002

syscheck.win_perm_after: { "allowed": ["DELETE", "READ_CONTROL", "WRITE_DAC",

Mar 18, 2025 @ 18:17:56.000

full_log: { "win": { "system": { "providerName": "Microsoft-Windows-Sysmon", "providerGuid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}", "eventId": "1", "version": "5", "level": "4", "task": "1", "opcode": "0", "keywords": "0x8000000000000000", "systemTime": "2025-03-18T20:38:40.2017521Z", "eventRecordID": "230448", "processID": "3136", "threadID": "4052", "channel": "Microsoft-Windows-Sysmon/Operational", "computer": "DESKTOP-3FAA43M", "severityValue": "INFORMATION", "message": "\nProcess Create:\r\nRuleName: technique_id=T1059,technique_name=Command-Line Interface\r\nUtcTime: 2025-03-18 20:38:40.193\r\nProcessGuid: {b6270aa7-d9d8-67d9-000000001100}

Mar 18, 2025 @ 18:17:55.295

agent.name: XDR_POC_WINDOWS

rule.groups: ransomware, ransomware_detection

cluster.node: blockbit-xdr-manager-worker-0

cluster.name: blockbit-xdr

input.type: log

agent.ip: 192.168.66.103

agent.id: 406

manager.name: blockbit-xdr-manager-worker-0

data.win.eventdata.originalFileName: VSSADMIN.EXE

data.win.eventdata.image: C:\Windows\System32\vssadmin.exe

data.win.eventdata.product: Microsoft Windows Operating System

data.win.eventdata.parentProcessGuid: {b6270aa7-1f1a-67d4-161a-000000001100}

data.win.eventdata.description: Command Line Interface for Microsoft Volume Shadow Copy Service

Mar 18, 2025 @ 18:13:34.355

agent.name: XDR_POC_WINDOWS

rule.groups: malware, ransomware, ransomware_pre_detection

cluster.node: blockbit-xdr-manager-worker-0

cluster.name: blockbit-xdr

input.type: log

agent.ip: 192.168.66.103

agent.id: 406

manager.name: blockbit-xdr-manager-worker-0

data.win.eventdata.originalFileName: VSSADMIN.EXE

data.win.eventdata.image: C:\Windows\System32\vssadmin.exe

data.win.eventdata.product: Microsoft Windows Operating System

data.win.eventdata.parentProcessGuid: {b6270aa7-1efb-67d4-ff19-000000001100}

data.win.eventdata.description: Command Line Interface for Microsoft Volume Shadow Copy Service

Log da ação de isolamento do endpoint.

4.2 Reversão de Alterações no Sistema

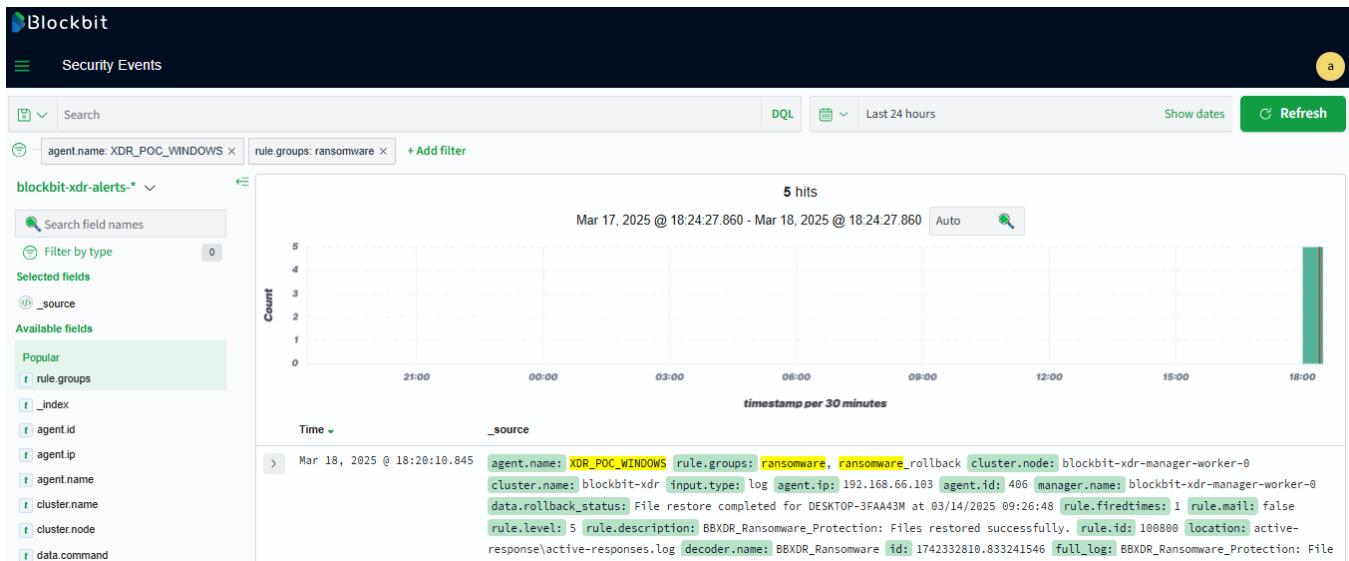
O Blockbit XDR é capaz de desfazer qualquer modificação realizada por um ataque, restaurando configurações do sistema, edições de registro e permissões de arquivos comprometidos.

4.3 Recuperação de Arquivos e Dados Criptografados

Para sistemas Windows, o Blockbit XDR pode recuperar eventos destrutivos, restaurando arquivos excluídos ou criptografados por ransomware automaticamente ou via console de administração.

Para a comprovação, verifique se o rollback foi ativado no evento (data.rollback_status).

Confirme a restauração bem-sucedida através dos logs no painel de eventos.



Exemplo de registro da ação de restauração de arquivos protegidos pelo Blockbit XDR.

5. Playbooks para Resolução de Incidentes

O Blockbit XDR permite a automação na correlação de eventos e a resposta a ameaças de forma eficiente. Este capítulo apresenta procedimentos detalhados para lidar com ataques de ransomware, atendendo aos requisitos do edital.

5.1 Playbook - Detecção e Contenção Automática

O Blockbit XDR correlaciona automaticamente os alertas relacionados ao mesmo ataque (Item 14), permitindo a rápida contenção e mitigação de ameaças.

Passos:

Filtragem Automática de Eventos:

- Utilize rule.group=ransomware para identificar atividades suspeitas.
- O sistema correlaciona automaticamente eventos relacionados ao mesmo ataque, agrupando-os para facilitar a análise.

Análise Automática de Logs e Ativação de Respostas:

- O Blockbit XDR aplica regras personalizadas para ativar detecções automaticamente.
- Quando uma ameaça é detectada, ações automáticas podem ser configuradas para resposta imediata.

Isolamento Automático do Endpoint:

- O XDR pode marcar um grupo completo de eventos ou eventos isolados como ameaça e iniciar ações de resposta e mitigação.
- Se um comportamento malicioso for identificado, a máquina infectada pode ser automaticamente removida da rede via Active Response.
- Também é possível aplicar um Playbook personalizado utilizando rule.groups ou rule.id por meio da API, ampliando a capacidade de resposta a incidentes e permitindo ações automatizadas e customizadas conforme a necessidade do ambiente.

Bloqueios Adicionais no Firewall:

- Com base nos eventos correlacionados, o XDR pode aplicar regras de firewall para impedir a comunicação do malware com servidores externos.

Escalamento Automático para a Equipe de Segurança:

- Caso um ataque seja detectado e medidas automatizadas sejam insuficientes, alertas podem ser enviados à equipe SOC para ações adicionais.

5.2 Playbook - Recuperação e Remediação

Caso o ransomware tenha causado impactos, o Blockbit XDR oferece mecanismos de recuperação e remediação de forma automatizada.

Passos:

Confirmação do Rollback Automático:

- O sistema verifica automaticamente a integridade de todo o sistema, como arquivos, configurações do sistema, registro e permissões de arquivos foram comprometidos (data.rollback_status).
- Caso o sistema tenha sido comprometidos e/ou arquivos criptografados, o Blockbit XDR aciona a recuperação, restaurando arquivos, configurações do sistema, edições de registro e permissões de arquivos, ou seja, todo o sistema.

Execução de Varredura de Malware e Correção de Sistemas:

- Após a contenção, o XDR pode iniciar automaticamente uma varredura avançada nos endpoints para remoção de arquivos maliciosos.
- As configurações do sistema podem ser restauradas automaticamente conforme padrões seguros.

Reativação do Endpoint e Retorno Seguro à Rede:

- Após a mitigação completa, o Blockbit XDR remove automaticamente as restrições da máquina e a reintegra à rede.

Marcação de Eventos e Relatório de Incidente:

- O administrador pode marcar um grupo de eventos como ameaça concluída e gerar relatórios para auditoria e futuras melhorias de segurança.

6. Conclusão

Essas funcionalidades garantem que o Blockbit XDR não apenas detecte, mas também responda e mitigue ameaças de forma automatizada, reduzindo o tempo de resposta e minimizando impactos operacionais.

Com esse guia, o administrador pode operar a solução com eficiência, garantindo proteção avançada contra ransomware e outras ameaças emergentes.

XDR - Custom Dashboards

O Blockbit XDR permite criar visualizações e dashboards customizados, de acordo com as necessidades da sua rede.

Ao clicar em Custom Dashboard, você irá para a lista de dashboards criados.

Custom Dashboards

 Search...

☐

Title

Type

Description

Last updated

Actions

☐

JG

Dashboard

Oct 11, 2024 @ 16:46:55.056



☐

JG Copy

Dashboard

aaaa

Oct 11, 2024 @ 16:47:11.653



☐

Jg dash 3

Dashboard

Oct 14, 2024 @ 17:25:31.819



Rows per page: 20

 1 

Use a barra de pesquisas (**Search**) para buscar um dashboard específico.

Para criar um dashboard, clique em **Create Dashboard**.

Os dashboards são classificados por:

Title: título do dashboard;

Type: tipo do dashboard;

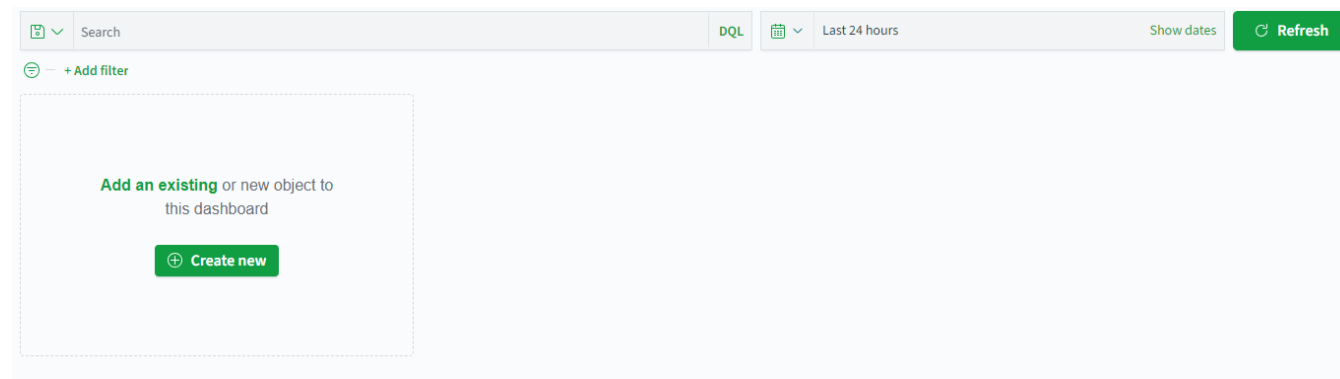
Description: descrição do dashboard;

Last updated: horário da última edição do dashboard.

O botão **Actions** () permite editar o dashboard.

XDR - Custom Dashboards - Create Dashboard

Ao clicar em Create Dashboard, você irá para esta página.

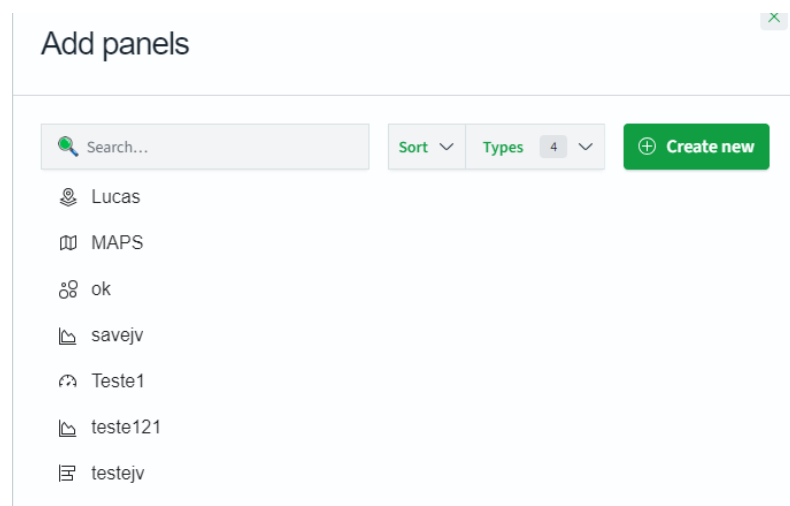


Search

A barra permite buscar por eventos específicos. Para mais informações, confira [Sistema de buscas](#).

Aqui, você poderá inserir uma visualização no dashboard ao clicar em **Add an existing** or new object to this dashboard.

Um modal irá se abrir com uma lista de visualizações já criadas:

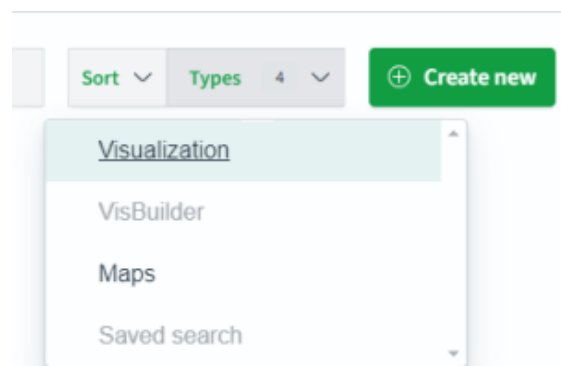


Para selecionar uma visualização, clique nele para inseri-lo no dashboard.

Para encontrar uma visualização específica, use a barra de buscas.

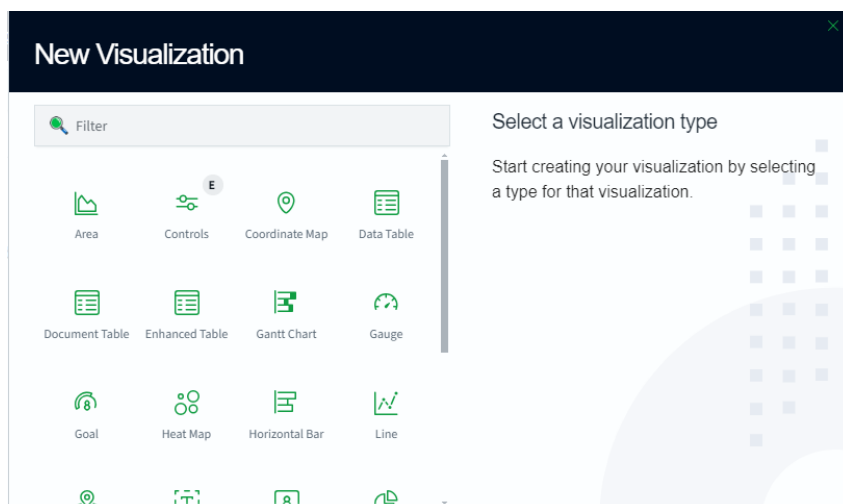
Em **Sort**, você pode organizar as visualizações de maneira ascendente ou decendente.

Em types, você pode selecionar as visualizações por tipo.



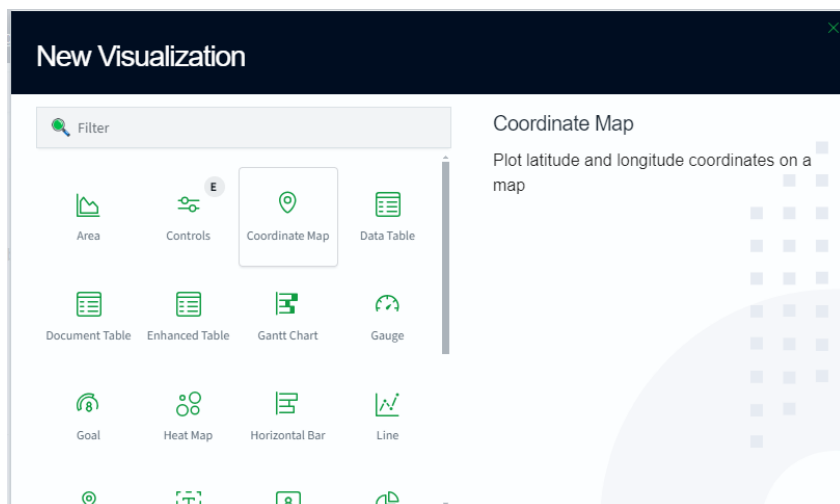
Para criar uma nova [visualização](#), clique em **Create new** ([+](#) **Create new**).

Um modal com as [visualizações disponíveis](#) irá abrir:



XDR - Custom Dashboards - Create Visualization

Ao clicar em Create new, um modal irá aparecer:

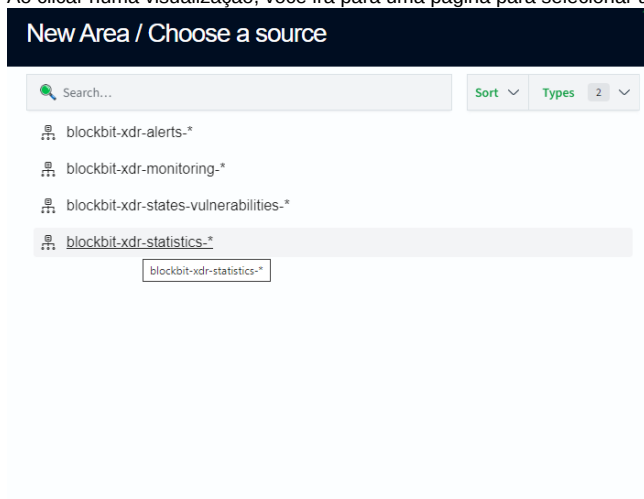


Este modal contém os tipos de visualizações suportados pelo Blockbit XDR.

Use a barra **Filter** para filtrar as visualizações disponíveis.

Ao passar o mouse sobre alguma visualização, uma breve explicação aparece à direita.

Ao clicar numa visualização, você irá para uma página para selecionar a fonte dos dados.



Use a barra **Search** para buscar uma fonte de dados.

Em **Sort**, você pode organizar em forma ascendente ou descendente.

Em **Types**, você pode filtrar as fontes por tipo.

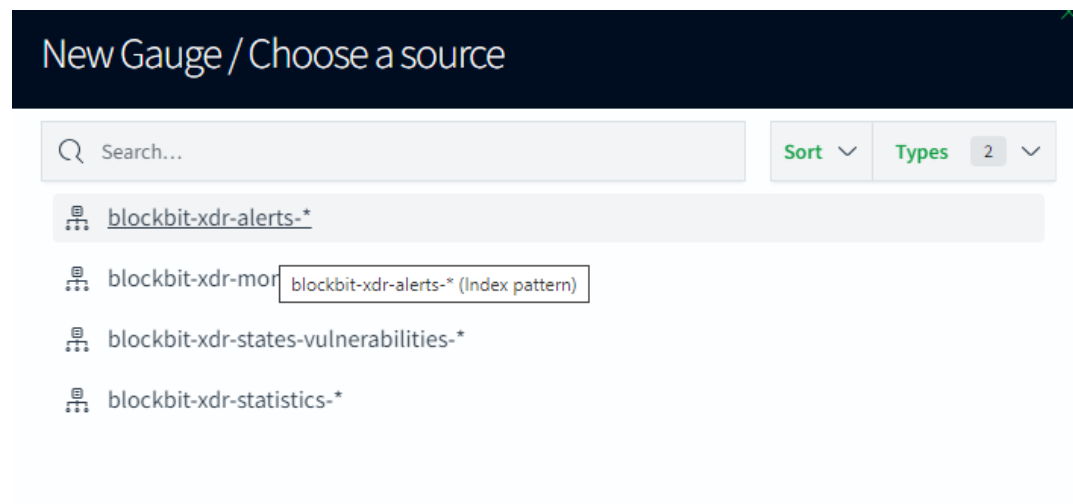
Para conferir todas as visualizações, acesse [Visualizações Disponíveis](#).

XDR - Custom Dashboards - How to - Criar visualização

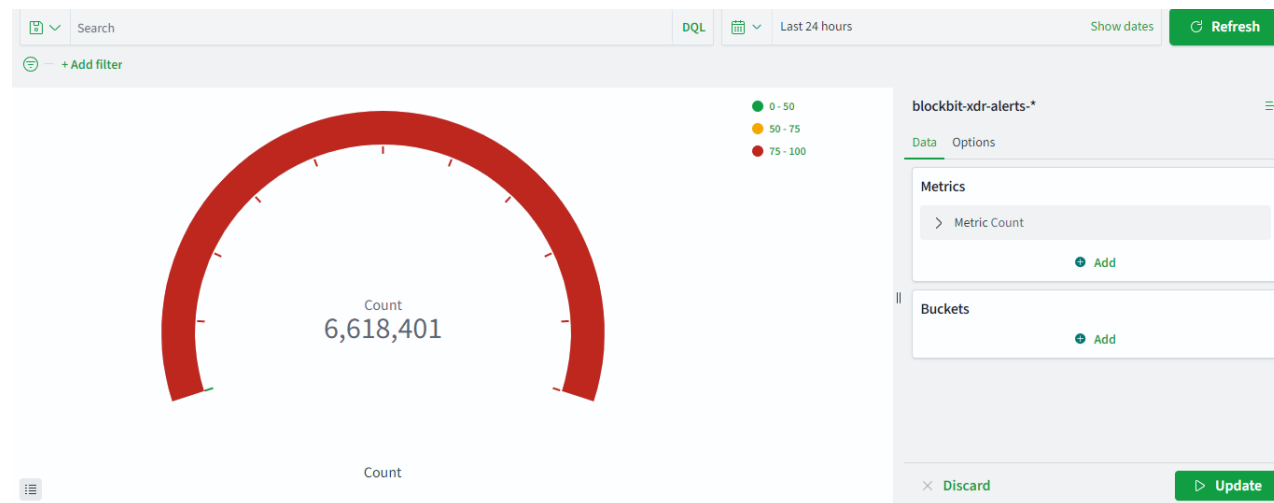
Neste how to você irá aprender a criar uma visualização tipo **Gauge** para o dado **rule.frequency**.

Depois de clicar em Dashboards > Create new, selecione Gauge no modal.

Selecione uma fonte de dados. Aqui foi selecionada blockbit-xdr-alerts-.



Você irá para esta tela:



O gráfico em questão conta todos os dados da fonte.

Clique em Metric count.

Um submenu irá abrir.

Em **Aggregation**, selecione **Average**.

Metrics

▼ Metric

Aggregation [Average help](#)

Average ▼

Metric Aggregations

✓ Average

Count

Max

Median

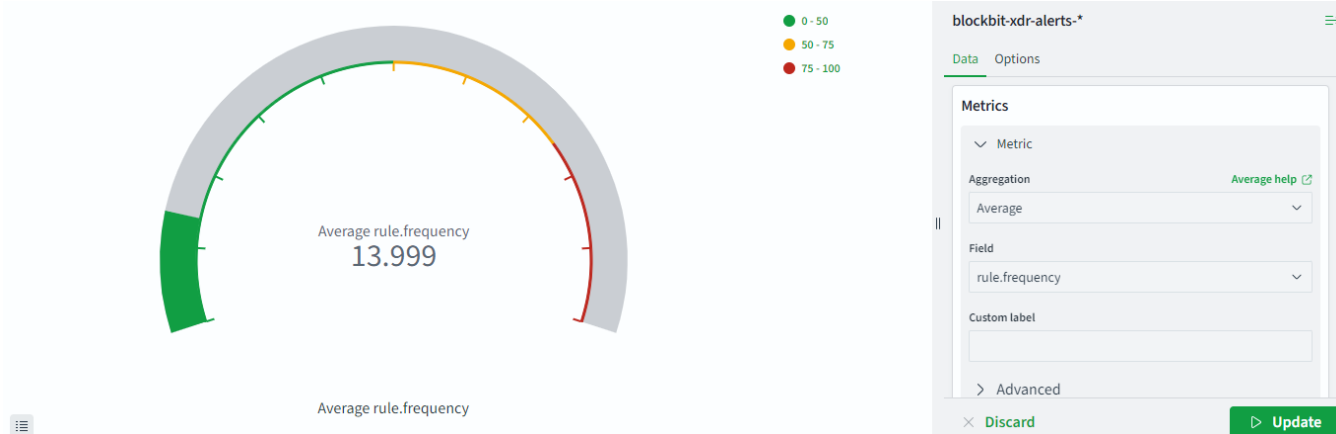
Min

Sum

Em **Field**, foi selecionado **rule.frequency**.

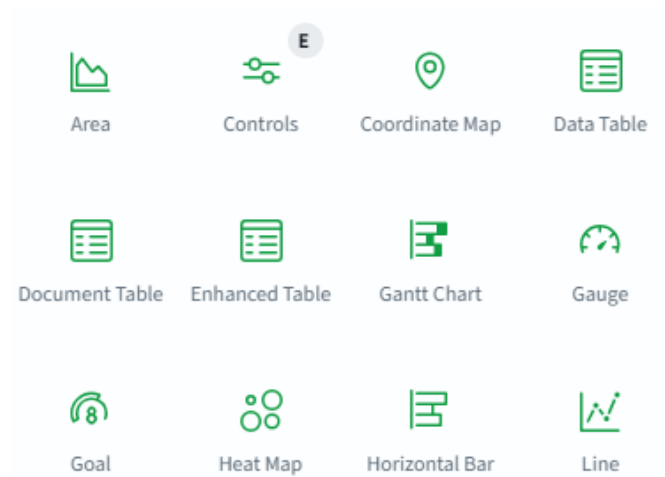
Clique em Update.

A tela irá mostrar a média do dado **rule.frequency** na fonte de dados **blockbit-xdr-alerts-** em relação aos dados totais.



XDR - Custom Dashboards - Visualizações

No Blockbit XDR, as seguintes visualizações estão disponíveis:



Area

Este tipo de visualização permite acompanhar mudanças ao longo do tempo.

Controls

A opção permite construir visualizações dinâmicas.

Coordinate Map

Esta visualização permite acompanhar dados num mapa-mundi com base em coordenadas geográficas.

Data Table

Esta visualização permite criar tabelas comparando valores numéricos.

Document Table

Funcionalidade parecida com o **Data table**, mas comparando conteúdo de documentos.

Enhanced Table

Funcionalidade parecida com o **Data table** com recursos adicionais.

Gantt Chart

Gráficos que mostram o começo, fim e a duração de eventos.

Gauge

Gráficos que mostram o quanto um recurso foi utilizado.

Goal

Gráficos que mostram o quando falta para alcançar um objetivo.

Heat map

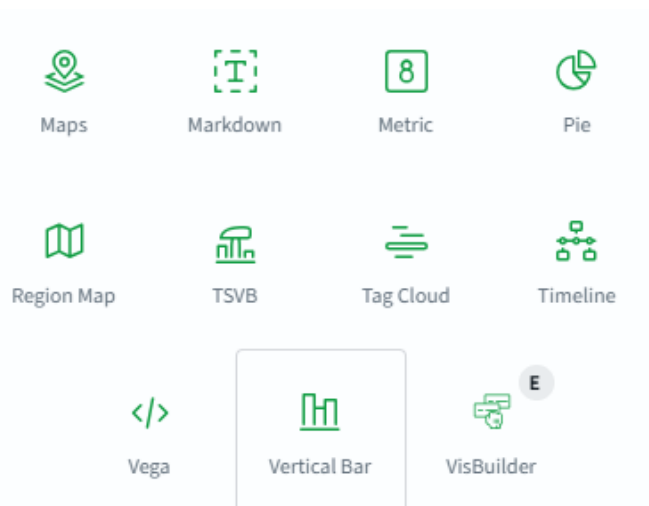
Gráfico que mostra a frequência de um evento ao longo do tempo.

Horizontal bar

Gráfico que representa horizontalmente a variação de um dado categórico ao longo do tempo.

Line

Gráfico que sumariza as mudanças de uma variável ao longo do tempo.



Maps

Ferramenta que permite a criação de mapas com informações diversas.

Markdown

Ferramenta que permite a criação de objetos usando linguagem Markup.

Metric

Ferramenta que permite comparar diferentes valores numéricos.

Pie

Gráfico que representa a porcentagem de cada componente dentro de uma totalidade.

Region map

Ferramenta que permite acompanhar eventos classificados por localidade.

TVSB

O time-series visual builder é uma ferramenta que permite criar visualizações com base no tempo.

Tag Cloud

Nuvem de palavras. Permite visualizar a frequência do uso de palavras.

Timeline

Linha do tempo. Permite visualizar dados ao longo do tempo.

Vega

É uma gramática de visualização que permite criar, compartilhar e salvar dados interativos de visualizações. Para mais informações, visite <https://vega.github.io/>.

Vertical bar

Gráfico que representa verticalmente a variação de um dado categórico ao longo do tempo.

VisBuilder

Ferramenta drag and drop para criar visualizações.

Para um exemplo da criação de visualização, acesse o [How To](#).

XDR - Reports

Nesta página, você pode acessar os relatórios produzidos pelo Analyzer. Todo relatório produzido pelo Blockbit XDR fica armazenado aqui.

Search...

Refresh

File	Size	Created ↓	Actions
blockbit-xdr-module-overview-pm-1723138691.pdf	57.98KB	Aug 8, 2024 @ 14:38:13.269	 

Rows per page: 10

< 1 >

Em **Search**, você pode procurar por relatórios.

Ao clicar em **Refresh**, você pode atualizar a lista de relatórios.

A lista de relatórios é classificada por:

Arquivo (**File**): nome do arquivo do relatório.

Tamanho (**Size**): tamanho do arquivo do relatório.

Criado (**Created**): data e hora da criação do arquivo do relatório.

Em **Actions**, você pode.

Baixar o arquivo do relatório em **Download report**.

Apagar o arquivo do relatório em **Delete report**.

O relatório será gerado em **PDF**.

blockbit-xdr-module-agents-020-general-1742283313.pdf1 / 9100%+

1

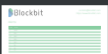


2



3





Blockbit

contato@blockbit.com
https://www.blockbit.com

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
020	...	...	BbXDR v1.0.0	blockbit-xdr-manager-worker-0	Microsoft Windows 10 Pro 10.0.19043.2130	Dec 26, 2024 @ 16:44:37.000	Mar 18, 2025 @ 04:35:05.000

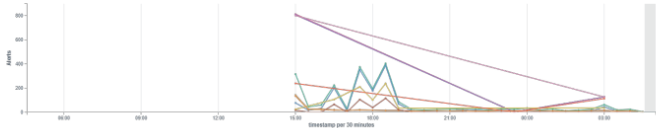
Groups: default, PD, TI

Browse through your security alerts, identifying issues and threats in your environment.

2025-03-17T04:34:16 to 2025-03-18T04:34:16

cluster.name: blockbit-xdr AND agent.id: 020

Alert groups evolution



Top 5 rule groups



66

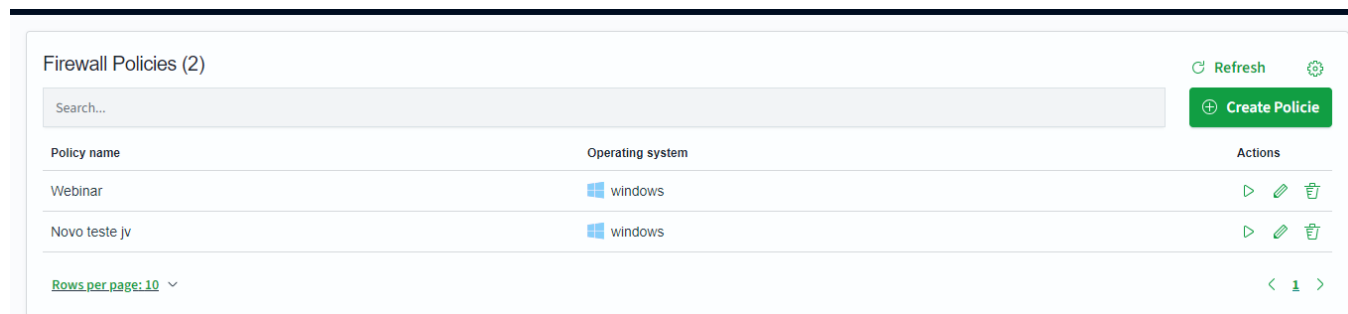
XDR - Endpoint Control Center

O Blockbit XDR Endpoint Control Center permite a criação e aplicação de políticas de segurança para endpoints, localizados em múltiplos sites, locais, departamentos e ambientes geograficamente, as configurações incluem regras de firewall, controle de portas USB e Bluetooth. Com essa funcionalidade, administradores podem gerenciar remotamente as políticas de segurança, garantindo proteção e conformidade em larga escala.

Os agentes do Blockbit XDR são capazes de receber programações diretamente do console de administração, permitindo a aplicação das políticas de forma individual ou em lote. Isso possibilita um gerenciamento centralizado e eficiente, reduzindo o tempo necessário para configurar e distribuir regras de segurança em múltiplos dispositivos.

Principais Funcionalidades

- Criação e Aplicação de Políticas de Firewall
 - Permite definir regras de filtragem de tráfego, controlando comunicações de rede nos endpoints para garantir segurança e integridade do ambiente.
- Gerenciamento de Portas USB e Bluetooth
 - Possibilita a criação de regras para bloquear, restringir ou permitir o uso de dispositivos USB e conexões Bluetooth, prevenindo vazamento de dados e ataques via mídia removível.
- Distribuição e Automação de Políticas
 - Os agentes recebem políticas de segurança diretamente do console e podem aplicá-las automaticamente, garantindo implantação rápida e eficiente em múltiplos dispositivos simultaneamente.



Policy name	Operating system	Actions
Webinar	windows	  
Novo teste jv	windows	  

Para buscar uma política específica, utilize a barra de pesquisas.

Para recarregar a lista, clique em **Refresh**.

Para [criar uma política](#), clique em **Create Policy** ().

Para selecionar os campos visíveis na lista, clique na engrenagem ().

Os campos da lista são:

ID: código identificador da política;

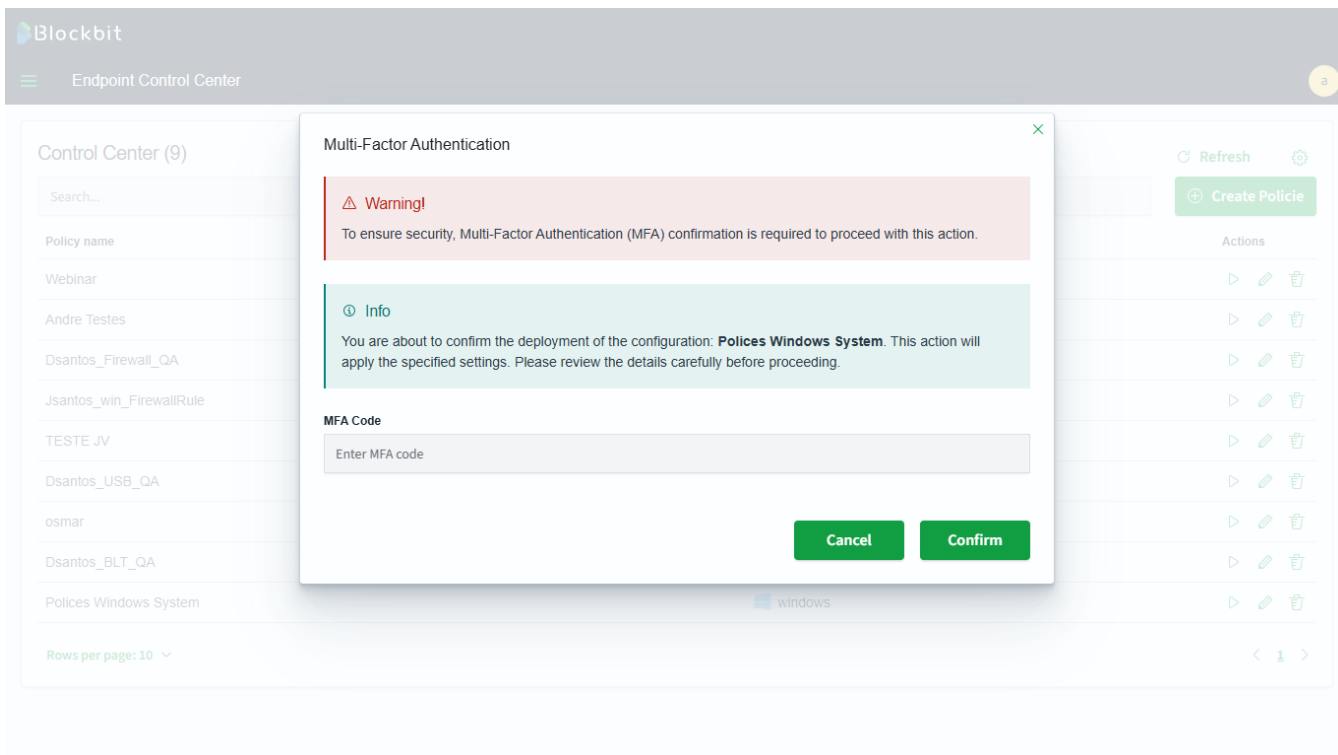
Policy name: nome da política;

Operating system: sistema operacional onde a política será aplicada;

Actions: ações disponíveis:

Deploy commands (): aplicar a política. Ao clicar nesse botão, será exigida a uma validação, sendo obrigatório inserir o código MFA (Autenticação Multifator) para garantir segurança e controle total sobre o processo. Para mais informações, visite [Multi Factor Authentication](#).

A exigência de MFA (Multi-Factor Authentication) ao aplicar políticas reforça a segurança, evitando modificações não autorizadas e garantindo que apenas administradores devidamente autenticados possam implementar alterações críticas no ambiente.



 Edit (): editar a política;

 Delete (): deletar a política.

Com essa abordagem, o Blockbit XDR possibilita um gerenciamento centralizado e seguro das políticas de firewall, USB e Bluetooth, garantindo proteção avançada e controle eficiente sobre os endpoints.

XDR - Endpoint Control Center - Criar política

Para criar uma política no Blockbit XDR, clique no botão **Create Policie** ().

Endpoints

Na aba **Endpoints**, você determina em quais endpoints a política será aplicada.

EndpointsGeneralAdvanced

Basic Settings

Policy Name

um dois

Select Operating System

Windows

Agents / Groups

Select Agents

Select agents...

Select Group

Select agent groups...

- Policy Name:** determine o nome da política;
- Select Operating System:** selecione o sistema operacional;
- Select Agents:** Selecione um ou mais agentes específicos para a aplicação da política, permitindo configurações personalizadas e envio de programações individuais diretamente do console de administração.
- Select Group:** Selecione um grupo de endpoints para aplicação da política de forma massiva, permitindo a **distribuição de configurações em lote** e a orquestração eficiente de múltiplos dispositivos simultaneamente.

General

Na aba **General**, você cria as políticas.

Exemplos:

Bluetooth Policies

☐ Disable All

Device Name	Device Type	Action	Actions
Redmi Buds 5	External	Allow	
Canon-Bluetooth-Printer	External	Allow	

+ Add Policy

Bluetooth Policies

☒ Enable All

Device Name	Device Type	Action	Actions
Redmi Buds 5	External	Deny	
Canon-Bluetooth-Printer	External	Deny	

+ Add Policy

Em **Bluetooth Policies**, você cria políticas específicas para conexões via bluetooth.

O switch **Enable All** () libera todos os periféricos **exceto os listados**. Ele vem habilitado por padrão. Ao mudar para o **Disable All**, ele bloqueia todos os periféricos **exceto os listados**.

Para criar uma política, clique em **Add Policy** ().

Device Name	Device Type	Action	Actions
Enter device name	External	Deny	

- Insira o nome do periférico em **Device Name**;
- Selecione o tipo do periférico em **Device Type**. São 2 tipos: **Internal** (interno) e **External** (externo);
- Selecione a ação a ser tomada em **Action**. São 2 ações: **Allow** (permitir) ou **Deny** (bloquear).

Em **Actions**, você pode deletar a política ao clicar na lixeira ().

USB Policies (5)

☒ Enable All USB Devices

Serial Number	Device Type	Action	Actions
130700000035AB0	Armazenamento em Massa	Full Block	
02662111C6B391BD	Armazenamento em Massa	Full Block	
Select or create options	Impressoras USB	Full Block	
Select or create options	Outros	Full Block	
Select or create options	Armazenamento em Massa	Full Block	

+ Add USB Policy

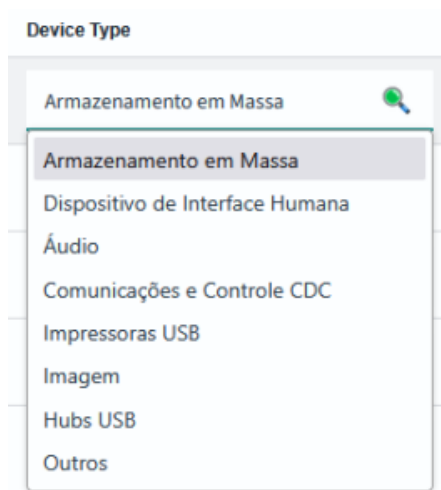
Em **USB Policies**, você cria políticas específicas para periféricos que se conectam via USB.

O switch **Enable All** ( **Enable All**) libera todos os periféricos **exceto os listados**. Ele vem habilitado por padrão. Ao mudar para o **Disable All**, ele bloqueia todos os periféricos **exceto os listados**.

Para criar uma política, clique em **Add USB Policy** ().

Insira o número de série do periférico em **Serial Number**;

Selecione o tipo do periférico em **Device Type**.



Os tipos de periférico são determinados pelo sistema operacional.

Selecione a ação a ser tomada em **Action**. São 3 ações: **Allow All Devices** (permitir todos os aparelhos), **Read-Only Access** (acesso apenas para leitura) ou **Full Block** (bloqueio geral).

Em **Actions**, você pode deletar a política ao clicar na lixeira ().

Firewall Rules (4)							
Domain	Source IP	Destination IP	Port	Protocol	Direction	Action	Actions
Public Doma 				TCP 	Inbound 	Allow 	
Public Doma 				TCP 	Outbound 	Allow 	
Public Doma 				TCP 	Inbound 	Block 	
Domain 				TCP 	Outbound 	Allow 	
							

Em **Firewall Rules**, você pode criar regras de firewall.

Para criar uma regra, clique em **Add Firewall Rule** ().

Selecione o tipo de domínio em **Domain**. São 3 tipos: **Public Domain** (domínio público), **Private Domain** (domínio privado) e **Domain** (domínio);

Insira o IP de origem em **Source IP**;

Insira o IP de destino em **Destination IP**;

Insira a porta em **Port**. Para inserir mais de uma porta, separe-as usando vírgulas (1000,2000 or 5000-5500);

Selecione o protocolo em **Protocol**.

Selecione a direção em **Direction**. Pode ser **Inbound** (chegando) ou **Outbound** (saindo).

Selecione a ação a ser tomada em **Action**. São 2 ações: **Allow** (permitir) ou **Deny** (bloquear).

Em **Actions**, você pode deletar a política ao clicar na lixeira ().

As regras de firewall configuradas pelo Blockbit XDR sempre terão prioridade sobre quaisquer outras regras criadas localmente no firewall do endpoint, garantindo um controle centralizado e eficaz da segurança da rede.

Advanced Settings

Advanced Settings

Warning!

Be careful when entering commands! Any executed configuration is your sole responsibility.

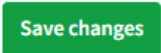
Script Commands

Em **Advanced Settings**, você pode inserir scripts, correlacionados ao sistema operacional selecionado, ou executar comandos em lote diretamente.

Cancel

Para cancelar, clique em **Cancel** ();

Save changes

Para salvar, clique em **Save Changes** ().

Exemplos da capacidade do Advanced Settings:

1. Script PowerShell - Atualização do Agente Blockbit XDR

```
# Definir variáveis
$AgentURL = "https://xdr-nome-do-cliente.blockbit.com/agents/blockbit-xdr-agent-1.0.0-1.msi"
$AgentInstaller = "$env:TEMP\blockbit-xdr-agent.msi"
$LogFile = "$env:TEMP\blockbit-xdr-install.log"

# Definir parâmetros de instalação
$InstallParams = "/q BBXDR_MANAGER='xdr-nome-do-cliente.blockbit.com' BBXDR_REGISTRATION_PASSWORD='XXXX'
BBXDR_REGISTRATION_SERVER='xdr-nome-do-cliente.blockbit.com' BBXDR_AGENT_GROUP='default'
BBXDR_AGENT_NAME='NOME-$ENV:COMPUTERNAME'"

# Verificar se o agente já está instalado
$AgentName = "Blockbit XDR Agent"
$Installed = Get-WmiObject -Query "SELECT * FROM Win32_Product WHERE Name LIKE '%$AgentName%'" | Select-Object -First 1

if ($Installed) {
    Write-Output "O agente Blockbit XDR já está instalado. Iniciando atualização..."
} else {
    Write-Output "O agente Blockbit XDR não está instalado. Iniciando a instalação..."
}
```

```
# Baixar o instalador
Write-Output "Baixando o agente do Blockbit XDR..."
Invoke-WebRequest -Uri $AgentURL -OutFile $AgentInstaller

# Instalar ou atualizar o agente
Write-Output "Instalando o agente do Blockbit XDR..."
Start-Process -FilePath "msiexec.exe" -ArgumentList "/i `"$AgentInstaller`" $InstallParams /L*v `"$LogFile`"" -Wait -NoNewWindow

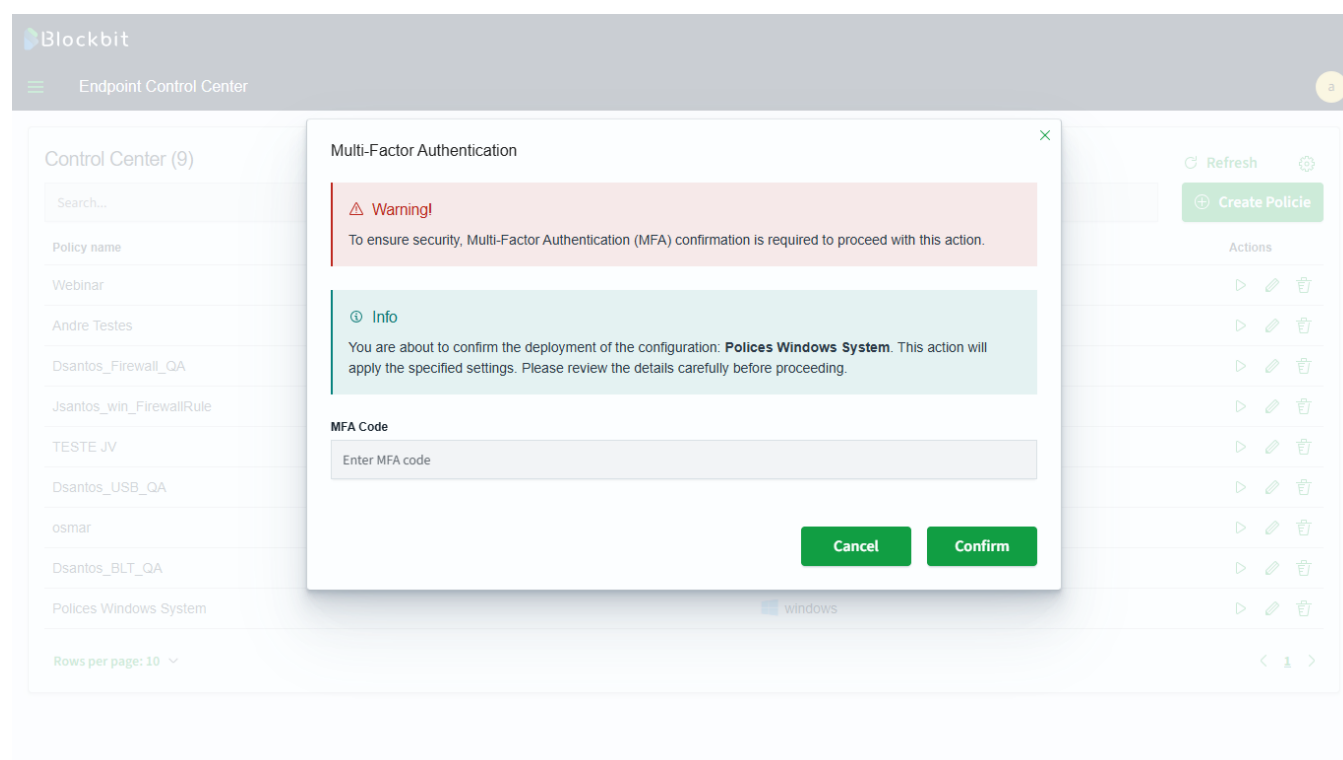
# Verificar se a instalação foi bem-sucedida
$InstalledAgain = Get-WmiObject -Query "SELECT * FROM Win32_Product WHERE Name LIKE '%$AgentName%'" | Select-Object -First 1
if ($InstalledAgain) {
    Write-Output "O agente Blockbit XDR foi instalado/atualizado com sucesso!"
} else {
    Write-Output "Falha na instalação do agente Blockbit XDR. Consulte o log em $LogFile para mais detalhes."
}

# Remover o instalador baixado
Remove-Item -Path $AgentInstaller -Force

Write-Output "Processo concluído."
```

A atualização do agente do Blockbit XDR nos endpoints ocorre de forma transparente e automatizada, garantindo zero impacto no desempenho ou na operação dos dispositivos protegidos. O processo é otimizado para evitar interrupções, assegurando a continuidade das atividades dos usuários.

A atualização do agente do Blockbit XDR, seja via API ou pelo script de atualização, ocorre somente sob demanda a partir da console de administração do Blockbit XDR, mediante ação direta do administrador, sendo obrigatória a validação com MFA (Autenticação Multifator) para garantir segurança e controle total sobre o processo.



2. Script PowerShell - Desativar o Agente Blockbit XDR por 15 Minutos

```
# Nome do serviço do agente Blockbit XDR
$ServiceName = "Blockbit XDR"

# Verificar se o serviço está em execução
$ServiceStatus = Get-Service -Name "$ServiceName" -ErrorAction SilentlyContinue

if ($ServiceStatus -and $ServiceStatus.Status -eq "Running") {
    Write-Output "Parando o serviço do agente Blockbit XDR..."
}
```

```

    Stop-Service -Name "$ServiceName" -Force
    Write-Output "O agente Blockbit XDR foi desativado."
} else {
    Write-Output "O serviço do agente Blockbit XDR já está parado ou não encontrado."
}

# Esperar 15 minutos (900 segundos)
Write-Output "Aguardando 15 minutos antes de reativar o agente..."
Start-Sleep -Seconds 900

# Reativar o serviço
Write-Output "Reativando o serviço do agente Blockbit XDR..."
Start-Service -Name "$ServiceName"

# Verificar se o serviço foi reativado corretamente
$ServiceStatus = Get-Service -Name "$ServiceName"
if ($ServiceStatus.Status -eq "Running") {
    Write-Output "O agente Blockbit XDR foi reativado com sucesso!"
} else {
    Write-Output "Falha ao reativar o agente Blockbit XDR. Verifique manualmente."
}

Write-Output "Processo concluído."

```

XDR - Endpoints Summary

Nesta página, você pode conferir endpoints disponíveis.

A primeira tela é uma lista dos agentes disponíveis.

Blockbit

Endpoints

3

Agents (24)

Refresh

Export formatted

Export Inventory

Refresh

Search

DQL

Name	IP address	Group(s)	Operating system	Cluster node	Version	Last keep alive	Status	Actions
		default	Microsoft Windows 10 Pro 10	blockbit-xdr-manager-worker-0	v1.0.0	Jan 21, 2025 @ 13:52:11.000	disconnected	
		default	Ubuntu	blockbit-xdr-manager-worker-0	v1.0.0	Jan 17, 2025 @ 11:53:14.000	disconnected	
		default	CentOS	blockbit-xdr-manager-worker-0	v1.0.0	Jan 17, 2025 @ 16:35:41.000	disconnected	
		default	macOS	blockbit-xdr-manager-worker-0	v1.0.0	Feb 17, 2025 @ 11:18:40.000	disconnected	
		default	Microsoft Windows 10	blockbit-xdr-manager-worker-0	v1.0.0	Feb 4, 2025 @ 04:33:24.000	disconnected	
		default	Microsoft Windows 10	blockbit-xdr-manager-worker-0	v1.0.0	Feb 10, 2025 @ 13:42:12.000	disconnected	
		default	Microsoft Windows 10	blockbit-xdr-manager-worker-0	v1.0.0	Feb 7, 2025 @ 13:24:43.000	disconnected	

Para procurar por um agente específico, utilize a barra de buscas (**Search**), onde você pode montar uma query para procurar por agentes.

Em **Refresh**, você pode recarregar a lista.

Em **Export formatted**, você pode exportar um arquivo .csv com a lista de agentes.

Em **Export inventory**, você pode criar um inventário dos agentes.

Export Inventory

Agents

Search and select agents for export inventory

Select Agents

Agents Group

Search and select agents group for export inventory

Select Agents Group

Agents System Operation

Search and select agents system operation for export inventory

Select Agents System Operation

To generate the inventory for all agents, simply do not select any of the filters above.

Return

Generate Inventory

Para criar o inventário, selecione os agentes, o grupo de agentes ou o sistema operacional.

Ao clicar em **Generate inventory**, será criado um arquivo .csv com um inventário dos agentes selecionados.

Para cada agente, há as seguintes características:

Name é o nome do agente.

IP address é o endereço IP do agente.

Group é o grupo que o agente faz parte. Ao clicar no grupo, apenas os agentes dele irão aparecer na lista.

Operating system é o sistema operacional do agente.

Cluster node é a localização do agente na rede.

Version é a versão do agente.

Last keep alive é a última verificação de conexão.

Status é o status do agente. São dois status: ativo (**active**) e desconectado (**disconnected**). Ao lado, há uma interrogação (). Ao passar o mouse sobre ela, são apresentadas informações do status.

Cada agente tem as seguintes ações:

Open summary panel for this agent (): Abre os detalhes do agente.

Open configuration for this agent (): Abre a lista de configurações do agente. Não é possível modificar as configurações do agente nesta interface.

Restart this agent (): Reinicia o agente.

Delete this agent (): Deleta o agente. Esta opção só se torna disponível quando o agente está desconectado.

XDR - Endpoints Summary - Configurações

No Blockbit XDR, os agentes podem ser configurados diretamente pela interface.

Configurações não suportadas pelo sistema operacional do agente aparecem como desabilitadas.

Configurações principais



Para acessar às configurações, clique no olho ().

Main configurations

Name	Description	Actions
Global Configuration	Logging settings that apply to the agent	
Communication	Settings related to the connection with the manager	
Anti-flooding settings	Agent bucket parameters to avoid event flooding	
Labels	User-defined information about the agent included in alerts	

Export PDF

Para exportar as configurações em PDF, clique em **Export PDF** ().

Configurações globais (Global Configuration)

São configurações para logs internos.

<

Global Configuration

Logging settings that apply to the agent

Global

▼

Main settings

Basic alerts and logging settings

?

Write internal logs in plain text

yes

Write internal logs in JSON format

no

Write internal logs in plain text: permite a criação de logs em plain text;

Write internal logs in JSON format: permite a criação de logs em JSON.

Communication

São configurações relacionadas à comunicação do agente com o manager.

Communication
Settings related to the connection with the manager

General

Main settings
Basic manager-agent communication settings

Method used to encrypt communications ☐

Remote configuration is enabled

Auto-restart the agent when receiving valid configuration from manager

Time (in seconds) between agent checkings to the manager

Time (in seconds) before attempting to reconnect

Configuration profiles

Server settings
List of managers to connect

Address	Port	Protocol	Maximum retries to connect	Retry interval to connect
xdr-dev.blockbit.com	1514	tcp	5	10

Method used to encrypt communications: método usado para criptografar a comunicação

Remote configuration is enabled: permite habilitar ou desabilitar a configuração remota;

Auto-restart the agent when receiving valid configuration from manager: reinicia o agente automaticamente ao receber uma configuração válida do manager;

Time (in seconds) between agent checkings to the manager: tempo entre checagens do agente com o manager;

Time (in seconds) before attempting to reconnect: tempo de espera antes da tentativa de reconexão;

Configuration profiles:

Server settings:

Aqui estão listados os managers disponíveis para conectar.

Eles são classificados em:

Address: URL do manager;

Port: porta do manager;

Protocol: protocolo do manager;

Maximum retries to connect: máximo de tentativas de conexão;

Retry interval to connect: intervalo em segundos entre as tentativas de conexão.

Anti-flooding settings

Aqui estão listados os parâmetros para evitar eventos de flooding.

Anti-flooding settings
Agent bucket parameters to avoid event flooding

General

Main settings
These settings determine the event processing rate for the agent

Buffer status

Queue size

Events per second

Buffer status: permite informar a quantidade de dados em espera;

Queue size: define o máximo de requisições em espera;

Events per second: define o máximo de eventos por segundo.

Auditing and policy monitoring

Aqui estão as configurações de auditoria e monitoramento de políticas.

Auditing and policy monitoring

Name	Description	Actions
Policy monitoring	Configuration to ensure compliance with security policies, standards and hardening guides	
OpenSCAP	Configuration assessment and automation of compliance monitoring using SCAP checks	
CIS-CAT	Configuration assessment using CIS scanner and SCAP checks	

Policy monitoring

Aqui estão as configurações de políticas.

Policy monitoring service status	enabled
Scan the entire system	no
Frequency (in seconds) to run the scan	43200
Check /dev path	yes
Check files	yes
Check network interfaces	yes
Check processes IDs	yes
Check network ports	yes
Check anomalous system objects	yes
Check trojans	yes
Check UNIX audit	no
Skip scan on CIFS/NFS mounts	yes
Rootkit files database path	etc/shared/rootkit_files.txt
Rootkit trojans database path	etc/shared/rootkit_trojans.txt

Policy monitoring service status: habilita o monitoramento de políticas;

Scan the entire system: permite escanear o sistema inteiro;

Frequency (in seconds) to run the scan: determina a frequência de escaneamento em segundos;

Check /dev path: permite checar os dispositivos conectados;

Check files: permite checar os arquivos;

Check network interfaces: permite checar as interfaces de rede;

Check processes IDs: permite checar os processos;

Check network ports: permite checar os arquivos;

Check anomalous system objects: permite checar o sistema para detectar objetos anômalos;

Check trojans: permite checar o sistema para detectar trojans;

Check UNIX audit: permite checar os logs de auditoria UNIX;

Skip scan on CIFS/NFS mounts: permite pular o escaneamento de arquivos CIFS/NFS.

Rootkit files database path: determina o diretório do rootkit;

Rootkit trojans database path: determina o diretório do rootkit de trojans.

SCA

Security configuration assessment status

Security configuration assessment status: enabled

Interval: 43200

Scan on start: yes

Skip nfs: yes

Policies

Name
/opt/blockbit-xdr/ruleset/sca/cis_centos8_linux.yml

Security configuration assessment status: habilita o SCA (Security Configuration Assessment);

Interval: determina o intervalo entre os escaneamentos;

Scan on start: habilita o escaneamento quando o sistema é iniciado;

Skip nfs: permite pular arquivos NFS;

Policies: aqui, as políticas são listadas pelo nome.

CIS-CAT

Aqui estão as configurações do CIS scanner e da checagem SCAP.

General

Main settings

General settings applied to all benchmarks

CIS-CAT integration status: disabled

Timeout (in seconds) for scan executions: 1800

Path to Java executable directory: wodles/java

Path to CIS-CAT executable directory: wodles/ciscat

Scheduling settings

Customize CIS-CAT scans scheduling

Interval between scan executions: 86400

Scan on start: yes

CIS-CAT integration status: Status da integração CIS-CAT. Pode ser habilitado ou desabilitado;

Timeout (in seconds) for scan executions: tempo máximo para os escaneamentos;

Path to Java executable directory: localização do diretório executável Java;

Path to CIS-CAT executable directory: localização do diretório executável CIS-CAT;

Interval between scan executions: intervalo entre escaneamentos;

Scan on start: habilita o escaneamento quando o sistema é iniciado.

System threats and incident response

Aqui estão as configurações de resposta a incidentes e ameaças ao sistema.

System threats and incident response		
Name	Description	Actions
Osquery	Expose an operating system as a high-performance relational database	
Inventory data	Gather relevant information about system operating system, hardware, networking and packages	
Active response	Active threat addressing by immediate response	
Commands	Configuration options of the Command wodle	

Osquery

Nesta página, estão as configurações do Osquery, ferramenta que permite criar consultas ao sistema.

Osquery DISABLED

Expose an operating system as a high-performance relational database

General

Main settings

General Osquery integration settings

Osquery integration status

disabled

Auto-run the Osquery daemon

yes

Path to the Osquery executable

Path to the Osquery results log file

Path to the Osquery configuration file

Use defined labels as decorators

yes

Osquery integration status: mostra a integração do Osquery ao agente. Tem dois status: **enabled** (habilitado) e **disabled** (desabilitado);

Auto-run the Osquery daemon: permite que o daemon do Osquery rode automaticamente;

Path to the Osquery executable: caminho do diretório do arquivo executável do Osquery;

Path to the Osquery results log file: caminho do diretório do arquivo de logs do Osquery;

Path to the Osquery configuration file: caminho do diretório do arquivo de configuração do Osquery;

Use defined labels as decorators: permite que as labels possam modificar o comportamento do Osquery.

Inventory data

Aqui estão as configurações sobre a coleta de informações do sistema.

< Inventory data ENABLED

Gather relevant information about system operating system, hardware, networking and packages

General

Main settings
General settings applied to all the scans

Syscollector integration status

enabled

Interval between system scans

3600

Scan on start

yes

Main settings: configurações gerais do escaneamento;

Syscollector integration status: mostra a integração do Syscollector ao agente. Tem dois status: **enabled** (habilitado) e **disabled** (desabilitado);

Interval between system scans: determina o intervalo entre escaneamentos;

Scan on start: habilita o escaneamento quando o sistema é iniciado.

Scan settings
Specific inventory scans to collect

Scan hardware info

yes

Scan current processes

yes

Scan operating system info

yes

Scan installed packages

yes

Scan network interfaces

yes

Scan listening network ports

yes

Scan all network ports

no

Scan settings: determina o que vai ser escaneado.

Scan hardware info: permite escanear informações de hardware;

Scan current processes: permite escanear processos correntes;

Scan operating system info: permite escanear informações de sistema;

Scan installed packages: permite escanear pacotes instalados;

Scan network interfaces: permite escanear interfaces de rede;

Scan listening network ports: permite escanear portas de escuta da rede;

Scan all network ports: permite escanear todas as portas da rede.

Active response

Aqui estão as configurações de resposta ativa e imediata.

< Active response

Active threat addressing by immediate response

General

Active response settings

Find here all the Active response settings for this agent

Active response status

Active response status:

mostra se o Active Response está habilitado no agente. Tem dois status: enabled (habilitado) e disabled (desabilitado).

Commands

Aqui são configurados os comandos.

Command definitions

Find here all the currently defined commands

vss

Command status

no

Command name

Command to execute

Interval between executions

43200

Run on start

yes

Ignore command output

no

Ignore checksum verification

no

À esquerda, estão listados os comandos.

Para cada comando, há as seguintes opções:

Command status: status do comando;

Command name: nome do comando;

Command to execute: arquivo a ser executado pelo comando;

Interval between executions: intervalo entre as execuções do comando;

Run on start: habilita o comando quando o sistema é iniciado.

Ignore command output: ignorar o resultado do comando;

Ignore checksum verification: ignorar a verificação de checksum.

Log collection

Exibe as configurações de logs.

Logs files

Exibe configurações de arquivos de logs.

Logs files

List of log files that will be analyzed

Log format

syslog

Log location

/var/log

Only receive logs occurred after start

yes

Filter logs using this XPATH query

-

Only receive logs occurred after start

-

Redirect output to this socket

agent

If the expression matches, the log will be ignored

-

The log will only be processed if the expression matches

-

À esquerda, estão listados os arquivos de logs.

Log format: formato do log;

Log location: diretório do log;

Only receive logs occurred after start: determina se logs ocorridos antes de começar serão aceitos;

Filter logs using this XPATH query: permite inserir uma consulta XPATH para filtrar logs;

Only receive logs occurred after start: determina se logs ocorridos antes de começar serão aceitos;

Redirect output to this socket: permite redirecionar resultados ao socket selecionado;

If the expression matches, the log will be ignored: permite inserir uma expressão que, caso o log contenha, ele será ignorado;

The log will only be processed if the expression matches: permite inserir uma expressão para exigir que o log contenha para ser processado.

Windows events logs

Permite configurar o processamento de logs do Windows.

Windows Events

Windows events logs

List of Windows logs that will be processed

Log format

eventchannel

Channel

Application

Query

-

Only future events

yes

Reconnect Time

5

À esquerda, estão listados os arquivos de logs.

Log format: determina o formato do log;

Channel: determina o canal do log;

Query: permite inserir uma consulta;

Only future events: determina se logs registrarão apenas eventos futuros;

Reconnect Time: determina o tempo de reconexão.

Integrity monitoring

Exibe as configurações de escaneamento e monitoramento de integridade para identificar mudanças em conteúdos, arquivos, atributos ou proprietários.

General

Configurações gerais.

Integrity monitoring status	enabled
Interval (in seconds) to run the integrity scan	43200
Time of day to run integrity scans	-
Day of the week to run integrity scans	-
Scan on start	yes
Skip scan on CIFS/NFS mounts	yes
Skip scan of /dev directory	yes
Skip scan of /sys directory	yes
Skip scan of /proc directory	yes
Remove old local snapshots	yes
Interval (in seconds) to check directories' SACLs	60
Command to prevent prelinking	-
Maximum event reporting throughput	50
Process priority	10
Database type	disk

Integrity monitoring status: status do monitoramento de integridade. São 2: **enabled** (habilitado) e **disabled** (desabilitado);

Interval (in seconds) to run the integrity scan: intervalo entre os escaneamentos;

Time of day to run integrity scans; horário que o agente será escaneado;

Day of the week to run integrity scans: dia que o agente será escaneado;

Scan on start: habilita o escaneamento quando o sistema é iniciado.

Skip scan on CIFS/NFS mounts: permite pular o escaneamento de arquivos CIFS/NFS;

Skip scan of /dev directory: permite pular o escaneamento do diretório /dev;

Skip scan of /sys directory: permite pular o escaneamento do diretório /sys;

Skip scan of /proc directory: permite pular o escaneamento do diretório /proc;

Remove old local snapshots: permite remover snapshots antigos;

Interval (in seconds) to check directories' SACLs: intervalo de checagem dos diretórios das listas de controle de acesso;

Command to prevent prelinking: comando para prevenir prelinking;

Maximum event reporting throughput: throughput máximo para relatar eventos;

Process priority: prioridade do processo;

Database type: tipo da base de dados.

Monitored

Configurações dos diretórios monitorados.

Monitored directories
These directories are included on the integrity scan

ft...

p

e...

3...

3p

n...

l...

i

nts

ads

top

...

tl...

...

ts

ds

...

b...

i...

Selected item

tu

Enable realtime monitoring

yes

Enable auditing (who-data)

no

Report file changes

no

Perform all checksums

no

Check sums (MD5 & SHA1)

no

Check MD5 sum

yes

Check SHA1 sum

yes

Check SHA256 sum

yes

Check files size

yes

Check files owner

yes

Check files groups

yes

Check files permissions

yes

Check files modification time

yes

Check files inodes

yes

Recursion level

256

Follow symbolic link

no

À esquerda, estão os diretórios monitorados. Para acessar a configuração, clique no diretório desejado.

Selected item: diretório selecionado;

Enable realtime monitoring: habilitar monitoramento em tempo real;

Enable auditing (who-data): permitir auditoria;

Report file changes: reportar mudanças em arquivos;

Perform all checksums: checar todos os checksums;

Check sums (MD5 & SHA1): checar checksums tipo **MD5** e **SHA1**;

Check MD5 sum: checar checksums tipo **MD5**;

Check SHA1 sum: checar checksums tipo **SHA1**;

Check SHA256 sum: checar checksums tipo **SHA256**;

Check files size: checar o tamanho dos arquivos;

Check files owner: checar o proprietário dos arquivos;

Check files groups: checar os grupos dos arquivos;

Check files permissions: checar as permissões dos arquivos;

Check files modification time: checar o tempo para modificar arquivos;

Check files inodes: checar os inodes (todas as informações, menos nome e data) de arquivos;

Recursion level: nível de recursividade;

Follow symbolic link: permite seguir links simbólicos (arquivos de sistema que apontam para outros arquivos de sistema).

Monitored registry entries

É a lista de registros monitorados. São classificados pelo nome de registro (Entry) e arquitetura (Arch).

Entry	Arch
H	32bit
H	32bit
H	32bit
H	32bit
H	32bit
H	32bit
H	32bit
H	32bit
H	32bit
H	64bit

Ignored

É a lista de registros ignorados.

Path
ini
Sregex
\$

Path: diretório do registro a ser ignorado;

Sregex: expressões regulares a serem ignoradas.

Synchronization

Configurações de sincronização de bases de dados.

Synchronization

Database synchronization settings

Synchronization status

enabled

Maximum interval (in seconds) between every sync

3600

Interval (in seconds) between every sync

300

Response timeout (in seconds)

30

Queue size of the manager responses

16384

Maximum message throughput

10

Number of threads

1

Synchronization status: status da sincronização;

Maximum interval (in seconds) between every sync: intervalo máximo em segundos entre as sincronizações;

Interval (in seconds) between every sync: intervalo em segundos entre as sincronizações;

Response timeout (in seconds): tempo em segundos para desistir da sincronização;

Queue size of the manager responses: tamanho da fila de respostas do manager;

Maximum message throughput: throughput máximo de mensagens;

Number of threads: número de instruções dadas à CPU.

Files limit

Determina o número máximo de arquivos monitorados.

File limit status	enabled
Maximum number of files to monitor	100000

File limit status: permite limitar arquivos;

Maximum number of files to monitor: determina o número máximo de arquivos monitorados.

Registry limit

Determina o número máximo de registros monitorados.

File limit status: permite limitar registros;

Maximum number of files to monitor: determina o número máximo de registros monitorados.

Exceções e Exclusões

As configurações acima, permitem configurações exceções, no mínimo na lista abaixo:

- Permite desativar ou ativar motores de proteção do endpoint.
- Permite criar exceções nas proteções do endpoint.
- Permite criar exceções e/ou exclusões de arquivos, por tipo de arquivos (mime-type), por hash e por pastas nas proteções e monitoramento do endpoint.
- Permite criar exceções e/ou exclusões programas, certificados digitais de fornecedores que assinam suas aplicações nas proteções e monitoramento do endpoint.
- Permite criar exceções e/ou exclusões por comportamento nas proteções e monitoramento do endpoint.

XDR - Endpoints Summary - Summary Panel

O Blockbit XDR integra o **Sysmon** no Windows e o **auditd** no Linux, permitindo o monitoramento detalhado de atividades do sistema. A solução registra eventos críticos, como execução de processos, modificações em arquivos e alterações no registro, proporcionando uma visão abrangente e forense das operações no endpoint.

Para facilitar a análise de ameaças, o Blockbit XDR apresenta de forma visual uma **árvore de processos**, permitindo que analistas de segurança visualizem a relação entre processos legítimos e suspeitos, identifiquem cadeias de execução maliciosas e compreendam o impacto de eventos no sistema.

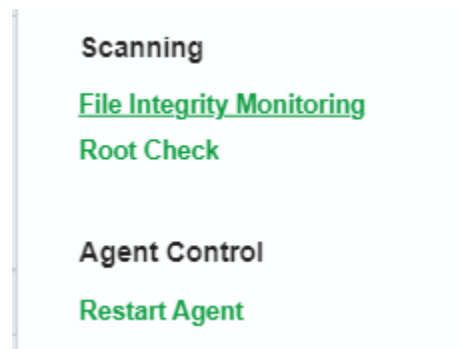
Esse recurso possibilita a detecção proativa de ameaças, investigação detalhada e resposta automatizada a incidentes, garantindo maior controle sobre a segurança do ambiente.

Na página, você pode conferir todas as informações e acessar todas as funcionalidades do XDR para o Agente.

Em **Applications**, você pode acessar todas as funcionalidades do XDR para o agente:



Em **Actions**, você pode tomar as seguintes ações:



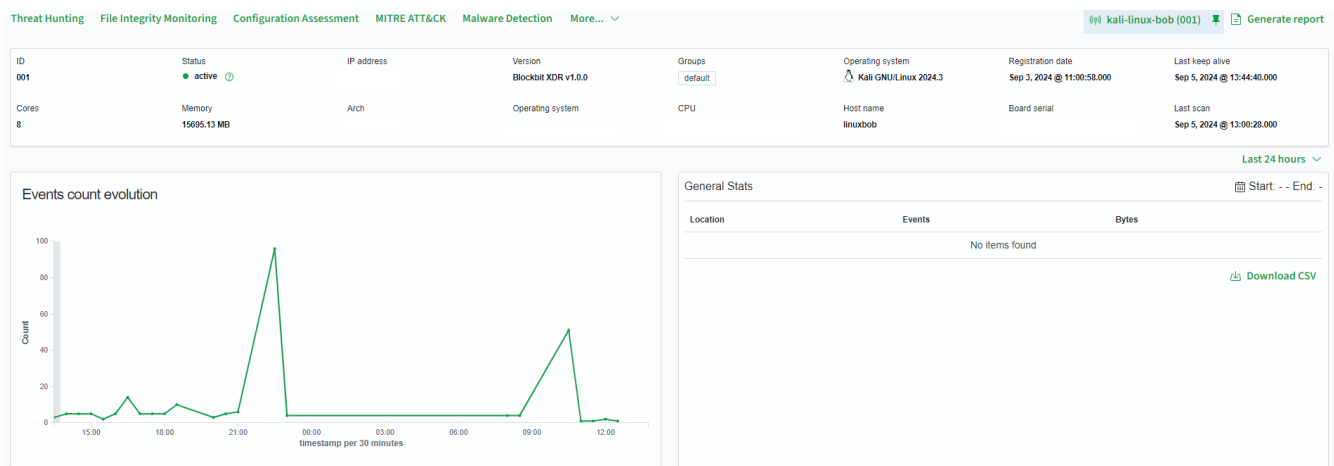
File Integrity Monitoring: escanear o agente utilizando o **File Integrity Monitoring** do Blockbit XDR;

Root Check: escanear o agente utilizando o Root Check, módulo de detecção de rootkits, malware, vulnerabilidades, configurações inadequadas e auditoria de conformidade que examina sistemas em busca de sinais de comprometimento;

O Root Check busca, entre outros:

- **Portas ocultas**
- **Arquivos e permissões incomuns**
- **Processos encobertos**
- **Mal funcionamento de software**
- **Malware Detection:** Identifica ameaças como rootkits, trojans, spyware e ransomwares em tempo real.
- **Threat Hunting:** Permite a busca ativa por ameaças ocultas dentro da rede e dos endpoints.
- **Configuration Assessment:** Avalia configurações de segurança para identificar vulnerabilidades e falhas de conformidade.
- **Vulnerability Detection:** Detecta vulnerabilidades exploráveis no sistema, correlacionando com bases de CVEs conhecidas.

Restart Agent: reiniciar o agente.



Todo o agente tem as seguintes características:

ID: Identificador do agente;

Status: status do agente. São dois status: ativo (**active**) e desconectado (**disconnected**).

IP address: endereço IP do agente;

Version: versão do agente;

Groups: grupos do agente;

Operating system: sistema operacional do agente;

Registration date: data e horário que o agente foi registrado;

Last keep alive: última verificação de conexão do agente;

Cores: número de processadores;

Memory: memória da máquina;

Arch: versão da arquitetura do processador;

Operating system: sistema operacional da máquina;

CPU: modelo do processador;

Host name: nome do servidor;

Board serial: número de série da máquina;

Last scan: Último escaneamento no agente.

Events count evolution: número de eventos por 30 minutos;

General Stats: estatísticas de eventos envolvendo o agente. São classificadas por localização (**Location**), eventos (**Events**) e tamanho (**Bytes**). Você pode mudar o intervalo de medição no lado superior direito.

FIM: Recent events

Time ↓	Path	Action	Rule description	Rule L.e...	Rule Id
Sep 5, 2024 @ 10:56:59.121		modified	Integrity checksum changed.	7	550
Sep 5, 2024 @ 10:56:59.121		modified	Integrity checksum changed.	7	550

SCA: Latest scans

Policy	End scan	Passed	Failed	Not applic...	Score
System audit for Unix based systems	Sep 5, 2024 @ 10:56:44.000	3	13	7	18%

MITRE ATT&CK

Top Tactics

Defense Evasion

Impact

PCI-DISS

Top 5 PCI-DISS

10.6.1

10.2.7

10.2.6

11.5

GDPR

Top 5 GDPR

IV_35.7.d

II_5.1.f

NIST-800-53

Top 5 NIST-800-53

AU.6

AU.14

AU.5

SI.7

HIPAAA

Top 5 HIPAAA

164.312.b

164.312.c.1

164.312.c.2

GPG13

Top 5 GPG13

10.1

4.10

4.11

TSC

Top 5 TSC

CC7.2

CC7.3

CC6.8

CC8.1

FIM: Recent events: [File integrity monitoring](#) para o agente;

SCA: Latest scans: [Configuration assessment](#) para o agente;

MITRE ATT&CK: estatísticas de [MITRE ATT&CK](#) específicas do agente;

PCI DSS: estatísticas de [PCI DSS](#) específicas do agente;

GDPR: estatísticas de [GDPR](#) específicas do agente;

NIST-800-53: estatísticas de [NIST-800-53](#) específicas do agente;

HIPAA: estatísticas de [HIPAA](#) específicas do agente;

GPG13: estatísticas de [GPG13](#) específicas do agente;

TSC: estatísticas de [TSC](#) específicas do agente;

Network interfaces (3)

Refresh

Export formatted

Search

DQL

Name ↑	MAC	State	MTU	Type
d		down	1500	ethernet
e		up	1500	ethernet
v		up	1500	ethernet

Rows per page: 10

<

1

>

Network settings (4)

Refresh

Export formatted

Search

DQL

Interface ↑	Address	Netmask	Protocol	Broadcast
c			ipn	
e			ipn	
v			ipn	
v			ipn	

Rows per page: 10

<

1

>

Ports (13)

Refresh

Export formatted

Search

DQL

Local port	Local IP address	Process	PID	State	Protocol
		NetworkManager			udp
		NetworkManager			udp
		NetworkManager			udp6
		chrome			udp
		chrome			udp
		chrome			udp
		chrome			udp
		msedge			udp
		msedge			udp
		msedge			udp

Rows per page: 10

<

1

2

>

Network interfaces: interfaces de rede.
Suas características são:

Name: nome;

MAC: endereço da interface de rede (MAC address);

State: estado. Pode estar funcionando (**up**) ou não (**down**);

MTU: tamanho máximo do pacote de dados;

Type: tipo de rede.

Network settings: configurações de rede.

Suas características são:

Interface : interface de rede;

Address: Endereço de rede. Pode ser padrão IPv4 ou IPv6;

Netmask: máscara de rede;

Protocol: protocolo de rede. Pode ser padrão IPv4 ou IPv6;

Broadcast: domínio de broadcast.

Ports: portas de rede.

Suas características são:

Local port: porta local;

Local IP address: endereço IP local;

Process: serviço executado;

PID: consumo de serviço;

State: estado. Pode estar funcionando (**up**) ou não (**down**);

Protocol: protocolo usado.

Processes:

Processes (245)

Refresh

Export formatted

Search

DQL

Name ↑	PID	Parent PID	VM size	Priority	NLWP	Command
Aggrega torHost. exe	7724	4300	6807552	8	2	C:\Windows\System32\Aggreg atorHost.exe
AnyDes k.exe	4176	1008	43143168	13	5	C:\Program Files (x86)\AnyDesk\AnyDesk.exe
AppVSh Notify.ex e	20416	1772	2514944	8	1	C:\Program Files\Common Files\microsoft shared\ClickToRun\AppVShNo tify.exe
Applicati onFram eHost.e xe	7068	1100	35880960	8	2	C:\Windows\System32\Applica tionFrameHost.exe
DDVColl ectorSv cApi.exe	9800	1008	4325376	8	2	C:\Program Files\Dell\DellDataVault\DDVC ollectorSvcApi.exe
DDVDat aCollect or.exe	3620	1008	127381504	8	23	C:\Program Files\Dell\DellDataVault\DDVD ataCollector.exe
DDVRul esProce ssor.exe	4824	1008	22777856	8	6	C:\Program Files\Dell\DellDataVault\DDVR ulesProcessor.exe

Suas características são:

Name (Nome do Processo): Exibe o nome do processo em execução no sistema.

PID (Process ID): Identificador único do processo, permitindo rastrear e gerenciar sua execução.

Parent PID (ID do Processo Pai): Indica o processo que originou a execução do processo atual. A partir desse identificador, é possível visualizar a árvore hierárquica dos processos, facilitando a análise de comportamentos suspeitos, como injeção de código e execução de malware.

VM Size (Tamanho da Memória Virtual): Representa a quantidade total de memória virtual alocada pelo processo, sendo um indicador importante para detecção de consumo anômalo de recursos.

Priority (Prioridade): Define a prioridade de execução do processo no sistema operacional, influenciando sua alocação de CPU e recursos. Processos com prioridade alta podem indicar tarefas críticas ou atividades suspeitas.

NLWP (Número de Threads): Exibe a quantidade de threads utilizadas pelo processo, sendo um fator relevante para identificar comportamentos anômalos, como malware que cria múltiplas threads para evitar detecção.

Packages:

Packages (229)

Refresh

Export formatted

Search

DQL

Name ↑	Architecture	Version	Vendor
7-Zip 21.07 (x64)	x86_64	21.07	Igor Pavlov
AnyDesk	i686	ad 7.0.15	AnyDesk Software GmbH
Blockbit Client	i686	1.2.4	Blockbit
Blockbit VPN Client	x86_64	4.39.9772	Projeto VPN Blockbit
Blockbit XDR Agent	i686	1.0.0	Blockbit XDR.
CleanUp!	i686		
Clima	x86_64	4.54.63007.0	Microsoft Corporation
Cortana	x86_64	4.2308.1005.0	Microsoft Corporation
Câmera	x86_64	2025.2501.1.0	Microsoft Corporation
DBeaver 24.3.3	x86_64	24.3.3	DBeaver Corp

Rows per page: 10 ▾

<

1

2

3

4

5

...

23

>

Pacotes Instalados (Packages)

Esta seção exibe a lista completa de aplicações e pacotes instalados no endpoint monitorado. A visualização facilita a auditoria de softwares, detecção de aplicações não autorizadas e controle de conformidade.

Campos e suas definições:

- Name: Nome do pacote ou aplicação instalada.
- Architecture: Arquitetura do sistema compatível com o pacote (ex: x86_64 ou i686).
- Version: Versão atual da aplicação ou componente instalado.
- Vendor: Fornecedor ou desenvolvedor responsável pela aplicação.

Além disso, a interface permite:

- Filtrar pacotes por nome, versão ou fornecedor via campo de busca.
- Atualizar a lista clicando em "Refresh".
- Exportar os dados no formato estruturado clicando em "Export formatted".
- Visualizar em múltiplas páginas, com paginação ajustável.

Essa funcionalidade é essencial para manter visibilidade total sobre o ambiente de software, garantindo controle, rastreabilidade e prevenção contra aplicações potencialmente indesejadas.

XDR - Endpoint Groups & Sub-Groups

Gestão de Grupos e Políticas Personalizadas no Blockbit XDR

O Blockbit XDR permite a implementação baseada em estrutura organizacional, garantindo que administradores possam gerenciar múltiplos sites, locais, departamentos e ambientes geograficamente separados dentro de um único console, sem restrições. Através da segmentação por grupos de endpoints e usuários, é possível aplicar políticas personalizadas e regras específicas para cada unidade organizacional.

Estrutura Organizacional

A solução permite a criação de Grupos e Subgrupos Personalizados:

Os administradores podem organizar endpoints em grupos distintos, refletindo a estrutura da organização, como departamentos, unidades de negócios, filiais ou regiões geográficas.

Cada grupo pode ter configurações individuais de segurança e monitoramento, garantindo proteção adequada para diferentes perfis de uso.

Gerenciamento Centralizado e Segmentação Flexível:

O console permite monitorar, aplicar políticas e tomar ações corretivas de forma individual ou em massa sobre qualquer grupo de endpoints.

Os grupos podem ser dinâmicos ou estáticos, garantindo maior flexibilidade para adaptar-se à infraestrutura da organização.

Aplicação de Políticas com Herança em Qualquer Nível:

O Blockbit XDR suporta herança de políticas, permitindo que regras definidas em um nível superior sejam aplicadas automaticamente a subgrupos e endpoints associados.

Os administradores podem definir configurações globais para a empresa e permitir que unidades individuais ajustem parâmetros específicos conforme necessário.

Políticas Baseadas em Grupos para Segurança e Monitoramento:

- Isolamento de Endpoints comprometidos, garantindo contenção de ameaças.
- Bloqueio de processos maliciosos e resposta automatizada a incidentes.
- Correção automática de configurações alteradas por malwares ou ataques.
- Definição de regras para prevenção de novas ameaças e mitigação de riscos.

Exceções e Exclusões Personalizadas por Grupo e subgrupos:

- Ativação ou desativação de motores de proteção específicos para determinados grupos.
- Exclusões por tipo de arquivo (MIME-Type), hash ou diretórios específicos. Exceções de programas, certificados digitais e aplicações confiáveis.
- Definição de exceções por comportamento suspeito, permitindo um controle granular sobre a resposta a ameaças.

Groups & Sub-groups (2)
From here you can list and check your groups and sub-groups, its agents and files.

⊕ Add new group

↺ Refresh

📄 Export formatted

Search

DQL

Name ↑	Agents	Actions
default	24	👁 ✎ 🗑 📁 📄
default_subgroup	0	👁 ✎ 🗑 📁 📄

Rows per page: 10

<

1

>

As ações disponíveis:

⊕

Add new group

↺

Refresh

📄

Export formatted

Para criar um grupo, clique em **Add new group**.

Crie um nome para o grupo e clique em **Save new group**.

Refresh: Atualiza as informações da janela.

Ao clicar em **Export formatted**, será criado um arquivo .csv com informações dos grupos.

Para cada grupo, há **cinco** ações:

Ver detalhes (**view details**) (🔍): serão apresentados detalhes dos agentes e arquivos do grupo. Para mais informações, vá em [View details](#).

Editar grupo (**Edit group configuration**) (✎): abre um editor com informações do grupo. Permitindo personalizar as configurações, regras e exceções dos endpoints pertencentes a esse Grupo ou Sub-grupo, para ativar as detecções automaticamente.

Exemplo:

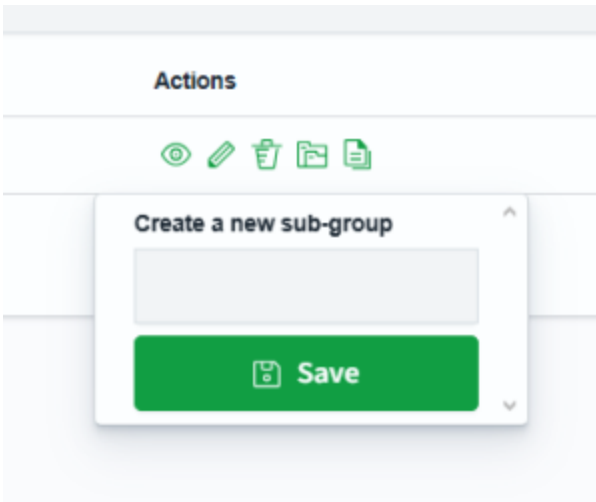
```

1 <agent_conf>
2   <!-- Regra para Detecção de Criptografia Suspeita -->
3   <group name="ransomware, crypto_activity">
4     <rule id="100010" level="10">
5       <decoded_as>system</decoded_as>
6       <field name="event_data.Image">.*(aes|crypt|7z|winrar|bitlocker|cipher|enc|gpg|openssl|sdelete|vssadmin|wbadmin|bcdedit|wvututil).*</field>
7       <description>Possible ransomware activity detected (encryption tool usage)</description>
8     </rule>
9   </group>
10  <!-- Regra para Identificação de Processos Maliciosos -->
11  <group name="ransomware, process_detection">
12    <rule id="100011" level="12">
13      <decoded_as>system</decoded_as>
14      <field name="event_data.Image">.*(wannacry|petya|locky|ryuk|maze|contij|revil|blackmatter).*</field>
15      <description>Known ransomware process detected</description>
16    </rule>
17  </group>
18  <!-- Regra para Detecção de Modificação Massiva de Arquivos -->
19  <group name="ransomware, file_changes">
20    <rule id="100012" level="10">
21      <decoded_as>system</decoded_as>
22      <field name="event_data.TargetFilename">.*\.(docx|xlsx|pdf|jpg|mp4|txt)</field>
23      <frequency>50</frequency>
24      <description>Possible ransomware activity: high file modification rate</description>
25    </rule>
26  </group>
27  <!-- Regra para detectar tentativa de apagar Shadow Copy -->
28  <group name="ransomware, shadow_copy_deletion">
29    <rule id="100013" level="12">
30      <decoded_as>system</decoded_as>
31      <field name="event_data.CommandLine">.*(vssadmin.exe delete shadow|wmic shadowcopy delete).*</field>
32      <description>ALERT! Tentativa de apagar Shadow Copy detectada</description>
33    </rule>
34  </group>
35  <!-- Configuração para bloquear hosts suspeitos -->
36  <command>
37    <name>disable-network</name>
38    <executable>disable-network.sh</executable>
39    <expect>srcip</expect>
40  </command>
41  <active-response>
42    <command>disable-network</command>
43    <location>local</location>
44    <level>12</level>
45  </active-response>

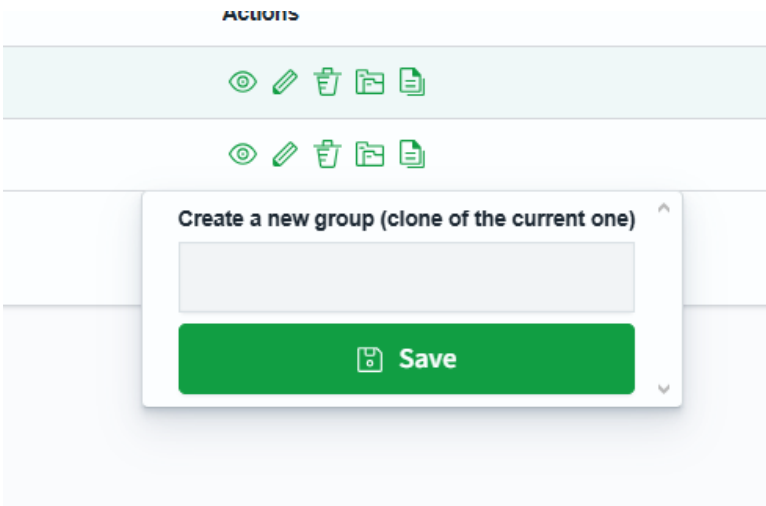
```

Deletar grupo (**Delete**) (🗑️): apaga o grupo ou subgrupo.

Adiciona Subgrupos (**Add Sub-groups**) (📁): Cria um subgrupo dentro de um grupo principal, permitindo personalizações, mas sempre herdando as configurações do grupo pai, mantendo a segurança padronizada.



Clone grupo (**Clone**) () : Duplica um grupo existente, copiando todas as configurações e endpoints, garantindo padronização e agilidade na criação de novos grupos



Na barra **Search**, você pode montar yma query para procurar por grupos.

	Search	run the search query
	name	filter by name
	count	filter by count
	configSum	filter by configuration checksum
	(	open group

Em **name**, você pode filtrar por nome.

Em **count**, você pode filtrar por quantidade.

Em **configsum**, você pode filtrar pelo checksum.

XDR - Endpoint Groups - Inheritance

O Blockbit XDR permite a aplicação e segmentação granular de políticas de segurança, garantindo herança de configurações em qualquer nível organizacional. A solução oferece flexibilidade para definir regras e políticas centralizadas, ao mesmo tempo em que possibilita ajustes específicos por site, local, departamento ou grupo de endpoints.

Com base em uma estrutura organizacional escalável, a console de administração do Blockbit XDR permite que administradores gerenciem múltiplas unidades sem restrição quanto ao número de sites ou locais distintos. Dessa forma, políticas de segurança podem ser aplicadas hierarquicamente, garantindo que configurações essenciais sejam herdadas pelos subníveis, enquanto ajustes personalizados podem ser implementados para atender a necessidades específicas de cada ambiente.

Além disso, o sistema de regras do Blockbit XDR possibilita a correlação inteligente de eventos, gerando alertas de segurança e permitindo a execução automática de ações de Active Response. As políticas aplicadas determinam quais eventos devem ser analisados, quando elevar o nível de severidade de um alerta e quais respostas automatizadas devem ser ativadas para mitigar ameaças em tempo real.

A seguir, explicamos como funciona essa “hierarquia” de regras e como elas podem se encadear ou sobrepor:

1. Sobreposição e Encadeamento de Regras

Regras Genéricas vs. Regras Específicas

Uma “regra genérica” pode detectar uma condição ampla (por exemplo, “Falha de login”). Em seguida, outra “regra mais específica” pode “pegar” aquele mesmo evento para verificar algo adicional (por exemplo, “Falha de login do usuário Administrator”). Esse encadeamento acontece por meio de diretivas como `<if_sid>` (que checa se uma regra anterior com determinado rule ID disparou) ou `<if_level>` (que avalia se a regra anterior tinha certo nível de severidade).

Substituição (replace) e Continuação (continue)

`<replace>true</replace>`: A regra que dispara por último pode substituir totalmente as configurações da regra anterior. Assim, ela pode elevar o nível (level), mudar a descrição e até redefinir o alerta.

`<continue>yes</continue>`: Indica que, depois de disparar aquela regra, o motor de análise continua procurando outras regras subsequentes que também possam se aplicar ao mesmo evento.

Efeito Prático: Hierarquia

Ao usar `<if_sid>`, `<replace>` e `<continue>`, podemos criar um “encadeamento” de regras onde eventos passam por várias camadas de verificação. Uma regra “mais específica” herda o evento de uma genérica e ajusta a severidade ou descrição, criando um alerta final mais preciso.

```

<id>T1059</id>
</mitre>
</rule>

<rule id="100621" level="12">
  <id>T1059</id>
  </mitre>
</rule>

<rule id="100622" level="12">
  <id>T1059</id>
  </mitre>
</rule>

<rule id="100623" level="12">
  <id>T1070.001</id>
  </mitre>
</rule>

<!-- Ransom note file creation -->

<rule id="100626" level="10" timeframe="50" frequency="3" ignore="300">
  <id>T1059</id>
  </mitre>
</rule>

<rule id="100627" level="7" timeframe="30" frequency="10" ignore="300">
  <id>T1059</id>
  </mitre>
</rule>

<rule id="100629" level="7" timeframe="300" frequency="2" ignore="300">
  <id>T1070.001</id>
  </mitre>
</rule>

</group>

<group name="ransomware,ransomware_detection">
  <rule id="100628" level="12" timeframe="300" frequency="2" ignore="300">
    <id>T1059</id>
    </mitre>
  </rule>
</group>

```

2. Ordem de Carregamento (Alfabética) e Enumeração dos Arquivos

Outra forma de entender "hierarquia" está na ordem em que as regras são lidas pelo sistema. O Blockbit XDR carrega os arquivos de regras em ordem alfabética:

Por isso, os arquivos de regras nativos são numerados (por exemplo, 0010-, 0020-, 0100-...) para garantir uma sequência lógica de carregamento.

Ao criar arquivos customizados, você pode dar nomes como 9999-custom_rules.xml para que ele seja carregado depois dos oficiais, permitindo que suas definições (ou overrides) prevaleçam em caso de conflitos.

A ordem de carregamento não substitui o encadeamento de regras em tempo de análise; porém, define quem "ganha" se houver duplicação de IDs ou se duas regras tiverem a mesma tag <rule id="...">.

Exemplo de trecho de configuração no ossec.conf (ou bbxdr.conf):

```

<ruleset>
  <!-- Regras padrão -->
  <rule_dir>ruleset/rules</rule_dir>
  <!-- Regras customizadas do usuário -->
  <rule_dir>etc/rules</rule_dir>
</ruleset>

```

Nesse caso, o conteúdo de ruleset/rules é lido primeiro, e depois o conteúdo de etc/rules. Dentro de cada pasta, a leitura segue a ordem dos nomes de arquivo em ordem alfanumérica.

```
sh-5.2# ls
0010-rules.config.xml      0110-ms_dhcp_rules.xml      0215-policy_rules.xml      0320-clan_av_rules.xml      0420-freeipa_rules.xml      0530-mysql_audit_rules.xml  0625-cisco-asa_rules.xml
0030-sysmon_id_11.xml     0115-arpwatch_rules.xml     0220-mssauth_rules.xml     0325-opensmtpd_rules.xml    0425-cisco-estreamer_rules.xml  0535-mariadb_rules.xml     0625-mcafee_epo_rules.xml
0045-win_event_channel.xml 0120-symantec_av_rules.xml  0225-mcafee_av_rules.xml    0330-sysmon_rules.xml      0430-ms_wdefender_rules.xml    0540-pfsense_rules.xml     0630-nexcloud_rules.xml
0050-audit_rules.xml      0125-symantec-ws_rules.xml  0230-ms-se_rules.xml        0335-unbound_rules.xml     0435-ms_logs_rules.xml         0545-osquery_rules.xml     0635-owb-zeeb_rules.xml
0070-hbaddr-sp4_rules.xml  0130-trend-osc_rules.xml    0235-vmware_rules.xml      0340-puppet_rules.xml     0440-ms_sqlserver_rules.xml    0550-kaspersky_rules.xml   0640-junos_rules.xml
0080-sysmon_id_13.xml     0135-horde_imp_rules.xml    0240-ids_rules.xml          0345-netscaler_rules.xml   0445-identity_guard_rules.xml  0555-azure_rules.xml       0645-panda-paps_rules.xml
0085-sendmail_rules.xml   0140-roundcube_rules.xml    0245-web_rules.xml          0350-amazon_rules.xml      0450-mongodb_rules.xml        0560-docker_integration_rules.xml  0650-checkpoint-smart1_rules.xml  0905-cisco-ftd_rules.xml
0090-firewall_rules.xml   0145-wordpress_rules.xml    0250-apache_rules.xml       0360-serv-u_rules.xml      0455-docker_rules.xml         0565-ms_ipsec_rules.xml    0655-gcp_rules.xml
0095-postfix_rules.xml     0150-cmsserver_rules.xml    0255-zeus_rules.xml         0365-auditd_rules.xml      0460-jenkins_rules.xml        0570-sca_rules.xml         0655-f5-bigip_rules.xml
0100-win-powerShell_rules.xml 0155-dovecot_rules.xml     0260-nginx_rules.xml        0375-usb_rules.xml         0470-vshell_rules.xml         0575-win-base_rules.xml    0700-paloalto_rules.xml
0095-oracledb_rules.xml   0160-vmpop3d_rules.xml      0265-php_rules.xml          0380-redis_rules.xml       0475-bbhttp_rules.xml         0580-win-security_rules.xml  0705-sophos_fw_rules.xml
0050-msexchange_rules.xml 0165-vmpop3d_rules.xml      0270-web_appsec_rules.xml    0385-oscsp_rules.xml       0480-quayguard_rules.xml      0585-win-application_rules.xml  0715-freebox_rules.xml
0025-eset-remote_rules.xml 0165-vpopmail_rules.xml    0275-squid_rules.xml        0390-fortiddos_rules.xml   0485-cylance_rules.xml        0590-win-system_rules.xml   0750-github_rules.xml
0035-courier_rules.xml     0165-vpopmail_rules.xml    0280-attack_rules.xml       0391-fortigate_rules.xml   0490-virustotal_rules.xml     0595-win-sysmon_rules.xml    0755-office365_rules.xml
0035-cloudflare-waf_rules.xml 0170-ftp_rules.xml         0285-systemd_rules.xml      0392-fortimail_rules.xml   0495-proxmox-ve_rules.xml     0600-win-wdefender_rules.xml  0775-arbor_rules.xml
0065-pix_rules.xml        0175-proftpd_rules.xml     0290-firewall_rules.xml     0393-fortimail_rules.xml   0500-owncloud_rules.xml      0601-win-vipre_rules.xml    0775-secure_rules.xml
0045-sysmon_id_10.xml     0180-macos_rules.xml        0295-mysql_rules.xml        0395-hp_rules.xml          0505-vols_rules.xml          0602-win-wfirewall_rules.xml  0780-fireeye_rules.xml
0070-netscreenfw_rules.xml 0185-vstftpd_rules.xml     0300-postgresql_rules.xml   0400-openvpn_rules.xml     0510-ciscat_rules.xml        0605-win-mcafee_rules.xml    0785-huawei-usg_rules.xml
0055-sysmon_id_20.xml     0190-macos_rules.xml        0305-dropbear_rules.xml     0405-rsa-auth-manager_rules.xml  0515-exim_rules.xml         0610-win-ms_logs_rules.xml    0800-sysmon_id_1.xml
0060-macos_rules.xml      0195-vstftpd_rules.xml     0310-openssh_rules.xml      0410-imperva_rules.xml     0520-vulnerability-detector_rules.xml  0615-win-mc-se_rules.xml    0810-sysmon_id_3.xml
0080-somocall_rules.xml   0200-vpn_concentrator_rules.xml 0315-apparmor_rules.xml     0415-sophos_rules.xml       0525-openvas_rules.xml       0620-win-generid_rules.xml    0820-sysmon_id_7.xml
sh-5.2#
```

3. Como Funciona na Prática

Criação de Arquivos de Regras

Cada arquivo .xml contém blocos <group> com <rule>. Você pode definir <match>, <field name="...">, <if_sid> e outras condições para detectar e correlacionar eventos.

Exemplo Simplificado:

```
<group name="login_failures">
<!-- Regra genérica: Falha de Login -->
<rule id="100000" level="5">
<match>Login failed</match>
<description>Falha genérica de login</description>
</rule>

<!-- Regra específica: Falha de Login do Admin, substitui a genérica -->
<rule id="100001" level="10">
<if_sid>100000</if_sid>
<match>administrator</match>
<replace>>true</replace>
<description>Falha de login do usuário administrator (crítica)</description>
</rule>
</group>
```

Primeiro, a regra 100000 reconhece “Login failed” e gera um alerta de nível 5. Depois, se o mesmo evento contiver “administrator”, a regra 100001 dispara (encadeada em 100000) e substitui (<replace>true</replace>) a anterior, elevando o nível para 10 e mudando a descrição.

Por que Enumerar Arquivos

Se você tivesse um arquivo “0010-windows_rules.xml” com regras genéricas de Windows e um “9999-custom_rules.xml” com regras específicas, o arquivo “9999-custom_rules.xml” será carregado por último.

Caso haja override de um rule id ou definições complementares, o seu arquivo customizado tem precedência na configuração final do manager.

XDR - Endpoint Groups - View details

Nesta página, são mostrados detalhes do grupo de agentes e arquivos.

< default

Manage agentsExport PDF

AgentsFiles

Agents (24)
From here you can list and manage your agents

RefreshExport formatted

Em **Export PDF** ([Export PDF](#)), você pode exportar um PDF com as configurações e/ou os agentes do grupo.

Em **Manage agents**, você pode adicionar ou remover agentes do grupo.

Blockbit

Endpoint Groups

a

< Manage agents of group Site-SP

Apply changes

Available agents

Filter...

389 - BLKBT-N-026
391 - LT-8WPT6R3
393 - BLKBT-N-111
394 - BLKBT-N-041
395 - BLKBT-N-002
396 - BLKBT-N-047
397 - BLKBT-N-066
398 - BLKBT-N-059
399 - BLKBT-N-100
400 - BLKBT-N-156
401 - BLKBT-N-094
402 - BLKBT-N-081
403 - BLKBT-N-018
404 - XDR_POC_Linux
405 - thcosta

Click here to load more agents

Add all items

Add selected items

Remove selected items

Remove all items

Current agents in the group (0)

Added: 2Removed: 0

Filter...

392 - BLKBT-N-105
390 - KAIO

Para adicionar ou remover agentes, utilize os botões entre as listas.

Para aplicar as mudanças, clique em **Apply changes** ([Apply changes](#)).

Nos grupos, há duas abas: Agents (Agentes) e Files (Arquivos)

AgentsFiles

Agents (24)
From here you can list and manage your agents

RefreshExport formatted

Search

DQL

Id ↑	Name	IP address	Operating system	Version	Status	Actions
------	------	------------	------------------	---------	--------	---------

Agents

< Brasilia

Manage agents

Export PDF

Agents

Files

Agents (4)

Refresh

Export formatted

From here you can list and manage your agents

Search

DQL

Id ↑	Name	IP address	Operating system	Version	Status	Actions
391	LT-8WPT6R3	192.168.1.10	 Microsoft Windows 11 Pro 10.0.22000.2538	v1.0.0	● active ⓘ	 
392	BLKBT-N-105	192.168.1.11	 Microsoft Windows 11 Pro 10.0.22631.5039	v1.0.0	● active ⓘ	 
393	BLKBT-N-111	192.168.1.12	 Microsoft Windows 11 Pro 10.0.26100.3194	v1.0.0	● disconnected ⓘ	 
394	BLKBT-N-041	192.168.1.13	 Microsoft Windows 11 Pro 10.0.22000.2538	v1.0.0	● active ⓘ	 

Rows per page: 15

< 1 >

Para cada agente, há as seguintes características.

O **Id** é o número identificador do agente.

Name é o nome do agente.

IP address é o endereço IP do agente.

Operating system é o sistema operacional do agente.

Version é a versão do agente.

Status é o status do agente. São dois status: ativo (**active**) e desconectado (**disconnected**).

Actions: ações sobre o agente:

Ir ao agente (**Go to the agent**): Abrirá as informações do agente no [Endpoint Summary](#).

Files

<

Brasilia

Edit group configuration

Export PDF

Agents

Files

Files (3)

Refresh

Export formatted

From here you can list and see your group files, also, you can edit the group configuration

Search

DQL

File ↑	Checksum	Actions
agent.conf	ab73af41699f13fdd81903b5f23d8d00	
ar.conf	c94cce6423fc68adb537890d6f14fbb8	
merged.mg	150e727c3ce8f3b83b575d45d4eaece8	

Rows per page: 15

<

1

>

Para cada arquivo, há as seguintes características:

Name é o nome do arquivo.

Checksum é o código de verificação do arquivo.

São duas ações por arquivo:

Ver arquivo (**See file content**): abrirá o conteúdo do arquivo.

Editar arquivo (**Edit**): abrirá um editor permitindo personalizar as configurações, regras e exceções dos endpoints pertencentes a esse Grupo ou Sub-grupo.

< agent.conf of Brasília group

Save

1 <agent_config>

2 <!-- Shared agent configuration here -->

3 </agent_config>

XDR - Endpoints Groups - Active Response

O Active Response do Blockbit XDR é um mecanismo automatizado de resposta a incidentes, projetado para mitigar ameaças em tempo real, aplicando ações de contenção e remediação de forma rápida e eficiente. Essa funcionalidade faz parte da abordagem SOAR (Security Orchestration, Automation and Response), permitindo a orquestração inteligente das respostas a eventos de segurança. As ações de remediação podem ser aplicadas simultaneamente em múltiplos sistemas e eventos reduzindo o tempo de reação e minimizando impactos operacionais.

Através do uso de Playbooks, o Active Response executa fluxos de automação predefinidos, garantindo que, ao detectar uma ameaça, o sistema possa bloquear, isolar, ou neutralizar automaticamente atividades maliciosas. Esses Playbooks podem ser personalizados para atender às necessidades específicas da organização, possibilitando desde o isolamento de endpoints até a revogação de credenciais comprometidas.

Com o Active Response, o Blockbit XDR transforma dados de ameaças em ações automatizadas, garantindo um ambiente mais seguro e resiliente contra ataques cibernéticos.

Abaixo seguem alguns dos exemplos que o Blockbit XDR possui:

Active Response / EXE	Regras associadas (rules_id)	Função resumida
notification_remove-threat (usa notification.exe + remove-threat.exe)	87105	Exibe uma notificação (notification.exe) e, em seguida, remove (ou coloca em quarentena) o arquivo malicioso do endpoint (remove-threat.exe).
remove-threat (remove-threat.exe)	87105	Efetua a remoção/quarentena do arquivo malicioso no endpoint.
firewall-drop (geralmente usa firewall_manager.exe ou network_block.exe)	2502, 5710	Bloqueia ou “dropa” conexões (por IP ou host) no firewall do sistema. Em Windows, pode usar “netsh.exe” em segundo plano.
rollback_windows (chama rollback.bat ou rollback.ps1)	100628	Reverte alterações feitas previamente (ex.: regras do firewall, remoção de arquivo), restaurando o estado anterior do endpoint.
notification_network_block (usa notification.exe + network_block.exe)	100628, 100616, 100200, 100904, 100063, 100238, 100194, 100915	Exibe uma notificação ao usuário/administrador e simultaneamente executa bloqueio de rede no endpoint (por IP, host, etc.).
network_block (network_block.exe)	100628, 100616, 100200, 100904, 100063, 100238, 100194, 100915	Bloqueia o tráfego de rede (por IP, URL) localmente no endpoint. Em algumas instalações, pode usar scripts auxiliares, como netsh.exe.
notification_win_security (usa notification.exe + windows_security.exe)	501, 503, 62152	Exibe alerta/aviso e aplica ajustes ou reforços de segurança no Windows (por exemplo, ativar políticas ou checar integridade do sistema).
windows_security (windows_security.exe)	501, 503, 62152	Realiza ações específicas de segurança no Windows (por ex., reforço de GPO, ativação de defesas, etc.).
yara_windows (normalmente chama yara.bat)	100303, 100304	Roda um scan YARA local no Windows para identificar padrões de malware ou IOCs (Indicators of Compromise).
yara_linux (equivalente em Linux)	100300, 100301	Versão de varredura YARA para sistemas Linux.
notification (notification.exe)	100508	Simplesmente gera uma notificação pop-up ou log local, avisando sobre o alerta disparado (sem tomar ações adicionais).
ensure_policies	111000, 111001	Em geral, chama binários de “endpoint_control” ou gerenciadores específicos (bluetooth_manager.exe, usb_manager.exe) para checar/aplicar políticas de hardware ou segurança.
bluetooth_manager.exe (dentro de endpoint_control)	N/D (varia)	Gerencia/desabilita conexões Bluetooth de acordo com regras de segurança ou políticas definidas.
firewall_manager.exe (dentro de endpoint_control)	N/D (varia)	Manipula as regras de firewall no endpoint; pode ser acionado pelos ARs “firewall-drop” ou “network_block”.
usb_manager.exe (dentro	N/D (varia)	Gerencia/desabilita dispositivos USB (armazenamento, Bluetooth dongles USB,

de endpoint_control)		etc.) conforme as políticas definidas.
endpoint_control.exe	N/D (varia)	Aplicativo genérico para executar funções de controle de endpoint; pode ser acionado para checar várias políticas (rede, USB, Bluetooth).
logger.exe	N/D	Ferramenta interna para gravação de logs adicionais relacionados às Active Responses ou à execução dos binários.
netsh.exe (nativo Windows)	N/D	Ferramenta padrão do Windows para manipular configurações de rede e firewall; pode ser usada “por trás” dos binários que fazem bloqueio.
notify_screen.exe	N/D	Similar ao notification.exe, porém gera uma interface de pop-up na tela do usuário, exibindo mensagens de alerta.
restart-bbxdr.exe	N/D	Reinicia o serviço/cliente do Blockbit XDR no endpoint (útil quando é necessário forçar recarregamento de configurações).
windows_defender.exe	N/D	Invoca o Microsoft Defender (em máquinas Windows) para realizar varreduras, atualizações ou ações de remoção.
route-null.exe	N/D	Possível ferramenta interna para inserir rotas nulas (bloqueio de roteamento) no sistema, função avançada de bloqueio de IP/tráfego.

O **SOAR** (Security Orchestration, Automation and Response) e o **Active Response** do Blockbit XDR estão em constante evolução para garantir a máxima segurança dos endpoints, acompanhando as mudanças no cenário de ameaças cibernéticas.

Além das respostas automatizadas nativas, é possível criar Playbooks personalizados, adaptando as ações de mitigação e remediação para atender às necessidades específicas de cada ambiente. Essa flexibilidade permite configurar respostas customizadas para diferentes sites, unidades organizacionais, grupos de endpoints e dispositivos individuais, garantindo uma orquestração inteligente e eficiente da segurança.

Com essa abordagem, o Blockbit XDR assegura que incidentes sejam tratados de maneira automatizada e contextualizada, reduzindo tempo de resposta e impactos operacionais.

XDR - Users

O Blockbit XDR permite definir quem vai acessar o que. Em Security, você pode criar usuários, definir papéis e dar ou retirar permissões.

Para criar e administrar papéis, vá em [Roles](#);

Para criar e administrar usuários, vá em [Users](#);

Para criar e administrar permissões, vá em [Permissions](#);

Para administrar a autenticação de fatores múltiplos, vá em [Multi Factor Authentication](#);

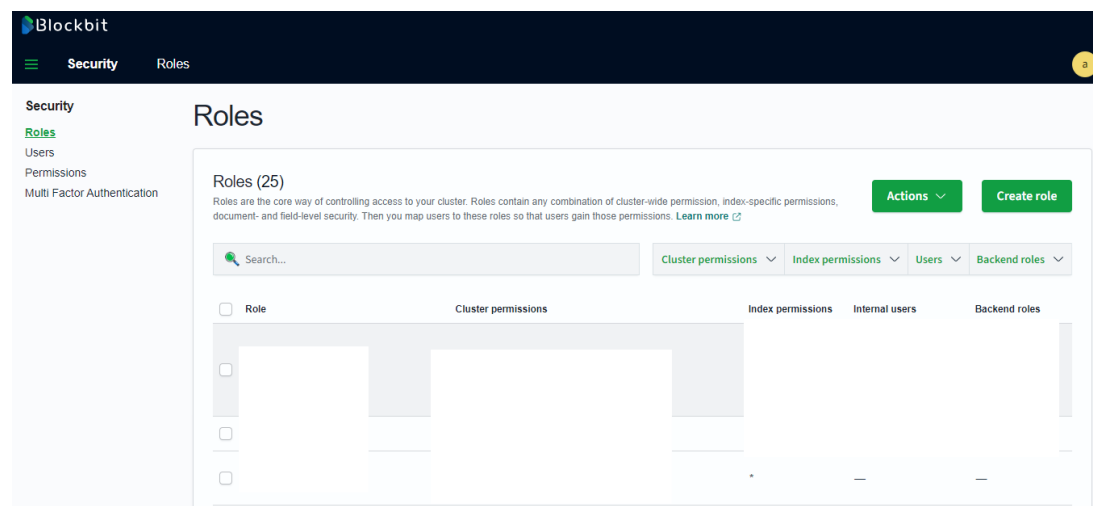
XDR - Security - Roles

Para determinar o que um usuário acessa e pode fazer, você pode criar papéis em Roles. Esses papéis são definidos pelas permissões dadas.

O **Blockbit XDR** oferece suporte à autenticação via **LDAP** e **SAML (versão 2.0 ou superiores)**, permitindo integração com diretórios corporativos e autenticação única (SSO). A solução possibilita a sincronização de usuários, grupos, unidades organizacionais, domínios e florestas, garantindo um gerenciamento centralizado, seguro e eficiente, facilitando a administração e o controle de acessos na organização.

- **LDAP:** Permite autenticação centralizada via servidores como Active Directory;
- **SAML:** Oferece autenticação única (SSO), permitindo que usuários acessem múltiplos sistemas sem precisar inserir credenciais.

As integrações são feitas pela **API do XDR**. Para integrar, entre em contato com a [equipe Blockbit](#).



Os papéis são classificados por:

Role: nome do papel;

Cluster permissions: permissões de acesso a recursos do cluster;

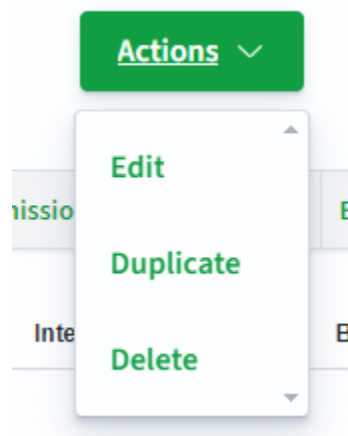
Index permissions: permissões de acesso aos recursos do index;

Internal users: usuário com acesso aos clusters e indexes;

Backend role: grupo de permissões padrão de um usuário.

Você pode buscar por uma regra específica em **Search**. Você pode refinar a busca selecionando permissões, usuários e papéis.

No botão **Actions**, são apresentadas as seguintes opções:



Edit: editar regra. Esta opção é habilitada quando uma regra é selecionada.

Duplicate: duplicar regra. Esta opção é habilitada quando uma regra é selecionada.

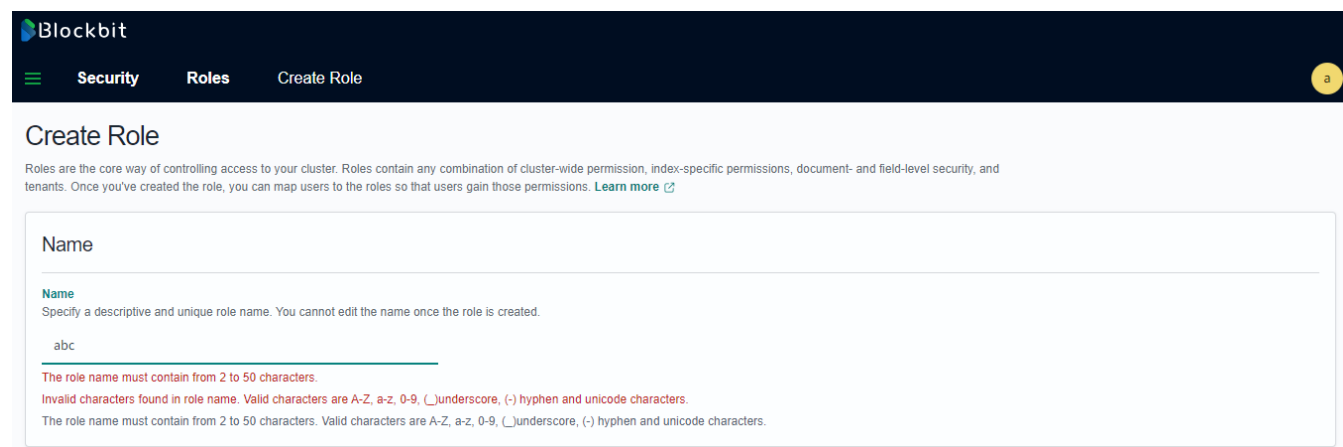
Delete: deletar regra. Você pode deletar mais de uma regra.

Para criar uma regra, clique em [Create role](#).

XDR - Security - Create role

Neste artigo, a **Role** é referida como **Papel**.

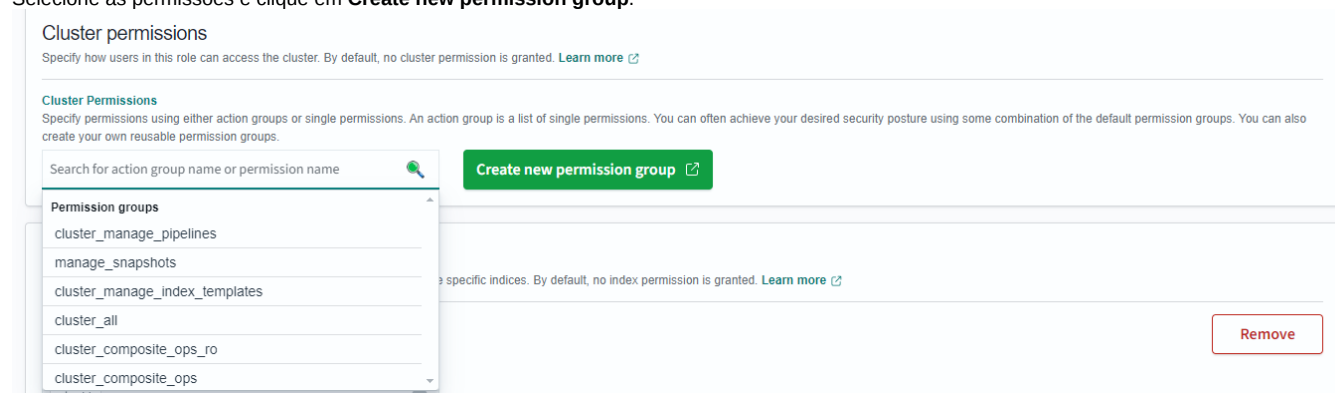
Para criar um papel, primeiro dê um nome.



The screenshot shows the 'Create Role' page in the Blockbit interface. The page has a dark blue header with the 'Blockbit' logo and navigation links for 'Security', 'Roles', and 'Create Role'. A yellow profile icon is in the top right. The main content area is titled 'Create Role' and includes a sub-header explaining that roles control access to the cluster. Below this is a form for creating a role, with a 'Name' field. The 'Name' field has a label 'Name' and a description: 'Specify a descriptive and unique role name. You cannot edit the name once the role is created.' The field contains the text 'abc'. Below the field, there are two error messages: 'The role name must contain from 2 to 50 characters.' and 'Invalid characters found in role name. Valid characters are A-Z, a-z, 0-9, (_) underscore, (-) hyphen and unicode characters. The role name must contain from 2 to 50 characters. Valid characters are A-Z, a-z, 0-9, (_) underscore, (-) hyphen and unicode characters.'

Depois, determine quais permissões este papel vai ter ao acessar o cluster.

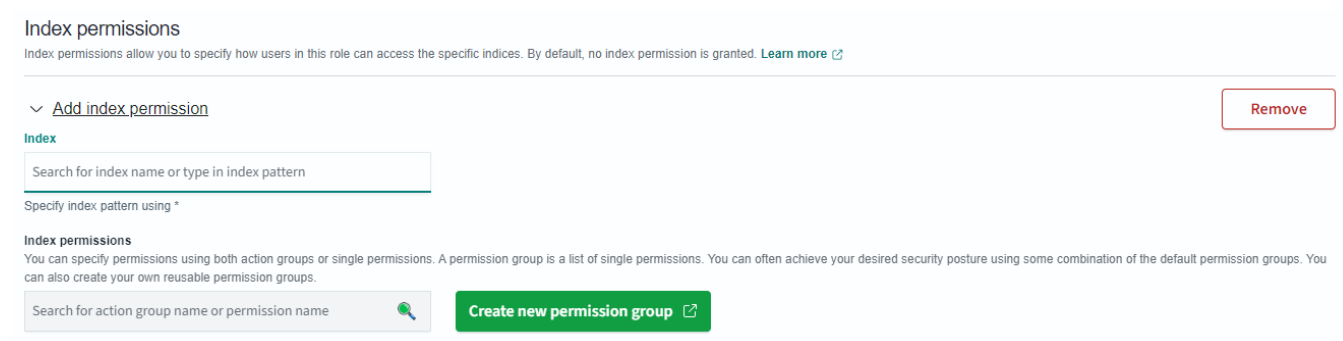
Selecione as permissões e clique em **Create new permission group**.



The screenshot shows the 'Cluster permissions' section in the Blockbit interface. It has a sub-header 'Cluster permissions' and a description: 'Specify how users in this role can access the cluster. By default, no cluster permission is granted. Learn more'. Below this is a 'Cluster Permissions' section with a description: 'Specify permissions using either action groups or single permissions. An action group is a list of single permissions. You can often achieve your desired security posture using some combination of the default permission groups. You can also create your own reusable permission groups.' There is a search bar for 'Search for action group name or permission name' and a green button labeled 'Create new permission group'. A dropdown menu is open, showing a list of 'Permission groups': 'cluster_manage_pipelines', 'manage_snapshots', 'cluster_manage_index_templates', 'cluster_all', 'cluster_composite_ops_ro', and 'cluster_composite_ops'. To the right of the dropdown, there is a 'Remove' button.

Depois, determine quais as permissões este papel vai ter ao acessar os **Indexes**:

Selecione os **indexes**.



The screenshot shows the 'Index permissions' section in the Blockbit interface. It has a sub-header 'Index permissions' and a description: 'Index permissions allow you to specify how users in this role can access the specific indices. By default, no index permission is granted. Learn more'. Below this is a section for 'Add index permission' with a 'Remove' button. There is a search bar for 'Search for index name or type in index pattern' and a description: 'Specify index pattern using *'. Below this is an 'Index permissions' section with a description: 'You can specify permissions using both action groups or single permissions. A permission group is a list of single permissions. You can often achieve your desired security posture using some combination of the default permission groups. You can also create your own reusable permission groups.' There is a search bar for 'Search for action group name or permission name' and a green button labeled 'Create new permission group'.

Depois, especifique permissões dentro deles

Can also create your own reusable permission groups.

get X crud X manage_data_streams X

Permission groups

- data_access
- delete
- manage_aliases
- search
- write
- indices_all

Create new permission group

Você também pode restringir o acesso a certos documentos do **Index** em **Document level security**.

Para isso, você precisa estruturar uma query em DSL (Domain-specific Language).

Exemplo:

```
{
  "bool": {
    "must": {
      "match": {
        "genres": "Comedy"
      }
    }
  }
}
```

Em **Field level security**, você pode restringir o acesso a certos campos de documentos.

Digite o nome do campo e selecione **Include**, para incluir entre os campos restritos, ou **Exclude**, para excluir dos campos restritos.

Em **Anonymization**, você pode mascarar certos campos. Basta digitar o nome do campo a ser anonimizado.

Document level security - optional

You can restrict a role to a subset of documents in an index. [Learn more](#)

```
{
  "bool": {
    "must": {
      "match": {
        "genres": "Comedy"
      }
    }
  }
}
```

Field level security - optional

You can restrict what document fields a user can see. If you use field-level security in conjunction with document-level security, make sure you don't restrict access to the field that document-level security uses.

Exclude



Type in field name

Anonymization - optional

Masks any sensitive fields with a random value to protect your data security.

Type in field name

Em **Tenant permission**, você define quais tenants (grupos de usuários que compartilha o acesso com privilégios) tem acesso a certos papéis.

Tenant permissions

Tenants are useful for safely sharing your work with other Blockbit XDR users. You can control which roles have access to a tenant and whether those roles have read and/or write access. [Learn more](#)

Tenant

Search tenant name or add a tenant pattern



global_tenant
admin_tenant

Read and Write



Remove

Em **Tenant**, selecione o tenant.

Ao lado, você pode definir os privilégios do tenant:

Read and write: pode ler e editar informações.

Read only: pode apenas ler informações.

XDR - Security - Users

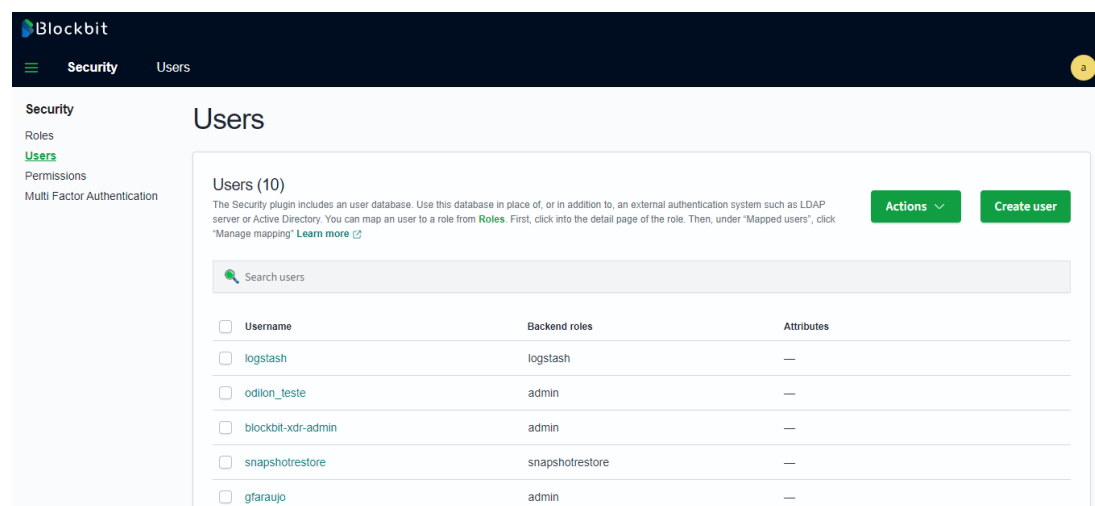
Quem acessa e administra o XDR são os usuários, ou pessoas autenticadas e com permissão para acessar a plataforma.

O **Blockbit XDR** suporta autenticação por **LDAP** e **SAML**, permitindo integração com outros diretórios e autenticação única (SSO), o que garante gerenciamento de acessos prático e seguro.

- **LDAP**: Permite autenticação centralizada via servidores como Active Directory;
- **SAML**: Oferece autenticação única (SSO), permitindo que usuários acessem múltiplos sistemas sem precisar inserir credenciais.

As integrações são feitas pela **API do XDR**. Para integrar, entre em contato com a [equipe Blockbit](#).

Ao clicar em User, você irá para a lista de usuários.



Os usuários são classificados em:

Username: nome do usuário;

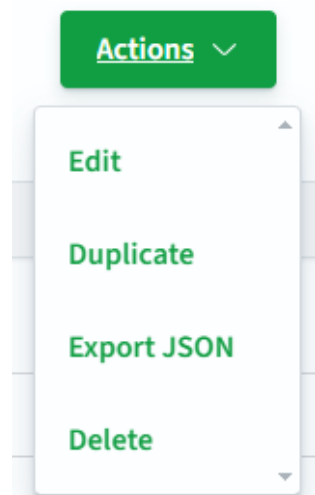
Backend role: grupo de permissões padrão de um usuário;

Attributes: características do usuário.

Você pode selecionar mais de um usuário ao clicar nas caixas.

Você pode buscar por um usuário específico em **Search users**.

No botão **Actions**, são apresentadas as seguintes opções:



Edit: editar usuário. Esta opção é habilitada quando um usuário é selecionado.

Duplicate: duplicar usuário. Esta opção é habilitada quando um usuário é selecionado.

Export JSON: exportar JSON com dados do usuário. Esta opção é habilitada quando um usuário é selecionado.

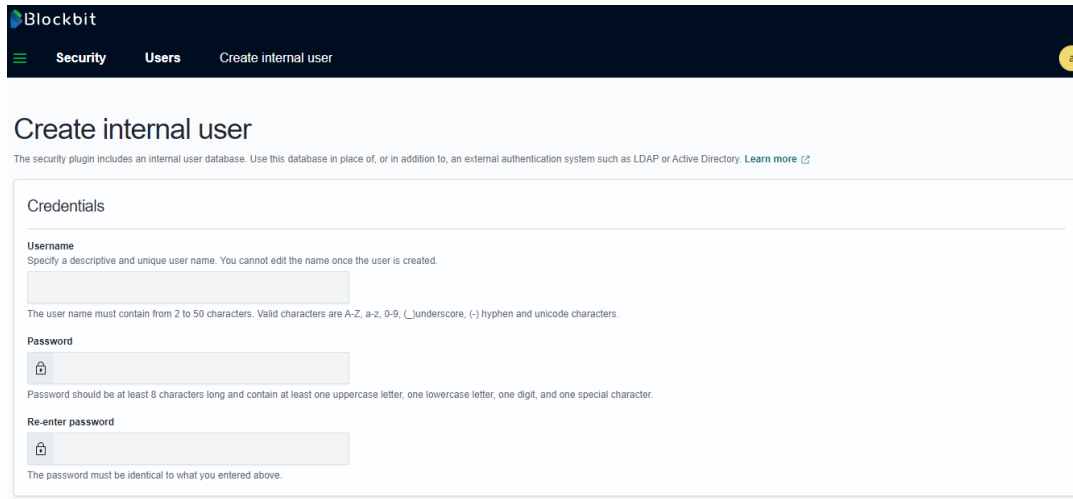
Delete: deletar usuário. Você pode deletar mais de um usuário.

Para criar um usuário, clique em [Create user](#).

XDR - Security - Create User

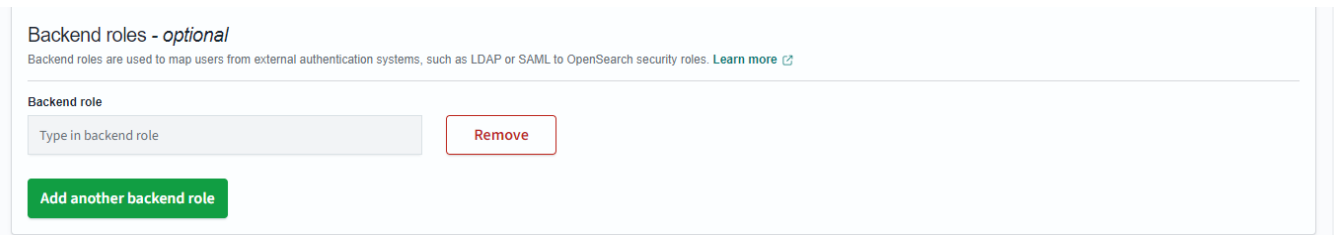
Para editar um usuário, o processo é o mesmo.

Para criar um usuário, primeiro crie um nome e uma senha:



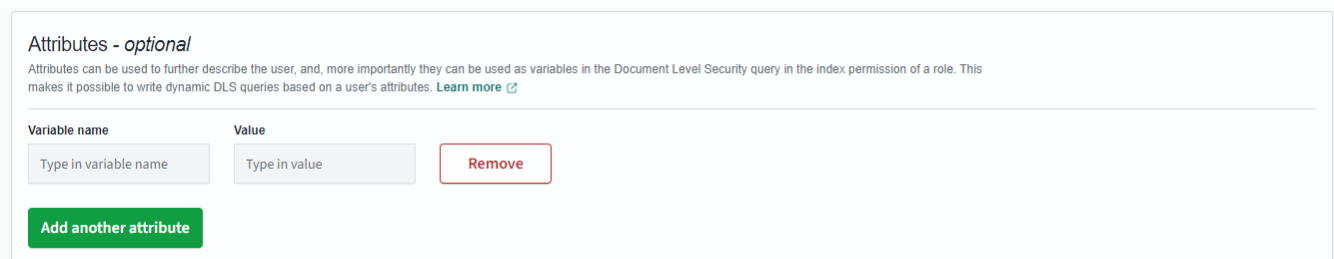
The screenshot shows the 'Create internal user' page in the Blockbit application. The header bar is dark blue with the Blockbit logo and navigation links for 'Security', 'Users', and 'Create internal user'. The main content area is titled 'Create internal user' and includes a sub-header explaining the security plugin's internal user database. Below this, there is a 'Credentials' section with three input fields: 'Username', 'Password', and 'Re-enter password'. Each field has a small lock icon indicating it is a password field. The 'Username' field has a note stating it must be 2 to 50 characters long and contain only valid characters (A-Z, a-z, 0-9, underscore, hyphen, and unicode). The 'Password' field has a note stating it must be at least 8 characters long and contain at least one uppercase letter, one lowercase letter, one digit, and one special character. The 'Re-enter password' field has a note stating it must be identical to the password entered above. A 'Learn more' link is provided for each note.

Depois, defina os papéis:



The screenshot shows the 'Backend roles - optional' section in the Blockbit application. The section title is 'Backend roles - optional' and it includes a sub-header explaining that backend roles are used to map users from external authentication systems. Below this, there is a 'Backend role' section with a text input field labeled 'Type in backend role' and a 'Remove' button. A green button labeled 'Add another backend role' is located below the input field. A 'Learn more' link is provided for the sub-header.

No final, defina os atributos:

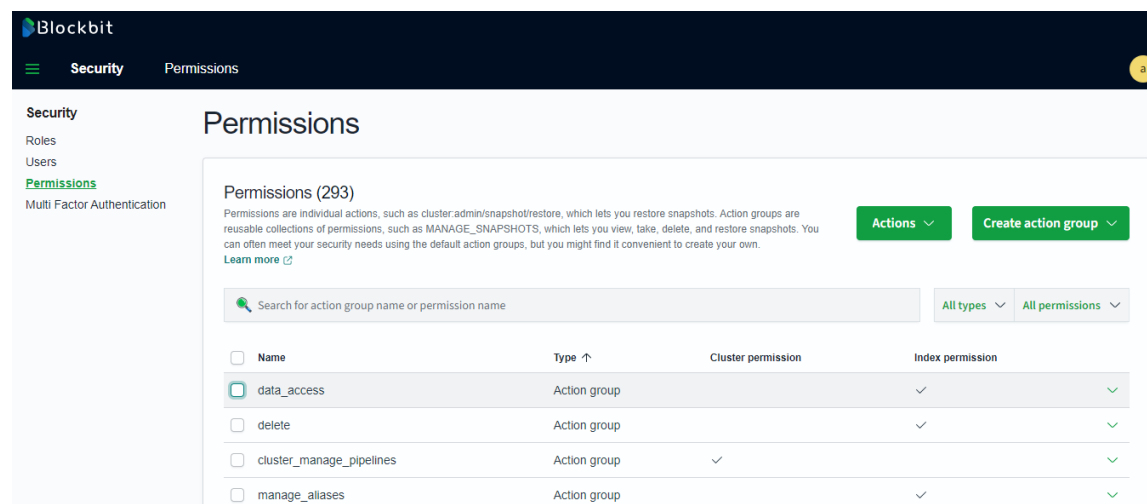


The screenshot shows the 'Attributes - optional' section in the Blockbit application. The section title is 'Attributes - optional' and it includes a sub-header explaining that attributes can be used to further describe the user and can be used as variables in the Document Level Security query. Below this, there is a table with two columns: 'Variable name' and 'Value'. The 'Variable name' column has a text input field labeled 'Type in variable name'. The 'Value' column has a text input field labeled 'Type in value'. A 'Remove' button is located to the right of the 'Value' input field. A green button labeled 'Add another attribute' is located below the input fields. A 'Learn more' link is provided for the sub-header.

Para criar o usuário, clique em **Create**.

XDR - Security - Permissions

Permissões são ações específicas que um usuário é autorizado a tomar.



Blockbit

Security Permissions

Security

Roles

Users

Permissions

Multi Factor Authentication

Permissions

Permissions (293)

Permissions are individual actions, such as cluster.admin/snapshot/restore, which lets you restore snapshots. Action groups are reusable collections of permissions, such as MANAGE_SNAPSHOTS, which lets you view, take, delete, and restore snapshots. You can often meet your security needs using the default action groups, but you might find it convenient to create your own. [Learn more](#)

[Actions](#) [Create action group](#)

Search for action group name or permission name

All types All permissions

☐ Name	Type ↑	Cluster permission	Index permission
☒ data_access	Action group		✓
☐ delete	Action group		✓
☐ cluster_manage_pipelines	Action group	✓	✓
☐ manage_aliases	Action group		✓

As permissões são classificadas por:

Name: nome da permissão;

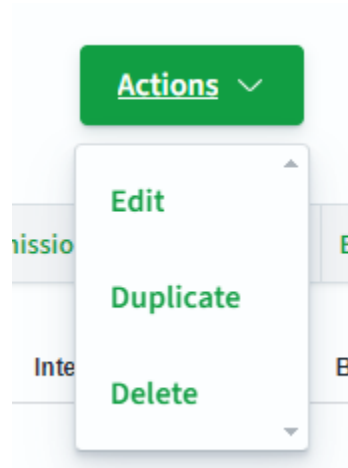
Type: tipo da permissão;

Cluster permissions: permissões de acesso a recursos do cluster;

Index permissions: permissões de acesso aos recursos do index;

Você pode buscar por uma permissão específica em **Search**. Você pode refinar a busca selecionando entre permissões únicas e grupos de ações e permissões de cluster e index.

No botão **Actions**, são apresentadas as seguintes opções:

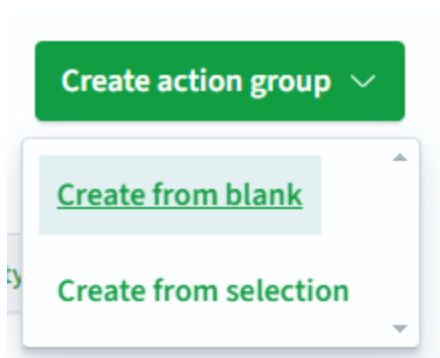


Edit: editar permissão. Esta opção é habilitada quando uma permissão é selecionada.

Duplicate: duplicar permissão. Esta opção é habilitada quando uma permissão é selecionada.

Delete: deletar permissão. Você pode deletar mais de uma permissão.

Para criar uma um grupo de ações, clique em **Create action group**.



Create from blank: criar um grupo de ações e selecionar as permissões manualmente;

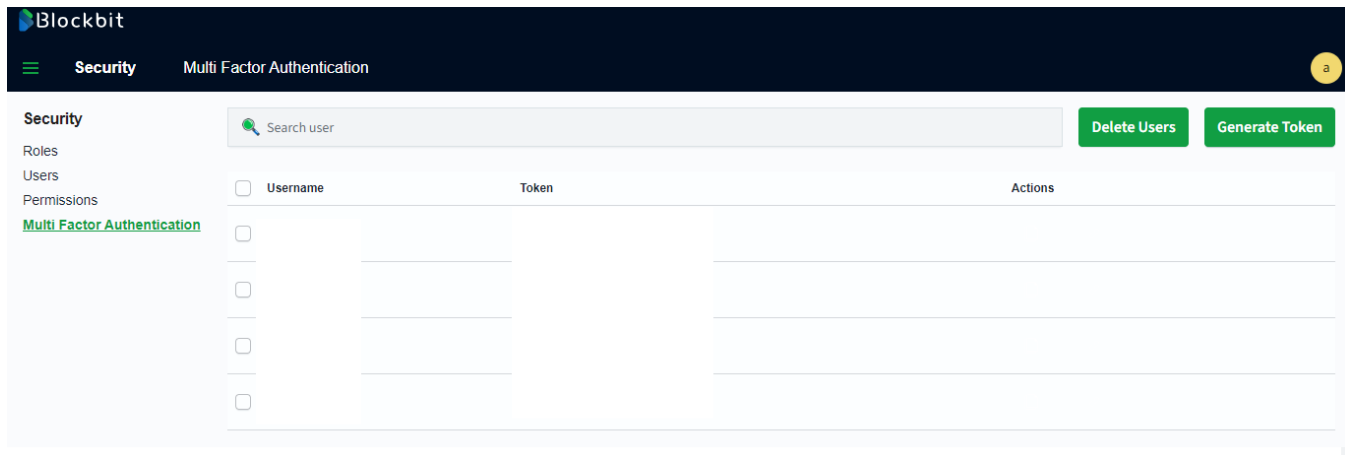
Create from selection: criar um grupo de ações a partir de permissões pré-selecionadas.

A form titled 'Create new action group' with a close button (X) in the top right corner. It has two main sections: 'Name' and 'Permissions'. The 'Name' section has a text input field and a note: 'Enter a unique name to describe the purpose of this group. You cannot change the name after creation. The name must contain from 2 to 50 characters. Valid characters are A-Z, a-z, 0-9, (_) underscore, (-) hyphen and unicode characters.' The 'Permissions' section has a search bar and a list of permissions: 'data_access', 'delete', 'cluster_manage_pipelines', 'manage_aliases', 'crud', 'manage_snapshots', and 'kibana_all_read'. At the bottom right are 'Cancel' and 'Create' buttons.

Para criar um grupo de ações, dê um nome e selecione as permissões.

XDR - Security - Multi Factor Authentication

A autenticação multi fator é uma forma de aumentar a segurança do acesso ao exigir mais de um fator para garantir a identidade de um usuário.

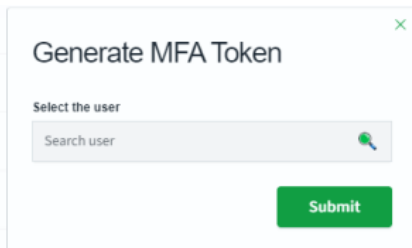


The screenshot shows the Blockbit Security interface for Multi Factor Authentication. The top navigation bar includes the Blockbit logo, a menu icon, and the text 'Security' and 'Multi Factor Authentication'. On the right of the header is a user profile icon labeled 'a'. The left sidebar contains a 'Security' section with links for 'Roles', 'Users', 'Permissions', and 'Multi Factor Authentication' (which is highlighted in green). The main content area features a search bar labeled 'Search user' with a magnifying glass icon. To the right of the search bar are two green buttons: 'Delete Users' and 'Generate Token'. Below these is a table with four columns: 'Username', 'Token', and 'Actions'. The 'Username' column contains a list of five users, each preceded by a checkbox. The 'Token' column is currently empty. The 'Actions' column contains a magnifying glass icon for each row.

No Blockbit XDR, um token aleatório é gerado para o usuário.

Os usuários são listados com os respectivos tokens.

Para gerar o token, clique em **Generate Token**.



The 'Generate MFA Token' modal form has a title bar with a close button (X). Below the title is a section labeled 'Select the user' containing a search bar with the placeholder text 'Search user' and a magnifying glass icon. At the bottom of the modal is a green 'Submit' button.

Selecione um usuário e clique em Submit. Você pode selecionar mais de um usuário.

O token irá para a lista.

Para deletar um ou mais tokens, selecione os usuários e clique em **Delete Users**.

XDR - Indices

No Blockbit XDR, os **Indices** são formas de estruturar documentos numa base de dados para facilitar o acesso.

Ao clicar em Indices, você poderá acessar:

[State Management Policies](#)
[Indices](#)

XDR - Indices - Indices

Indices são tabelas de dados que armazenam e organizam documentos.
Documentos são unidades básicas de dados representadas por um JSON e identificados por um ID único dentro de um **índice**.

Esses documentos são armazenados em **shards**, que são hospedados em um data node. Quando você busca um dado no Blockbit XDR, a requisição interage com diversos shards, podendo ser **primários** ou **replicados**.

No Blockbit XDR, você pode administrar os índices na aba **Indices**.

Indices (52)

Refresh

Actions

Create Index

Search

Show data stream indices

Index	Health	Managed b...	Status	Total size	Size of pri...	Total docu...	Deleted do...	Primaries	Replicas
	Yellow	No	Open	389.3mb	389.3mb	18132	0	1	1
	Yellow	No	Open	2mb	2mb	1173	0	1	1
	Yellow	No	Open	1.7mb	1.7mb	1015	0	1	1
	Yellow	No	Open	954kb	954kb	485	0	1	1
	Yellow	No	Open	988.7kb	988.7kb	469	0	1	1
	Yellow	No	Open	829.8kb	829.8kb	386	0	1	1
	Yellow	No	Open	880kb	880kb	492	0	1	1
	Yellow	No	Open	937kb	937kb	542	0	1	1

Para buscar um index específico, utilize a barra de pesquisa (**Search**).

Para mostrar índices em data stream, ou que utilizam dados contínuos, clique em **Show data stream indices**.

Os índices são classificados por:

- Index:** nome do index;
- Health:** saúde do índice. Pode ser Verde (boa), amarela (média) ou vermelha (ruim);
- Status:** estado do index. Pode ser Open (aberto) ou closed (fechado);
- Total size:** tamanho total do index;
- Size of primaries:** tamanho dos shards primários;
- Total documents:** número total de documentos;
- Deleted documents:** número de documentos deletados;
- Primaries:** shards primários;
- Replicas:** shards replicados.

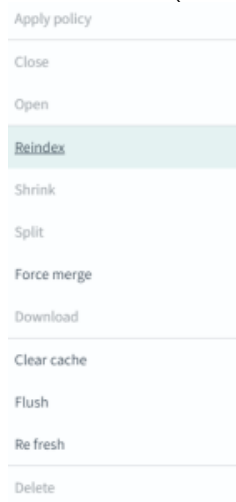
Ao clicar num index, você também poderá configurá-lo.

No botão **Refresh** (

Refresh

), os índices são atualizados;

No botão **Actions** (), são apresentadas as seguintes ações;



Apply policy: aplicar política aos índices selecionados;

Close: fechar os índices selecionados;

Open: abrir os índices selecionados;

Reindex: reindexar os índices selecionados;

Shrink: comprimir os índices selecionados;

Split: dividir os índices selecionados;

Force merge: fundir os índices selecionados;

Download: baixar os índices selecionados;

Clear cache: limpar o cache;

Flush: remover permanentemente;

Refresh: atualizar;

Delete: apagar.

Para criar um index, clique em **Create index** ().

XDR - Indices - Indices - Create index

Para criar um index, primeiro, você define o nome dele.

Define index

Index name

Specify a name for the new index.

Must be in lowercase letters. Cannot begin with underscores or hyphens.
Spaces, commas, and characters :, " , * , + , / , , | , ? , # , > are not allowed.

Index alias - optional

Allow this index to be referenced by existing aliases or specify a new alias.

Select aliases or specify new aliases. 

Em **Index name**, insira o nome do index;

Em **Index alias**, você pode definir um **alias**, ou um grupo de indices.

Index settings

Number of primary shards

Specify the number of primary shards for the index. Default is 1.
The number of primary shards cannot be changed after the index is created.

1

Number of replicas

Specify the number of replicas each primary shard should have. Default is 1.

1

Refresh interval

Specify how often the index should refresh, which publishes the most recent changes and make them available for search. Default is 1 second.

1s

[> Advanced settings](#)

Depois, defina as configurações do index em **Index Settings**.

Determine o número de shards primárias em **Number of primary shards**;

Determine o número de réplicas em **Number of replicas**;

Determine os intervalos de atualização do index em **Refresh interval**.

Em **Advanced settings**, você pode modificar configurações avançadas por meio de um JSON.

✓ Advanced settings

Specify advanced index settings

Specify a comma-delimited list of settings. [View index settings.](#)

All the settings will be handled in flat structure. [Learn more.](#)

```
1 {  
2   "index.number_of_shards": 1,  
3   "index.number_of_replicas": 1,  
4   "index.refresh_interval": "1s"  
5 }
```

Para definir como um documento será armazenado num index, vá em **Index mapping**.

Index mapping – optional

Define how documents and their fields are stored and indexed. [Learn more](#)

Mappings and field types cannot be changed after the index is created.

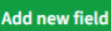
Visual Editor

JSON Editor

You have no field mappings.

Add new field

Add new object

Em **Add new field** () , adicione uma categoria de dados.

Field name

Field type

Actions

text



Dê um nome para a categoria e determine o seu tipo em **Field type**. Para deletar, clique em **Delete** ()

Em **Add new object** () , adicione um objeto JSON.

Field name

Field type

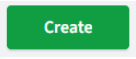
Actions

object



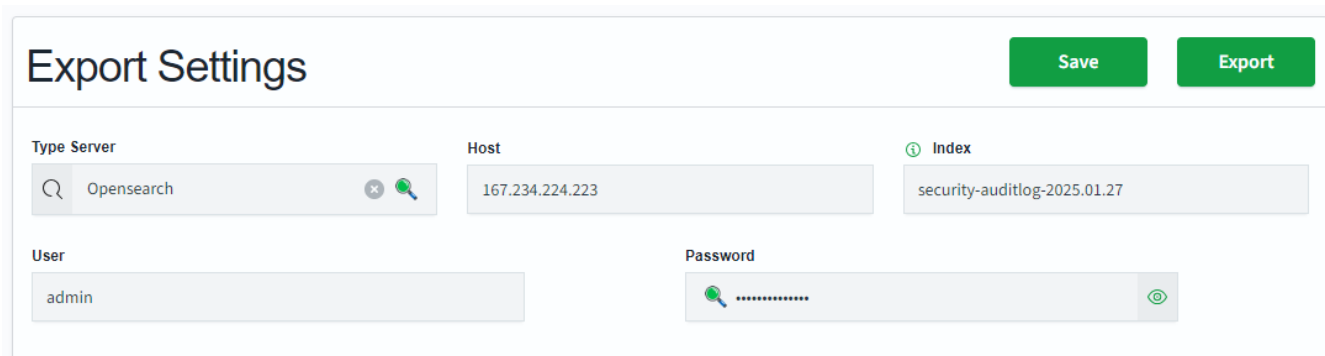
Dê um nome para a categoria e determine o seu tipo em **Field type**. No botão + () , você pode criar uma categoria ou um objeto embutido.

Para deletar, clique em **Delete** () .

Para criar o index, clique em **Create** ().

XDR - Indices - Settings

O Blockbit XDR permite exportar logs de auditoria em formato JSON e/ou Syslog.



The 'Export Settings' form is located at the top of the page. It features a title 'Export Settings' on the left and two green buttons, 'Save' and 'Export', on the right. Below the title, there are four input fields: 'Type Server' with a dropdown menu showing 'Opensearch', 'Host' with the text '167.234.224.223', 'Index' with the text 'security-auditlog-2025.01.27', 'User' with the text 'admin', and 'Password' with a masked password field and an eye icon to toggle visibility.

Type Server: Servidores de logging. São suportados Opensearch (de XDR para XDR) e SysLog (XDR para o SysLog);

Host: IP do host exportado;

Index: índice exportado. Qualquer índice listado pode ser exportado, como de auditoria e eventos.

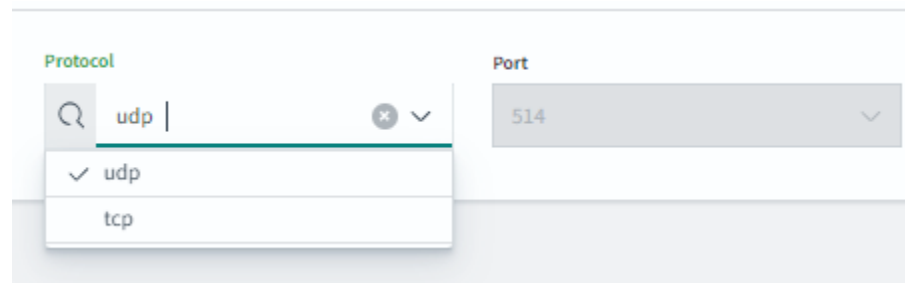
Para exportar uma categoria de índices, utilize um asterisco (*) para selecionar tudo que foi digitado antes dele. (exemplo: **auditlog-2025*** exporta todos os índices de 2025. **auditlog-2025.01*** exporta todos os índices de janeiro de 2025, ou de eventos blockbit-xdr-alerts-1.x-2025.01*);

Quando o servidor é **Opensearch**, o sistema irá pedir as credenciais do administrador.

User: usuário que irá exportar o log;

Password: senha do usuário que irá exportar o log.

Quando o servidor é **SysLog**, o sistema irá pedir para configurar o protocolo de rede.

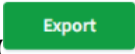


This form section shows the 'Protocol' and 'Port' settings. The 'Protocol' field is a dropdown menu with 'udp' selected, and a search bar above it. The 'Port' field is a dropdown menu with '514' selected. The 'Protocol' dropdown is open, showing 'udp' and 'tcp' options.

Protocol: protocolo de rede. São suportados **UDP** (porta 514) e **TCP** (porta 601).

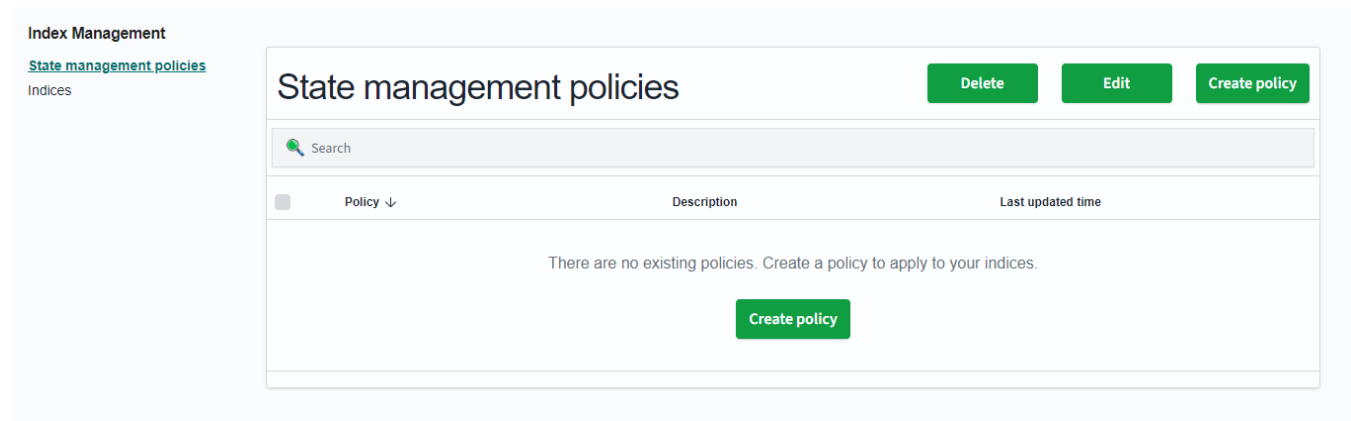
Port: porta.

Para salvar, aperte **Save** ().

Para exportar, aperte **Export** ().

XDR - Indices - State Management Policies

Em **State Management Policies**, você pode criar políticas para gerenciar índices.



Ao clicar, você verá uma lista de políticas. Elas são classificadas por:

Policy: nome da política;

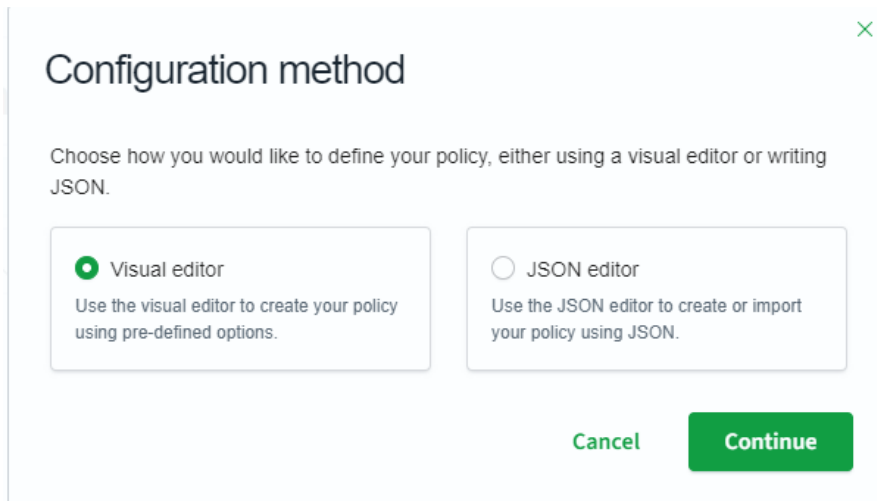
Description: descrição da política;

Last updated time: horário da última atualização da política.

Para buscar uma política específica, use a barra de busca (**Search**).

Para editar uma política, clique em **Edit**.

Para criar uma política, clique em **Create policy**.



Há duas formas:

Visual editor: utilize o editor do Blockbit XDR para criar políticas;

JSON editor: crie ou importe um arquivo JSON com a política.

XDR - Indices - State Management Policies - JSON editor

Ao selecionar o JSON editor, você irá para esta página:

Create policy

Name policy

Policies let you automatically perform administrative operations on indices.

Policy ID

example_policy

Specify a unique ID that is easy to recognize and remember.

Define policy

Copy

Auto indent

You can think of policies as state machines. "Actions" are the operations ISM performs when an index is in a certain state. "Transitions" define when to move from one state to another. [Learn more](#)

1 {
2
3 "policy": {
4 "description": "A simple default policy that changes the replica count between hot and cold states.",
5 "default_state": "example_hot_state",
6 "states": [
7 {

Para criar uma política, primeiro dê um nome em **Policy ID**.

Depois, em **Define policy**, você pode criar ou colar um JSON com as definições da política.

Clique em **Copy** para copiar o JSON.

Clique em **Auto indent** para indentar automaticamente o JSON.

127

XDR - Indices - State Management Policies - Visual editor

Ao selecionar o Visual editor, você irá para esta página:

Create policy

Policies let you automatically perform administrative operations on indices. [Learn more](#)

Policy info

Policy ID

Specify a unique and descriptive ID that is easy to recognize and remember.

hot_cold_workflow

Description

Describe the policy.

A sample description of the policy

Para criar uma política, primeiro dê um nome em **Policy ID**.

Você pode adicionar uma descrição em **Description**.

Error notification – optional

You can set up an error notification for when a policy execution fails. [Learn more](#)

Channel ID

Manage channels

Em Error notification, você pode gerenciar as notificações de erro

Insira o canal onde a notificação será apresentada em **Channel ID**.

Em **Manage Channels**, você pode criar canais.

Em **ISM templates**, você pode inserir templates para automatizar algumas operações, como mudar o estado de uma política após certo tempo.

ISM templates – optional

Specify ISM template patterns that match the index to apply the policy. [Learn more](#)

No ISM templates

Your policy currently has no ISM templates defined. Add ISM templates to automatically apply the policy to indices created in the future.

Add template

Para adicionar um template, clique em **Add template**.

Index patterns

Add index patterns

Priority

1

Remove

Add template

Insira o Index pattern (ID de referência do índice) e defina a prioridade. Depois, clique em Add template. Para deletar, clique em Remove.

128

Em **States**, você pode determinar os estados que cada **índice** irá passar. Em cada estado, o ISM template irá realizar ações específicas.

States (0)

You can think of policies as state machines. "Actions" are the operations ISM performs when an index is in a certain state. "Transitions" define when to move from one state to another. [Learn more](#) 

Initial state 

No states

Your policy currently has no states defined. Add states to manage your index lifecycle.

[Add state](#)

Em **Initial state**, você pode buscar por um estado inicial.

Para criar um estado, clique em **Add state**.

Create state: aaa

State name

aaa

Order

Add after 



Nomeie o estado em **State name**.

Em **Order**, você define a aplicação do estado entre outros estados.

Clique em **Add action** para adicionar uma ação.

Actions

Actions are the operations ISM performs when an index is in a certain state.

No actions have been added.

[+ Add action](#)

Para criar uma ação, defina o tipo:

Add action

Actions are the operations ISM performs when an index is in a certain state. [Learn more](#)

Action type

Select the action you want to add to this state.

Clique em **Add transition** para definir as condições de mudança de estado.

Transitions

Transitions define the conditions that need to be met for a state to change. After all actions in the current state are completed, the policy starts checking the conditions for transitions.

No transitions have been added.

+ Add Transition

Para adicionar uma transição, defina o estado anterior e as condições:

Add transition

Transitions define the conditions that need to be met for a state to change. After all actions in the current state are completed, the policy starts checking the conditions for transitions. [Learn more](#)

Destination state

If entering a state that does not exist yet then you must create it before creating the policy.

Condition

Specify the condition needed to be met to transition to the destination state.

No Condition

XDR - Audit

O Blockbit XDR permite gerar logs de auditoria, que rastreiam acessos ao cluster

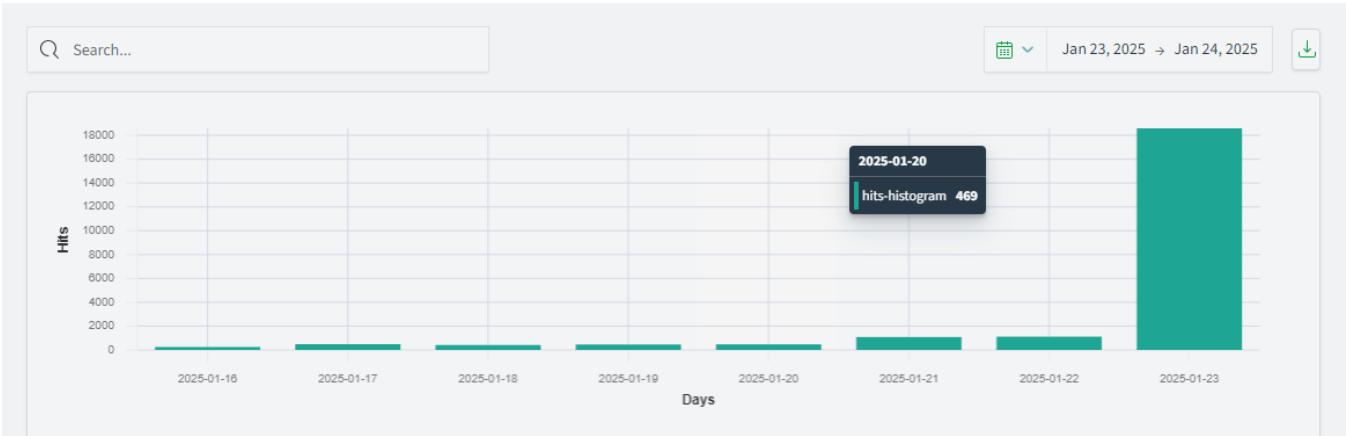
Ao clicar em Audit, você poderá acessar:

[Overview](#)

[Settings](#)

XDR - Audit - Overview

O gráfico mostra o número de logs de auditoria por dia.
Para mais informações, passe o mouse sobre as barras.



Para pesquisar, use a barra de busca.
Para definir o intervalo, use o calendário. Mais informações em [sistema de buscas](#).

Para baixar um arquivo CSV com os logs de auditoria, use o botão de download ().

Abaixo do gráfico, há uma lista de logs gerados.

Columns Density Full screen

Timestamp	Audit cat...	Audit clu...	Audit for...	Audit no...	Audit no...	Audit no...	Audit req...	Audit req...	Audit req...	Audit req...
2025-01-23T...		blockbit-xdr	4					admin	TRANSPORT	REST
2025-01-23T...		blockbit-xdr	4							REST
2025-01-23T...		blockbit-xdr	4							REST
2025-01-23T...		blockbit-xdr	4							REST
2025-01-23T...		blockbit-xdr	4						TRANSPORT	REST
2025-01-23T...		blockbit-xdr	4						TRANSPORT	REST
2025-01-23T...		blockbit-xdr	4							REST
2025-01-23T...		blockbit-xdr	4							REST
2025-01-23T...		blockbit-xdr	4							REST
2025-01-23T...		blockbit-xdr	4							REST
2025-01-23T...		blockbit-xdr	4							REST

Rows per page: 10 < 1 2 3 4 5 ... 15 >

O botão **columns** permite definir quais categorias serão mostradas.

☒ @timestamp	=
☒ audit_category	=
☒ audit_cluster_name	=
☒ audit_format_version	=
☒ audit_node_host_address	=
☒ audit_node_host_name	=
☒ audit_node_id	=
☒ audit_request_body	=
☒ audit_request_effective_user	=
☒ audit_request_layer	=
☒ audit_request_origin	=
☒ audit_request_privilege	=
☒ audit_request_remote_address	=
☒ audit_trace_resolved_indices	=
☒ audit_trace_task_id	=
☒ audit_transport_headers	=

Show all
Hide all

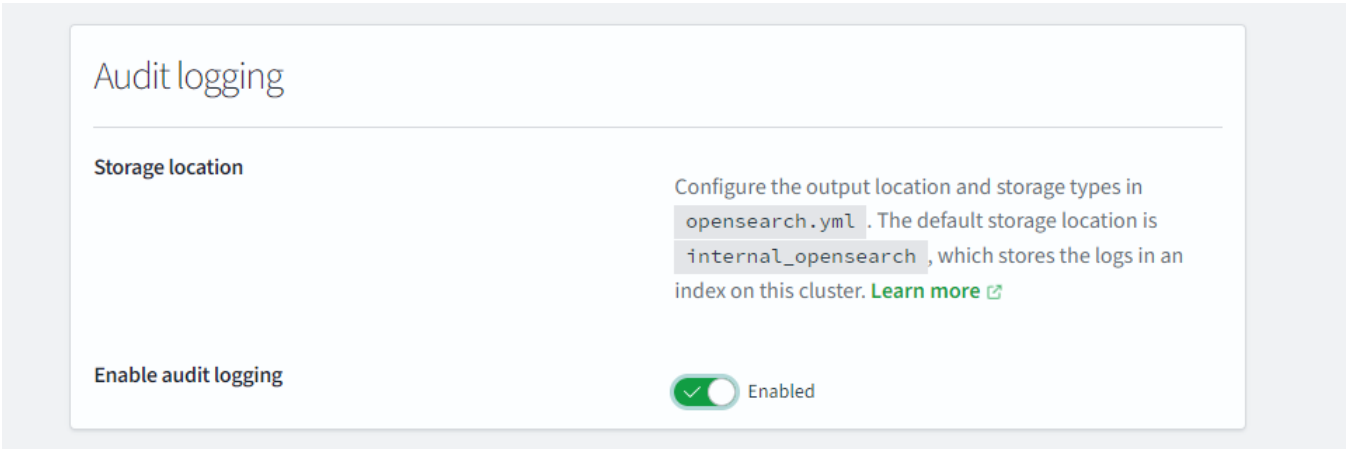
- @timestamp:** data e hora do log;
- audit_category:** categoria do log.
As categorias são: FAILED_LOGIN, MISSING_PRIVILEGES, BAD_HEADERS, SSL_EXCEPTION, OPENSEARCH_SECURITY_INDEX_ATTEMPT, AUTHENTICATED e GRANTED_PRIVILEGES.
- audit_cluster_name:** nome do cluster auditado;
- audit_format_version:** a versão do formato da mensagem;
- audit_node_host_address:** o endereço do host do node onde o evento foi gerado;
- audit_node_host_name:** o nome do host do node onde o evento foi gerado;
- audit_node_host_id:** o id do host do node onde o evento foi gerado;
- audit_request_body:** o corpo da requisição HTTP;
- audit_request_effective_user:** qual usuário cuja autenticação falhou;
- audit_request_layer:** a camada que gerou a requisição. pode ser TRANSPORT ou REST;
- audit_request_origin:** a camada de origem da requisição. pode ser TRANSPORT ou REST;
- audit_request_privilege:** o privilégio necessário para a requisição;
- audit_request_remote_address:** o IP que gerou a requisição;
- audit_trace_resolved_indices:** o nome dos índices resolvidos afetados pela requisição;
- audit_trace_task_id:** identificação da requisição;
- audit_transport_headers:** o header da requisição;
- audit_transport_request_type:** o tipo da requisição.

O botão **Density** permite aumentar ou diminuir a densidade da lista;

O botão **Full screen** coloca a lista em tela inteira.

XDR - Audit - Settings

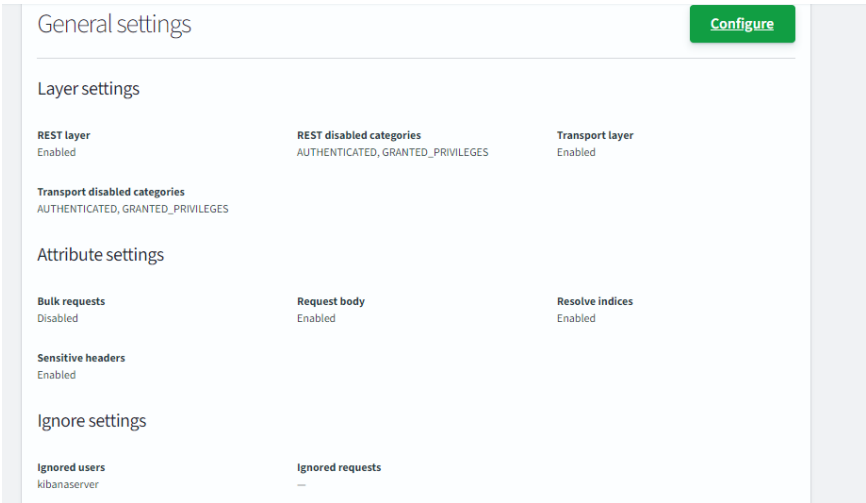
Em Settings, você pode definir as configurações dos logs de auditoria.



Para determinar onde os logs serão armazenados, visite [este site](#).

Habilite os logs de auditoria em **Enable audit logging**.

Em **General settings**, você encontra as configurações gerais. Para defini-las, clique em **Configure** ().



REST layer: habilita a auditoria de eventos na camada REST;

REST disabled categories: defina as categorias que serão ignoradas na camada REST;

Transport layer: habilita a auditoria de eventos na camada Transport;

Transport disabled categories: defina as categorias que serão ignoradas na camada Transport;

Bulk requests: resover requisições em massa na auditoria;

Request body: incluir o corpo da requisição na auditoria.

Resolve indices: resolver indices na auditoria;

Sensitive headers excluir headers sensíveis na auditoria;

Ignored users: usuários a ser ignorados na auditoria;

Ignored requests: padrões em requisições a ser ignorados na auditoria.

Em **Compliance settings**, você encontra configurações de conformidade. Para defini-las, clique em **Configure** ([Configure](#)).

Compliance settings

[Configure](#)

Compliance mode

Compliance logging
Enabled

Config

Internal config logging
Enabled

External config logging
Disabled

Read

Read metadata
Enabled

Ignored users
kibanaserver

Watched fields
--

Write

Write metadata
Enabled

Log diffs
Disabled

Ignored users
kibanaserver

Watch indices
--

Compliance logging: habilitar logs de conformidade;

Internal config logging: habilitar logs de eventos de index de segurança interna;

External config logging: habilitar logs de configuração externa;

Read

Eventos do tipo **Read** são aqueles onde uma requisição **não modifica** um documento.

Read metadata: habilitar logs apenas de metadados de documentos. Ao habilitar esta opção, nenhum campo de documentos será considerado para o log;

Ignored users: usuários a ser ignorados na auditoria;

Watched fields: listar índices e campos a ser observados durante eventos tipo **read**. Ao adicionar um index, será gerado **1 log por documento**.

Write

Eventos do tipo **Write** são aqueles onde uma requisição **modifica** um documento.

Read metadata: habilitar logs apenas de metadados de documentos. Ao habilitar esta opção, nenhum campo de documentos será considerado para o log;

Log diffs: incluir apenas diferenças entre eventos do tipo **write**.

Ignored users: usuários a ser ignorados na auditoria;

Watched indices: listar índices a ser observados durante eventos tipo **write**. Ao adicionar um index, será gerado **1 log por documento**.

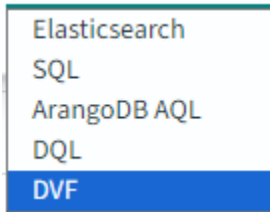
XDR - Quarantine

Arquivos suspeitos são colocados em quarentena pelo Blockbit XDR para evitar danos ao sistema. Na seção Quarantine, você pode checar os arquivos suspeitos e decidir entre permitir a execução, deletá-los ou restaurá-los.

Dashboard			7	
Search			DVF	
Detection ID	Process Name	Status	Actions	
A1}		Quarantined	    	
CA}	exe	Quarantined	    	
3}	exe	Quarantined	    	
C}	.exe	Quarantined	    	

Para ver a lista de arquivos em quarentena, primeiro selecione o agente.

Na barra de pesquisas, você pode buscar por um arquivo específico. À direita da barra, você pode selecionar a linguagem das consultas.



Abaixo, estão listados os processos em quarentena.

Os processos são classificados em:

Detection ID: identificador dado ao arquivo pelo Blockbit XDR;

Process name: nome do arquivo;

Status: status do arquivo. Pode ser **Quarantined** (em quarentena), **Removed** (removido), **Allowed** (permitido na quarentena) ou **Restored** (restaurado no local original);

Para cada arquivo, há 4 ações disponíveis:

View threat details (): abre um modal com detalhes do arquivo. No modal, você pode administrar o arquivo.

Quarantine Details 

```
{
  "AMProductVersion": "4.18.24898.11",
  "ActionSuccess": true,
  "AdditionalActionsBitMask": 0,
  "CimClass": {
    "CimClassMethods": [],
    "CimClassProperties": [
      "ActionSuccess = False",
      "AdditionalActionsBitMask",
      "AMProductVersion = \"\\\"\",
      "CleaningActionID",
      "CurrentThreatExecutionStatusID",
      "DetectionID",
      "DetectionSourceTypeID",
      "DomainUser",
      "InitialDetectionTime",
      "LastThreatStatusChangeTime",
      "ProcessName",
      "ProcessID"
    ]
  }
}
```

 Restore

 Allow

 Remove

Download (): Permite o download seguro do arquivo para o ambiente do administrador, garantindo que sua extração ou análise ocorra sem risco de execução acidental ou comprometimento do sistema. O download será protegido por autenticação e criptografia para evitar manipulações indevidas.

Restore (): Restaura o arquivo para o seu local original, permitindo que seja carregado, acessado e executado no endpoint. Essa ação só deve ser realizada caso o arquivo tenha sido verificado e considerado seguro.

Allow (): Adiciona o arquivo (com base no seu hash) ou o programa à lista de permissões, permitindo que ele seja executado, carregado ou manipulado em futuras tentativas, como em um novo download ou execução pelo usuário.

Remove (): Exclui permanentemente o arquivo da quarentena, impedindo sua restauração ou execução no sistema. Essa ação é irreversível e deve ser utilizada para eliminar arquivos maliciosos com segurança.

XDR - Configuration Assessment

O Configuration Assessment busca vulnerabilidades nas configurações selecionadas pelos agentes na rede.

Policy

CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0

Rows per page: 15 < 1 >

CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0 ⓘ

Passed112

Failed280

Not applicable3

Score28%

End scanMar 18, 2025 @ 08:29:05.000

Checks (395)

Refresh Export formatted

Search

ID ↑	Title	Target	Result
26000	Ensure 'Enforce password history' is set to '24 or more password(s)'.	Command: net.exe accounts	Failed
26001	Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'.	Command: net.exe accounts	Failed
26002	Ensure 'Minimum password age' is set to '1 or more day(s)'.	Command: net.exe accounts	Failed
26003	Ensure 'Minimum password length' is set to '14 or more character(s)'.	Command: net.exe accounts	Failed
26004	Ensure 'Password must meet complexity requirements' is set to 'Enabled'.	Command: powershell Get-ADDefaultDomainPasswordPolicy -Current LoggedOnUser	Failed

Ao clicar em **Export formatted**, será criado um arquivo .csv com informações da checagem.

No começo da tela, são listados os resultados da checagem :

Passed: configurações consideradas satisfatórias;
Failed: Configurações consideradas insatisfatórias;

Not applicable: Configurações que não foram consideradas no escaneamento;

Score: Porcentagem das configurações consideradas satisfatórias;

End scan: Momento do fim do escaneamento.

Você pode conferir a descrição e o checksum do agente ao clicar no informacional.

CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0 ⓘ

Show policy checksum

Passed113

Checks (304)

Policy description:

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows 10 Enterprise.

Policy checksum:

Abaixo, serão apresentadas as checagens individuais com:

ID: identificador da checagem;

Title: Título da checagem;

Target: alvo da checagem;

Result: resultado da checagem.

Ao clicar no resultado, são apresentadas mais informações sobre o teste.

15500
Ensure 'Enforce password history' is set to '24 or...
Command: net.exe accounts
● Failed

Rationale

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Remediation

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies>Password Policy\Enforce password history

Ao clicar em Inventory, você pode conferir a lista de agentes que foram testados.

Policy	Description	End scan	Passed	Failed	Not applicable	Score
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0	This document provides prescriptive guidance f...	Aug 14, 2024 @ 08:10:18.000	113	278	3	28%

Rows per page: 15 < 1 >

- Policy:** Nome do agente;
- Description:** descrição do agente;
- End scan:** Momento do fim do escaneamento.
- Passed:** configurações consideradas satisfatórias;
- Failed:** Configurações consideradas insatisfatórias;
- Not applicable:** Configurações que não foram consideradas no escaneamento;
- Score:** Porcentagem das configurações consideradas satisfatórias.

XDR - Malware Detection

O Blockbit XDR emprega um conjunto robusto de técnicas avançadas para a detecção e mitigação de malwares, garantindo proteção contínua contra ameaças conhecidas e desconhecidas (Zero Day), ataques sem arquivo, ransomware, mineradores, APTs (Advanced Persistent Threats) e movimento lateral.

A solução opera de forma independente, permitindo a detecção e resposta a ameaças mesmo sem conexão com a rede ou o console de administração.

As principais abordagens empregadas incluem:

Monitoramento Contínuo de Endpoints e Servidores:

Identificação de comportamentos suspeitos e atividades anômalas em tempo real, garantindo proteção contra ataques de dia zero. Detecção autônoma de ameaças, mesmo quando o endpoint está offline, sem necessidade de conexão com a nuvem ou com o console de administração.

Análise de Arquivos e Processos:

Uso de regras avançadas de detecção para identificar atividades maliciosas, incluindo malware sem assinatura e explorações em tempo real. Monitoramento e análise comportamental para identificar ataques sem arquivos (fileless malware) e ameaças baseadas em RAM, que escapam de métodos tradicionais de detecção.

Antes de enviar um alerta ao console de administração, o agente examina as informações do processo localmente, avaliando comportamento, assinaturas e características do executável.

Proteção contra-ataques de Dia Zero e Explorações Avançadas:

Análise de comportamento para detectar e bloquear ameaças sem depender de assinaturas tradicionais. Monitoramento ativo de zero-day exploits, ransomware, mineradores de criptomoedas e técnicas avançadas de ataque, mitigando riscos antes que causem danos.

Integração com Inteligência de Ameaças e Indicadores de Comprometimento (IoCs):

Correlação automática de eventos com bases de dados globais de ameaças, sem necessidade de consulta externa para respostas imediatas. Análise aprofundada de IPs, domínios, hashes de arquivos e padrões de ataque para prever e bloquear ameaças emergentes.

File Integrity Monitoring (FIM):

Monitoramento contínuo de modificações em arquivos críticos do sistema, detectando alterações suspeitas, tentativas de exclusão e manipulação de registros do sistema. Detecção de comportamentos típicos de ransomware e rootkits, garantindo a integridade do ambiente protegido.

Detecção Avançada de Malware com YARA e Análise Heurística:

Identificação de padrões de malware desconhecidos por meio de regras comportamentais e assinaturas customizadas. Avaliação heurística avançada, permitindo detectar ameaças emergentes sem necessidade de assinaturas pré-existentes.

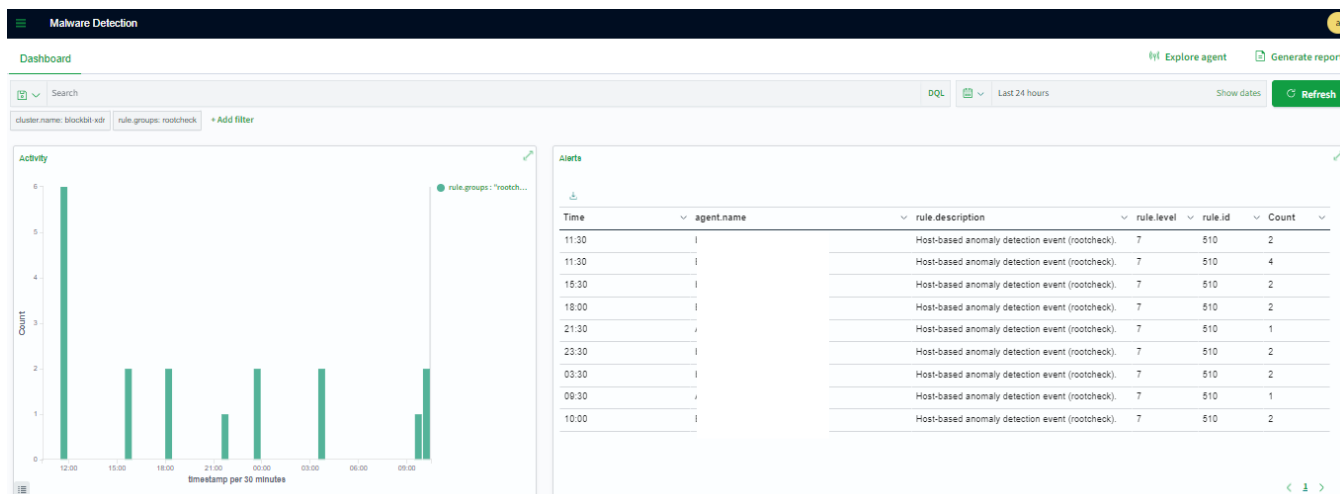
Análise Multi-Motor com VirusTotal e Threat Intelligence:

Escaneamento de arquivos e URLs utilizando múltiplos mecanismos de detecção de ameaças. Correlação de inteligência de ameaças para identificar padrões de comportamento malicioso e mitigar riscos de forma proativa. Resposta rápida a incidentes, bloqueando automaticamente arquivos e processos suspeitos antes que possam comprometer o ambiente.

Independência Operacional do Agente:

O agente do Blockbit XDR não depende do console de administração ou da nuvem para detectar e responder a ameaças sofisticadas, garantindo proteção autônoma e contínua. Mesmo em ambientes isolados, o agente pode identificar e bloquear ataques zero-day, fileless malware, ransomware, mineradores e técnicas de movimento lateral, assegurando proteção total.

Nesta página, você pode conferir alertas de anomalias que podem ser malwares ao longo de um intervalo selecionado.



Search

A barra permite buscar por eventos específicos. Para mais informações, confira [Sistema de buscas](#).

Clique em **Explore agent** para selecionar o agente. Para mais informações, confira [Selecionar agente](#).

Para criar um relatório, clique em **Generate report**. Os relatórios são armazenados em [Reports](#).

Gráficos

Clique em  para expandir o gráfico.

Clique em  para baixar os dados. O arquivo pode vir formatado ou livre.

Activity: gráfico de anomalias detectadas em intervalos de 30 minutos. Ao passar o mouse sobre um ponto do gráfico, você pode conferir a quantidade de eventos no momento selecionado.

Alerts: lista de alertas. Podem ser classificados de acordo com:

Time: horário de detecção;

agent.name: nome do agente que gerou o alerta;

rule.description: descrição da regra que gerou o alerta;

rule.level: nível da regra que gerou o alerta;

rule.id: identificador da regra que gerou o alerta;

count: mostra quantas vezes a mesma regra e agente geraram o alerta.

XDR - File Integrity Monitoring

O File Integrity Monitoring (FIM) do Blockbit XDR realiza o monitoramento contínuo de arquivos, diretórios e chaves de registro em todos os volumes, discos locais, dispositivos removíveis e voláteis, detectando em tempo real qualquer tentativa de criação, modificação ou exclusão. Com isso, o sistema garante visibilidade total sobre alterações suspeitas, possibilitando respostas automáticas como bloqueio de processos maliciosos, restauração de arquivos comprometidos e isolamento do endpoint, assegurando a integridade dos dados e a continuidade das operações.

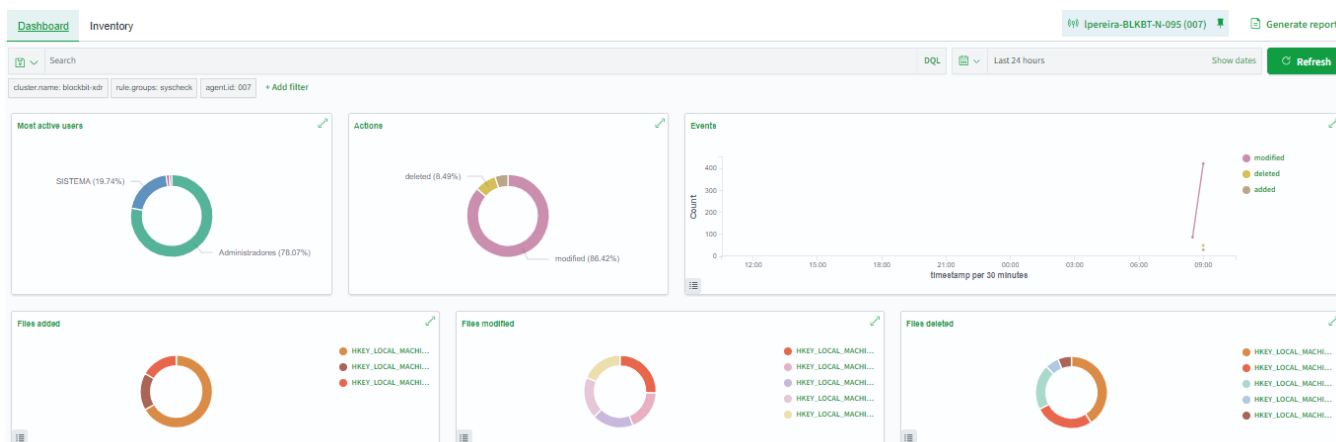
O **File Integrity Monitoring** suporta:

Monitoramento contínuo de arquivos e registros essenciais.

Identificação de mudanças suspeitas.

Geração de alertas em tempo real para ação rápida.

Aqui, você pode conferir as modificações nos arquivos separadas por usuários.



Search

A barra permite buscar por eventos específicos. Para mais informações, confira [Sistema de buscas](#).

Clique em **Explore agent** para selecionar o agente. Para mais informações, confira [Selecionar agente](#).

Para criar um relatório, clique em **Generate report**. Os relatórios são armazenados em [Reports](#).

Em **Dashboard**, você pode conferir as principais informações do agente selecionado.

Most active users: usuários individuais mais ativos.

Action: ações mais utilizadas.

- **Add:** adicionar arquivo;

- **Modify:** modificar arquivo;

- **Delete:** apagar arquivo.

Events: número de eventos contados a cada 30 minutos.

Files added: Nomes dos últimos arquivos adicionados.

Files modified: Nomes dos últimos arquivos modificados.

Em **Inventory**, você tem uma lista dos arquivos no endpoint do agente.

São mostradas as seguintes informações de cada arquivo.

Size: tamanho do arquivo.

Ao clicar num arquivo, um modal com informações adicionais e eventos envolvendo o arquivo é aberto.

Além dos detalhes mostrados na lista geral, a página também mostra:

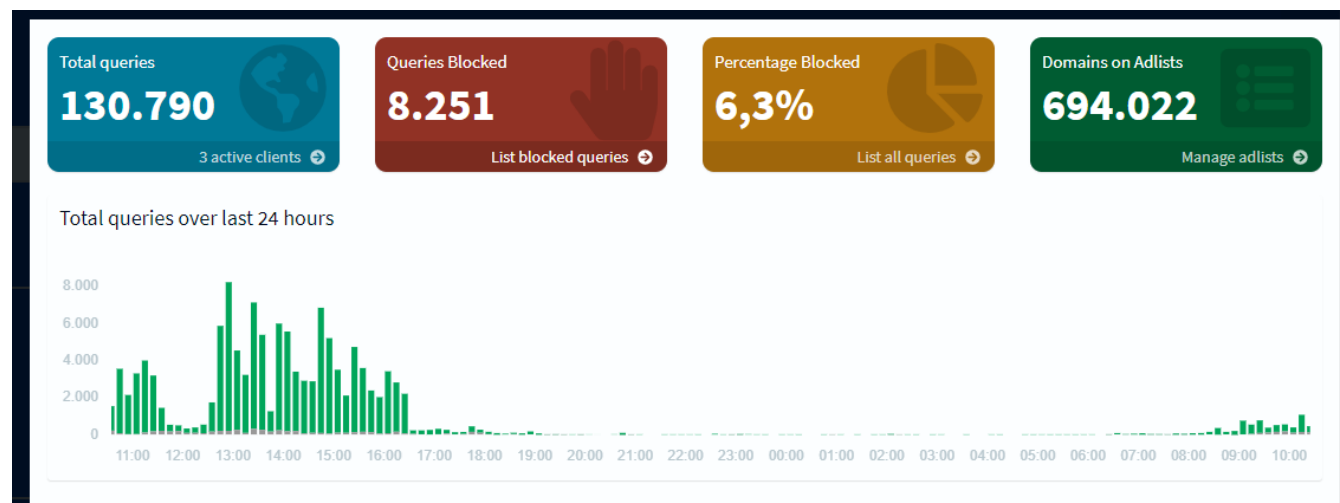
Permissions: permissões do arquivo.

Abaixo, estão os eventos mais recentes envolvendo o arquivo. Ao clicar num evento , os dados serão mostrados. Para mais informações, visite [Dados Coletados](#).

XDR - Secure Internet Gateway

O Secure Internet Gateway é um buraco negro de DNS que protege a sua rede de conteúdos indesejados. Ele funciona comparando consultas de DNS com uma lista dinâmica de domínios maliciosos. Quando uma consulta aponta para um domínio da lista, o Secure Internet Gateway manda uma resposta com um IP não roteável.

Para acessar o Secure Internet Gateway, você precisa de uma senha específica. Para não precisar inserir a senha em todo acesso, clique em Remember Me! 🗑️



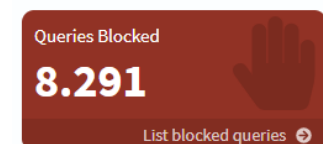
O dashboard do Secure Internet Gateway é dividido em:

Total queries



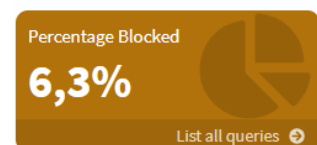
É o total de consultas na rede. Você também pode checar os clientes ativos no momento. Ao clicar, você irá para a lista de clientes.

Queries Blocked



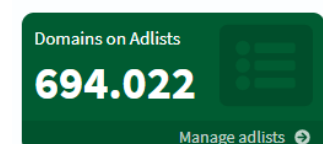
É o número de consultas bloqueadas. Ao clicar, você irá para a lista de consultas bloqueadas.

Percentage Blocked



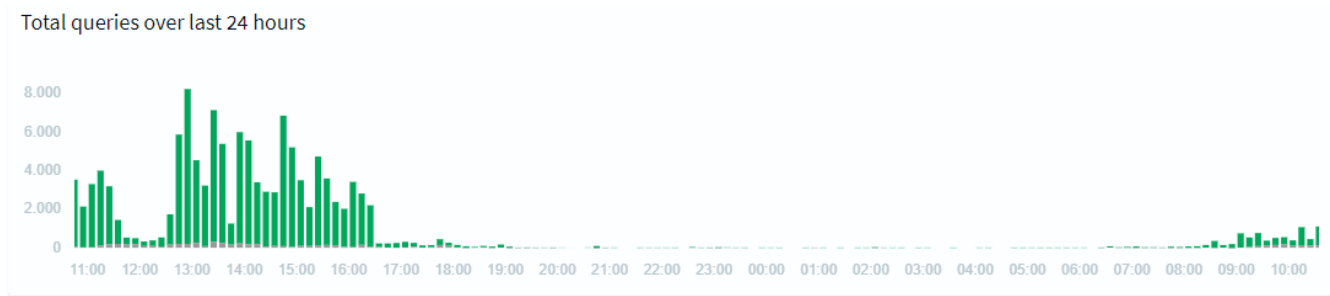
É a porcentagem de consultas bloqueadas. Ao clicar, você irá para as consultas mais recentes.

Domains on Adlists



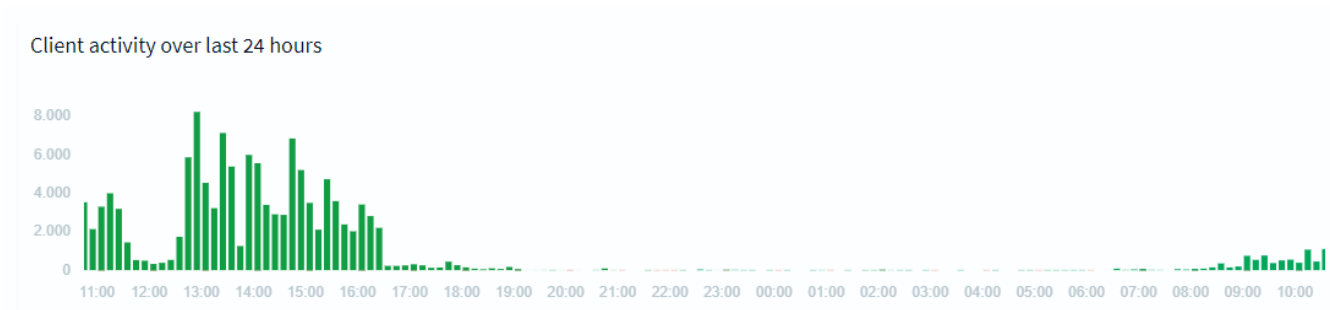
É o número de domínios na Adlist (lista de domínios bloqueados pelo bloqueador de anúncios). Ao clicar, você irá para a lista de dompinios.

Total queries over last 24 hours



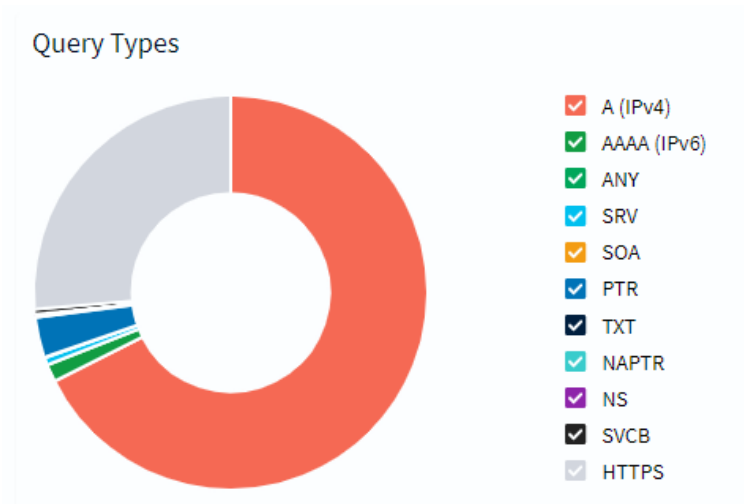
O gráfico mostra o número de chamados nas últimas 24 horas separados por intervalos de 10 minutos.

Client activity over last 24 hours



O gráfico mostra a atividade dos clientes nas últimas 24 horas separados por intervalos de 10 minutos.

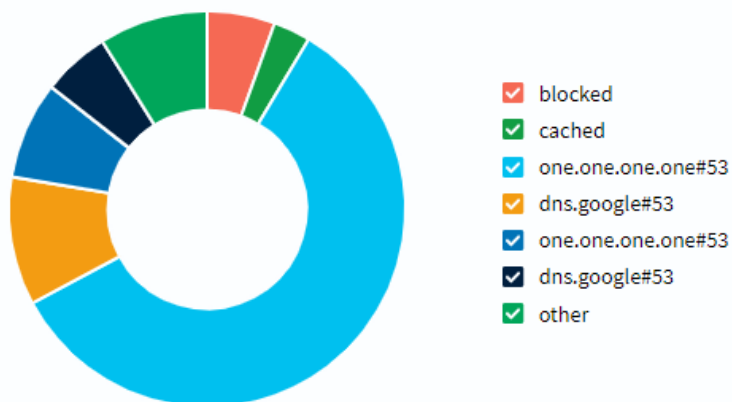
Query types



O gráfico separa as consultas por tipo. Ao passar o mouse, você confere a porcentagem de cada tipo de consulta.

Upstream servers

Upstream servers



O gráfico separa os servidores mais utilizados para upload. Ao passar o mouse, você confere a porcentagem do uso de cada servidor.

Top Permitted Domains

Top Permitted Domains

Domain	Hits	Frequency
www.google.com	2790	
gateway.fe2.apple-dns.net	1995	
teams.events.data.microsoft.com	1675	
lb._dns-sd._udp.0.20.16.172.in-addr.arpa	1450	
teams.microsoft.com	1369	
mmx-ds.cdn.whatsapp.net	1278	
lb._dns-sd._udp.relax.blockbit.com	1271	
outlook.office365.com	1219	
gateway.icloud.com	1204	

A lista mostra os domínios permitidos mais acessados. Ela é separada em:

Domain: URL do domínio;

Hits: número de acessos;

Frequency: frequência de acessos.

Top Blocked Domains

Top Blocked Domains		
Domain	Hits	Frequency
graph.facebook.com	1288	
mobile.pipe.aria.microsoft.com	1268	
horizon-track.globo.com	484	
web.facebook.com	351	
app-measurement.com	339	
7ba3f64df98de730df38846b54ecbdf7f61f80f.cws.conviva.com	277	
mqtt-mini.facebook.com	261	
www.facebook.com	236	

A lista mostra os domínios bloqueados mais acessados. Ela é separada em:

Domain: URL do domínio;

Hits: número de acessos;

Frequency: frequência de tentativas.

Top Clients (total)

Top Clients (total)		
Client	Requests	Frequency
10-244-2-12.ama-metrics-operator-targets.kube-system.svc.cluster	117468	
10-244-1-35.ingress-nginx-pi-hole-tcp-controller.pi-hole.svc.clu	9861	
localhost	143	

A lista mostra os clientes com mais requisições. Ela é separada em:

Client: ID do cliente;

Requests: número de requisições;

Frequency: frequência de requisições.

Top Clients (blocked only)

Top Clients (blocked only)

Client	Requests	Frequency
10-244-2-12.ama-metrics-operator-targets.kube-system.svc.cluster	6389	
10-244-1-35.ingress-nginx-pi-hole-tcp-controller.pi-hole.svc.clu	1759	

A lista mostra os clientes com mais requisições bloqueadas. Ela é separada em:

Client: ID do cliente;

Requests: número de requisições;

Frequency: frequência de requisições.

XDR - Secure Internet Gateway - Groups

O Secure Internet Gateway permite a criação de grupos de clientes ou domínios.

Com eles, você pode habilitar ou desabilitar o bloqueio de DNS simultaneamente em todos os elementos do grupo.

Para criar um grupo, dê um nome, descreva e aperte Add ().

Para criar mais de um grupo, insira os nomes e separe por espaço.

Para utilizar espaços, coloque o nome do grupo entre aspas (" ").

Add a new group

Name:

Group name or space-separated group names

Description:

Group description (optional)

Hints:

1. Multiple groups can be added by separating each group name with a space

2. Group names can have spaces if entered in quotes. e.g "My New Group"

Add

Abaixo, há um lista de grupos.

List of groups

Show 10 entries

Search:

Previous

Next

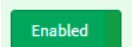
	Name	Status	Description	
☐	Default	Enabled	The default group	
☐	group	Enabled	New group	
☐	group,	Enabled		
☐	nouvelle	Enabled		

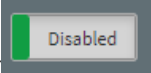
☐

Previous

Next

Showing 1 to 4 of 4 entries

Os grupos são criados com o bloqueio de DNS habilitado por padrão. Clique em Enabled() para desabilitar.

Para habilitar, clique em disabled ().

Para editar o nome e a descrição, clique nos campos **Name** ou **Description**.

Para apagar o grupo, clique na lixeira().

Você pode apagar mais de um grupo simultaneamente. Para isso, selecione os grupos e clique em apagar todos ().

Para selecionar todos os grupos, clique na caixa verde escura () sem nenhum grupo selecionado ou no + () com pelo menos um grupo selecionado.

XDR - Secure Internet Gateway - Groups - Adlists

Uma **Adlist** é uma lista de domínios conhecidos por entregar publicidade. Ao bloquear as consultas de DNS desses domínios, o conteúdo de publicidade de uma página não é carregado.

Nesta página, você pode adicionar adlists e separá-las em grupos.

Após atualizar uma adlist, atualize o Gravity (lista de domínios bloqueados).

Add a new adlist

Address:

URL or space-separated URLs

Comment:

Adlist description (optional)

Hints:

- Please run `blockbithole -g` or update your gravity list [online](#) after modifying your adlists.
- Multiple adlists can be added by separating each *unique* URL with a space
- Click on the icon in the first column to get additional information about your lists. The icons correspond to the health of the list.

Add

Para adicionar uma adlist, insira a URL em **Address**, descreva em **Comment** aperte Add ().
Para inserir mais de uma URL, separe por espaço.

List of adlists

Show 10 entries

Search:

Previous 2 Next

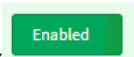


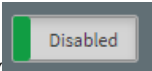
	Address	Status	Comment	Group assignment	
☒	 https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts	Enabled	Migrated f	Default	
☐	 https://easylist.to/easylist/easylist.txt	Enabled		Default	
☐	 https://raw.githubusercontent.com/nottracking/hosts-blocklists/master/hostnames.txt	Enabled		Default	
☐	 https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt	Enabled		Default	
☐	 https://raw.githubusercontent.com/Spam404/lists/master/main-blacklist.txt	Enabled		Default	

Em **List of adlists** há uma lista de adlists.

Em **Address**, estão listadas as URLs das adlists.

Ao clicar nos ícones  e , você tem informações adicionais da adlist.

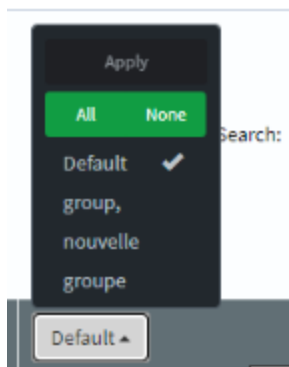
As adlists são inseridas como habilitadas por padrão. Em **Status**, Clique em Enabled() para desabilitar.

Para habilitar, clique em disabled ().

Para editar a descrição, clique no campo **Comment**.

Em **Group assignment** você pode colocar a adlist em algum grupo.

Clique no botão com o nome do grupo (nesse caso, Default) e selecione para qual grupo a adlist irá.



Para apagar a adlist, clique na lixeira().



Você pode apagar mais de uma adlist simultaneamente. Para isso, selecione as adlists e clique em apagar todos ().



Para selecionar todas as adlists, clique na caixa verde escura () sem nenhuma adlist selecionada ou no + () com pelo menos uma adlist selecionada.

XDR - Secure Internet Gateway - Groups - Clients

Para colocar um cliente no grupo, selecione na lista dos clientes conhecidos e clique em  ou aperte **enter**.

Known clients:

Select client...

Comment:

Client description (optional)

Confirming your entry with .

ibnets (CIDR notation, like `192.168.2.0/24`), their MAC addresses (like `aa:bb:cc:dd:ee:ff`) are connected to (prefaced with a colon, like `eth0:aa:bb:cc:dd:ee:ff`).

address, host name or interface recognition as the two latter will only be available after some time hop away from your blockbit-sgi.

Add

Um cliente pode estar descrito pelo seu endereço IPv4 ou IPv6, IP Subnet, MAC Address, hostname ou interface onde está conectado.

Em **List of configured clients**, você pode determinar para qual grupo o cliente irá.

Clique no botão com o nome do grupo (nesse caso, Default) e selecione para qual grupo o cliente irá.

List of configured clients

Show 10 entries

✓

🗑️

Client	Comment	
✓ 🗑️		Default Previous Next

Showing 1 to 1 of 1 entries

Para editar a descrição, clique no campo **Comment**.

Para retirar o cliente da lista, clique na lixeira().

Você pode retirar mais de um cliente simultaneamente. Para isso, selecione os clientes e clique em retirar todos ().

Para selecionar todos os clientes, clique na caixa verde escura () sem nenhum cliente selecionado ou no + () com pelo menos um cliente selecionado.

XDR - Secure Internet Gateway - Groups - Domains

O Secure Internet Gateway tem duas listas de domínios:

Whitelist: lista de domínios aceitáveis;

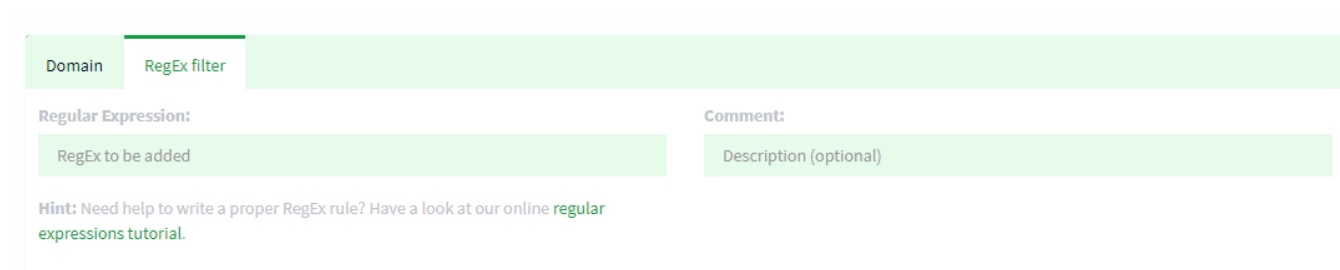
Blacklist: lista de domínios inaceitáveis.

Você pode adicionar um domínio ou uma expressão regular (Regular Expression ou RegEx) para qualquer uma das listas.



Para adicionar um domínio, insira a URL no campo **Domain** e uma descrição em **Comment**.

Você pode adicionar o domínio como **Wildcard**. Esse domínio irá corresponder a consultas a domínios não existentes.



Para adicionar uma RegEx, insira a expressão no campo **Regular Expression** e uma descrição em **Comment**.

Para adicionar à Blacklist, clique em Add to Blacklist ().

Para adicionar à Whitelist, clique em Add to Whitelist ().

Em **List of domains**, há uma lista dos domínios ou RegEx e seus grupos.

List of domains

☒ Exact whitelist
 ☒ Regex whitelist
 ☒ Exact blacklist
 ☒ Regex blacklist

Show 10 entries

Search: Previous Next

	Domain/RegEx	Type	Status	Comment	Group assignment	
☐		Exact blacklist	Enabled		Default	
☐		Exact blacklist	Enabled	Added from Query Log	Default	
☐		Exact whitelist	Enabled	Added from Query Log	Default	
☐		Regex blacklist	Enabled		Default	
☐		Regex whitelist	Enabled		Default	

Showing 1 to 5 of 5 entries

Em **Type**, você pode mudar o tipo de registro do domínio.

Exact whitelist: coloca o domínio exato na Whitelist.

Regex whitelist: aplica a regra determinada pela RegEx para colocar na Whitelist.

Exact blacklist: coloca o domínio exato na Blacklist.

Regex blacklist: aplica a regra determinada pela RegEx para colocar na Blacklist.

Você pode filtrar os registros por tipo no canto superior direito.

☒ Exact whitelist
 ☒ Regex whitelist
 ☒ Exact blacklist
 ☒ Regex blacklist

Os domínios entram na lista com o bloqueio de DNS habilitado por padrão. Em **Status**, Clique em Enabled() para desabilitar.

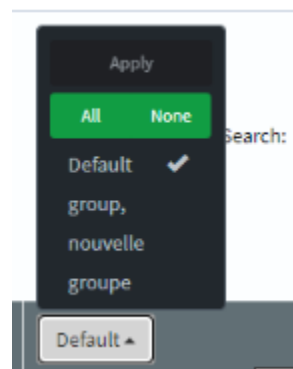


Para habilitar, clique em disabled ().

Para editar a descrição, clique no campo **Comment**.

Em **Group assignment** você pode colocar o domínio ou a RegEx em algum grupo.

Clique no botão com o nome do grupo (nesse caso, Default) e selecione para qual grupo o cliente irá.



Para apagar o domínio ou a RegEx, clique na lixeira().

Você pode apagar mais de um domínio ou a RegEx simultaneamente. Para isso, selecione os domínios ou RegEx e clique em apagar todos ().

Para seleccionar todos os domínios ou RegEx, clique na caixa verde escura () sem nenhum domínio ou RegEx seleccionado ou no + () com pelo menos um domínio ou RegEx seleccionado.

XDR - Secure Internet Gateway - Local DNS

Nesta seção, você pode listar servidores locais de DNS. Esses servidores resolvem domínios dentro da rede local ao invés de servidores externos. Você pode os servidores por pares domínio/IP ou CNAME.

DNS Records

Esta opção lista pares domínio/IP.

Domain:

Domain or comma-separated list of domains

IP Address:

Associated IP address

Note:

The order of locally defined DNS records is:

1. The device's host name and

pi.hole

2. Configured in a config file in

/etc/dnsmasq.d/

3. Read from

/etc/hosts

4. Read from the "Local (custom) DNS" list (stored in

/etc/pihole/custom.list

)

Only the first record will trigger an address-to-name association.

Add

Para adicionar um par, insira o domínio em **Domain** e o endereço IP associado a ele em **IP Address**. Depois, clique em Add (

Add

)

Em **List of local DNS domains**, há uma lista de pares domínio/IP.

List of local DNS domains

Show

10

entries

Search:

Domain	IP	Action
www.domain.com	2.2.2.2	
www.site.org	1.1.1.1	

Showing 1 to 2 of 2 entries

Previous

Next

Domain é o domínio;
IP é o IP associado ao domínio.

Para apagar o par, clique na lixeira().

CNAME Records

Esta opção lista pares de domínio de alias e domínio canônico.
Exemplo: blog.site.com é um domínio alias e [www.site.com](#) é o domínio canônico.

Add a new CNAME record

Domain:

Domain or comma-separated list of domains

Target Domain:

Associated Target Domain

Note:

The target of a **CNAME** must be a domain that the blockbit-sgi already has in its cache or is authoritative for. This is a universal limitation of **CNAME** records.

The reason for this is that blockbit-sgi will not send additional queries upstream when serving **CNAME** replies. As consequence, if you set a target that isn't already known, the reply to the client may be incomplete. blockbit-sgi just returns the information it knows at the time of the query. This results in certain limitations for **CNAME** targets, for instance, only active DHCP leases work as targets - mere DHCP *leases* aren't sufficient as they aren't (yet) valid DNS records.

Additionally, you can't **CNAME** external domains (**bing.com** to **google.com**) successfully as this could result in invalid SSL certificate errors when the target server does not serve content for the requested domain.

Add

Em **Domain**, insira o domínio alias.

Em **Target Domain**, adicione o domínio canônico.

Add

Para adicionar, clique em Add ().

Em **List of local CNAME records**, há uma lista de pares **Domain** e **Target**.

List of local CNAME records

Show 10 entries

Search:

Domain	Target	Action
about.site.com	www.site.com	
blog.site.com	www.site.com	

Showing 1 to 2 of 2 entries

Previous

Next

Domain é o domínio alias;

Target é o domínio canônico.



Para apagar o par, clique na lixeira().

XDR - Secure Internet Gateway - Query Log

A página lista as consultas mais recentes.

Para buscar uma consulta específica, utilize a barra de pesquisas.

Você pode determinar quantas consultas são exibidas por página. Para mostrar todas, clique em show all.

Time	Type	Domain	Client	Status	Reply	Action
2025-02-12 15:54:48	A			Blocked (gravity)	IP (0.0ms)	<button>Whitelist</button>
2025-02-12 15:54:46	A			OK (answered by)	CNAME (1.7ms)	<button>Blacklist</button>
2025-02-12 15:54:46	A			OK (answered by)	CNAME (5.7ms)	<button>Blacklist</button>

Time: data e hora da consulta;

Type: tipo da consulta. Cada tipo recupera dados diferentes;

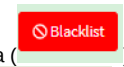
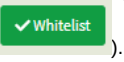
Domain: domínio que a consulta espera uma resposta;

Client: cliente que a consulta espera uma resposta;

Status: estado da consulta. Pode ser Blocked (consulta bloqueada) ou OK (consulta respondida);

Reply: tempo e tipo da resposta;

Action: ações possíveis.

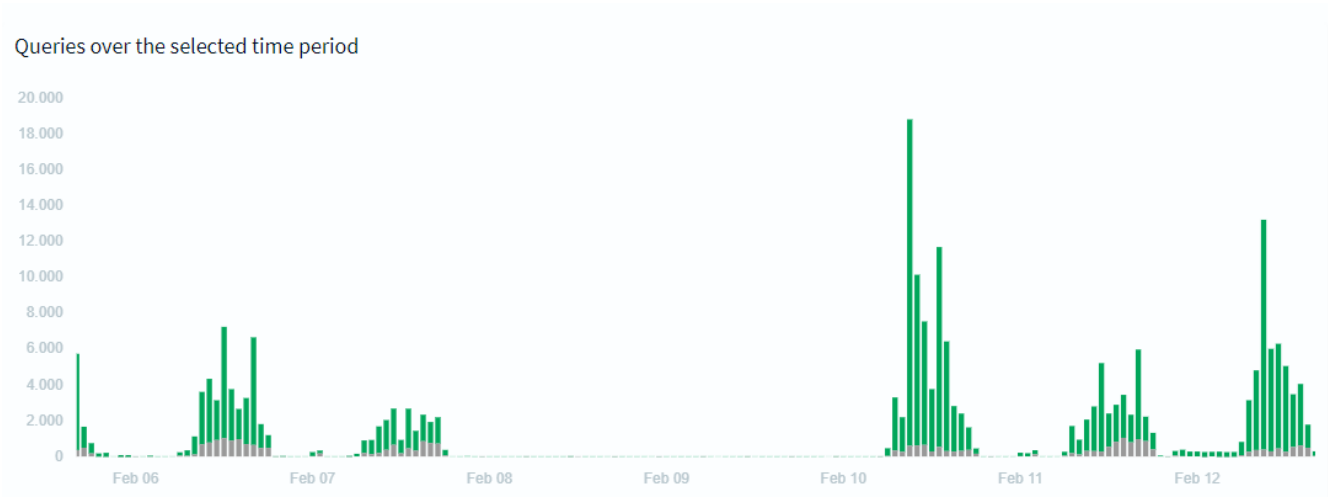
- Se uma consulta foi respondida, ela pode ser bloqueada e ir para a lista negra ();
- Se uma consulta foi bloqueada, ela pode ser liberada e ir para a lista branca (.

XDR - Secure Internet Gateway - Query Log - Long Term Data

Nessas páginas, você pode acompanhar dados ao longo de um intervalo específico.
Para mostrar, selecione o intervalo de tempo em Select date and time range. Para um intervalo específico, escolha Custom range.

Graphics

Esta página mostra número de consulta ao longo do tempo em forma de gráfico.



Query log

Esta página lista as consultas no intervalo selecionado.

Total queries

0

Total Queries

É o total de consultas na rede.

Queries Blocked

0

Queries Blocked

É o número de consultas bloqueadas.

Queries Blocked (Wildcard)

0

Queries Blocked (Wildcards)

É o número de consultas bloqueadas e redirecionadas para um domínio padrão.

Percentage Blocked



É a porcentagem de consultas bloqueadas.

A lista de consultas tem os seguintes dados:

Time: data e hora da consulta;

Type: tipo da consulta. Cada tipo recupera dados diferentes;

Domain: domínio que a consulta espera uma resposta;

Client: cliente que a consulta espera uma resposta;

Status: estado da consulta. Pode ser Blocked (consulta bloqueada) ou OK (consulta respondida);

Reply: tempo e tipo da resposta;

Action: ações possíveis.

- Se uma consulta foi respondida, ela pode ser bloqueada e ir para a lista negra ();
- Se uma consulta foi bloqueada, ela pode ser liberada e ir para a lista branca ().

Top Domains

Top Domains		
Domain	Hits	Frequency
www.google.com	8193	
gateway.fe2.apple-dns.net	2703	
outlook.office365.com	2410	
mmx-ds.cdn.whatsapp.net	2371	
chat.cdn.whatsapp.net	2367	
in.appcenter.ms	2160	
i.instagram.com	1809	
www.msftconnecttest.com	1761	
teams.microsoft.com	1692	
teams.events.data.microsoft.com	1482	

A lista mostra os domínios permitidos mais acessados. Ela é separada em:

Domain: URL do domínio;

Hits: número de acessos;

Frequency: frequência de acessos.

Top Blocked Domains

Top Blocked Domains		
Domain	Hits	Frequency
graph.facebook.com	1288	
mobile.pipe.aria.microsoft.com	1268	
horizon-track.globo.com	484	
web.facebook.com	351	
app-measurement.com	339	
7ba3f64df98de730df38846b54ecbdf7f61f80f.cws.conviva.com	277	
mqtt-mini.facebook.com	261	
www.facebook.com	236	

A lista mostra os domínios bloqueados mais acessados. Ela é separada em:

Domain: URL do domínio;

Hits: número de acessos;

Frequency: frequência de tentativas.

Top Clients (total)

Top Clients (total)		
Client	Requests	Frequency
	117468	
	9861	
	143	

A lista mostra os clientes com mais requisições. Ela é separada em:

Client: ID do cliente;

Requests: número de requisições;

Frequency: frequência de requisições.

XDR - Threat Hunting

O Threat Hunting no Blockbit XDR é um processo de busca ativa por ameaças, permitindo que analistas de segurança investiguem ataques cibernéticos em estágio inicial, atividades suspeitas e anomalias comportamentais, mesmo antes de alertas.

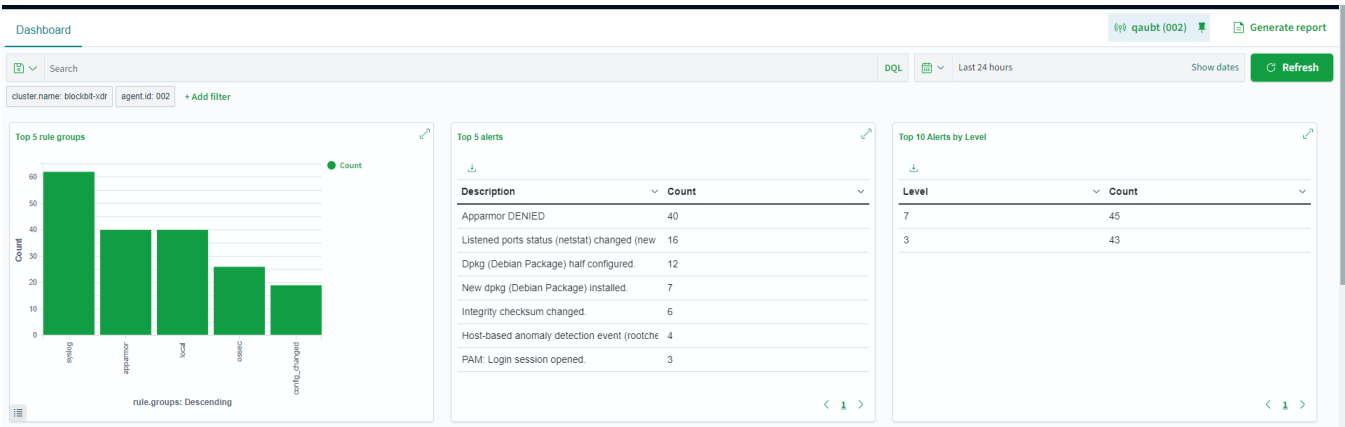
O Blockbit XDR oferece fluxos de trabalho completos para pesquisa e investigação de ameaças, unindo automação, inteligência artificial e análise manual. Por meio de uma linha do tempo interativa, é possível conduzir análises forenses aprofundadas, visualizando toda a sequência de eventos e processos relacionados à ameaça, desde sua origem até o impacto final. Essa abordagem permite identificar o comportamento do ataque, os vetores de entrada e os ativos comprometidos, proporcionando uma resposta ágil e precisa.

Com o Blockbit XDR, você pode:

- Analisar comportamentos incomuns e anomalias em endpoints, rede e aplicações.
- Correlacionar automaticamente eventos e indicadores de comprometimento (IoCs).
- Acessar e filtrar logs detalhados para identificar padrões de ataque e movimentação lateral.
- Criar e automatizar regras de busca e detecção personalizadas.
- Mapear ameaças no framework MITRE ATT&CK, facilitando uma resposta estratégica e eficaz.

Com esse fluxo de trabalho estruturado, o Blockbit XDR permite que analistas identifiquem e neutralizem ameaças avançadas, como APT (Advanced Persistent Threats), ataques sem arquivos (fileless malware), exploits zero-day e tentativas de exfiltração de dados, reduzindo riscos e fortalecendo a segurança da organização.

Nesta página, você pode conferir as ameaças em curso.

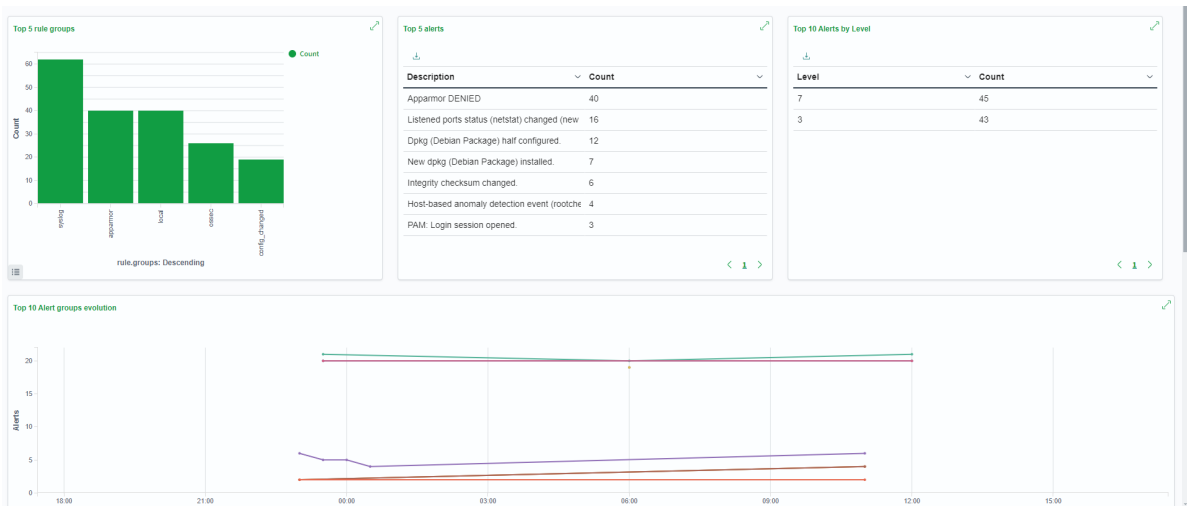


Search

A barra permite buscar por eventos específicos. Para mais informações, confira [Sistema de buscas](#).

Clique em **Explore agent** para selecionar o agente. Para mais informações, confira [Selecionar agente](#).

Para criar um relatório, clique em **Generate report**. Os relatórios são armazenados em [Reports](#).



A página apresenta os seguintes gráficos:

Top 5 rule groups: grupos de regras que mais geraram alertas;

Top 5 alerts: alertas mais comuns;

Top 10 alerts by level: nível de regra que apareceram mais alertas;

Top 10 Alerts group evolution: Número de alertas por período de 30 minutos separados por grupo.

Alerts: Número de alertas por 30 minutos.

Abaixo, está a lista de alertas.

Security Alerts						
Time	Technique(s)	Tactic(s)	Description	Level ↑	Rule ID	
> Aug 21, 2024 @ 00:02:31.736			Agent event queue is back to normal load.	3	205	
> Aug 20, 2024 @ 20:59:57.368			Web server 400 error code.	5	31101	
> Aug 20, 2024 @ 20:59:57.368			Web server 400 error code.	5	31101	
> Aug 20, 2024 @ 20:59:57.396			Web server 400 error code.	5	31101	
> Aug 20, 2024 @ 20:59:57.396			Web server 400 error code.	5	31101	
> Aug 20, 2024 @ 20:59:57.396			Web server 400 error code.	5	31101	
> Aug 20, 2024 @ 20:59:57.432			Web server 400 error code.	5	31101	
> Aug 20, 2024 @ 20:59:57.453			Web server 400 error code.	5	31101	
> Aug 20, 2024 @ 20:59:57.503			Web server 400 error code.	5	31101	

Time: horário do alerta.

Technique(s): técnicas detectadas no alerta.

Tactic(s): táticas detectadas no alerta.

Description: descrição do alerta.

Level: nível da regra violada.

Rule ID: identificação da regra violada.

Ao clicar em cada evento, você poderá conferir os dados envolvidos. Para mais informações, confira [Dados Coletados](#).

XDR - Threat Monitor - CTI

O Blockbit XDR oferece o Threat Monitor - CTI, espaço onde você pode guardar, organizar e visualizar a sua base de conhecimento de ameaças e observações.

XDR - Threat Monitor - CTI - Dashboard

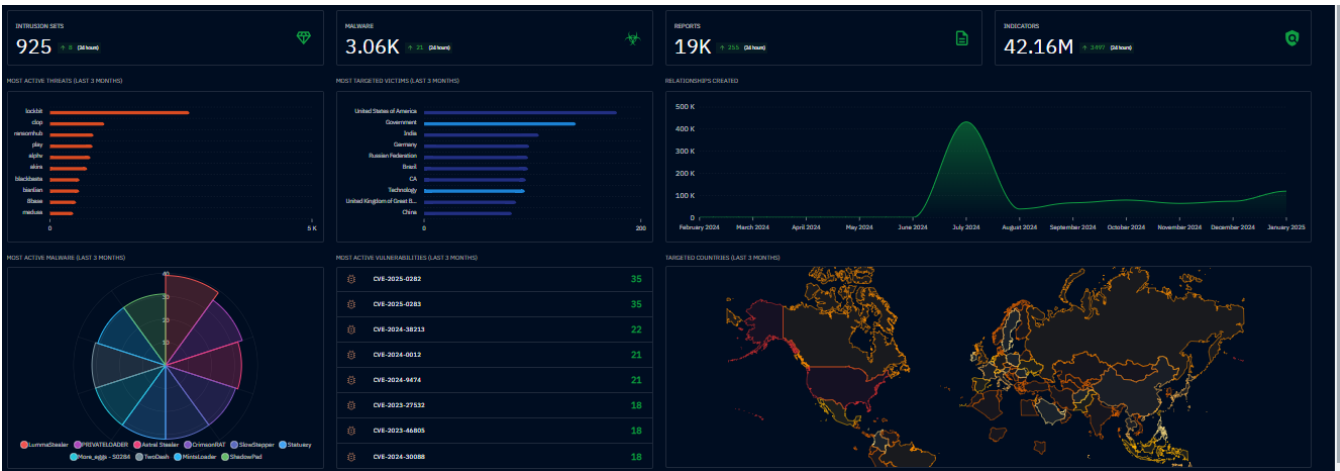
A primeira página que você encontra é o Dashboard. Aqui estão as principais informações sobre o que está acontecendo na sua organização.

Para encontrar qualquer elemento na plataforma, utilize a barra de buscas.

Em **Advanced Search** () , você acessa uma lista de arquivos e elementos da base de conhecimento.

Em **Bulk Search** () , você pode buscar por lotes de elementos ao inserir palavras-chave.

No canto superior direito, há 4 ações disponíveis. Para mais informações, visite [Ações](#).



Intrusion sets: número de conjuntos de intrusão (atividades maliciosas consistentes);

Malware: número de malwares;

Reports: número de relatos;

Indicators: Número de indicadores.

Os gráficos são divididos em:

Most active threats (last 3 months): lista de ameaças mais presentes nos últimos 3 meses;

Most targeted victims (last 3 months): lista de vítimas atacadas com mais intensidade nos últimos 3 meses;

Relationships created: número de relações criadas nos últimos 12 meses separadas por mês;

Most active malware (last 3 months): malwares mais ativos nos últimos 3 meses;

Most active vulnerabilities (last 3 months): vulnerabilidades com mais relações nos últimos 3 meses;

Targeted countries (last 3 months): países atacados com mais intensidade nos últimos 3 meses.

Em **Latest reports**, há uma lista com os últimos relatos.

Estes relatos são divididos por:

Type: tipo. Ao clicar na etiqueta, você será redirecionado para uma página com informações sobre o tipo da ameaça;

Value: valor;

Author: autor da ameaça;

Date: data da ameaça;

Labels: etiquetas recebidas pela ameaça. As etiquetas servem para classificar a ameaça;

Markings: marcações recebidas pela ameaça. As marcações servem para classificar o status da ameaça;

Platform creation date: data que a ameaça foi catalogada na plataforma.

Ao lado, há mais um gráfico:

Most active labels (last 3 months): etiquetas mais dadas nos últimos 3 meses.

XDR - Threat Monitor - CTI - Dashboard - Ações

No canto superior direito, há 4 ações disponíveis:



Notifications (): notificações.

Aqui você pode conferir as notificações do sistema.

São classificadas por:

☐	OPERATION	MESSAGE	ORIGINAL CREATL...	TRIGGER
--------------------------	-----------	---------	--------------------	---------

Operation: operação que gerou a notificação;

Message: mensagem da notificação;

Original creation date: data da notificação;

Trigger: gatilho responsável pela notificação.



Triggers (): gatilhos.

Aqui você pode conferir os gatilhos que geram notificações.

São classificados por:

TYPE	NAME ▼	NOTIFICATION	TRIGGERING ON	DETAILS
------	--------	--------------	---------------	---------

Type: tipo do gatilho;

Name: nome do gatilho;

Notification: notificação gerada pelo gatilho;

Triggering on: o que gerou o gatilho;

Details: detalhes do gatilho.



Profiles (): perfis.

Aqui você pode administrar o usuário.

Profile

Profile

Name

Email address

Organizations

Firstname

Lastname

Description

Aqui você pode mudar os dados do usuário como nome, email, organização e descrição.

User experience

User experience

Theme
Default

Language
Automatic

Unit system
Automatic

Show left navigation submenu icons

Auto collapse submenus in left navigation

When an event happens on a knowledge you participate, you will receive notification through your personal notifiers

Personal notifiers
User interface Default mailer

Aqui você pode mudar;

Theme: tema do CTI (modo claro ou escuro);

Language: língua do CTI;

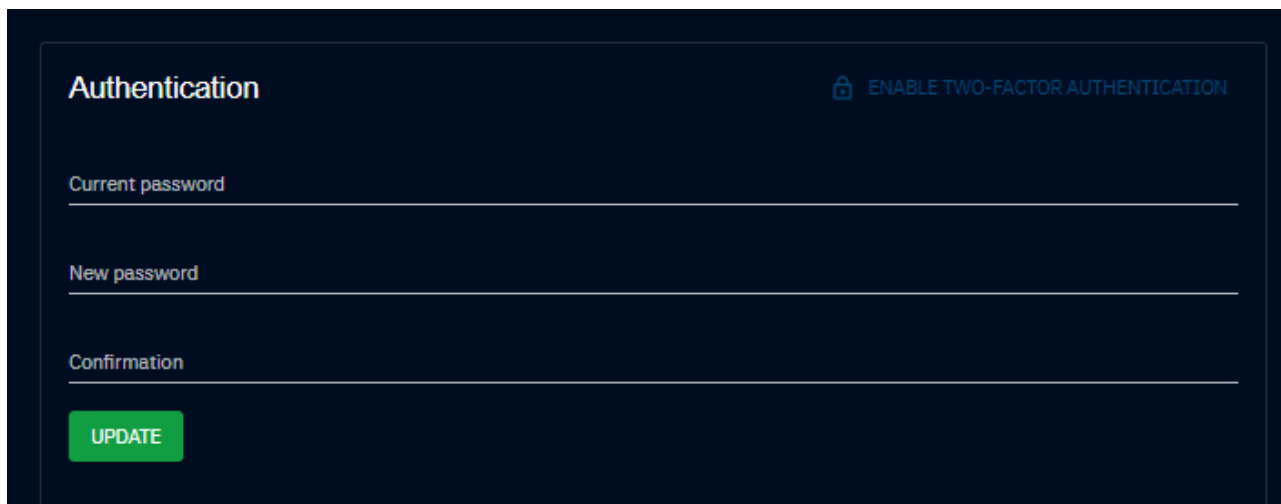
Unit system: sistema de medidas (métrico ou imperial).

Show left navigation submenu icons: mostrar ícones do submenu à esquerda;

Auto collapse submenu in left navigations: minimizar automaticamente o submenu à esquerda.

Abaixo, há um espaço para tags sobre interesses de notificação.

Authentication

A dark-themed form titled "Authentication". In the top right corner, there is a link with a padlock icon and the text "ENABLE TWO-FACTOR AUTHENTICATION". The form contains three input fields: "Current password", "New password", and "Confirmation". Below these fields is a green button labeled "UPDATE".

Authentication

ENABLE TWO-FACTOR AUTHENTICATION

Current password

New password

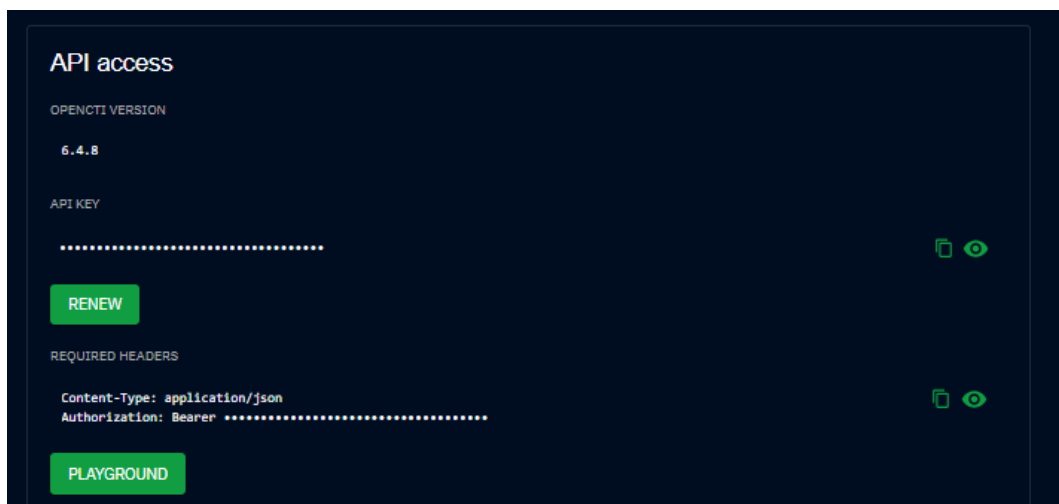
Confirmation

UPDATE

Aqui você pode mudar a sua senha. Insira a senha atual, a nova senha e repita a nova senha. Para mudar, clique em **Update** (UPDATE).

Para habilitar a autenticação em dois fatores, clique em **Enable two-factor authentication**.

API access

A dark-themed form titled "API access". It displays the "OPENCTI VERSION" as "6.4.8". Below this is the "API KEY" section, which shows a masked key with a copy icon and a toggle for visibility. A green "RENEW" button is located below the API key. The "REQUIRED HEADERS" section shows "Content-Type: application/json" and "Authorization: Bearer " followed by a masked token, with a copy icon and a toggle for visibility. At the bottom is a green "PLAYGROUND" button.

API access

OPENCTI VERSION

6.4.8

API KEY

RENEW

REQUIRED HEADERS

Content-Type: application/json

Authorization: Bearer

PLAYGROUND

Aqui você pode administrar o acesso à API.

Para renovar a chave da API, clique em **Renew** (RENEW);

Para acessar o ambiente, clique em **Playground** (PLAYGROUND).

Feedback

The image shows a dark-themed feedback form interface. At the top, there is a header bar with a 'Write' tab and a 'Preview' tab, followed by a rich text editor toolbar with icons for bold, italic, underline, link, unlink, list, and other formatting options. Below the header, the form contains several sections: 'Confidence level' with a value of '100' and a dropdown menu showing '1 - Confirmed by other sources'; 'Rating' with five smiley face icons, the last one being green; 'Entities' with a green plus icon; 'Associated file' with a green button labeled 'SELECT YOUR FILE' and the text 'No file selected.'; and 'Labels' with a plus icon and a dropdown arrow. At the bottom right, there are two buttons: a green 'CANCEL' button and a blue 'CREATE' button.

Aqui você pode criar um feedback da plataforma.

Determine:

Description: descrição do feedback,

Confidence level: insira o nível de confiança e a probabilidade de estar correto;

Rating: selecione a nota para o seu humor. Uma carinha significa insatisfeito. Cinco carinhas, satisfeito.

Entities: insira as entidades envolvidas;

Associated file: insira o arquivo associado;

Labels: insira as etiquetas associadas.

Logout: deslogar do CTI.

XDR - Threat Monitor - CTI - Analyses

Nesta página, estão agrupadas as análises sobre ameaças.

Para buscar um resultado, utilize a barra de buscas. Você pode filtrar as buscas em **Add filter**.

Ao selecionar um elemento, a barra de ações aparece. As seguintes ações estão disponíveis:

- Update** (🔧): atualizar;
- Rule rescan** (🔍): escanear novamente a regra;
- Enrichment** (🔄): buscar novos dados;
- Merge** (👤): fundir dados;
- Add in container** (📁): adicionar dados a um contêiner.

Reports

Aqui estão localizados objetos tipo Report, que são coleções de descrições de ameaças focadas em tópicos.

☐	NAME	TYPE	AUTHOR	CREATORS	LABELS	DATE	STATUS	MARKING
☐	DNS Early Detection - Fast...	THREAT-REP...	AlienVault	admin	information stealer, fake	Feb 28, 2025	NEW	TLP:CLEAR
☐	Long Live The Vo1d Botnet: New...	THREAT-REP...	AlienVault	admin	botnet, void, proxy	Feb 28, 2025	NEW	TLP:CLEAR
☐	akira has published a new...	RANSOMWA...	Ransomware.Live	admin	No label	Feb 28, 2025	NEW	TLP:CLEAR

- Os objetos são divididos por:
- Name:** nome do objeto;
 - Type:** tipo do objeto. Ao clicar na etiqueta, você será redirecionado para uma página com informações sobre a ameaça;
 - Author:** autor da ameaça;
 - Creators:** criador do objeto;
 - Labels:** etiquetas recebidas pela ameaça. As etiquetas servem para classificar a ameaça;
 - Date:** data da ameaça;
 - Status:** status do objeto;
 - Markings:** marcações recebidas pela ameaça. As marcações servem para classificar o status da ameaça.

Groupings

Aqui estão os objetos tipo Grouping, que são investigações em curso sobre ameaças.

☐	NAME	CONTEXT	AUTHOR	CREATORS	LABELS	ORIGINAL CRE	STATUS	MARKING
☐	NAT	SUSPICIOUS...	MongoDB	admin	No label	Jul 31, 2024	DISABL...	TLP:AMB...

- Os objetos são divididos por:
- Name:** nome do objeto;

Context: contexto do objeto;

Author: autor da ameaça;

Creators: criador do objeto;

Labels: etiquetas recebidas pela ameaça. As etiquetas servem para classificar a ameaça;

Original creation: criação da ameaça;

Status: status do objeto;

Markings: marcações recebidas pela ameaça. As marcações servem para classificar o status da ameaça.

Malware analyses

Aqui estão as análises de Malware.

☐	RESULT NAME	PRODUCT	OPERATING SYSTEM	AUTHOR	CREATORS	LABELS	SUBMISSION DATE	MARKING
--------------------------	-------------	---------	------------------	--------	----------	--------	-----------------	---------

As análises são divididas em:

Result name: nome da análise;

Product: resultado da análise;

Operating system: sistema operacional;

Author: autor da análise;

Creators: criador da análise;

Labels: etiquetas recebidas pela ameaça. As etiquetas servem para classificar a ameaça;

Submission date: data de entrega da análise;

Markings: marcações recebidas pela ameaça. As marcações servem para classificar o status da ameaça.

Notes

Notas são anotações feitas pelos usuários do CTI.

☐	ABSTRACT	TYPE	AUTHOR	CREATORS	LABELS	ORIGINAL CRE	STATUS	MARKING
--------------------------	----------	------	--------	----------	--------	--------------	--------	---------

São divididas em:

Abstract: resumo da nota;

Type: tipo da nota;

Author: autor da nota;

Creators: criador da nota;

Labels: etiquetas recebidas pela nota. As etiquetas servem para classificar a nota;

Original creation date: data de criação da nota;

Status: status da nota.

Markings: marcações recebidas pela nota. As marcações servem para classificar o status da nota.

External references

Referências externas são bases de conhecimento de fora do CTI.

☐	SOURCE NAME	EXTERNAL ID	URL	CREATORS	ORIGINAL CREATION DAT	
☐	cve@mitre.org	-	http://marc.info/?l=bugtraq&m=107696235424865&w=2	admin	Jul 22, 2024	>
☐	cve@mitre.org	-	http://www.securityfocus.com/archive/1/262074	admin	Jul 22, 2024	>

São divididas em:

Source name: nome da referência;

External ID: identificador da referência;

URL: URL da referência;

Creators: criador da referência;

Original creation date: data de criação da referência;

XDR - Threat Monitor - CTI - Cases

Aqui estão agrupados os casos que precisam de atenção.

Para buscar um resultado, utilize a barra de buscas. Você pode filtrar as buscas em **Add filter**.

Ao selecionar um elemento, a barra de ações aparece. As seguintes ações estão disponíveis:

 **Update** (): atualizar;

 **Rule rescanner** (): escanear novamente a regra;

 **Enrichment** (): buscar novos dados;

 **Merge** (): fundir dados;

 **Add in container** (): adicionar dados a um contêiner.

Incident Responses

Aqui estão agrupadas as respostas a incidentes.

☐	NAME	PRIORITY	SEVERITY	ASSIGNEES	CREATORS	LABELS	ORIGINAL CRE	STATUS	MARKING
☐	CVE-2024-6387	P1	HIGH	-	admin	No label	Jul 31, 2024	DISABL...	NONE

Name: nome do caso;

Priority: prioridade do caso;

Severity: severidade do caso;

Assignees: responsáveis pelo caso.

Labels: etiquetas recebidas pelo caso. As etiquetas servem para classificar o caso;

Original creation: criação do caso;

Status: status do caso;

Markings: marcações recebidas pelo caso. As marcações servem para classificar o status do caso.

Requests for information

Aqui estão agrupados os pedidos de informação.

☐	NAME	PRIORITY	SEVERITY	ASSIGNEES	CREATORS	LABELS	ORIGINAL CI	STATUS	MARKING
--------------------------	------	----------	----------	-----------	----------	--------	-------------	--------	---------

Name: nome do pedido;

Priority: prioridade do pedido;

Severity: severidade do pedido;

Assignees: responsáveis pelo pedido.

Labels: etiquetas recebidas pelo pedido. As etiquetas servem para classificar o pedido;

Original creation: criação do pedido;

Status: status do pedido;

Markings: marcações recebidas pelo pedido. As marcações servem para classificar o status do pedido.

Requests for takedown

Aqui estão os pedidos para retirada de acesso.

☐	NAME	PRIORITY	SEVERITY	ASSIGNEES	CREATORS	LABELS	ORIGINAL CI	STATUS	MARKING
--------------------------	------	----------	----------	-----------	----------	--------	-------------	--------	---------

Name: nome do pedido;

Priority: prioridade do pedido;

Severity: severidade do pedido;

Assignees: responsáveis pelo pedido.

Labels: etiquetas recebidas pelo pedido. As etiquetas servem para classificar o pedido;

Original creation: criação do pedido;

Status: status do pedido;

Markings: marcações recebidas pelo pedido. As marcações servem para classificar o status do pedido.

Tasks

Aqui estão agrupadas as tarefas distribuídas.

☐	NAME	DUE DATE	ASSIGNEES	LABELS	STATUS
--------------------------	------	----------	-----------	--------	--------

Name: nome da tarefa;

Due date: prazo da tarefa;

Assignees: responsáveis pela tarefa.

Labels: etiquetas recebidas pela tarefa. As etiquetas servem para classificar a tarefa;

Original creation: criação da tarefa;

Status: status da tarefa;

Feedbacks

Aqui estão agrupadas as avaliações dos casos.

☐	NAME ▲	RATING	AUTHOR	CREATORS	LABELS	ORIGINAL CRE	STATUS	MARKING
--------------------------	--------	--------	--------	----------	--------	--------------	--------	---------

Nome: nome da avaliação;

Rating: avaliação;

Author: autor da avaliação;

Creators: criadores da avaliação;

Labels: etiquetas recebidas pela avaliação. As etiquetas servem para classificar a avaliação;

Original creation: criação da avaliação;

Status: status da avaliação;

Markings: marcações recebidas pela avaliação. As marcações servem para classificar o status da avaliação.

XDR - Threat Monitor - CTI - Observations

Aqui estão listados os elementos a serem observados.

Para buscar um resultado, utilize a barra de buscas. Você pode filtrar as buscas em **Add filter**.

Ao selecionar um elemento, a barra de ações aparece. As seguintes ações estão disponíveis:

Update (

Rule rescan (

Enrichment (

Merge (

Add in container (

Observables

Aqui estão listados os objetos observáveis, ou elementos imutáveis.

☐	TYPE	REPRESENTATION	AUTHOR	CREATORS	LABELS	PLATFORM CRI	MARKING
--------------------------	------	----------------	--------	----------	--------	--------------	---------

Type: tipo do objeto.

Representation: ID do objeto;

Author: Criador do objeto;

Creators: quem observou o objeto.

Labels: etiquetas recebidas pelo objeto. As etiquetas servem para classificar o objeto;

Platform creation date: data da criação do observável;

Markings: marcações recebidas pelo objeto. As marcações servem para classificar o status do objeto.

Artifacts

Aqui estão listados os artefatos, que são observáveis particulares.

☐	VALUE	FILE NAME	MIME/TYPE	FILE SIZE	AUTHOR	CREATORS	LABELS	PLATFORM CRI	MARKING
--------------------------	-------	-----------	-----------	-----------	--------	----------	--------	--------------	---------

Value: valor do artefato;

File name: nome do arquivo;

MIME/Type: tipo do artefato;

File size: tamanho do arquivo;

Author: Criador do artefato;

Creators: quem observou o artefato.

Labels: etiquetas recebidas pelo artefato. As etiquetas servem para classificar o artefato;

Platform creation date: data da criação do artefato;

Markings: marcações recebidas pelo artefato. As marcações servem para classificar o status do artefato.

Indicators

Aqui estão listados os indicadores, ou objetos de detecção.

☐	PATTERN TYPE	NAME	AUTHOR	CREATORS	LABELS	ORIGINAL CREATION DAT	MARKING
--------------------------	--------------	------	--------	----------	--------	-----------------------	---------

Pattern type: tipo de padrão de busca. Este padrão serve para identificar ameaças potenciais;

Name: nome do objeto;

Author: Criador do objeto;

Creators: quem criou o objeto.

Labels: etiquetas recebidas pelo objeto. As etiquetas servem para classificar o objeto;

Platform creation date: data da criação do objeto;

Markings: marcações recebidas pelo objeto. As marcações servem para classificar o status do objeto.

Infrastructures

Aqui estão listadas as infraestruturas, que são recursos utilizados por uma ameaça em suas atividades.

☐	NAME	TYPE	AUTHOR	CREATORS	LABELS	ORIGINAL CRE	MARKING
--------------------------	------	------	--------	----------	--------	--------------	---------

Name: nome do objeto;

Type: tipo do objeto;

Author: Criador do objeto;

Creators: quem criou o objeto.

Labels: etiquetas recebidas pelo objeto. As etiquetas servem para classificar o objeto;

Original creation date: data da criação do objeto;

Markings: marcações recebidas pelo objeto. As marcações servem para classificar o status do objeto.

XDR - Threat Monitor - CTI - Threats

Esta aba é parte biblioteca do CTI. Aqui estão listados verbetes de ameaças.

As ameaças estão divididas em:

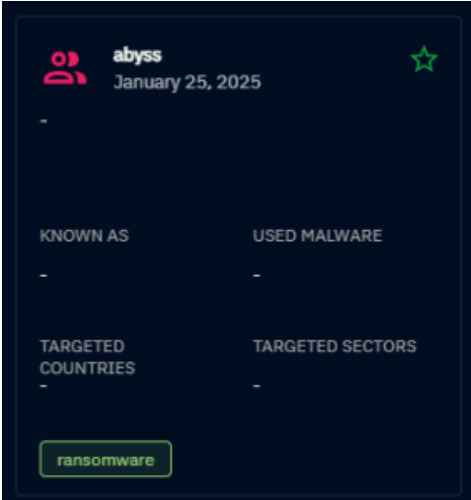
Threat actors (groups): grupos conhecidos por ataques.

Threat actors (individuals): indivíduos conhecidos por ataques.

Intrusion sets: atividades maliciosas consistentes, ou elementos técnicos e não-técnicos que correspondem com o quando, como e porquê da ação de uma ameaça;

Campaigns: séries de ataques que ocorrem durante um período ou com alvos consistentes.

Para buscar um resultado, utilize a barra de buscas. Você pode filtrar as buscas em **Add filter**.



Além do nome, data e labels, cada verbete recebe um card com as seguintes informações:

Known as: apelido da ameaça;

Used malware: malwares utilizados;

Targeted countries: países afetados;

Targeted sectors: setores afetados.

Ao clicar num label, você terá todas as informações presentes no CTI específicas para o verbete.

XDR - Threat Monitor - CTI - Arsenal

Esta aba é parte da biblioteca do CTI. Aqui estão listados os elementos para um ataque.
Para buscar um resultado, utilize a barra de buscas. Você pode filtrar as buscas em **Add filter**.

Malware

Malwares são qualquer pedaço de código feito para causar dano ou acessar indevidamente um sistema.
Aqui os malwares estão divididos por verbetes.



#HSTR:HackTool:Win32/Mimikatz

July 22, 2024

☆

KNOWN AS

-

CORRELATED INTRUSION SETS

-

TARGETED COUNTRIES

-

TARGETED SECTORS

Government

No label

Além do nome, data e labels, cada verbete recebe um card com as seguintes informações:

Known as: apelido da ameaça;

Correlated intrusion sets: conjuntos de intrusão relacionados;

Targeted countries: países afetados;

Targeted sectors: setores afetados.

Ao clicar num label, você terá todas as informações presentes no CTI específicas para o verbete.

Channels

Aqui estão listados os canais por onde os atores disseminam informações.

☐	NAME ▲	TYPES	LABELS	ORIGINAL CREATION DAT	MODIFICATION DATE
--------------------------	--------	-------	--------	-----------------------	-------------------

Name: nome do canal;

Type: tipo do canal;

Labels: etiquetas recebidas pelo canal. As etiquetas servem para classificar o canal;

Original creation date: data de criação do canal;

Modification date: data de modificação do canal;

Tools

Aqui estão listadas ferramentas legítimas que podem ser utilizadas em ataques.

☐	NAME ▲	TYPES	LABELS	ORIGINAL CREATION DAT	MODIFICATION DATE
--------------------------	--------	-------	--------	-----------------------	-------------------

Name: nome da ferramenta;

Type: tipo da ferramenta;

Labels: etiquetas recebidas pela ferramenta. As etiquetas servem para classificar a ferramenta;

Original creation date: data de criação da ferramenta;

Modification date: data de modificação da ferramenta;

Vulnerabilities

Aqui estão listadas as vulnerabilidades conhecidas que podem ser exploradas em um ataque.

☐	NAME ▲	CVSS3 - SEVERITY	LABELS	ORIGINAL CREATION DAT	MODIFICATION DATE	CREATORS
--------------------------	--------	------------------	--------	-----------------------	-------------------	----------

Name: nome da vulnerabilidade;

CVSS3 - Severity: severidade da vulnerabilidade;

Labels: etiquetas recebidas pela vulnerabilidade. As etiquetas servem para classificar a vulnerabilidade;

Original creation date: data de criação da vulnerabilidade;

Modification date: data de modificação da vulnerabilidade;

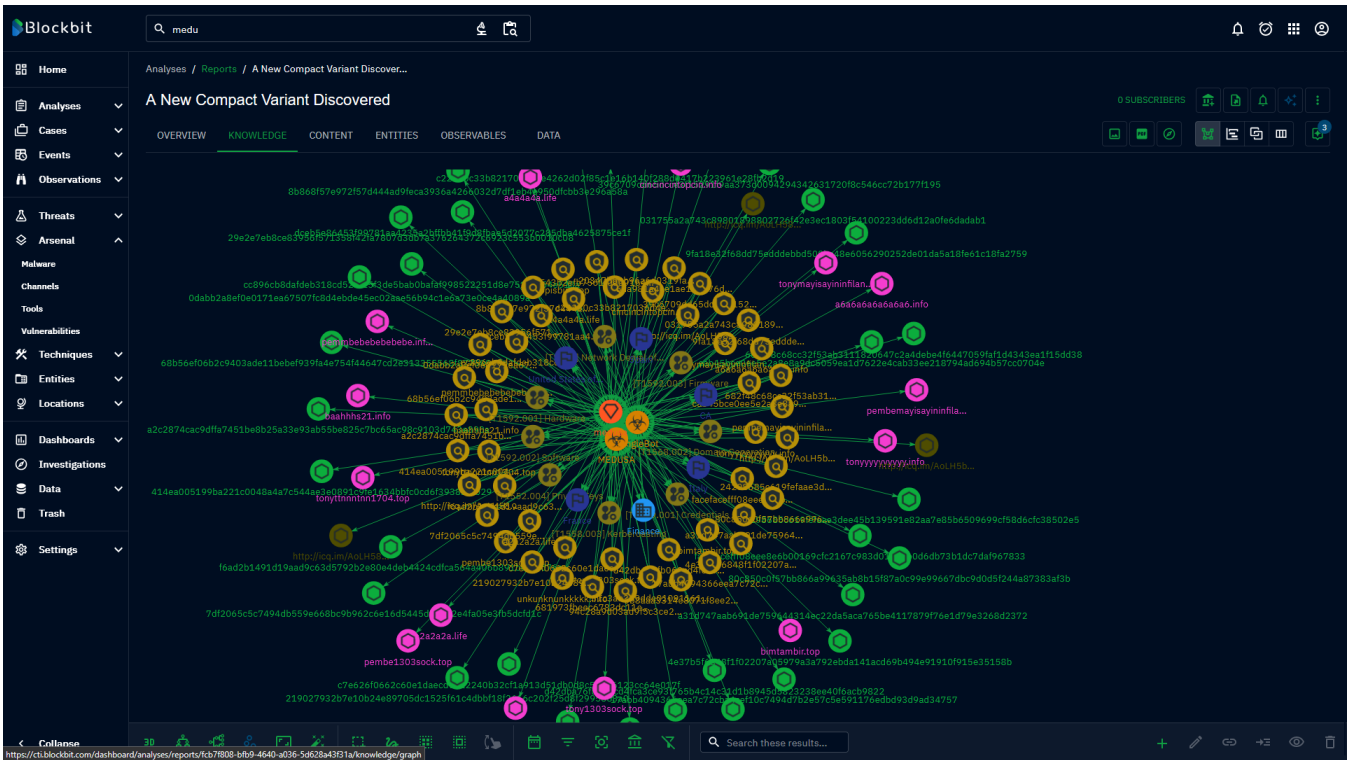
Creators: quem criou o verbete da vulnerabilidade.

KNOWLEDGE sobre o Ransomware Medusa

A imagem mostra uma representação gráfica de inteligência cibernética gerada a partir da análise de uma amostra do ransomware Medusa, exibida na aba "Knowledge" do módulo Arsenal do OpenCTI.

No centro do gráfico está o nó principal, representando a amostra ou campanha de ataque associada ao Medusa. A partir dele, são mapeadas múltiplas conexões com entidades relacionadas como:

- **Técnicas Táticas e Procedimentos (TTPs):** métodos usados pelo ransomware, como movimentação lateral, execução de payloads e evasão de defesa.
- **Indicadores (IOCs):** domínios, IPs, hashes, e artefatos identificados como parte da cadeia de ataque.
- **Infraestruturas:** domínios e servidores usados como C2 (Command and Control), além de destinos de exfiltração de dados ou para entrega de payloads.
- Atores ou grupos de ameaça com comportamento semelhante ou histórico ligado a ataques com o Medusa.
- Campanhas, observações e malwares relacionados, criando um ecossistema visual do ataque.



XDR - Threat Monitor - CTI - Techniques

Esta aba é parte da biblioteca do CTI. Aqui estão listadas as técnicas para um ataque.

Para buscar um resultado, utilize a barra de buscas. Você pode filtrar as buscas em **Add filter**.

Attack patterns

Aqui estão listados os padrões de ataque utilizados por uma ameaça. Esses padrões são baseados no [MITRE ATT&CK](#).

☐	KILL CHAIN PHASE	ID	NAME ^	LABELS	ORIGINAL CREATION DAT	MODIFICATION DATE
--------------------------	------------------	----	--------	--------	-----------------------	-------------------

Kill chain phase: fase do MITRE ATT&CK;

ID: identificador;

Name: nome do padrão

Labels: etiquetas recebidas. As etiquetas servem para classificar o padrão;

Original creation date: data de criação do padrão;

Modification date: data de modificação do padrão;

Além disso, estão listadas:

Narratives: são as narrativas utilizadas por atores para um ataque;

Course of action: ações tomadas para prevenir ou responder um ataque;

Data components: valores de uma fonte de dados que podem ser detectados;

Data sources: fontes de dados que podem ser coletados.

São classificados por:

☐	NAME ^	LABELS	ORIGINAL CREATION DAT	MODIFICATION DATE
--------------------------	--------	--------	-----------------------	-------------------

Name: nome do elemento

Labels: etiquetas recebidas. As etiquetas servem para classificar o elemento;

Original creation date: data de criação do elemento;

Modification date: data de modificação do elemento;

XDR - Threat Monitor - CTI - Entities

Esta aba é parte da biblioteca do CTI. Aqui estão listadas as entidades que podem estar envolvidas em um ataque.

Para buscar um resultado, utilize a barra de buscas. Você pode filtrar as buscas em **Add filter**.

Sectors

Aqui estão listados os setores que podem ser alvo de um ataque.

	Academic Institutions	This sector does not have any description.
	Accounting	This sector does not have any description.

São listados por **Tipo** e uma descrição.

Events

Aqui estão listados eventos no mundo real.

NAME ▾	TYPES	START DATE	END DATE	ORIGINAL CREATION DATE
--------	-------	------------	----------	------------------------

Name: nome do evento;

Type: tipo do evento;

Start date: data do começo do evento;

End date: data do fim do evento;

Original creation date: data de criação do evento;

Organizations

Aqui estão listadas organizações no mundo real.

NAME ▾	LABELS	ORIGINAL CREATION DATE	MODIFICATION DATE
--------	--------	------------------------	-------------------

Name: nome da organização;

Labels: etiquetas recebidas pela organização. As etiquetas servem para classificar a organização;

Original creation date: data de criação da organização;

Modification date: data de modificação da organização;

Systems

Aqui estão listados sistemas e tecnologias

NAME ▾	LABELS	ORIGINAL CREATION DATE	MODIFICATION DATE
--------	--------	------------------------	-------------------

Name: nome do sistema;

Labels: etiquetas recebidas pelo sistema. As etiquetas servem para classificar o sistema;

Original creation date: data de criação do sistema;

Modification date: data de modificação do sistema;

Individuals

Aqui estão listados indivíduos.

NAME ▼	LABELS	ORIGINAL CREATION DATE	MODIFICATION DATE
--------	--------	------------------------	-------------------

Name: nome do indivíduo ;

Labels: etiquetas recebidas pelo indivíduo. As etiquetas servem para classificar o indivíduo;

Original creation date: data de criação do indivíduo;

Modification date: data de modificação do indivíduo;

XDR - Threat Monitor - CTI - Locations

Esta aba é parte da biblioteca do CTI. Aqui estão listadas localidades do mundo real.

Para buscar um resultado, utilize a barra de buscas. Você pode filtrar as buscas em **Add filter**.

NAME ▼	ORIGINAL CREATION DATE	MODIFICATION DATE
--------	------------------------	-------------------

Name: nome da localidade;

Original creation date: data de criação da localidade;

Modification date: data de modificação da localidade;

As localidades são divididas em:

Regions: grandes áreas, como continentes;

Countries: países do mundo;

Areas: regiões extensas, como unidades subnacionais;

Cities: cidades do mundo;

Positions: localidade precisa no globo.

XDR - Threat Monitor - CTI - Events

Nesta página, estão agrupados todos os eventos.

Para buscar um resultado, utilize a barra de buscas. Você pode filtrar as buscas em **Add filter**.

Ao selecionar um elemento, a barra de ações aparece. As seguintes ações estão disponíveis:

- Update** (🔧): atualizar;
- Rule rescan** (🔍): escanear novamente a regra;
- Enrichment** (🔄): buscar novos dados;
- Merge** (👤): fundir dados;
- Add in container** (📁): adicionar dados a um contêiner.

Incidents

Aqui estão listados os Incidentes, que são eventos negativos ocorrendo no sistema.

☐	NAME	INCIDENT	SEVERITY	ASSIGNEES	CREATORS	LABELS	ORIGINAL CRE	STATUS	MARKING
--------------------------	------	----------	----------	-----------	----------	--------	--------------	--------	---------

- Name:** nome do incidente;
- Incident type:** tipo do incidente;
- Severity:** severidade do incidente;
- Assignees:** responsáveis pelo incidente;
- Creators:** criadores do aviso do incidente;
- Labels:** etiquetas recebidas pelo incidente. As etiquetas servem para classificar o incidente;
- Original creation date:** data da criação do incidente;
- Status:** status do incidente;
- Markings:** marcações recebidas pelo incidente. As marcações servem para classificar o status do incidente.

Sightings

Aqui estão listados os avistamentos, que são eventos observáveis ocorrendo no sistema. Cada avistamento é tratado como **entidade**.

☐	QUALIFICATION	N	NAME	ENTITY TYPE	ENTITY	FIRST OBS.	LAST OBS. ▼	CONFIDENCE	STATUS
--------------------------	---------------	---	------	-------------	--------	------------	-------------	------------	--------

- Qualification:** qualificação da entidade. Pode ser **false positive** (falso positivo) ou **true positive** (positiva).
- Nb.:** entidades filtradas.
- Name:** nome da entidade;
- Entity type:** tipo da entidade;
- Entity:** entidade;
- First obs.:** data da primeira aparição;
- Last obs.:** data da última aparição;
- Confidence:** confiabilidade da informação;

Status: status do avistamento;

Observed data

Aqui estão listados os extratos de um log que contém dados a serem observados.

☐	NAME	NB.	FIRST OBS.	LAST OBS. ▼	AUTHOR	LABELS	MARKING
--------------------------	------	-----	------------	-------------	--------	--------	---------

Name: nome do dado observável;

Nb.: dados filtrados.

First obs.: data da primeira aparição;

Last obs.: data da última aparição;

Author: autor da observação;

Labels: etiquetas recebidas pela observação. As etiquetas servem para classificar a observação;

Markings: marcações recebidas pela observação. As marcações servem para classificar o status da observação.

XDR - Threat Monitor - CTI - Data

Nesta aba, você pode consultar comportamento, relações e ingestão de dados.

Entities

Aqui, você pode consultar [entidades](#).

☐	TYPE	NAME	AUTHOR	CREATORS	LABELS	PLATFORM CREATION DATE	MARKING
--------------------------	------	------	--------	----------	--------	------------------------	---------

- Type:** tipo da entidade;
- Name:** nome de entidade;
- Author:** autor da entidade;
- Creators:** criador da entidade;
- Labels:** etiquetas recebidas pela entidade. As etiquetas servem para classificar a entidade;
- Platform creation date:** data de criação;
- Markings:** marcações recebidas pela entidade. As marcações servem para classificar o status da entidade.

Relationships

Aqui estão listadas as relações criadas entre diversos dados.

☐	FROM TYPE	FROM NAME	TYPE	TO TYPE	TO NAME	AUTHOR	CREATOR	PLATFORM CREATION DATE	MARKING
--------------------------	-----------	-----------	------	---------	---------	--------	---------	------------------------	---------

- As relações são classificadas por:
- From type:** tipo de origem;
- From name:** nome de origem;
- Type:** tipo da relação;
- To type:** tipo de destino;
- To name:** nome de destino;
- Author:** autor da relação;
- Creators:** criador da relação;
- Platform creation date:** data de criação;
- Markings:** marcações recebidas pela relação. As marcações servem para classificar o status da relação.

Ingestion

Nesta aba, você pode consultar os fluxos de ingestão de dados (streams e feeds).

 Workers statistics

3

CONNECTED WORKERS

0

QUEUED BUNDLES

0/s

BUNDLES PROCESSED

257.4/s

READ OPERATIONS

0.2/s

WRITE OPERATIONS

241.09M

TOTAL NUMBER OF DOCUMENTS

 Registered connectors

#	NAME	TYPE	AUTOMATIC TRIGGER	MESSAGES	STATUS	MODIFIED
---	------	------	-------------------	----------	--------	----------

Workers statistics: aqui estão estatísticas dos fluxos conectados:

Connected workers: fluxos conectados.

Queued bundles: conjuntos na fila;

Bundles processed: conjuntos processados;

Read operations: número de operações do tipo **read** por segundo;

Write operations: número de operações do tipo **Write** por segundo;

Total number of documents: número total de documentos.

Os conectores registrados são listados por:

Name: nome do conector;

Type: tipo do conector;

Automatic trigger:

Messages: número de mensagens recebidas;

Status: status do conector;

Modified: data de modificação do conector.

A ingestão pode vir das seguintes fontes:

OpenCTI Streams: streams do OpenCTI.

TAXII feeds: feeds criados usando protocolo TAXII (Trusted Automated eXchange of Intelligence Information);

TAXII streams: streams criados usando protocolo TAXII (Trusted Automated eXchange of Intelligence Information);

RSS feeds: feeds criados usando o formato RSS (*Rich Site Summary*);

CSV feeds: feeds criados usando o formato CSV (*comma-separated value*).

Import

Aqui, você pode importar arquivos.



Para importar um arquivo, clique na nuvem (



Para copiar e colar os conteúdos do arquivo, clique neste ícone: .

NAME	CREATOR	LABELS	MODIFICATION DATE
------	---------	--------	-------------------

Os arquivos são classificados em:

Name: nome do objeto;

Creators: criador do objeto;

Labels: etiquetas recebidas pelo arquivo. As etiquetas servem para classificar o arquivo;

Modification date: data de modificação do arquivo;

Processing

Aqui você pode conferir as tarefas.

IN PROGRESS TASKS	
	No task
COMPLETED TASKS	
	No task

In progress tasks: tarefas em andamento;

Completed tasks: tarefas completas.

Data sharing

Aqui estão listados os streams e feeds RSS e TAXII.

RSS

NAME ▼	DESCRIPTION	STREAM ID	PUBLIC	STATUS	FILTERS
--------	-------------	-----------	--------	--------	---------

Name: nome do stream;

Description: descrição do stream;

Stream ID: ID do stream;

Public: diz se o stream é público ou não;

Status: status do stream;

Filters: filtros aplicados no stream.

TAXII

NAME ▼	DESCRIPTION	COLLECTION	FILTERS
--------	-------------	------------	---------

Name: nome do stream ou feed;

Description: descrição do stream ou feed;

Collection: tipo. Pode ser stream ou feed;

Filters: filtros aplicados no stream.

XDR - Threat Monitor - CTI - Trash

Aqui estão listados os elementos descartados.

☐	TYPE	REPRESENTATION	DELETED BY	DELETION DATE ▲	MARKING
--------------------------	------	----------------	------------	-----------------	---------

Type: tipo do elemento;

Representation: ID do elemento;

Deleted by: quem deletou o elemento;

Deletion date: quando o elemento foi deletado;

Marking: marcações recebidas pelo elemento. As marcações servem para classificar o status do elemento.

XDR - Threat Monitor - CTI - Settings

Aqui estão listadas as etiquetas e marcações.
Para buscar um resultado, utilize a barra de buscas.

Security

Aqui são listadas as etiquetas de entidades.

TYPE	DEFINITION ▾	COLOR	ORDER	ORIGINAL CREATION ...
------	--------------	-------	-------	-----------------------

- Type: tipo da etiqueta;
- Definition: definição da etiqueta;
- Color: cor da etiqueta;
- Order: ordem da etiqueta;
- Original creation: data da criação da etiqueta.

Para criar uma nova etiqueta, clique no + no canto inferior direito da tela ().

Type

Definition

Color

Order

CANCELCREATE

- Determine:
- Type: tipo da etiqueta;
 - Definition: definição da etiqueta;
 - Color: cor da etiqueta;
 - Order: ordem da etiqueta;

Para criar, clique em **create** (.

Para cancelar, clique em **cancel** (.

Taxonomies

Aqui estão listadas as etiquetas de taxonomia.

☐ VALUE ▴	COLOR	PLATFORM CREATION DATE
----------------------------------	-------	------------------------

Value: valor da etiqueta

Color: cor da etiqueta;

Platform creation date: data da criação da etiqueta.



Para criar uma nova etiqueta, clique no + no canto inferior direito da tela ().

Value

Color

CANCEL

CREATE

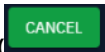
Determine:

Value: valor da etiqueta

Color: cor da etiqueta;



Para criar, clique em **create** ().



Para cancelar, clique em **cancel** ().

Kill chain phases

Aqui estão listadas as etiquetas de fases do ataque

☐	KILL CHAIN NAME	PHASE NAME	ORDER ▲	ORIGINAL CREATIO
--------------------------	-----------------	------------	---------	------------------

Kill chain name: nome da fase no MITRE ATT&CK;

Phase name: tipo da fase;

Order: ordem da etiqueta;

Original creation: data da criação da etiqueta.



Para criar uma nova etiqueta, clique no + no canto inferior direito da tela ().

Kill chain name

Phase name

Order

CANCEL

CREATE

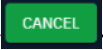
Determine:

Kill chain name: nome da fase no MITRE ATT&CK;

Phase name: tipo da fase;

Order: ordem da etiqueta;

Para criar, clique em **create** ().

Para cancelar, clique em **cancel** (.

Vocabularies

Aqui estão listados os Vocabulário.

NAME ▾	USED IN	DESCRIPTION
--------	---------	-------------

Name: nome do vocabulário;

Used in: onde ela é usado;

Description: descrição do vocabulário;

Ao clicar em qualquer categoria, você irá para uma lista de entradas.

☐	NAME ▾	USED IN	ALIASES	DESCRIPTION	USAGES	ORDER
--------------------------	--------	---------	---------	-------------	--------	-------

Name: nome da entrada;

Used in: onde ela é usada;

Aliases: outros nomes que a entrada é conhecida;

Description: descrição da entrada;

Usages: número de usos da entrada;

Order: ordem da entrada.

Status templates

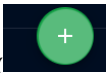
Aqui estão listadas etiquetas de status.

NAME ▲	COLOR	USAGES
--------	-------	--------

Name: nome da etiqueta de status;

Color: cor da etiqueta de status;

Usages: número de usos da da etiqueta de status;

Para criar uma nova etiqueta, clique no + no canto inferior direito da tela (.

A dark-themed form with two input fields: 'Name' and 'Color'. The 'Color' field has a color palette icon to its right. At the bottom right, there are two buttons: a green 'CANCEL' button and a blue 'CREATE' button.

Determine:

Name: nome da etiqueta de status;

Color: cor da etiqueta de status;

Para criar, clique em **create** ().

Para cancelar, clique em **cancel** ().

Case templates

Aqui estão listadas etiquetas de casos.

NAME ▲	DESCRIPTION	TASKS
--------	-------------	-------

Name: nome da etiqueta;

Description: descrição da etiqueta:

Tasks: tarefas relacionadas à etiqueta.

Para criar uma nova etiqueta, clique no + no canto inferior direito da tela (.

A dark-themed form for creating a case template. It has three main sections: 'Name' (a single-line text input), 'Description' (a rich text editor with a toolbar containing 'Write', 'Preview', bold, italic, underline, link, quote, code, image, list, and table icons), and 'Tasks' (a list input with a '+' and a dropdown arrow). At the bottom right, there are two buttons: a green 'CANCEL' button and a blue 'CREATE' button.

Determine:

Name: nome da etiqueta;

Description: descrição da etiqueta:

Tasks: tarefas relacionadas à etiqueta.

Para criar, clique em **create** ().

Para cancelar, clique em **cancel** ().

Users

Aqui estão listados os usuários da plataforma.

NAME ▾	EMAIL	FIRSTNAME	LASTNAME	MAX CONFIDENCE	2FA	PLATFORM CREATION ...
--------	-------	-----------	----------	----------------	-----	-----------------------

Name: nome do usuário;

Email: e-mail do usuário;

First name: primeiro nome do usuário;

Last name: último sobrenome do usuário;

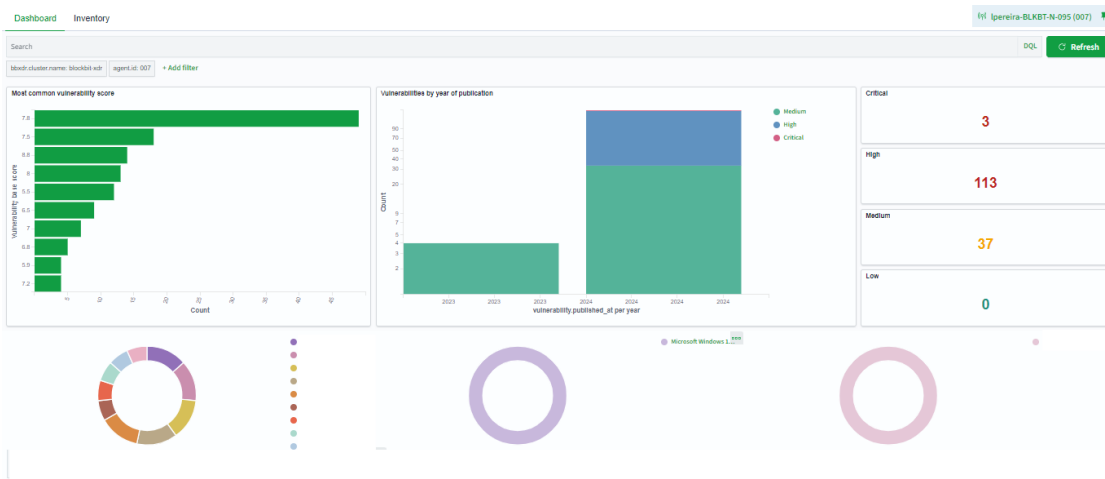
Max confidence: confiança máxima do usuário;

2FA: indica se o usuário habilitou autenticação de dois fatores;

Platform creation: data de criação do perfil do usuário.

XDR - Vulnerability detection

Nesta página, você pode conferir as vulnerabilidades detectadas pelos agentes.



Search

A barra permite buscar por eventos específicos. Para mais informações, confira [Sistema de buscas](#).

Clique em **Explore agent** para selecionar o agente. Para mais informações, confira [Agentes](#).

Ao passar o mouse sobre algum elemento, este botão aparece: . Ao clicar nele, você pode visualizar dados ou requisições. Ao clicar em Download CSV, você pode baixar um arquivo CSV com os dados.

As vulnerabilidades são classificadas por severidade:

Critical: Crítica;

High: Alta;

Medium: Média;

Low: Baixa.

As vulnerabilidades são filtradas por severidade ao clicar em cada classificação.

Abaixo, estão listados dados relevantes sobre vulnerabilidades. São mostrados os elementos e o número de vezes que aparecem. Você pode classificar os dados por ordem ascendente ou descendente.

Top 5 vulnerabilities: são mostradas as vulnerabilidades que mais aparecem;

Top 5 OS: são mostrados os sistemas operacionais com mais vulnerabilidades;

Top 5 agents: são mostrados os agentes com mais vulnerabilidades;

Top 5 packages: são mostrados os pacotes com mais vulnerabilidades.

Há também gráficos com dados sobre vulnerabilidades.

Most common vulnerability score: mostra a classificação de severidade mais comum das vulnerabilidades detectadas. Vai de 0 (baixa) a 10 (crítica);

Most vulnerable OS families: classifica famílias de sistemas operacionais por número de vulnerabilidades detectadas;

Vulnerabilities by year of publication: mostra o número de vulnerabilidades detectadas pelo ano de publicação e severidade.

XDR - Vulnerability detection - Inventory

Aqui são listadas as vulnerabilidades encontradas na rede.

Search

bxdr.cluster.name: blockbit-xdr

+ Add filter

DQL

Refresh

72,731 hits

Export Formated

47 columns hidden

Density

Sort fields

Full screen

agent.name	package.name	package.version	vulnerability.description	vulnerability.severity	vulnerability.id
	kernel-devel		In the Linux kernel, the following vulne...		
	kernel-devel		In the Linux kernel, the following vulne...	Medium	
	kernel-devel		In the Linux kernel, the following vulne...		
	kernel-devel		In the Linux kernel, the following vulne...		
	kernel-devel		In the Linux kernel, the following vulne...		
	kernel-devel		In the Linux kernel, the following vulne...	Medium	
	kernel-devel		A flaw was found in the Linux kernel's ...	Medium	
	kernel-devel		In the Linux kernel, the following vulne...		
	kernel-devel		In the Linux kernel, the following vulne...		
	kernel-devel		An issue was discovered in drivers/tty/...	Medium	
	kernel-devel		In the Linux kernel, the following vulne...		
	kernel-devel		In the Linux kernel, the following vulne...		

Search

A barra permite buscar por eventos específicos. Para mais informações, confira [Sistema de buscas](#).

Clique em **Explore agent** para selecionar o agente. Para mais informações, confira [Agentes](#).

Em **Refresh**, você pode recarregar a lista.

No cabeçalho, há o número de vulnerabilidades.

72,731 hits

Export Formated

47 columns hidden

Density

Sort fields

Full screen

Em **Export formatted**, você pode exportar um arquivo .csv com a lista de agentes;

Em **Columns hidden**, você pode adicionar ou retirar colunas. As colunas são baseadas nos dados coletados. Para mais informações, visite [Dados Coletados](#);

Em **Density**, você pode selecionar a densidade das informações mostradas;

Em **Sort fields**, você pode reordenar os campos que aparecem;

Em **Full screen**, você pode ligar o modo tela cheia.

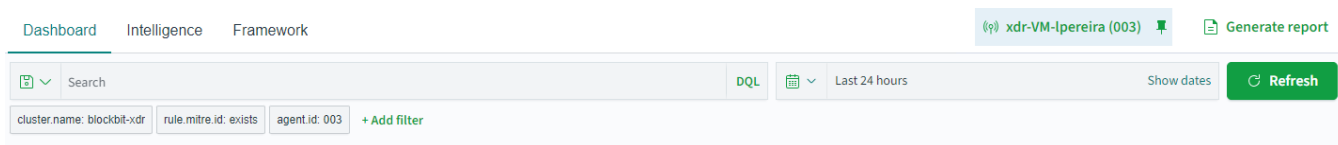
XDR - MITRE ATT&CK

Você pode pesquisar e visualizar indicadores de comprometimento (IoCs) dentro do ambiente monitorado pelo Blockbit XDR. Os alertas são classificados automaticamente de acordo com táticas e técnicas do MITRE ATT&CK, permitindo que analistas de segurança compreendam a progressão do ataque e investiguem sua origem.

Ao identificar um IoC, o Blockbit XDR permite criar uma linha do tempo detalhada do incidente, correlacionando eventos e mostrando a trajetória da ameaça dentro da rede. Isso possibilita a detecção de padrões de ataque, identificação de vetores de intrusão e resposta rápida a ameaças persistentes.

Para mais informações, visite a página [MITRE ATT&CK](#).

Esta seção é dividida em 3 abas:



Dashboard: gráficos de eventos classificados pelo MITRE ATT&CK.

Intelligence: biblioteca com informações de agentes maliciosos, ataques, recursos, técnicas e mitigações.

Framework: permite conferir e filtrar alertas por táticas e técnicas.

Search

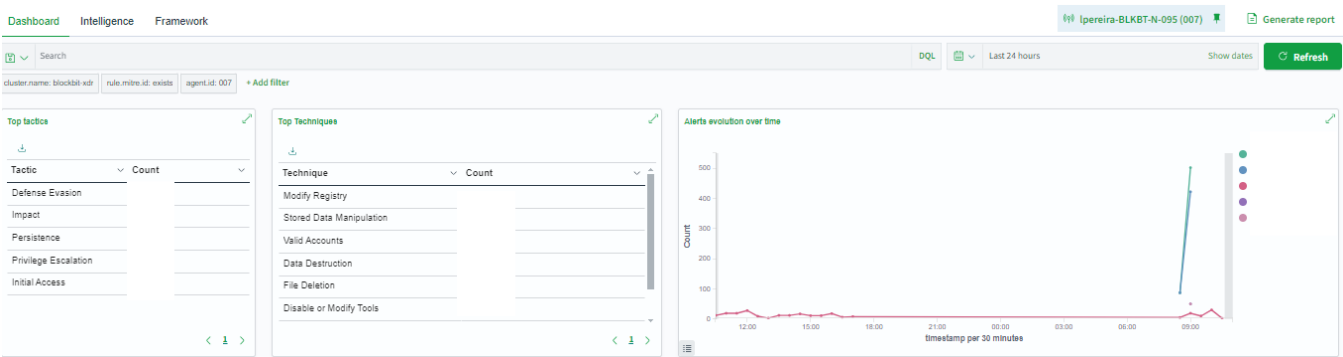
A barra permite buscar por eventos específicos. Para mais informações, confira [Sistema de buscas](#).

Clique em **Explore agent** para selecionar o agente. Para mais informações, confira [Agentes](#).

Para criar um relatório, clique em **Generate report**. Os relatórios são armazenados em [Reports](#).

XDR - MITRE ATT&CK - Dashboard

No **Dashboard**, você pode conferir gráficos relativos a cada tipo de ameaça catalogado no MITRE ATT&CK.



Em **Top tactics**, são elencadas as táticas que mais geraram alertas;

Em **Top techniques**, são elencadas as técnicas que mais geraram alertas;

Em **Alerts evolution over time**, são mostrados alertas por tipo em intervalos de 30 minutos.

XDR - MITRE ATT&CK - Framework

O Blockbit XDR oferece um sistema avançado de correlação automática de alertas, agrupando eventos relacionados ao mesmo ataque para uma análise mais eficiente e uma resposta rápida a incidentes. A solução permite que administradores personalizem as configurações por grupos de endpoints, garantindo que as políticas de detecção e resposta sejam aplicadas de acordo com a criticidade de cada ambiente monitorado.

Blockbit

MITRE ATT&CK

Explore agent

DashboardIntelligenceFramework

SearchDQLLast 24 hoursShow datesRefresh

cluster.name: blockbit-xdrrule.mitre.id: existsAdd filter

IMPACT

EXFILTRATION

Fast Flux DNS0Application Layer Protocol0Custom Cryptographic Prot...0Remote Access Software0Multilayer Encryption0Traffic Signaling0Standard Cryptographic Pr...0Protocol Tunneling0Domain Generation Algorit...0Mail Protocols0Communication Through R...0External Proxy0Proxy0Dynamic Resolution0

COLLECTION

LATERAL MOVEMENT

Data Destruction14135Stored Data Manipulation6119Account Access Removal4Service Stop3Disk Structure Wipe0Direct Network Flood0Stored Data Manipulation0External Defacement0OS Exhaustion Flood0Application Exhaustion Flood0Disk Wipe0Application or System Expl...0Disk Structure Wipe0

Exfiltration Over Web Service0Scheduled Transfer0Exfiltration Over Other Net...0Exfiltration Over Bluetooth0Automated Exfiltration0Exfiltration Over Symmetric...0Traffic Duplication0Exfiltration to Code Reposit...0Exfiltration Over Asymmetri...0Exfiltration Over C2 Channel0Exfiltration Over Alternative...0Exfiltration over USB0Data Compressed0

Archive via Utility0Screen Capture0Adversary-in-the-Middle0Keylogging0Data from Configuration Re...0Sharepoint0Audio Capture0Archive via Custom Method0Email Collection0Data from Removable Media0Local Data Staging0Local Email Collection0Automated Collection0

Lateral Tool TransferRemote ServicesExploitation of Remote Ser...Remote Desktop ProtocolVNCTaint Shared ContentApplication Access TokenSSHSshApplication Deployment So...Replication Through Remo...SSH HijackingSMB/Windows Admin SharesUse Alternate Authentication...

Blockbit

MITRE ATT&CK

Explore agent

DashboardIntelligenceFramework

SearchDQLLast 24 hoursShow datesRefresh

cluster.name: blockbit-xdrrule.mitre.id: existsAdd filter

LATERAL MOVEMENT

DISCOVERY

CREDENTIAL ACCESS

DEFENSE EVASION

PRIVILEGE ESCALATION

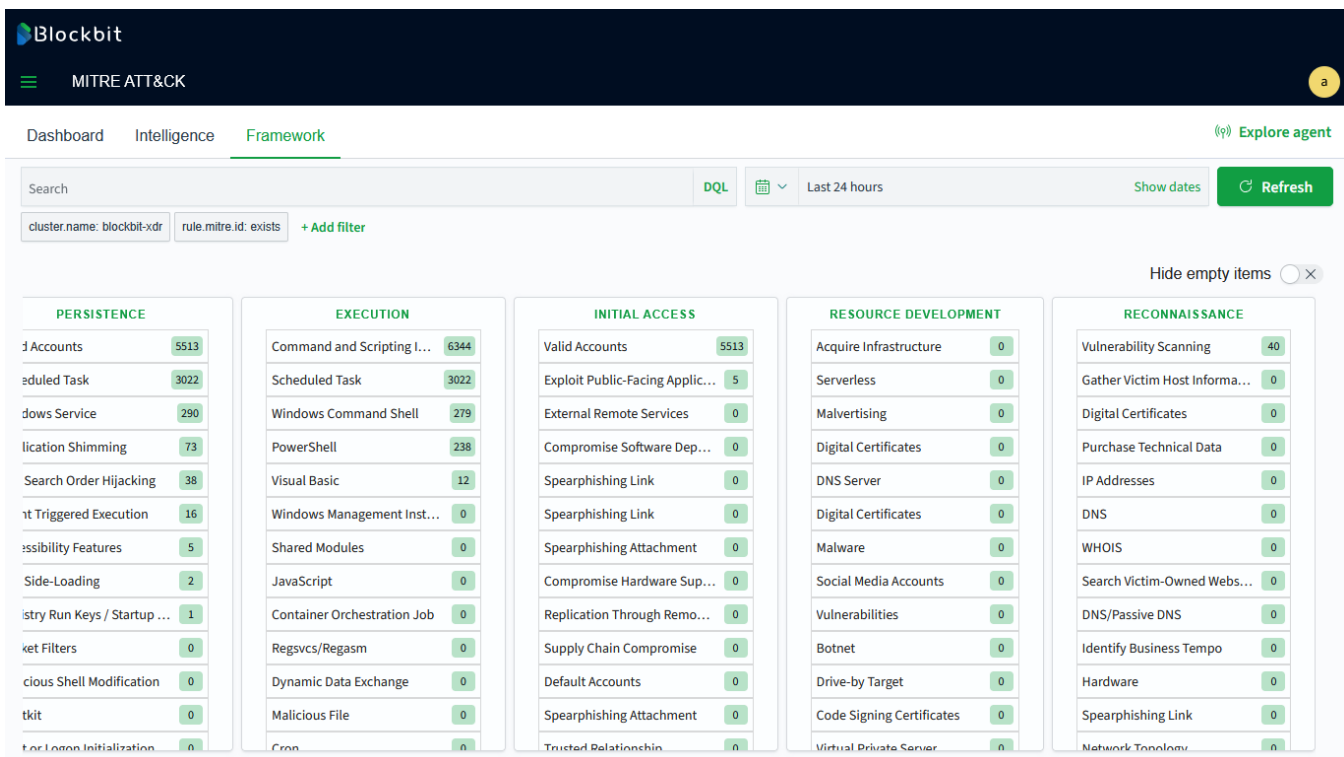
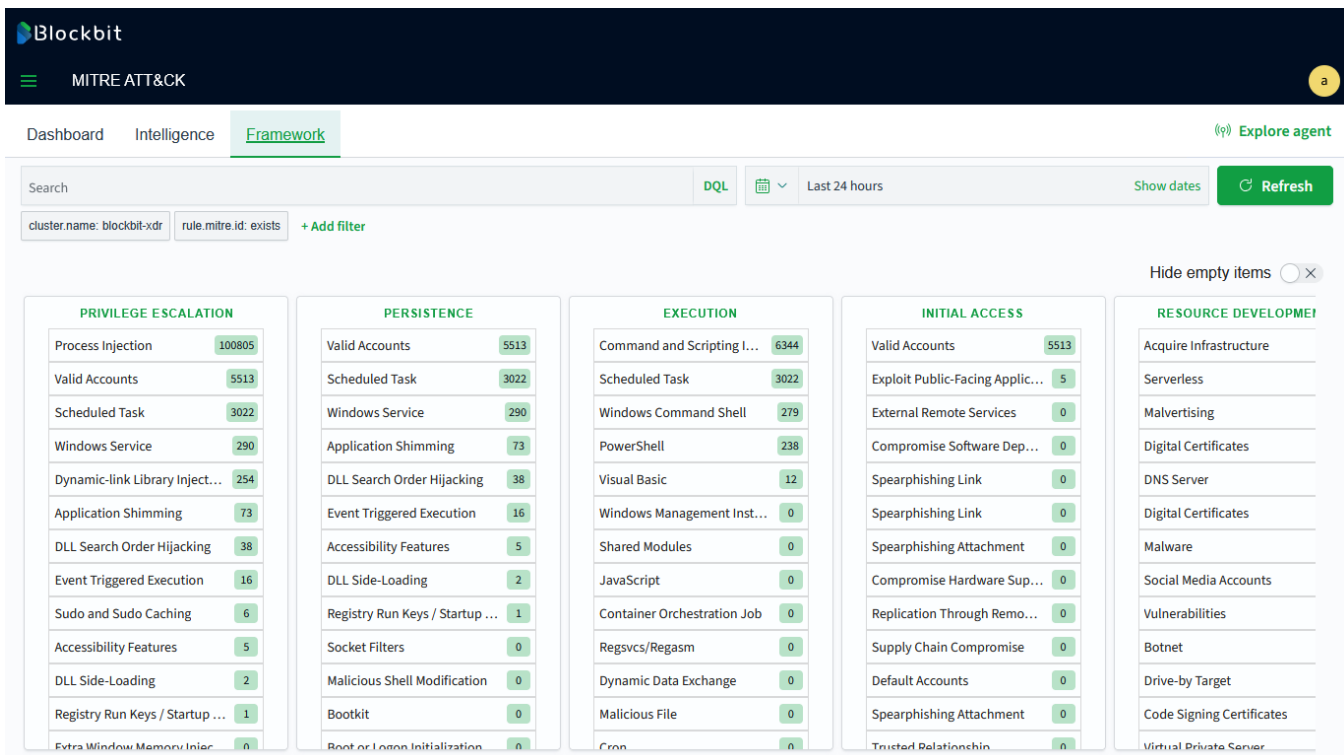
Lateral Tool Transfer384Remote Services11Exploitation of Remote Ser...7Remote Desktop Protocol1VNCTaint Shared Content0Application Access Token0SSHSshApplication Deployment So...Replication Through Remo...SSH HijackingSMB/Windows Admin SharesUse Alternate Authentication0

Account Discovery1046File and Directory Discovery4System Owner/User Discov...0Container and Resource Dis...0Internet Connection Discov...0Permission Groups Discovery0Cloud Groups0Group Policy Discovery0Device Driver Discovery0Domain Account0Security Software Discovery0Local Account0Custom Checks0

LSASS Memory2Password Guessing1Adversary-in-the-Middle0Pluggable Authentication M...0Keylogging0OS Credential Dumping0LLMNR/NBT-NS Poisoning a...0Steal Web Session Cookie0Security Account Manager0Cloud Instance Metadata API0Securityd Memory0Cloud Instance Metadata API0Password Cracking0

Process Injection100805File Deletion14157Modify Registry6887Valid Accounts5513Dynamic-link Library Inject...254Disable or Modify Tools219Obfuscated Files or Inform...142DLL Search Order Hijacking38System Binary Proxy Execut...16Sudo and Sudo Caching6DLL Side-Loading2DLL Side-Loading2Extra Window Memory Injec0

Process Injection1Valid AccountsScheduled TaskWindows ServiceDynamic-link Library Inject...Application ShimmingDLL Search Order HijackingEvent Triggered ExecutionSudo and Sudo CachingAccessibility FeaturesDLL Side-LoadingRegistry Run Keys / Startup ...Extra Window Memory Injec...



A lista completa das técnicas do Framework Mitre:

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access

- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Nesta página, os alertas são classificados automaticamente por táticas e técnicas, permitindo que os analistas compreendam o padrão e o comportamento da ameaça. Cada técnica agrupa as táticas relacionadas, proporcionando uma visão estruturada da evolução do ataque.

- A barra Search permite buscar eventos específicos, facilitando a investigação de ameaças.
- A opção "Hide techniques with no alerts" pode ser ativada para ocultar técnicas sem alertas, permitindo um foco maior nas ameaças ativas.
- Ao passar o mouse sobre uma técnica, aparecem opções de interação e investigação detalhada, possibilitando a tomada de decisões ágeis.



Show in dashboard (): irá criar um dashboard específico para esta técnica.



Inspect in security events (): irá abrir a página Security events com dados específicos da técnica.

Ao clicar em cada técnica, você abrirá uma lista das últimas vezes que eventos na categoria foram detectados.

Technique details

ID

T1078.002

Tactics

Persistence

Privilege Escalation

Defense Evasion

Initial Access

Version

1.3

No topo, há o ID da técnica e as táticas a ela associada.

Search	DQL	 Last 24 hours	Show dates	 Refresh	
+ Add filter					
Time ↓	Technique(s)	Tactic(s)	Level	Rule ID	Description
> Aug 15, 2024 @ 10:01:52.675	T1021.001	Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	92653	User: BLOCKBIT\pereira logged using Remote Desktop Connection (RDP) from ip:172.28.0.25.
	T1078.002				
> Aug 15, 2024 @ 10:01:52.586	T1021.001	Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	92653	User: BLOCKBIT\pereira logged using Remote Desktop Connection (RDP) from ip:172.28.0.25.
	T1078.002				
> Aug 15, 2024 @ 09:28:43.656	T1021.001	Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	92653	User: BLOCKBIT\pereira logged using Remote Desktop Connection (RDP) from ip:172.28.0.25.
	T1078.002				
> Aug 15, 2024 @ 09:28:43.449	T1021.001	Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	92653	User: BLOCKBIT\pereira logged using Remote Desktop Connection (RDP) from ip:172.28.0.25.
	T1078.002				

Abaixo, estão os eventos mais recentes onde a técnica foi detectada, classificados por horário, técnicas conjuntas, táticas associadas, nível, ID da regra e descrição.

XDR - MITRE ATT&CK - Intelligence

Em **Intelligence**, você vai encontrar uma biblioteca com informações sobre agentes maliciosos, ataques, recursos, técnicas e mitigações.

GROUPS	MITIGATIONS	SOFTWARE	TACTICS
APT38	Password Filter DLL Mitigation	HDoor	Credential Access
Indrik Spider	Space after Filename Mitigation	TrickBot	Execution
NEODYMIUM	HISTCONTROL Mitigation	PowerDuke	Impact
Elderwood	Credentials in Files Mitigation	EKANS	Persistence
SideCopy	Exploitation for Credential Access Mitigation	BLINDINGCAN	Privilege Escalation
GALLIUM	Query Registry Mitigation	Wiarp	Lateral Movement
APT17	Login Item Mitigation	RCSession	Defense Evasion
APT3	Setuid and Setgid Mitigation	Spark	Exfiltration
GCMAN	Compiled HTML File Mitigation	QuietSieve	Discovery
Kimsuky	Data Destruction Mitigation	SynAck	Collection
EXOTIC LILY	Windows Management Instrumentation Event Subscription Mitigation	Bumblebee	Resource Development
admin@338	File System Permissions Weakness Mitigation	MURKYTOP	Reconnaissance
Patchwork	Applnit DLLs Mitigation	GRIFFON	Command and Control
APT41	Launch Agent Mitigation	Exaramel for Windows	Initial Access

As informações são divididas por assuntos:

Groups: grupos que empreendem ataques maliciosos;

Mitigations: técnicas de mitigação de ataques;

Software: softwares utilizados em ataques maliciosos;

Tactics: os objetivos e estratégias de ataques maliciosos;

Techniques: as técnicas utilizadas em ataques maliciosos.

Para procurar um verbete específico, use a barra de buscas (**Search in all resources**).

Ao clicar num verbete, você vai encontrar mais detalhes. Há informações gerais (ID, nome, horários de criação e modificação e versão) e uma descrição do elemento. Abaixo, há uma relação de artigos onde o elemento pode aparecer. (Exemplo: a técnica "Malicious file" aparece na página do software "BLINDINGCAN")

BLINDINGCAN



BLINDINGCAN is a remote access Trojan that has been used by the North Korean government since at least early 2020 in cyber operations against defense, engineering, and government organizations in Western Europe and the US.(Citation: US-CERT BLINDINGCAN Aug 2020)(Citation: NHS UK BLINDINGCAN Aug 2020)

[Access the original source](#)

Groups

[Lazarus Group](#)

Techniques

[Match Legitimate Name or Location](#)

[Obfuscated Files or Information](#)

[Web Protocols](#)

[Code Signing](#)

[Rundll32](#)

[Deobfuscate/Decode Files or Information](#)

[Standard Encoding](#)

[Malicious File](#)

Ao clicar em **Access the original source**, uma nova aba irá abrir com a documentação referente na página do [MITRE ATT&CK](#).

XDR - Malware Sandboxing

O Blockbit XDR utiliza o Sandbox da Blockbit para abrir programas ou arquivos suspeitos num lugar seguro. Para mais informações, visite [Blockbit ATP Sandbox](#).

XDR - Security Operations

Esta seção apresenta dashboards com alertas de eventos que violam diretrizes de 6 regulamentos:

LGDP (Lei Geral de Proteção de Dados): Lei brasileira que controla a privacidade e o uso/tratamento de dados pessoais.

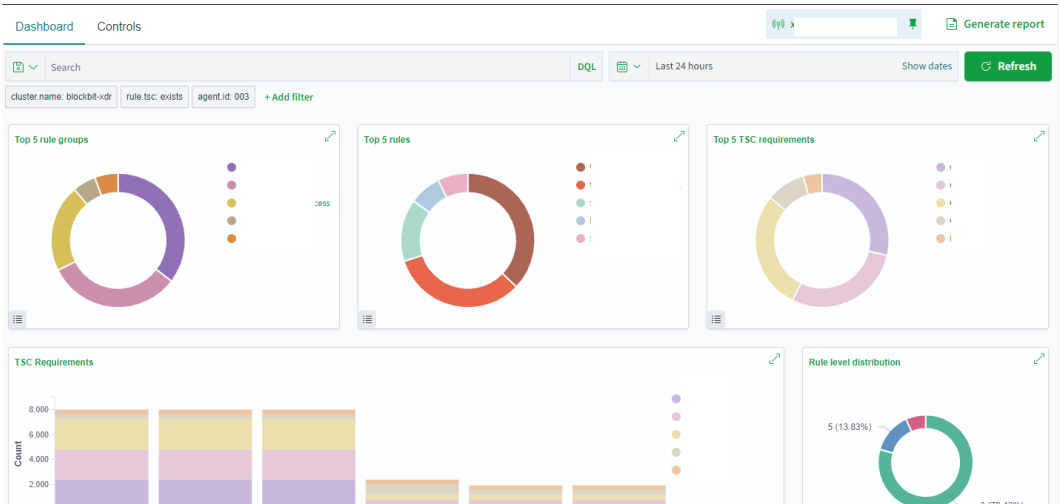
PCI DSS (Payment Card Industry Data Security Standard): Padrão de segurança de dados do setor de cartões de pagamento.

GDPR (General Data Protection Law): Lei de proteção de dados da União Europeia.

HIPAA (Health Insurance Portability and Accountability Act): Lei dos EUA que regulamenta a coleta, o uso e a proteção de informações de saúde.

NIST 800-53 (National Institute of Standards and Technology Special Publication 800-53): Padrão de segurança da informação para agências federais dos EUA.

TSC (Trust Service Criteria): Critérios para avaliar a adequação de soluções para os padrões de segurança de uma organização.



Search

A barra permite buscar por eventos específicos. Para mais informações, confira [Sistema de buscas](#).

Clique em **Explore agent** para selecionar o agente. Para mais informações, confira [Selecionar agente](#).

Para criar um relatório, clique em **Generate report**. Os relatórios são armazenados em [Reports](#).

Dashboard

Cada regulamento tem um dashboard específico:

[LGPD](#)

[GDPR](#)

[HIPAA](#)

[NIST 800-53](#)

[PCI DDS](#)

[TSC](#)

Controls

Nesta página, você pode conferir os alertas separados por requerimento.

Requirements

Hide empty items ☐

Filter requirements 1 1.4 - Install personal firewall software or equivalent function... 88 1.3.4 - Do not allow unauthorized outbound traffic from the ... 4 1.1.1 - A formal process for approving and testing all network... 0	2 2.2 - Develop configuration standards for all system comp... 1316 2.2.4 - Configure system security parameters to prevent mis... 49 2.2.3 - Implement additional security features for any requir... 38 2.2.2 - Enable only necessary services, protocols, daemons, ... 3	4 4.1 - Use strong cryptography and security protocols (for ex... 126
5 5.2 - Ensure that all anti... 15 5.1 - Deploy anti... 8	6 6.5 - Address common coding vulnerabilities in softwar... 5093498 6.2 - Ensure that all system components and software are pr... 13 6.5.8 - Improper access control (such as insecure direct obj... 4 6.5.1 - Injection flaws, particularly SQL injection. Also consi... 0 6.5.2 - Buffer overflows 0 6.5.5 - Improper error handling 0 6.5.7 - Cross 0 6.5.10 - Broken authentication and session management. 0 6.6 - For public 0	8 8.1.5 - Manage IDs used by third parties to access, support, ... 15 8.2.4 - Change user passwords/passphrases at least once ev... 14 8.1.8 - If a session has been idle for more than 15 minutes, r... 12 8.1.2 - Control addition, deletion, and modification of user l... 6 8.1.4 - Remove/disable inactive user accounts within 90 days. 0 8.1.6 - Limit repeated access attempts by locking out the us... 0 8.5.1 - Additional requirement for service providers: Service... 0 8.7 - All access to any database containing cardholder data (... 0

Para mostrar apenas requerimentos com alertas, clique em **Hide requirements with no alerts**.

Ao clicar em cada requerimento, vão ser mostrados os subparágrafos.

Ao clicar em cada subparágrafo, vão ser mostradas a descrição e os alertas relacionados.

Você pode usar o campo **Filter requirements** para filtrar requerimentos.

Ao passar o mouse sobre um requerimento, aparecerá uma breve descrição dele e dois botões:

1 1.4 - Install personal firewall software or equivalent fu... 88 1.3.4 - Do not allow unauthorized outbound traffic from the	2 2.2 - Develop configuration standards for all system comp... 1314 1.4 - Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee	4.1 - Use strong cryptography
--	--	--------------------------------------

Show requirement in Dashboard (): Irá mostrar os dados específicos do requerimento no Dashboard.

Inspect requirement in Security Events (): Irá abrir uma página com dados do requerimento no Security Events.

Ao clicar no requerimento, um modal com a descrição dele irá abrir.

1.1.1

Goals

Build and Maintain a Secure Network



Requirement description

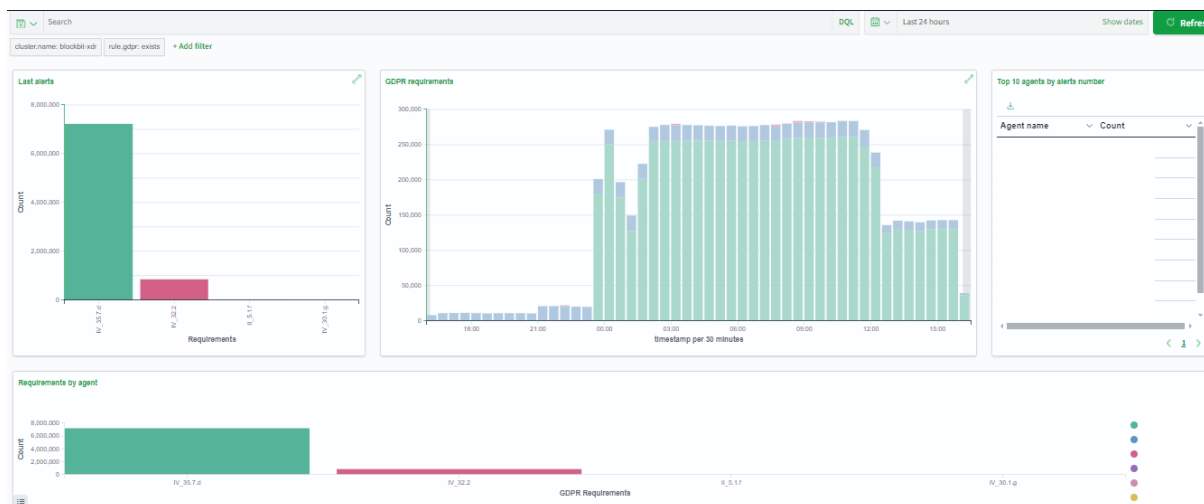
A formal process for approving and testing all network connections and changes to the firewall and router configurations

XDR - Security Operations - GDPR

A **GDPR** (**General Data Protection Law**) é a lei de proteção de dados da União Europeia.

No Dashboard, são mostrados os seguintes

gráficos:



Last alerts: últimos alertas por artigo;

GDPR Requirements: número de alertas a cada 30 minutos;

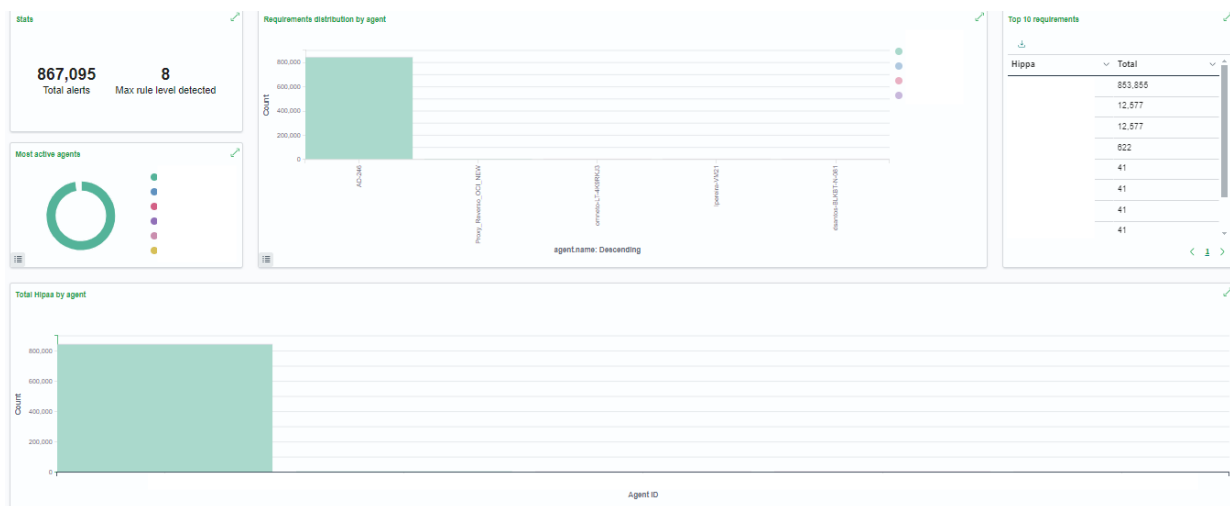
Top 10 agents by alerts number: agentes com mais alertas vinculados;

Requirements by agents: alertas vinculados a agentes divididos por artigos.

XDR - Security Operations - HIPAA

A **HIPAA** (Health Insurance Portability and Accountability Act) é a lei dos EUA que regulamenta a coleta, o uso e a proteção de informações de saúde.

No Dashboard, são mostrados os seguintes dados:



Stats: são mostradas duas estatísticas:

- **Total alerts:** número total de alertas de violação do HIPAA;
- **Max rule level detected:** maior nível de regra violada.

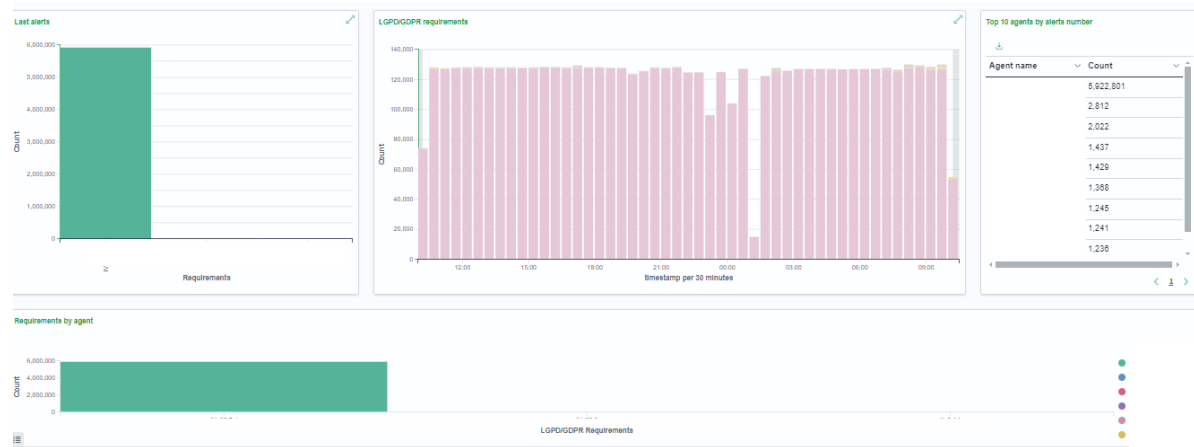
Requirements distribution by agent: violações distribuídas por agentes;

Top 10 requirements: requerimentos com mais violações;

Total HIPAA by Agent: violações por agente ao longo do tempo.

XDR - Security Operations - LGPD

A **LGPD** (Lei Geral de Proteção de Dados) é a lei brasileira que controla a privacidade e o uso/tratamento de dados pessoais.



Last alerts: últimos alertas por artigo;

LGPD/GDPR Requirements: número de alertas a cada 30 minutos;

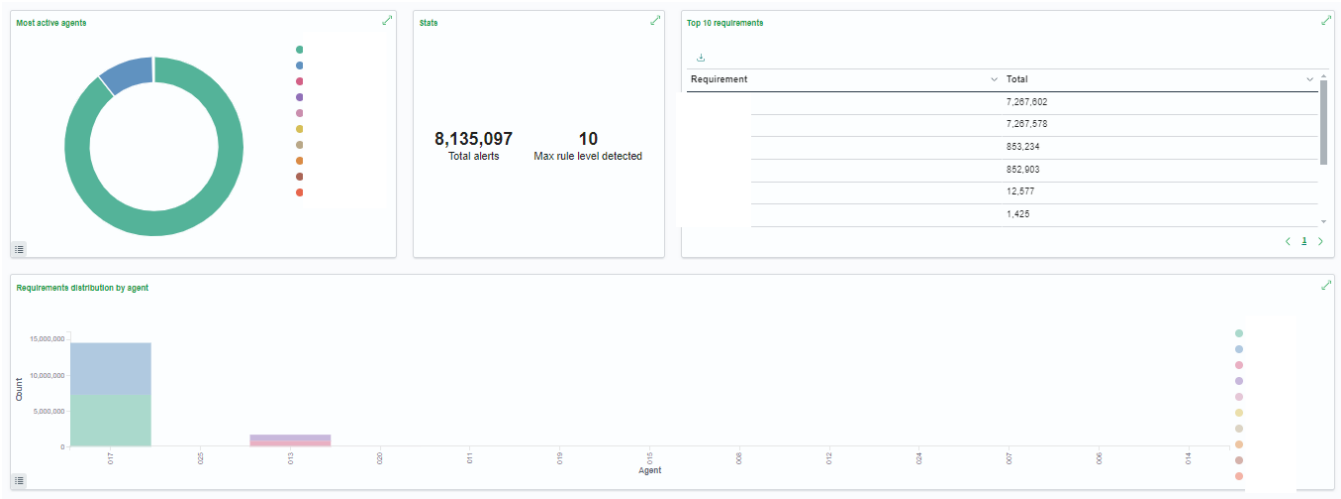
Top 10 agents by alerts number: agentes com mais alertas vinculados;

Requirements by agents: alertas vinculados a agentes divididos por artigos.

XDR - Security Operations - NIST 800-53

O [NIST 800-53](#) (National Institute of Standards and Technology Special Publication 800-53) é o padrão de segurança da informação para agências federais dos EUA.

No Dashboard, são mostrados os seguintes dados:

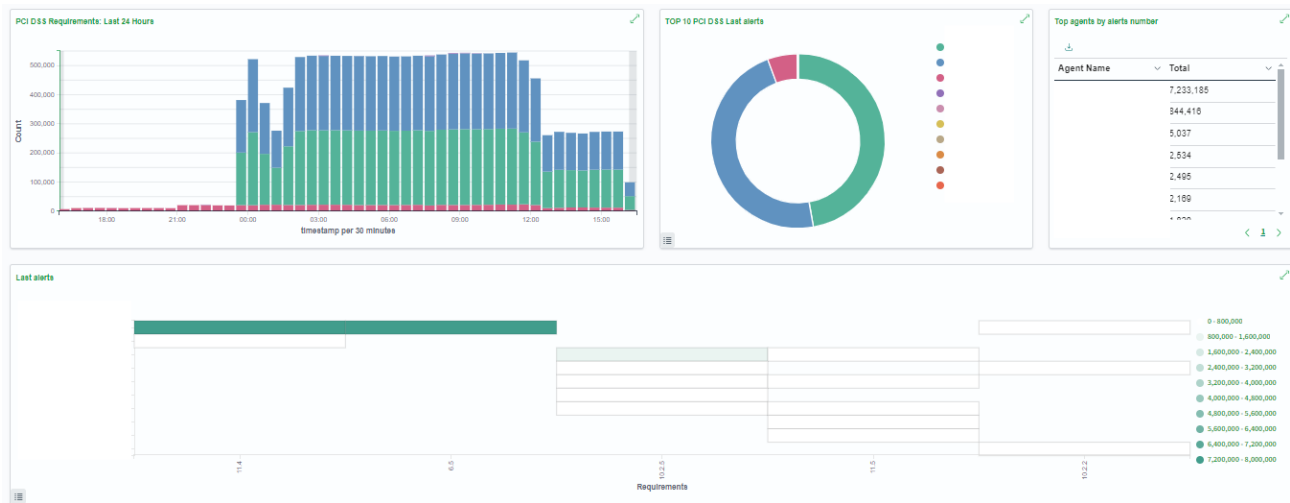


- Most active agents:** agentes com mais alertas;
- Stats:** são mostradas duas estatísticas:
- **Total alerts:** número total de alertas de violação do NIST 800-53;
 - **Max rule level detected:** maior nível de regra violada.
- Top 10 requirements:** requerimentos com mais violações;
- Requirements distribution by agent:** violações distribuídas por agentes.

XDR - Security Operations - PCI DDS

O **PCI DSS** (**Payment Card Industry Data Security Standard**) é o padrão de segurança de dados do setor de cartões de pagamento.

No Dashboard, são mostrados os seguintes gráficos:



PSI DDS Requirements: Last 24 Hours: número de alertas por 30 minutos nas últimas 24 horas;

Top 10 PCI DDS Last Alerts: requerimentos com mais alertas vinculados;

Top 10 agents by alerts number: agentes com mais alertas vinculados;

Last Alerts: últimos alertas.

XDR - Security Operations - TSC

TSC (Trust Service Criteria) são critérios do American Institute of Certified Public Accountants (Instituto Americano de Contadores Públicos Certificados) para avaliar a adequação de soluções para os padrões de segurança de uma organização.

No Dashboard, são mostrados os seguintes dados:



Top 5 rule groups: grupos de regras com mais violações.

Top 5 rules: regras com mais violações.

Top 5 TSC requirements: requerimentos com mais violações;

XDR - Cloud Security

O Blockbit XDR pode ser utilizado para monitorar instâncias de nuvem.

Ao coletar **Metadados**, o Blockbit XDR obtém informações como **ID da instância, região, tipo de máquina, tags e configurações de rede** via APIs dos provedores de nuvem.

Tratando esses dados com inteligência artificial, o Blockbit XDR pode **aplicar políticas automaticamente**, permitindo **Ajuste Dinâmico e Resposta Ativa**.

Se a máquina mudar de estado (exemplo: **alteração de tags, região ou recursos**), o Blockbit XDR **reajusta automaticamente** suas configurações. Isso permite reações rápidas, como **bloquear acessos suspeitos** ou **ativar proteções adicionais** conforme necessário.

O Blockbit XDR permite aumentar a segurança nas seguintes plataformas de nuvem:

- [Docker](#)
- [Amazon Web Services](#)
- [Google Cloud](#)
- [GitHub](#)
- [Azure/Microsoft 365](#)

As integrações são feitas pela [API do XDR](#). Para integrar, entre em contato com a [equipe Blockbit](#).

XDR - Cloud Security - Amazon Web Services

Os agentes utilizam o **AWS Instance Metadata Service (IMDS)** para coletar informações como **ID da instância, tipo de máquina, região, VPC e tags associadas**. Com esses dados/metadados, a solução ajusta automaticamente as políticas de segurança conforme o perfil da instância na nuvem AWS.

XDR - Cloud Security - Azure/Microsoft 365

A integração com o **Azure Instance Metadata Service (IMDS)** permite que os agentes identifiquem detalhes (metadados) como **ID da VM, SKU, grupo de recursos e rede virtual**. Dessa forma, as políticas de segurança são aplicadas de acordo com a configuração do ambiente Azure.

Panel

Nesta página, é possível monitorar as atividades na nuvem com mais detalhes.

Subscription 0 User Type 0 Result Status 0 Last 24 hours Show dates Refresh

cluster.name: blockbit-xdr rule.groups: office365 + Add filter Advanced filters

Top users
User Count ↓
No items found

Top client IP address
Client IP address Count ↓
No items found

Top rules
Rule Count ↓
No items found

Top operations
Operation Count ↓
No items found

A barra permite buscar por eventos específicos. Para mais informações, confira [Sistema de buscas](#).

Ao clicar em **Refresh**, você pode atualizar a lista de relatórios.

Ao clicar no switch **Advanced filters**, você acessa 3 novos filtros:

Subscription: permite filtrar por assinatura;

User Type: permite filtrar por tipo de usuário. Ao clicar, vão aparecer os perfis criados em [Users](#);

Result Status: permite filtrar por status do resultado.

Os 4 painéis mostram listas de eventos mais comuns e sua contagem.

Top Users: exibe os usuários mais ativos;

Top Client IP Address: exibe os IPs de clientes que mais acessaram os serviços monitorados;

Top Rules: exibe as regras de segurança mais acionadas;

Top Operations: exibe as operações mais executadas;

XDR - Cloud Security - Docker

Para ambientes baseados em **Docker e Kubernetes**, os agentes do **Blockbit XDR** acessam **variáveis de ambiente e configurações da infraestrutura de orquestração**, como **ID do contêiner, namespace, labels, volume mounts e configurações de rede**. Isso permite que a segurança seja aplicada com base no contexto do contêiner, protegendo cargas de trabalho dinâmicas sem impactar a performance.

XDR - Cloud Security - GitHub

Para ambientes de **CI/CD**, os agentes extraem metadados dos **runners do GitHub Actions**, como **ID do runner**, **tipo de ambiente (self-hosted ou GitHub-hosted)**, **repositório**, **branch** e **eventos acionadores**. Com base nisso, a solução aplica medidas de segurança para garantir que execuções automatizadas sejam protegidas contra acessos indevidos ou falhas de segurança.

Panel

Nesta página, é possível monitorar as atividades na nuvem com mais detalhes.

Actor0

Organization0

Repository0

Action0

📅

Last 24 hours

Show dates

🔄

Refresh

cluster.name: blockbit-xdr

rule.groups: github

+ Add filter

ⓧ

Advanced filters

📄

Actors

Actor

Count ↓

No items found

Organizations

Organization

Count ↓

No items found

Repositories

Repository

Count ↓

No items found

Actions

Action

Count ↓

No items found

A barra permite buscar por eventos específicos. Para mais informações, confira [Sistema de buscas](#).

Ao clicar em **Refresh**, você pode atualizar a lista de relatórios.

Ao clicar no switch **Advanced filters**, você acessa 3 novos filtros:

Subscription: permite filtrar por assinatura;

User Type: permite filtrar por tipo de usuário. Ao clicar, vão aparecer os perfis criados em [Users](#);

Result Status: permite filtrar por status do resultado.

Os 4 painéis mostram listas de eventos mais comuns e sua contagem.

Actors: exibe os usuários mais ativos;

Organizations: exibe as organizações com mais atividade;

Repositories: exibe os repositórios mais acessados;

Actions: exibe as ações mais executadas;

XDR - Cloud Security - Google Cloud

Na GCP, os agentes acessam o **GCP Instance Metadata Server**, obtendo informações (metadados) como **zona, nome do projeto, etiquetas e identidade da VM**. Isso possibilita a configuração dinâmica da segurança, adaptando-se ao contexto da infraestrutura do Google Cloud.

XDR - Downloads

- **Sistemas operacionais suportados**

- a. Windows: ([Link](#))
 - i. Windows Server 2008 (todas as versões), 2011, 2012, 2012 R2, 2016, 2019, 2022, 2025 e superiores;
 - ii. Windows versão 7 (todas as versões), 8.1, 10, 11 e superiores;
- b. macOS
 - i. Big Sur, Monterey, Ventura, Sonoma, Sequoia e superiores;
 - ii. ARM ([Link](#))
 - iii. AMD/Intel ([Link](#))
- c. Linux
 - i. Ubuntu, Debian, Raspbian, Fedora, CentOS, Red Hat Enterprise Linux (RHEL), Rocky Linux, AlmaLinux, SUSE Linux Enterprise ou OpenSUSE;
 - ii. Nuvens públicas, como AWS Linux, Oracle Linux, Azure Linux ou Google Cloud Ubuntu Pro;
 - iii. RPM ([Link](#))
 - iv. DEB ([Link](#))

Blockbit ATP Sandbox - Guia do Administrador

Index

--

Blockbit ATP Sandbox - Introdução e Login

O Blockbit Advanced Threat Protection Sandbox é um ambiente de testes isolado e totalmente automatizado que abre/executa programas ou arquivos suspeitos sem afetar a aplicação, sistema ou plataforma nas quais estes são encontrados.

Após todos os testes serem executados, as assinaturas e reputações são checadas, o link/arquivo/programa/aplicativo são analisados e seu comportamento traçado, para que possamos entender o potencial das ameaças e mitigar o dano de fontes desconhecidas em um ambiente de produção.

Estas são algumas das técnicas utilizadas pelo Sandbox:

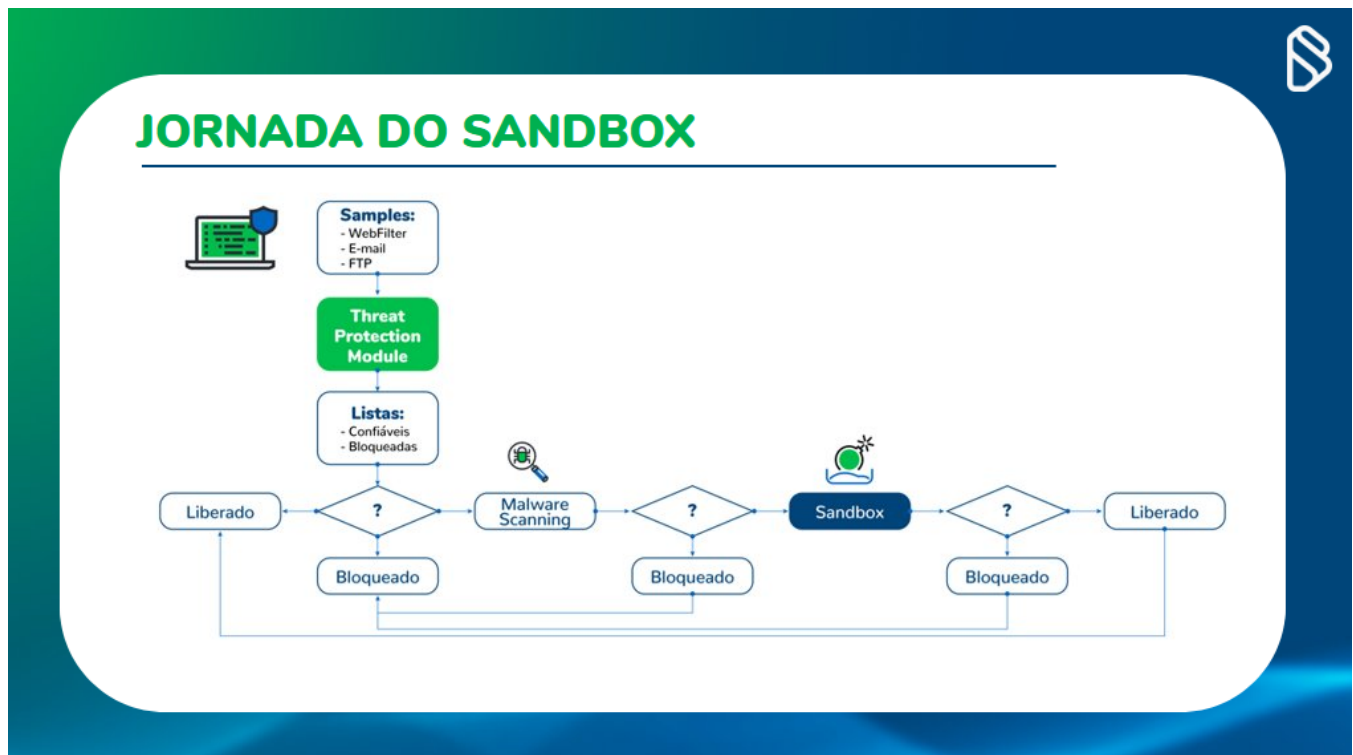
Zero-day Identification: É a possibilidade de identificar ameaças sem assinatura baseado em seu comportamento e pontuação no sistema de *Machine Learning*.

Machine Learning for Malware Detection: Utiliza diversas técnicas de detecção de malware consolidadas através de um algoritmo de auto-aprendizado.

IA for Malware Detection: Analisa o comportamento de arquivos e URLs em ambientes controlados (sandboxes), identificando atividades suspeitas, anomalias e padrões maliciosos que podem indicar a presença de malware, mesmo quando o código analisado não é reconhecido por antivírus tradicionais. Essa abordagem permite detectar ameaças desconhecidas (zero-day), malware sem assinatura e comportamentos evasivos, elevando significativamente a eficácia da proteção.

Analysis of Threat Behavior: Permite o monitoramento de cada um dos passos do malware, seu processo de carregamento na memória, arquivos executados ou modificados, manipulação de registros, tráfego de rede, etc.

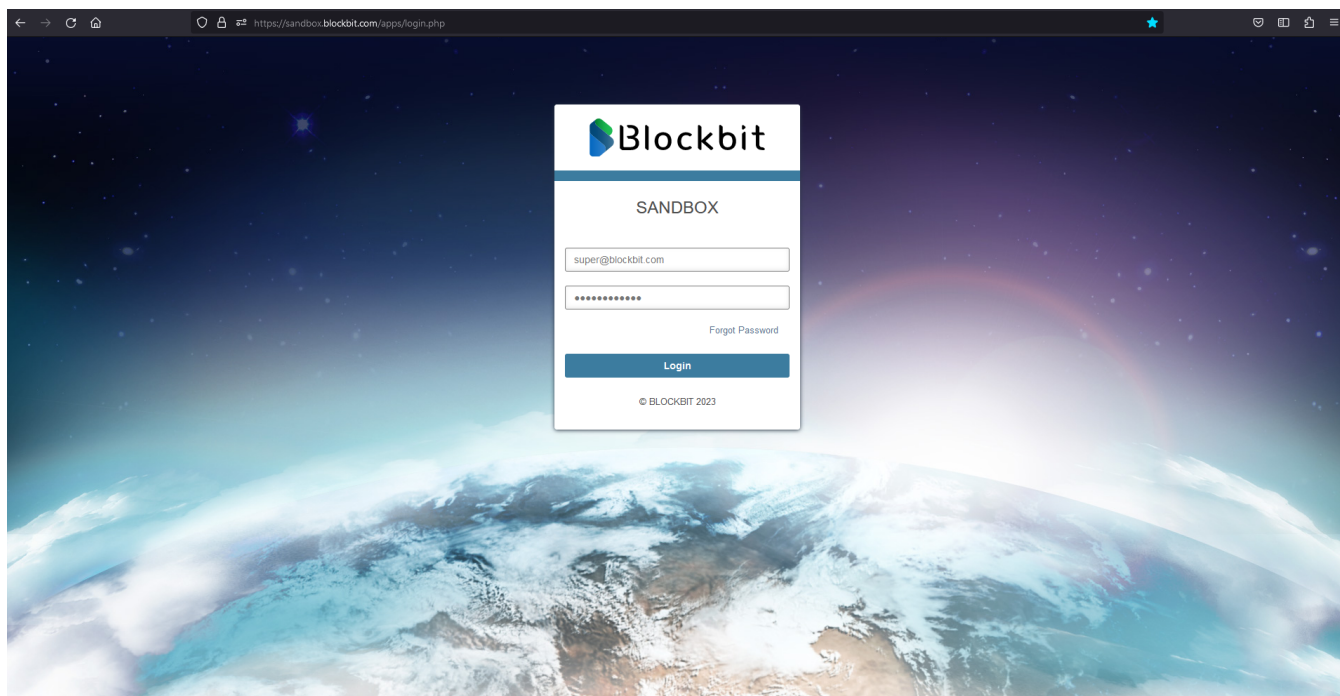
Abaixo, podemos ver o fluxo de processos do Sandbox:



Processos de análise do Sandbox

Como podemos ver na imagem, quando malware ou aplicações suspeitas são encontradas, são executadas no Sandbox, para que suas características sejam todas compreendidas e então expostas em detalhes nas seções e relatório que analisaremos a seguir.

Login e Acesso



Tela de Login do Sandbox

Para realizar seu login no Sandbox, utilize o e-mail e senha fornecidos pela Blockbit em ambos os campos que podemos ver na imagem acima.

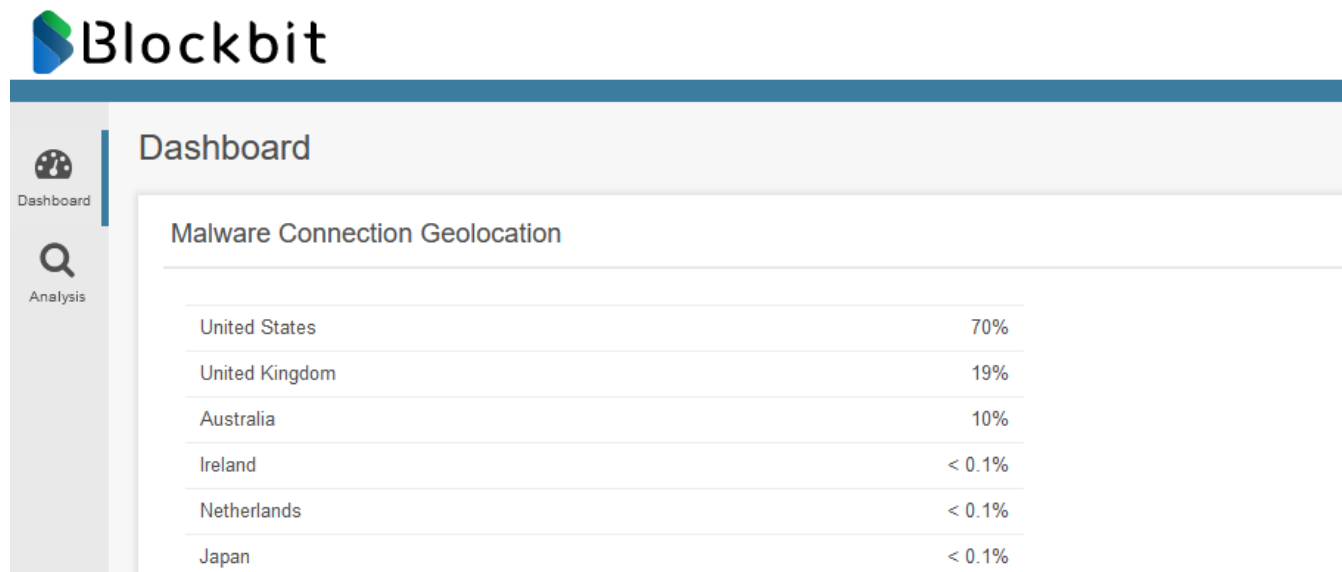
Caso a senha seja perdida, é possível ser recuperada clicando em "Forgot Password" e seguindo os passo subsequentes para registrar uma nova senha.

Na próxima seção, analisaremos as funcionalidades disponíveis para a análise de assinaturas.

Blockbit ATP Sandbox - Seções

O Sandbox tem duas seções principais: Dashboard e Analysis. Em Dashboard, podemos ver as estatísticas e informações sobre assinaturas analisadas recentemente.

Na seção Analysis, podemos ver detalhes individuais sobre cada assinatura registrada e dados e relatórios ainda mais detalhados.



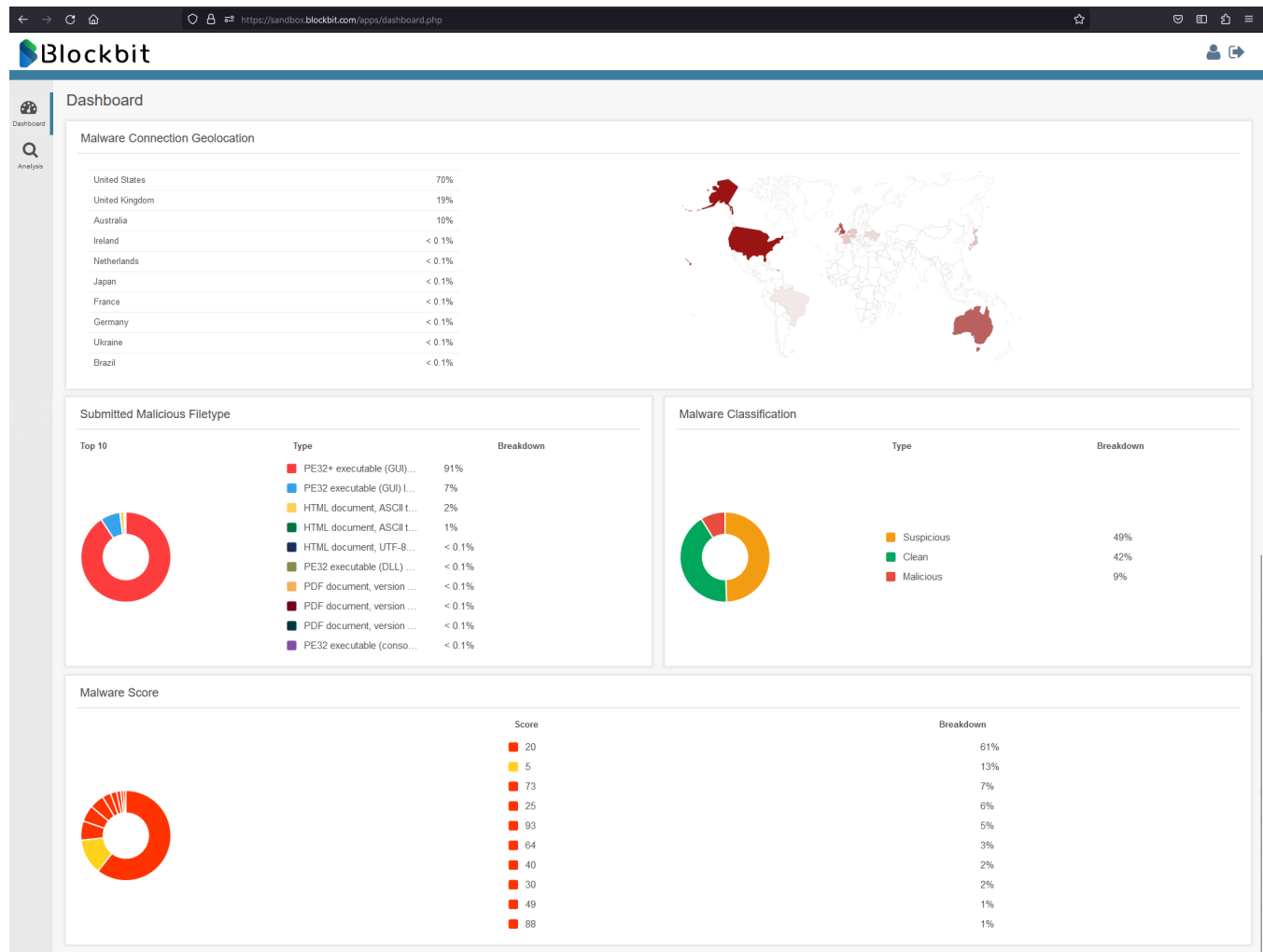
Sandbox - Dashboard e Analysis

Na próxima página, analisaremos ambas as seções com mais detalhes.

- [Dashboard](#)
- [Analysis](#)

Blockbit ATP Sandbox - Dashboard

A seção Dashboard é composta de quatro painéis que exibem dados de geolocalização, tipo de arquivo, classificação e pontuação das assinaturas que foram analisadas:



Dashboard - Painéis

Malware Connection Geolocation: Exibe o total de assinaturas analisadas por país, e o total (em porcentagem) de malware detectado.

Submitted Malicious Filetype: Em um top 10, mostra os tipos mais comuns de arquivos maliciosos, submetidos para análise.

Malware Classification: Classifica os malwares encontrados como: Suspeitos, limpos ou maliciosos.

Malware Score: Pontuação para medir o nível de ameaça representado pelo malware, e o nível de breakdown.

Blockbit ATP Sandbox - Analysis

A aba Analysis contém todas as informações obtidas a partir das assinaturas analisadas:

Blockbit

Analysis

Search for... Go!

Submit

< 1 2 3 4 5 >

Submission Date	First Submission	MD5SUM	Filename	Submitted by	Status	Score	Actions
2023-05-21 18:07	2023-05-21 18:07	c43fa9acce0a1d52adfc83980366760	52f1a8433ce9bbd931bf1bb379afa2b8	Projetos	Reported	100	  
2023-05-20 18:07	2023-05-20 18:07	b65c032897c8256b9bde6c48dc90356e	52f1a8433ce9bbd931bf1bb379afa2b8	Projetos	Reported	88	  
2023-05-19 18:07	2023-05-19 18:07	21b533645Fe6b33871600919f8e3e629	52f1a8433ce9bbd931bf1bb379afa2b8	Projetos	Reported	88	  
2023-05-18 20:07	2023-05-18 20:07	b1555de7b2e3d9c8e968663b7cc44cd	115414a53a14cec793bcb31d40e9be	Projetos	Reported	0	  
2023-05-18 13:26	2023-05-18 13:26	e30b92f9ed1eed554ba6319457bca5f	c5c0f1b1ac68a7806d958ba1005c86f	Projetos	Reported	50	  
2023-05-17 18:10	2023-05-17 18:10	8665d82295768d6e931e4836a767a5ae	8527ea002abf7fb1b659297d5b2a81ef	Projetos	Reported	20	  
2023-05-17 18:03	2023-05-17 18:03	c8152da524fc4fddacf53b18f64db254	d1989bc970eb3619d1d1defa1ae65e	Projetos	Reported	20	  
2023-05-17 18:03	2023-05-17 18:03	3486754bc97885c88586ddad335eb2fa	05bc1fe8c78de63dc95472017683839	Projetos	Reported	23	  
2023-05-17 18:03	2023-05-17 18:03	c45c98a933ce1eca45f5765bc0f62f7b	4fb2044ec5244b7efcca6c7ec5c428ac	Projetos	Reported	23	  
2023-05-17 18:03	2023-05-17 18:03	4663821c6bcc2887e7459843a11678c6	530ac99c00118823369dce6b1f99936	Projetos	Reported	0	  

Analysis

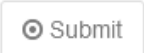
Menu principal

As principais ferramentas de navegação disponíveis são a barra de pesquisa, que permite a busca de assinaturas por palavras-chave, bem como as páginas contendo as assinaturas listadas, que também são navegáveis através dos números das páginas conforme demonstrado na imagem abaixo:

Search for... Go!

< 1 2 3 4 5 >

Barra de pesquisa e Menu de navegação

Botão Submit []: Esta opção permite a submissão de arquivos suspeitos para análise. revisar este item, pode estar impreciso.

Colunas

Estes são os dados de identificação dos arquivos analisados:

Submission Date	First Submission	MD5SUM	Filename	Submitted by	Status	Score	Actions
-----------------	------------------	--------	----------	--------------	--------	-------	---------

Colunas - Informações dos arquivos

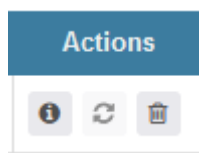
- Submission Date:** Data na qual o arquivo foi submetido para análise.
- First Submission:** Data inicial de submissão.
- MD5SUM:** Código alfanumérico único gerado pelo sistema para marcar um arquivo.
- Filename:** Nome original do arquivo.

Submitted by: Usuário pelo qual o arquivo foi submetido a análise.

Status: Situação atual da assinatura.

Score: Pontuação em uma escala de 0 a 100, quanto ao nível de ameaça da assinatura.

Actions: Ações que podem ser tomadas ao manusear os arquivos:



Ações

Informações: Exibe dados detalhados sobre o arquivo selecionado.

Atualizar: Atualiza os dados, e caso mais informações estejam disponíveis, serão exibidas.

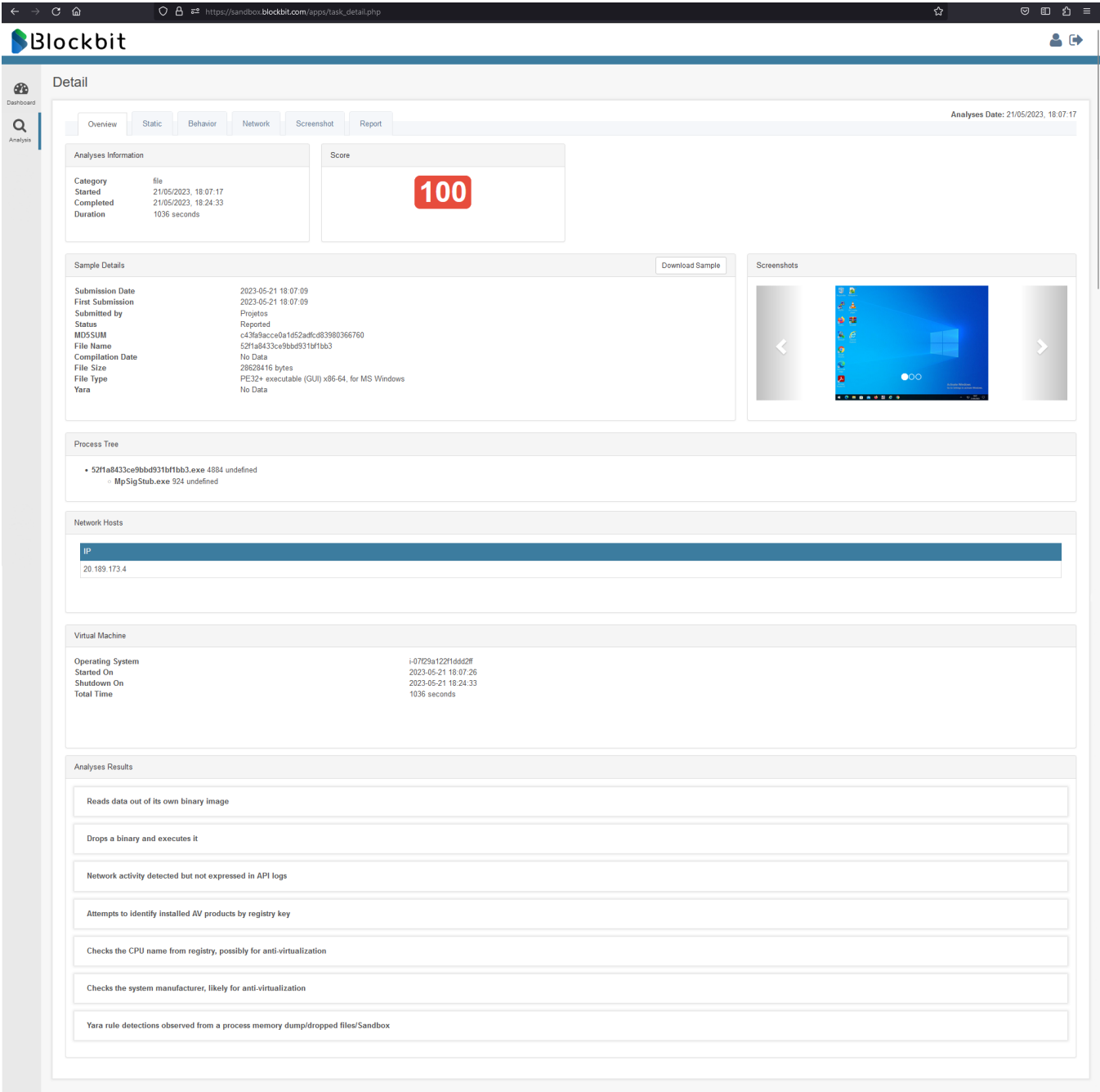
Apagar: Apaga a assinatura selecionada.

Na próxima seção, veremos mais detalhes sobre as assinaturas, após sua análise.

Blockbit ATP Sandbox - Overview

As informações exibidas na opção "Detail", estão disponíveis para cada uma das assinaturas na lista principal.

A seguir analisaremos a aba Overview:



Aba Overview

Analysis Information: Este campo contém a categoria do objeto analisado. Também mostra as datas inicial e final da análise, bem como a duração do processo.

Score: A pontuação de risco da assinatura analisada.

Sample Details: Este campo possui uma opção que permite ao usuário baixar o arquivo que foi analisado [Download Sample]. Também exibe dados como, a primeira data e a data mais recente nas quais os arquivos foram submetidos, por quem o arquivo foi submetido, status, MD5SUM, nome original do arquivo, data de compilação, tamanho e tipo.

Screenshots: Neste campo, prints de tela da máquina virtual na qual os testes foram feitos são exibidos.

Process Tree: Exibe os arquivos executáveis que foram rodados pela assinatura maliciosa.

Network Hosts: Mostra o IP do ambiente virtual no qual a aplicação foi executada.

Virtual Machine: Dados sobre a máquina virtual que foi criada para a análise.

Analyses Results: Este campo descreve a maneira como a aplicação maliciosa funciona. Fornece detalhes sobre o comportamento, e as principais áreas afetadas pela assinatura.

Blockbit ATP Sandbox - Static

Nesta seção analisaremos as informações disponíveis na aba Static:

Dashboard

Analysis

Overview

Static

Behavior

Network

Screenshot

Report

Analyses Date: 21/05/2023, 18:07:17

Static Details

MD5

c43fa9acce0a1d52adfc833980366760

SHA1

dc78d8f8acd4c86a6354ad58a1b29068fa6e114

SHA256

b3eb021854c7f6d49b6ec78800b0b59638224ef64a7dc4109e21ef9d5cf9a619

SHA512

32183ac0645639190bed121f0d5a8d68d98a5c2462cc5d9926a906177d9a3992763e3431c901db1c18ca5683b43d2e9436c90787ba00789b7b0c0494ea075

CRC32

E03FEFD5

Ssdeep

786432_OyBrl619wi4nvUD9Vv0ijOCYkpeRVxQLsPGlkqGebE8KnBmW4FXULwkWj OyBA1uwmmXo7wQLm+hbEdaBW4qJE

Sections

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
No Data				

Strings

[This program cannot be run in DOS mode.
.text
' .rdata
@ .data
.pdata
@ .rsrc
@ .reloc
x UATALJAJAWH
D\$xE3
A_APAIAI]

Imports

No Data

Aba Static

Static details: Nesta painel podemos ver detalhes sobre as chaves de criptografia utilizadas na assinatura, e o arquivo MD5 do arquivo.

Sections: Este campo exibe detalhes sobre a máquina virtual utilizada na análise, tais como o nome, endereço virtual, tamanho utilizado em disco, tamanho dos dados utilizados e também o nível de entropia (aleatoriedade) presente na codificação do arquivo malicioso.

Strings: Detalhes dos strings e do comportamento operacional do malware.

Imports: Arquivos que foram importados pelo arquivo malicioso.

Blockbit ATP Sandbox - Behavior

Nesta seção, são mostradas as ações tomadas pelo malware, os arquivos que tentou corromper, acessar, copiar ou deletar. De igual maneira, as chaves de registro com as quais o malware interagiu:

Dashboard

Analysis

Detail

OverviewStaticBehaviorNetworkScreenshotReport

Analyses Date: 21/05/2023, 18:07:17

Process Tree

52f1a8433ce9bbd931bf1bb3.exe 4260 "C:\Users\ADMINI~1\AppData\Local\Temp\52f1a8433ce9bbd931bf1bb3.exe"
MpSigStub.exe 4804 C:\Users\ADMINI~1\AppData\Local\Temp\3900BA95-5068-4ADD-9361-59452735E89C\MpSigStub.exe /stub 1.1.18500.10 /payload 1.389.2032.0 /program C:\Users\ADMINI~1\AppData\Local\Temp\52f1a8433ce9bbd931bf1bb3.exe

52f1a8433ce9bbd931bf1bb3.exe

PID: 4884
Parent PID: 4260
Full Path: C:\Users\Administrator\AppData\Local\Temp\52f1a8433ce9bbd931bf1bb3.exe
Command Line: "C:\Users\ADMINI~1\AppData\Local\Temp\52f1a8433ce9bbd931bf1bb3.exe"

Calls

Time	TID	API	Arguments	Status	Return
No Data	No Data	NtWaitForSingleObject	0 [object Object] 1 [object Object] 2 [object Object]	Success	No Data
No Data	No Data	NtAllocateVirtualMemory	0 [object Object] 1 [object Object] 2 [object Object] 3 [object Object] 4 [object Object]	Success	No Data
No Data	No Data	LdrLoadDll	0 [object Object] 1 [object Object] 2 [object Object]	Success	No Data

Process Tree (Árvore de Processos)

A seção Process Tree exibe a hierarquia dos processos gerados e executados pelo arquivo analisado. Essa visualização permite compreender como o malware se comporta e se propaga dentro do sistema.

- Processo Primário: Mostra o arquivo executável inicial, identificando seu nome, PID (Process Identifier), caminho completo e argumentos de execução.
- Processos Filhos: Exibe os processos secundários iniciados pelo arquivo principal, incluindo detalhes sobre como e por que foram gerados.
- Relação entre Processos: A estrutura em árvore facilita a identificação de técnicas como process hollowing, injeção de código, execução de scripts maliciosos e tentativas de persistência.

Permite detectar comportamentos anômalos, como um malware iniciando múltiplos processos para evasão ou ataques fileless executados diretamente na memória.

Informações do Processo

A seção abaixo da árvore de processos detalha informações do executável em análise, incluindo:

- PID (Process ID): Identificador do processo em execução.
- Parent PID: Indica qual processo pai originou a execução do arquivo analisado.
- Full Path: Caminho completo do arquivo executado no sistema.
- Command Line: Comando exato usado para iniciar o processo, o que pode revelar técnicas como argumentos maliciosos para execução furtiva.

Permite rastrear a origem e o comportamento de processos maliciosos, ajudando na análise forense e na criação de regras de mitigação.

Calls (Chamadas de API do Sistema)

A seção Calls lista as chamadas de API feitas pelo malware durante a execução, ajudando a identificar técnicas e ações maliciosas.

- Time (Tempo): Momento exato da execução da chamada de API.
- TID (Thread ID): Identificador da thread onde a chamada foi feita.
- API: Nome da função chamada no sistema operacional, como NtAllocateVirtualMemory (alocação de memória, usada por malwares para injeção de código).
- Arguments (Argumentos): Parâmetros passados para a API, que podem indicar tentativas de modificar arquivos, acessar memória de outros processos ou realizar comunicação em rede.
- Status: Indica se a execução foi bem-sucedida ou falhou.
- Return: Mostra o valor retornado pela função, útil para identificar se um malware conseguiu completar uma ação maliciosa.

Permite entender exatamente como o malware interage com o sistema, ajudando a detectar táticas de exploração, roubo de credenciais e ataques de injeção de código.

Dashboard

Analysis

Blockbit

Accessed Files

C:\Windows\system32\version.dll
C:\Device\NPF{...}
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.20200_4_to_1_1_20300_3_mpengine.dll_p
C:\Windows\system32\advapi32.dll
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.20200_4_to_1_1_20300_3_mpengine.dll_p
C:\Windows\system32\cabinet.dll
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.20200_4_to_1_1_20300_3_mpengine.dll_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\WpSigStub.exe
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.387_0_0_to_1_389_0_0_mpabase_vdm_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpasdlta.vdm
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.387_0_0_to_1_389_0_0_mpabase_vdm_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpavdlta.vdm
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpavdlta.vdm
C:\Users\...
C:\Users\Administrator\...
C:\Users\Administrator\AppData\...
C:\Users\Administrator\AppData\Local\...
C:\Windows\system32\kernel.appcore.dll
C:\Windows\Temp\MpSigStub.log
C:\Windows\system32\kernel32.dll

Read Files

C:\Device\NPF{...}
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.20200_4_to_1_1_20300_3_mpengine.dll_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\WpSigStub.exe
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.387_0_0_to_1_389_0_0_mpabase_vdm_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpasdlta.vdm
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.387_0_0_to_1_389_0_0_mpabase_vdm_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpavdlta.vdm
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpavdlta.vdm
C:\Users\...
C:\Users\Administrator\...
C:\Users\Administrator\AppData\...
C:\Users\Administrator\AppData\Local\...
C:\Windows\system32\kernel.appcore.dll
C:\Windows\Temp\MpSigStub.log
C:\Windows\system32\WpSigStub.exe
C:\ProgramData\Microsoft\Windows Defender\Platform4.18.2203.5-0\MpClient.dll
C:\Windows\system32\userenv.dll
C:\Windows\system32\msasn1.dll

Modified Files

C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.20200_4_to_1_1_20300_3_mpengine.dll_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\WpSigStub.exe
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.387_0_0_to_1_389_0_0_mpabase_vdm_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpasdlta.vdm
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.387_0_0_to_1_389_0_0_mpabase_vdm_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpavdlta.vdm
C:\Windows\Temp\MpSigStub.log
C:\Users\Administrator\AppData\Local\Temp\82DF69B0-FD07-44EA-8FB6-2B61A6B5EE14MPTelemetrySubmit\839E20E5-08A9-43B6-9ACC-B5474DDAE282
C:\Users\Administrator\AppData\Local\Temp\82DF69B0-FD07-44EA-8FB6-2B61A6B5EE14MPTelemetrySubmit\client_manifest.txt
C:\Users\Administrator\AppData\Local\Temp\82DF69B0-FD07-44EA-8FB6-2B61A6B5EE14MPTelemetrySubmit\watson_manifest.txt
C:\ProgramData\Microsoft\Windows\WER\Temp
C:\ProgramData\Microsoft\Windows\WER\Temp\9dce91f9-6c1c-4fa-903a-302e6bdf194b
C:\ProgramData\Microsoft\Windows\WER\ReportQueue
C:\ProgramData\Microsoft\Windows\WER\Temp\fa74581-62d8-4f19-9b17-1d8c0d339eed
C:\ProgramData\Microsoft\Windows\WER\ReportArchive
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\aa3e90e-5e5b-47d9-98e0-d17c9da633dc
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\6b5c577a-b703-45a3-a492-3360520f011
C:\ProgramData\Microsoft\Windows\WER\Temp\WER\IC76.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER\ID52.tmp.xml

Deleted Files

C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.20200_4_to_1_1_20300_3_mpengine.dll_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\WpSigStub.exe
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.387_0_0_to_1_389_0_0_mpabase_vdm_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpasdlta.vdm
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\1.387_0_0_to_1_389_0_0_mpabase_vdm_p
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpavdlta.vdm
C:\Users\Administrator\AppData\Local\Temp\3980BA86-5068-4ADD-9361-59452F35E89E\mpavdlta.vdm
C:\ProgramData\Microsoft\Windows\WER\Temp\WER\IC76.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER\ID52.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER\IC76.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER\ID52.tmp.xml
C:\Windows\Temp\MpSigStub.log
C:\Users\Administrator\AppData\Local\Temp\82DF69B0-FD07-44EA-8FB6-2B61A6B5EE14MPTelemetrySubmit\watson_manifest.txt
C:\Users\Administrator\AppData\Local\Temp\82DF69B0-FD07-44EA-8FB6-2B61A6B5EE14MPTelemetrySubmit\client_manifest.txt
C:\Users\Administrator\AppData\Local\Temp\82DF69B0-FD07-44EA-8FB6-2B61A6B5EE14MPTelemetrySubmit

Created Registry Keys

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MpSigStub\LastStartTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MpSigStub\LastExitCode
REGISTRY\7650016-94cc-5b68-3eb4-cbf45f6a82c\RootInventoryApplicationFileWritePermissionsCheck
REGISTRY\7650016-94cc-5b68-3eb4-cbf45f6a82c\RootInventoryApplicationFilePermissionsCheckTestKey
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\InstallLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Advanced Threat Protection\InstallLocation

Dados sobre comportamento do malware em relação aos arquivos

Accessed, read, modified and deleted files: Estes são os arquivos com os quais o malware interagiu, e cada seção denota esta interação.

Created registry keys: Chaves de registro que foram criadas pelo malware.

[illegible]

As listas acima compõe um mapeamento das ações do malware em relação aos arquivos do sistema e chaves de registro.

Blockbit ATP Sandbox - Network

Esta seção traz informações sobre as tentativas da assinatura maliciosa em acessar certas portas e protocolos:

Blockbit

Dashboard

Analysis

Detail

OverviewStaticBehaviorNetworkScreenshotReport

Analyses Date: 21/05/2023, 18:07:17

Type
UDP (7)

Source	Source Port	Destination	Destination Port
10.28.5.76	61526	1.1.1.1	53
10.28.5.76	63115	1.1.1.1	53
10.28.5.76	57907	1.1.1.1	53
10.28.5.76	62150	1.1.1.1	53
10.28.5.76	64609	8.8.8.8	53
10.28.5.76	56782	1.1.1.1	53
10.28.5.76	57992	1.1.1.1	53

Aba Network

- Source:** O IP fonte.
- Source Port:** As portas fonte pelas quais tentativas de comunicação ocorreram.
- Destination:** O gateway de destino.
- Destination Port:** A porta destino para qual a tentativa de comunicação da assinatura maliciosa ocorreu.

Type

UDP (7)

Hosts (1)

DNS (2)

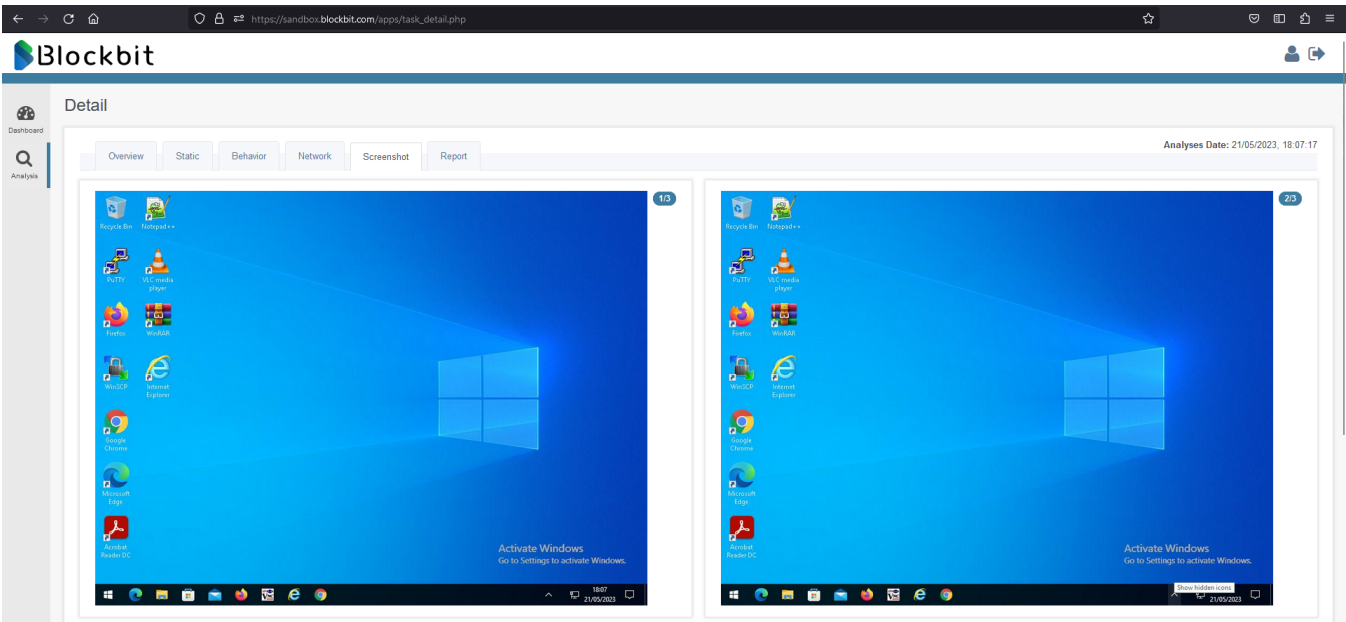
UDP (7)

ICMP (1)

Tipos de protocolo de rede

Blockbit ATP Sandbox - Screenshot

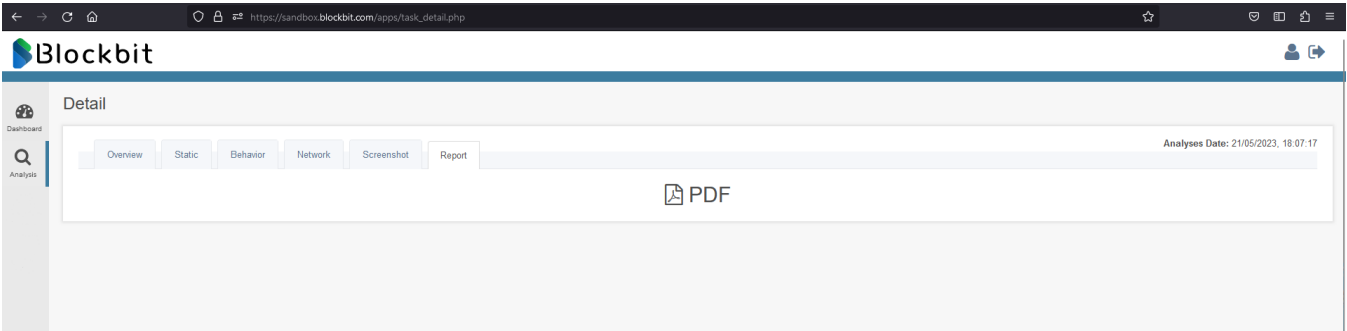
A seção screenshot mostra imagens do ambiente virtual no qual a análise foi realizada:



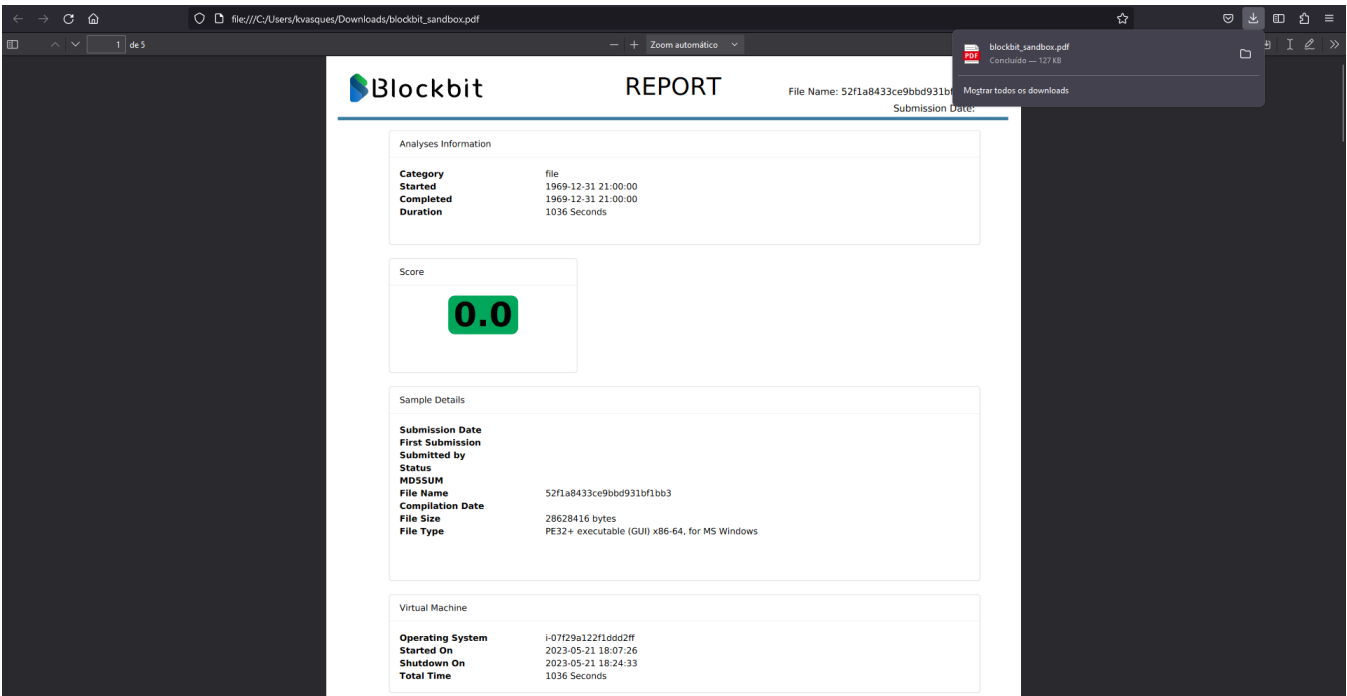
Seção Screenshot

Blockbit ATP Sandbox - Report

Nesta seção é possível ver um relatório contendo as informações mais relevantes sobre a assinatura, o qual pode ser baixado no formato PDF:



Aba Report



Relatório em PDF