Blockbit

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.

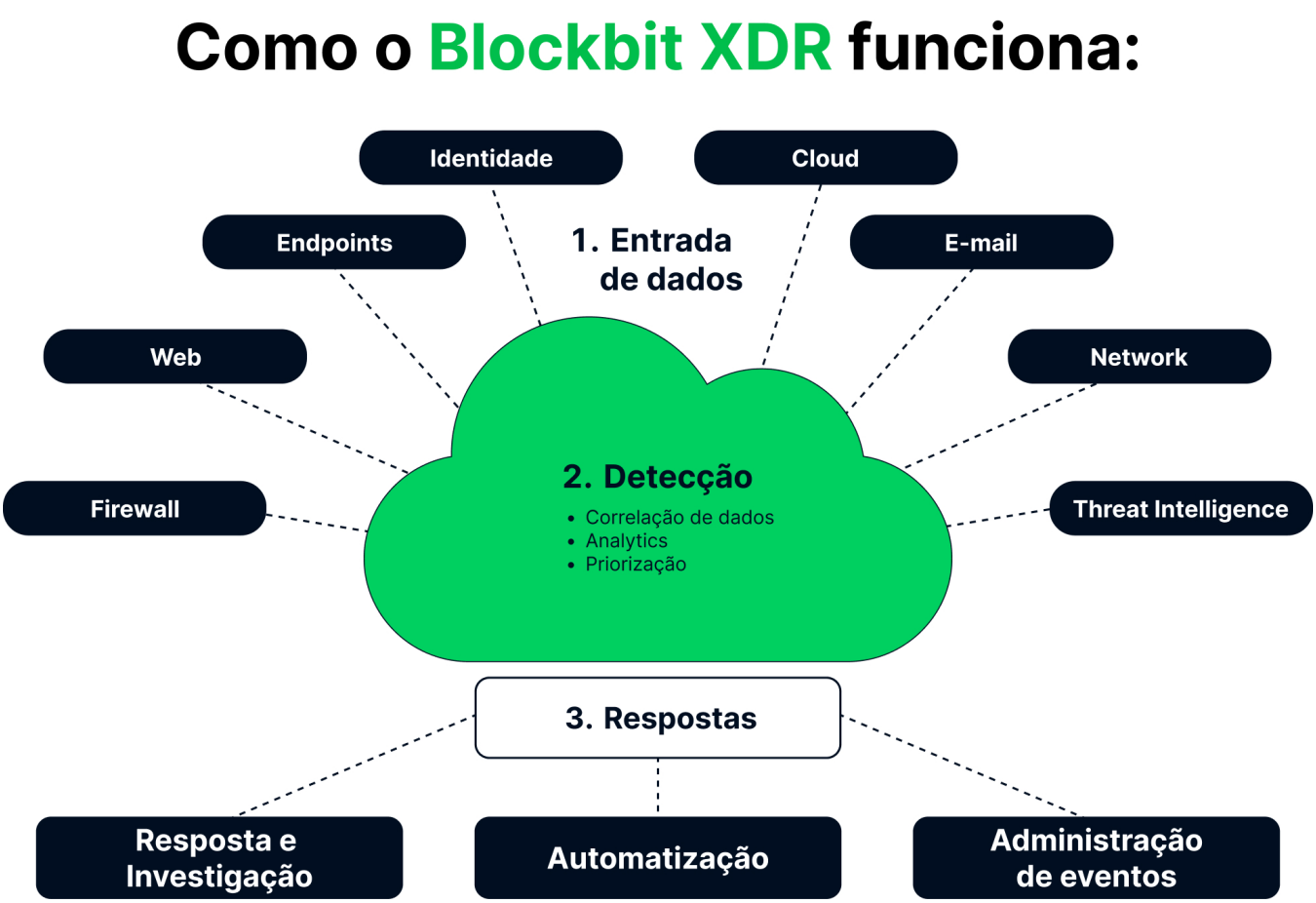
O Blockbit XDR (eXtended Detection & Response) é uma solução avançada de cibersegurança, projetada para oferecer visibilidade, proteção e resposta abrangentes a ameaças em múltiplos vetores, incluindo endpoints, redes, e-mails e ambientes em nuvem.

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.



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.

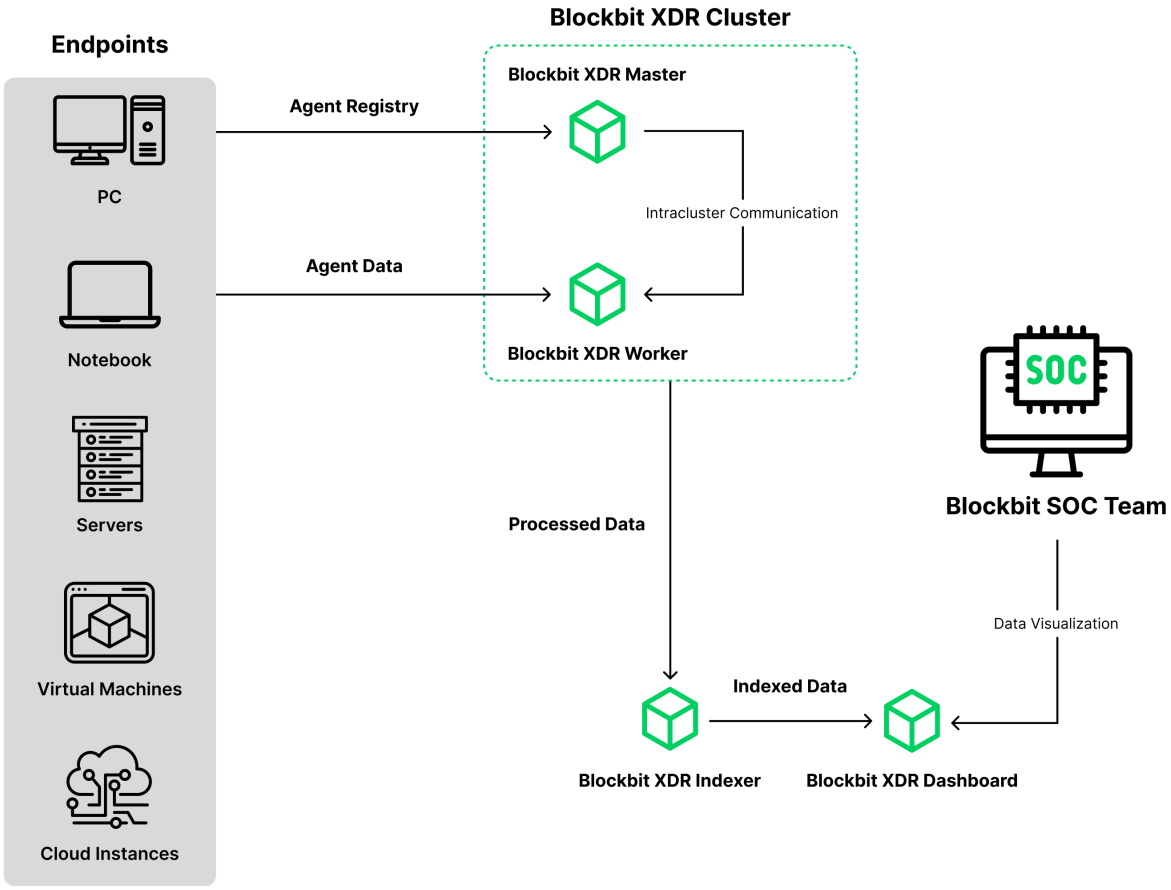
- **Tamanho do agente:** entre 50 e 100 MB;
- **Requisito de memória:** entre 10 e 50 MB;
- **Requisito de disco:** entre 50 e 100 MB;
- **Requisito de rede:** 10 KB/sec;
- **Requisito para conectividade entre agentes:** Portas **1514/TCP** e **1515/TCP** abertas para a Internet.

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 Admininstração 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 endpoin:

```
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 habilidado 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:

```
eyJhbGciOiJFUzUxMiIsInR5cCI6IkpXVCJ9.
eyJpc3MiOiJ3YXp1aCIsImF1ZCI6IldhenVoIEFQSSBSRVNUIiwibmJmIjoxNzA3ODk4NTEzLCJleHAiOjE3MDc4OTk0MTMsInN1YiI6IndhenVo
IiwicnVuX2FzIjpmYWxzZSwicmJhY19yb2xlcyI6WzFdLCJyYmFjX21vZGUiOiJ3aGl0ZSJ9.ACcJ3WdV3SnTOC-
PV2oGZGCyH3GpStSOu161UHHT7w6eUm_REOP_g8SqqIJDDW0gCcQNJTEECortIuI4zj7nybNhACRlBrDBZoG4Re4HXEpAchyFQXwq0SsZ3HHSj7e
JinBF0pJDG0D8d1_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 hostnamens 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/analysisd (:)
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.

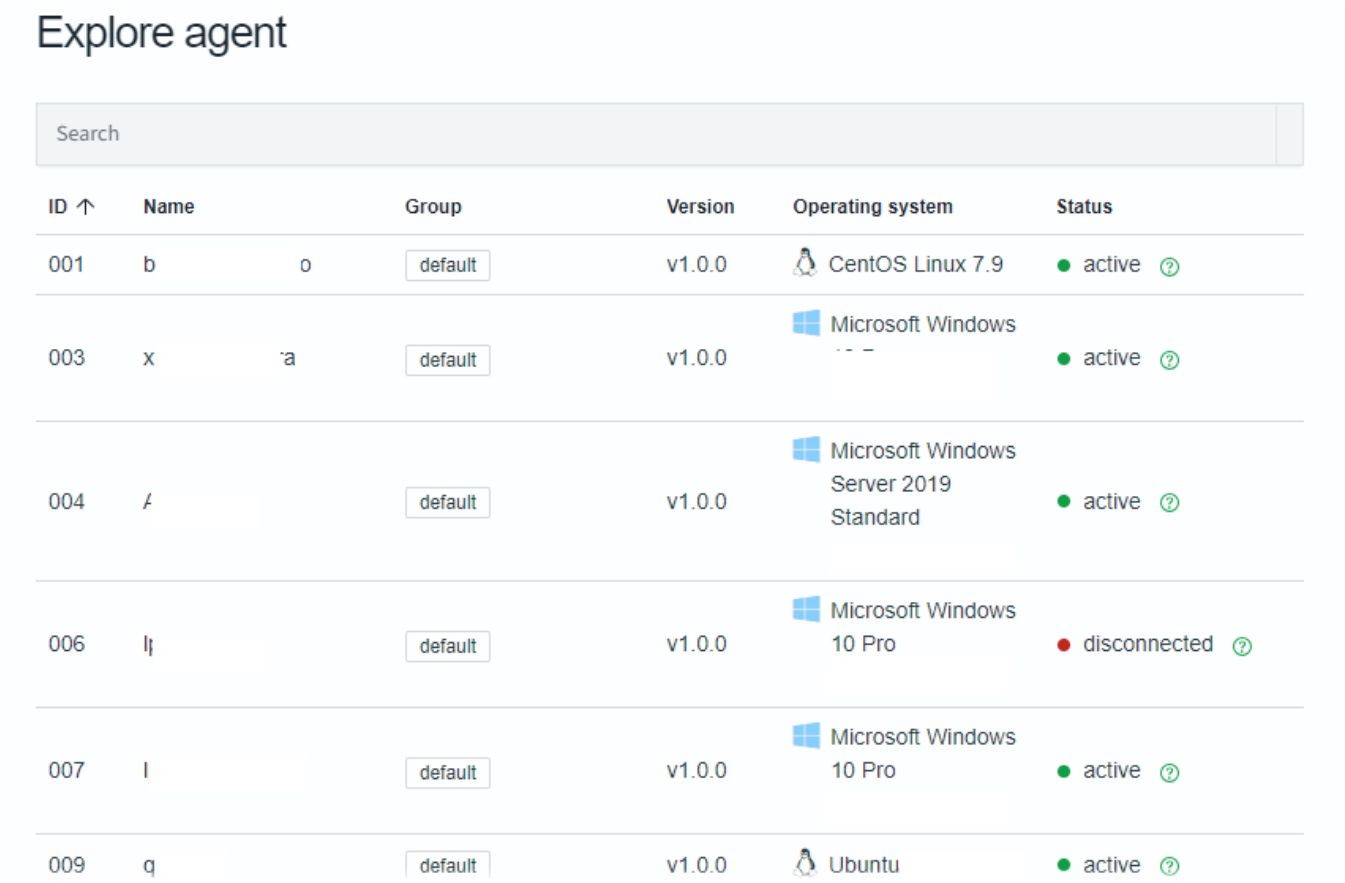
Na lista, cada agente corresponde a um endpoint.

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.



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 **B BXDR_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.

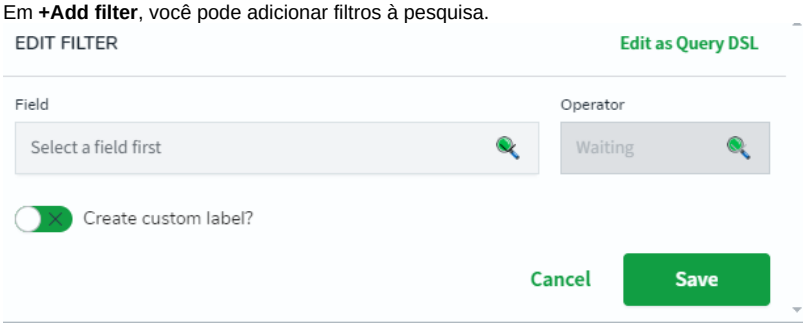

Blockbit
Log in to Blockbit XDR
Username
Password
MFA Code
Log in

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.



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

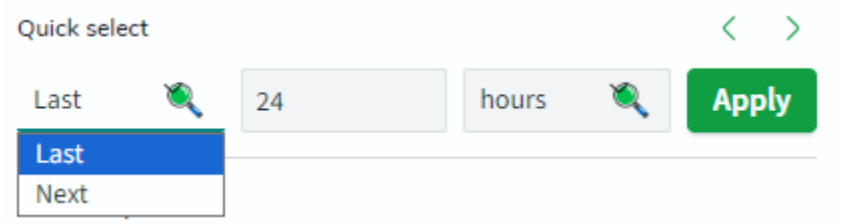
Ao clicar em **create custom label?**, você pode criar um nome específico para a query.

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

Clique em salvar ( ) para salvar a query.

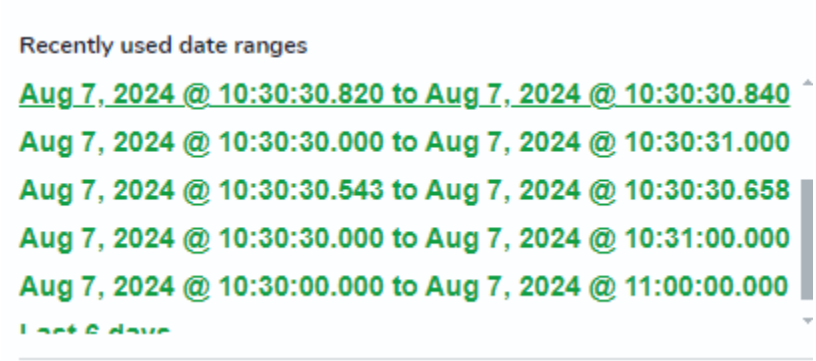
Ao clicar no calendário ( ), um modal irá abrir e você poderá selecionar um intervalo de tempo para verificar os eventos de segurança.

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**.

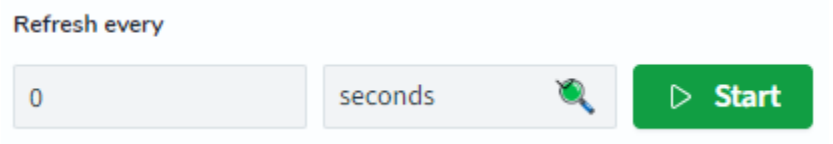


Em **Commonly used**, você poderá usar um intervalo pré-programado (ex: últimos 15 minutos).

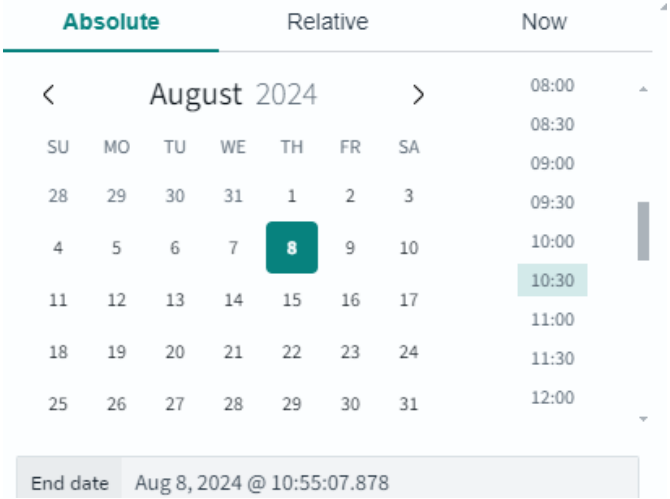
Em **Recently used date ranges**, você poderá reutilizar um intervalo de tempo.



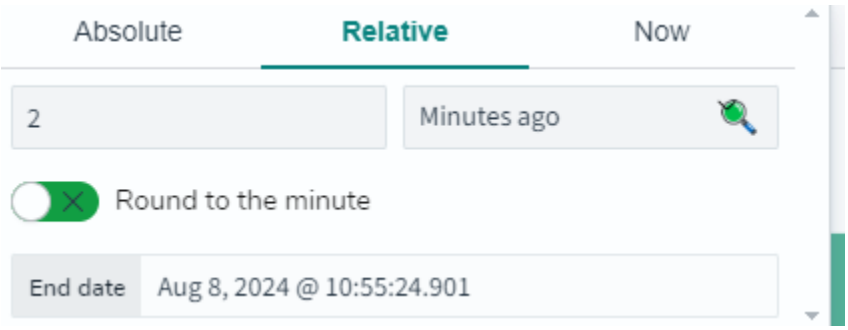
Em **Refresh every**, você poderá configurar a atualização automática da página. Você pode determinar a quantidade e a duração do intervalo. Para aplicar, clique em **Start**.



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).



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



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.

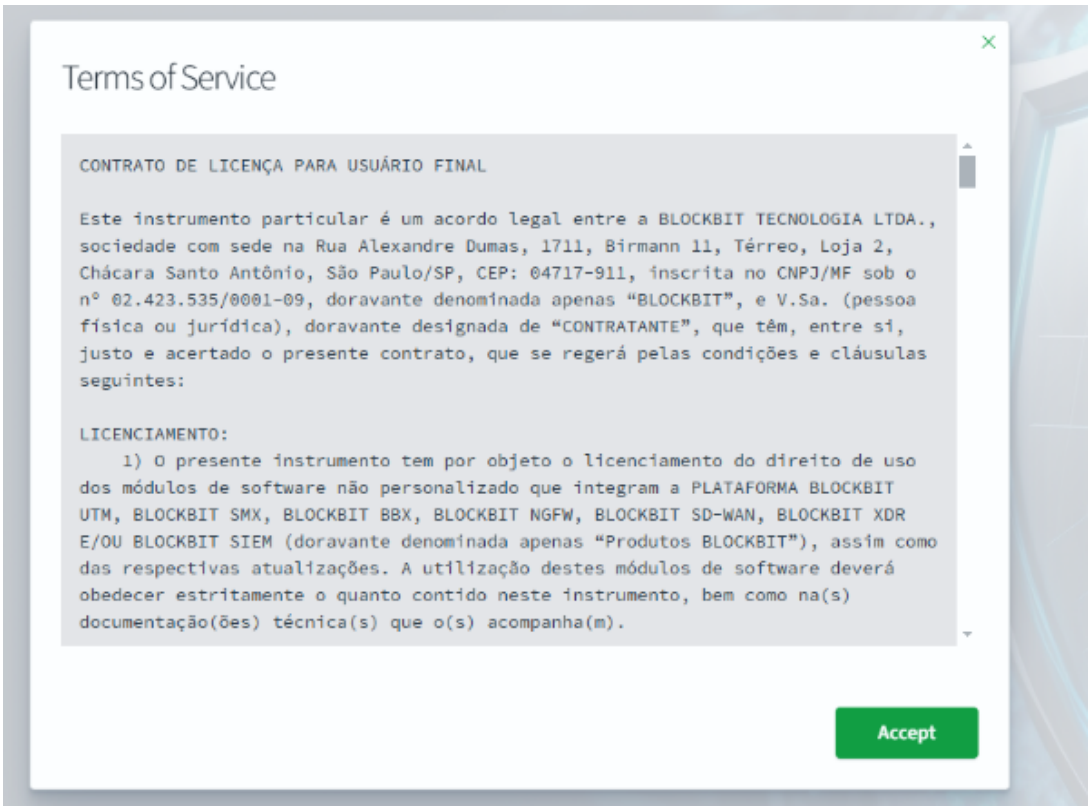
Ao acessar a plataforma, o usuário será direcionado para a tela de login, onde poderá autenticar-se utilizando uma das seguintes opções:

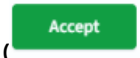
- **Usuário Local + MFA:** Utiliza credenciais cadastradas diretamente no Blockbit XDR, exigindo nome de usuário, senha e um token de autenticação multifator (MFA).
- **SSO via LDAP + MFA:** Permite a autenticação integrada com um servidor LDAP corporativo, adicionando uma camada extra de segurança com 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:



Clique em **Accept (** 

)para aceitar.

XDR - Dashboard

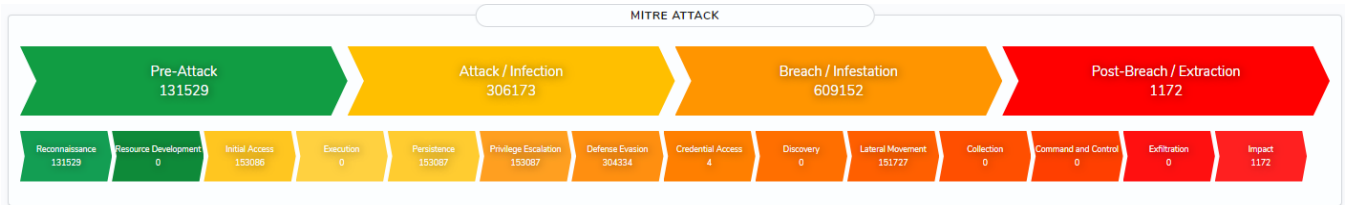
O Dashboard do Blockbit XDR oferece uma interface intuitiva e centralizada, proporcionando uma visão abrangente da segurança do ambiente em tempo real. Com gráficos interativos, painéis personalizáveis e alertas priorizados, os administradores podem monitorar eventos críticos, analisar ameaças e tomar 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.

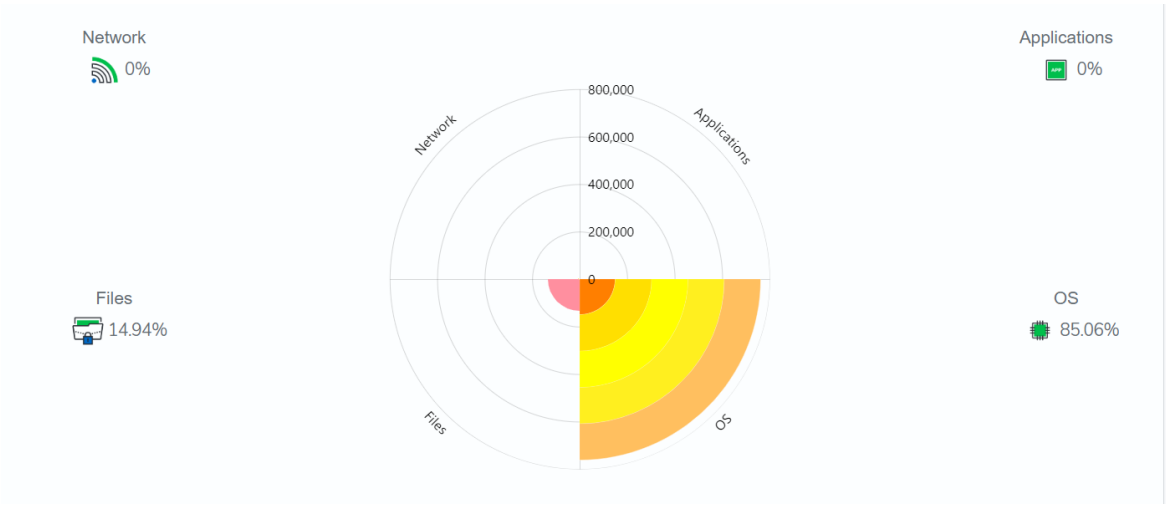
Técnicas

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

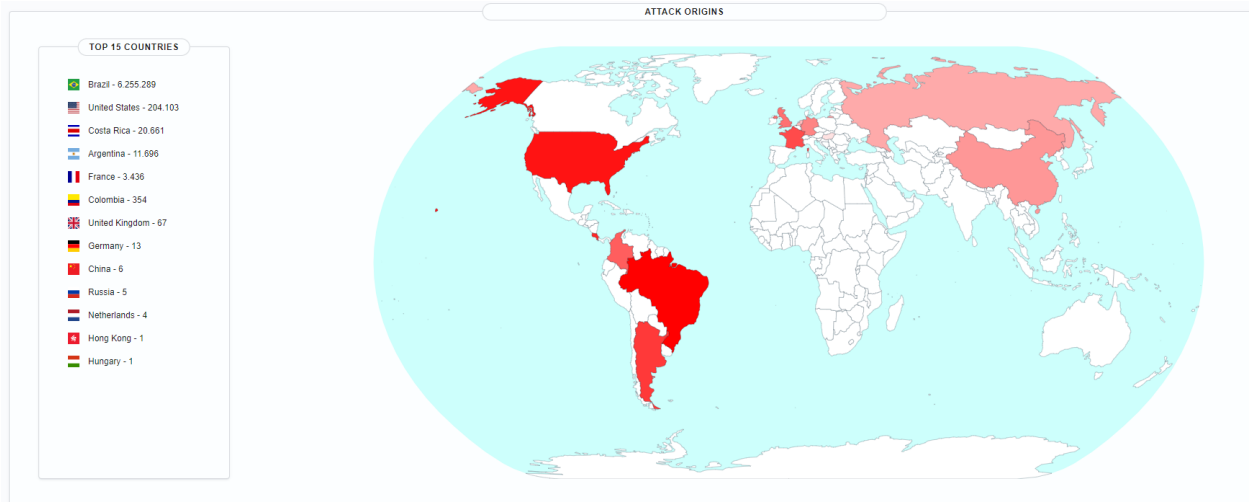
O Blockbit XDR apresenta dois gráficos divididos em 4 seções. Cada seção tem 1/4 de um círculo, onde cada faixa ataques divididos por severidade. Quanto mais ao centro, mais severo.



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**
Reconaissance	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 desapercebido.

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

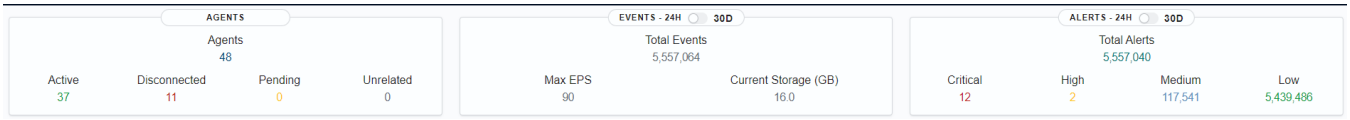
Severidade	**Crítica**
Command and control	Tentativa de comunicação com sistemas comprometidos para controlá-los.
Exfiltration	Tentativa de roubo de dados.
Impact	Tentativa de manipular, interromper ou destruir um sistema ou seus dados.

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.

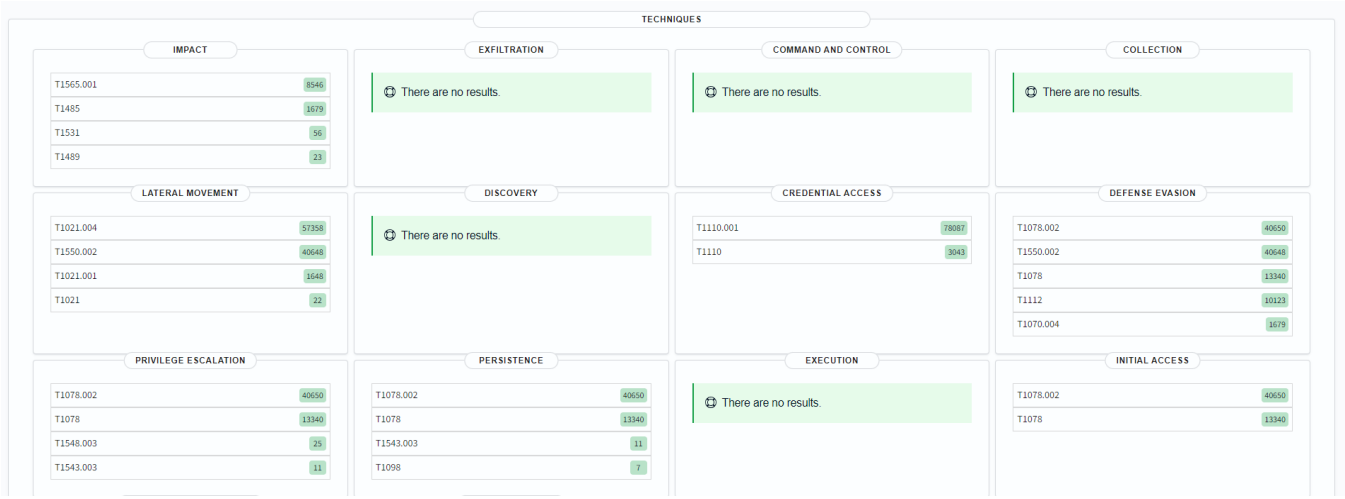
Total alerts

- 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.

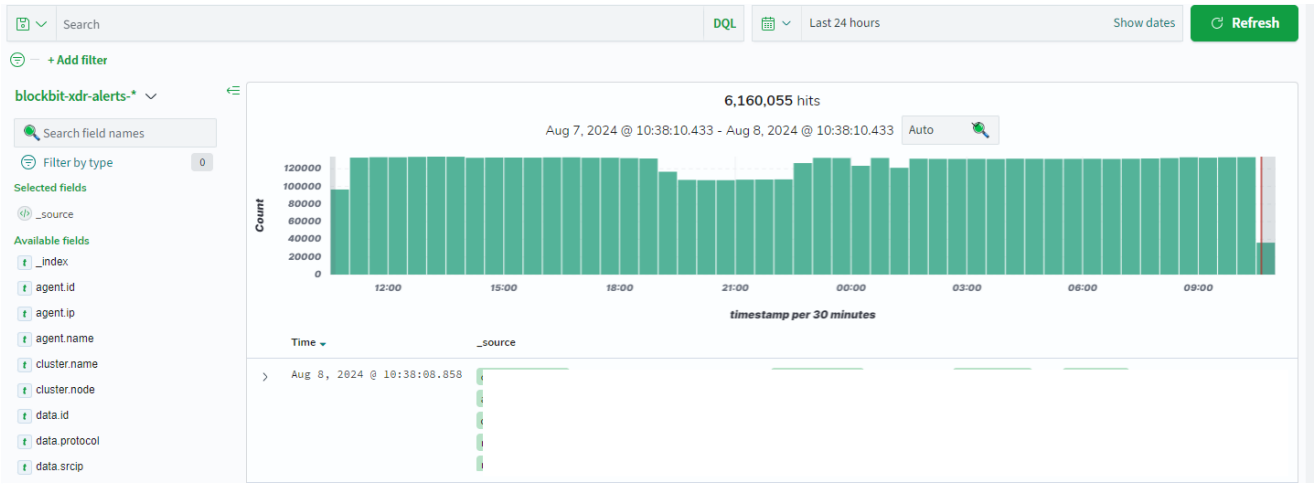
Ao clicar, você será direcionado à página Security events com informações de ataques utilizando a tática selecionada.

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.

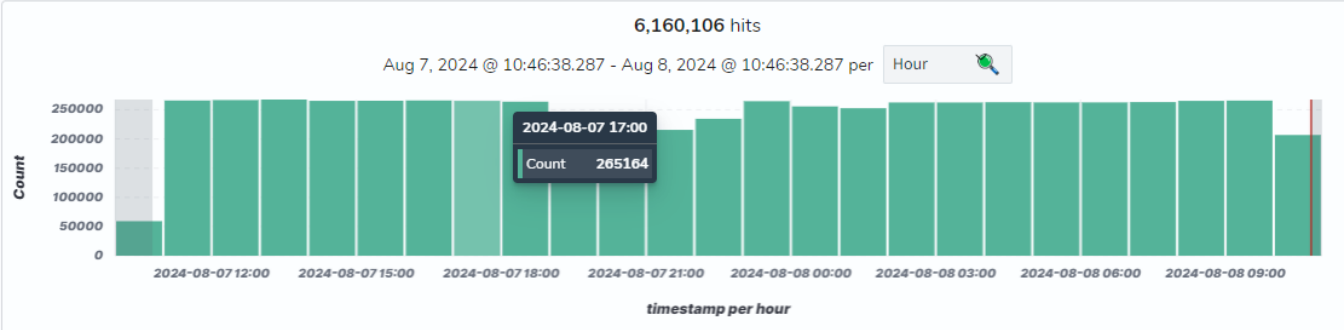
Remediação e Mitigação

- O Blockbit XDR pode marcar um grupo completo de eventos ou eventos isolados como ameaça e iniciar ações de resposta e mitigação, incluíndo **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.

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

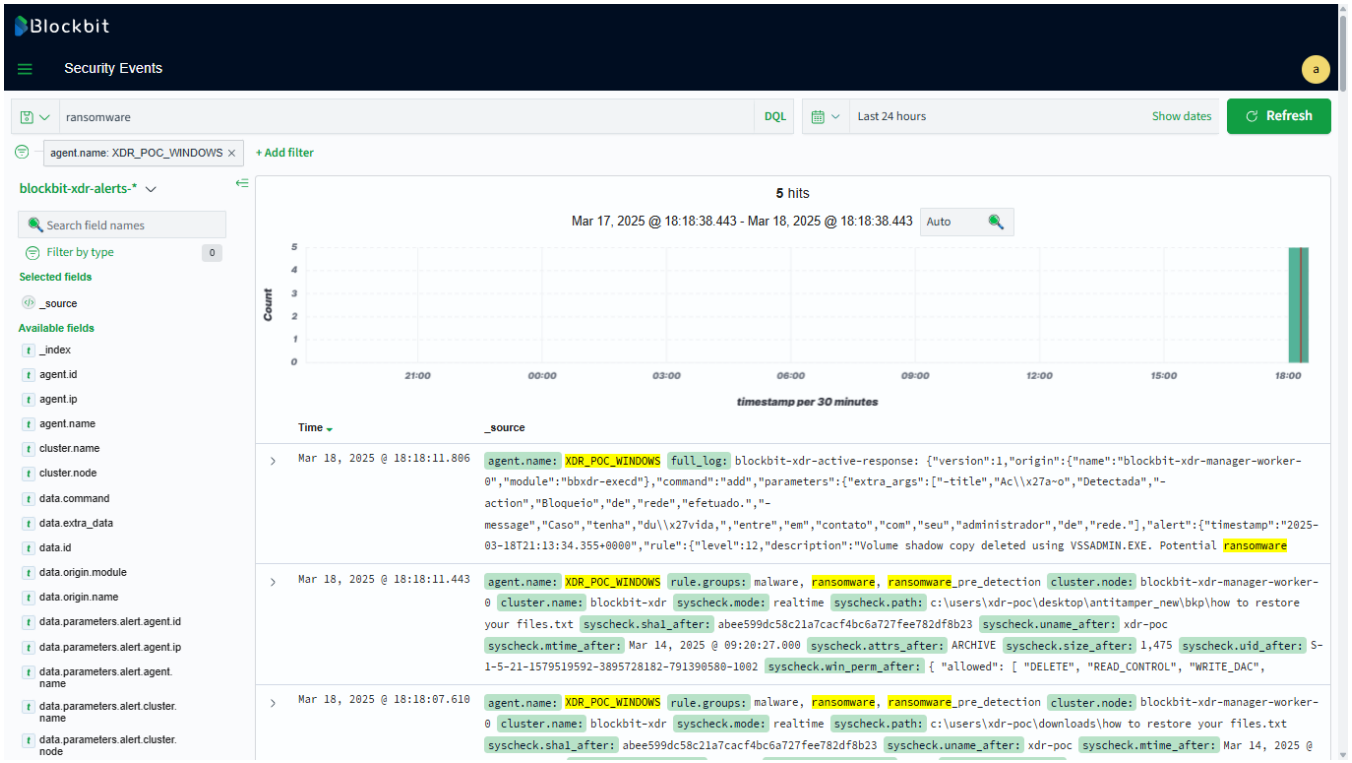
O Blockbit XDR é uma solução avançada de segurança que permite a detecção, correlação e resposta a incidentes de ransomware utilizando múltiplos vetores de análise e resposta automatizada. Este guia visa orientar o administrador na investigação e mitigação de ataques, utilizando a filtragem por rule.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

2. Identificação de Eventos Relacionados a Ransomware

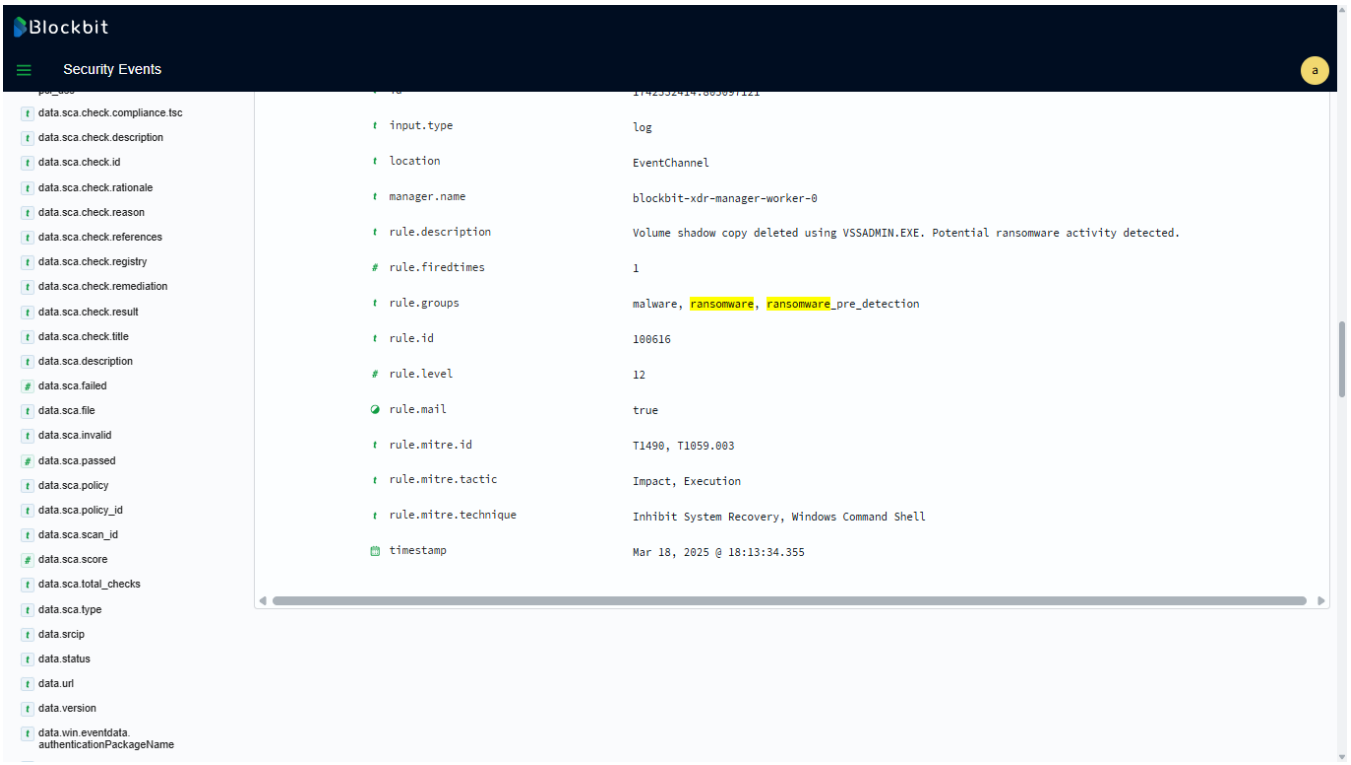
2.1 Aplicação de Filtros

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

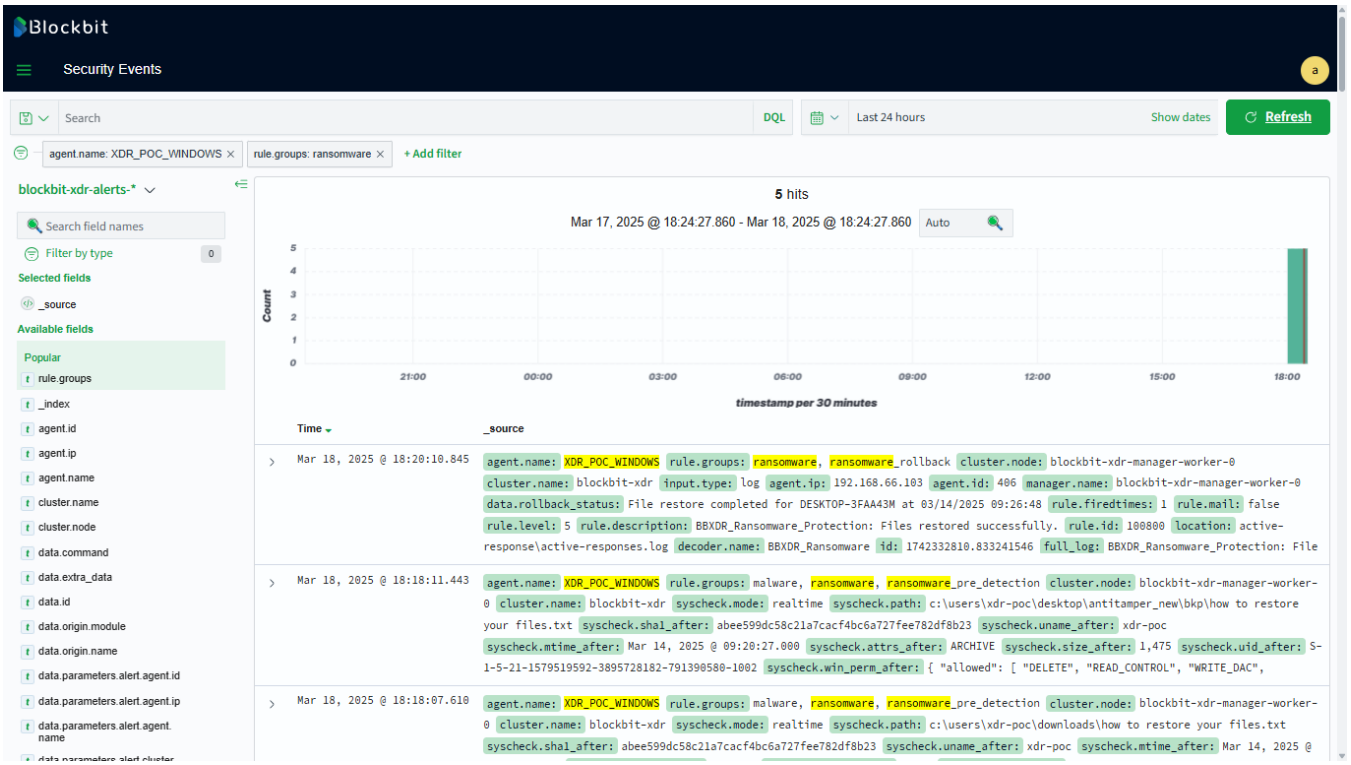
Acesse a interface de Security Events.
No campo de busca, insira "ransomware" ou utilize o filtro rule.group=ransomware.
Visualize os eventos relacionados à detecção de ransomware no ambiente.



Logs do início do incidente



Exibe um alerta de pré-detecção de ransomware.



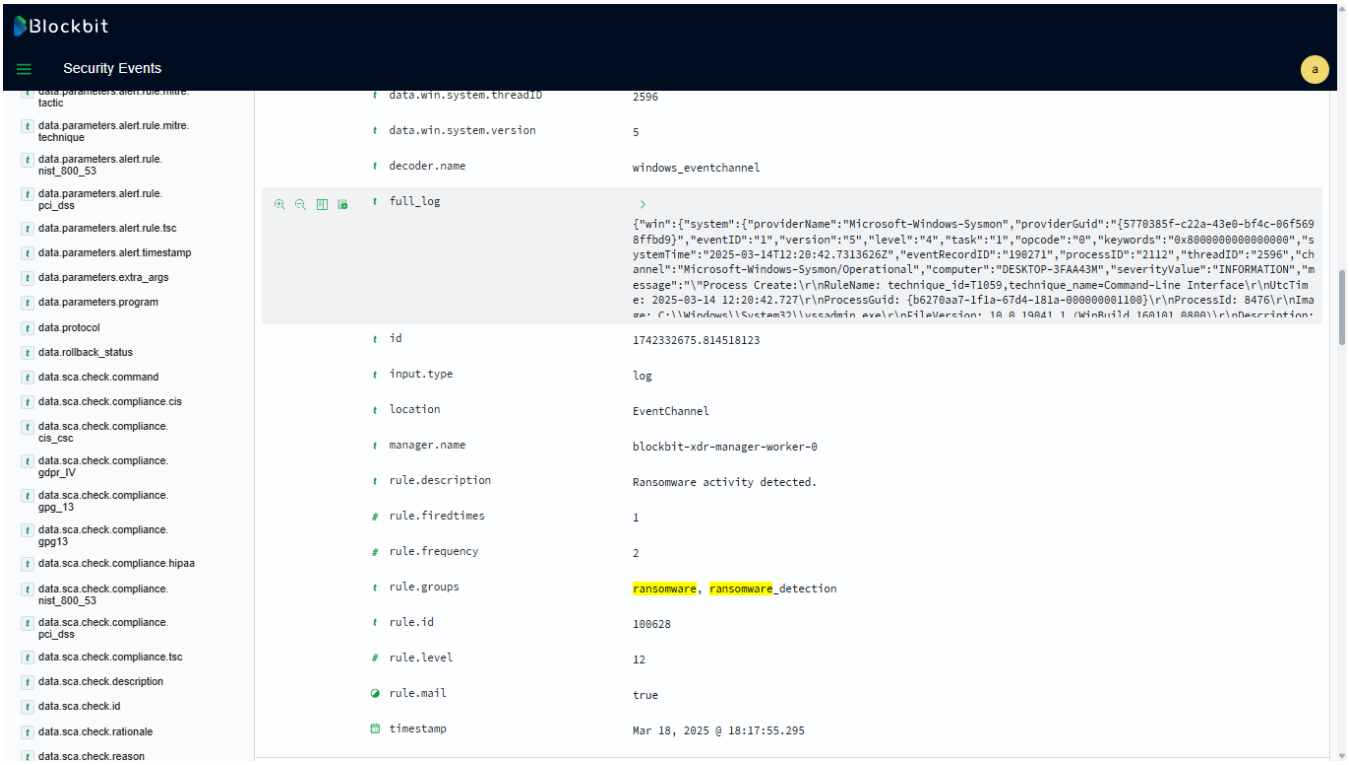
Aplicação do filtro rule.group="ransomware".

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).
Analise 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.



Logs confirmando o ataque.

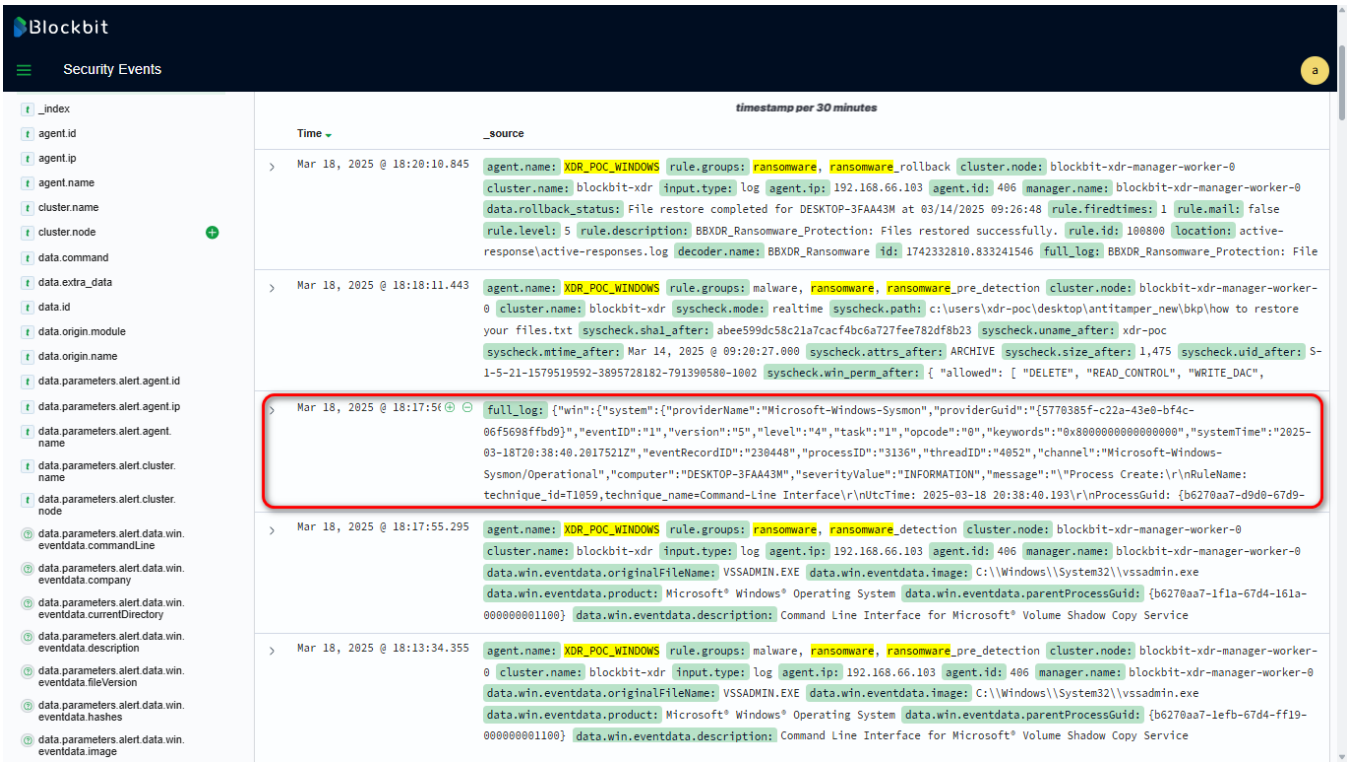
4. Respostas Automáticas e Ações Mitigatórias

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.



Log da ação de isolamento do endpoint.

4.2 Reversão de Alterações no Sistema

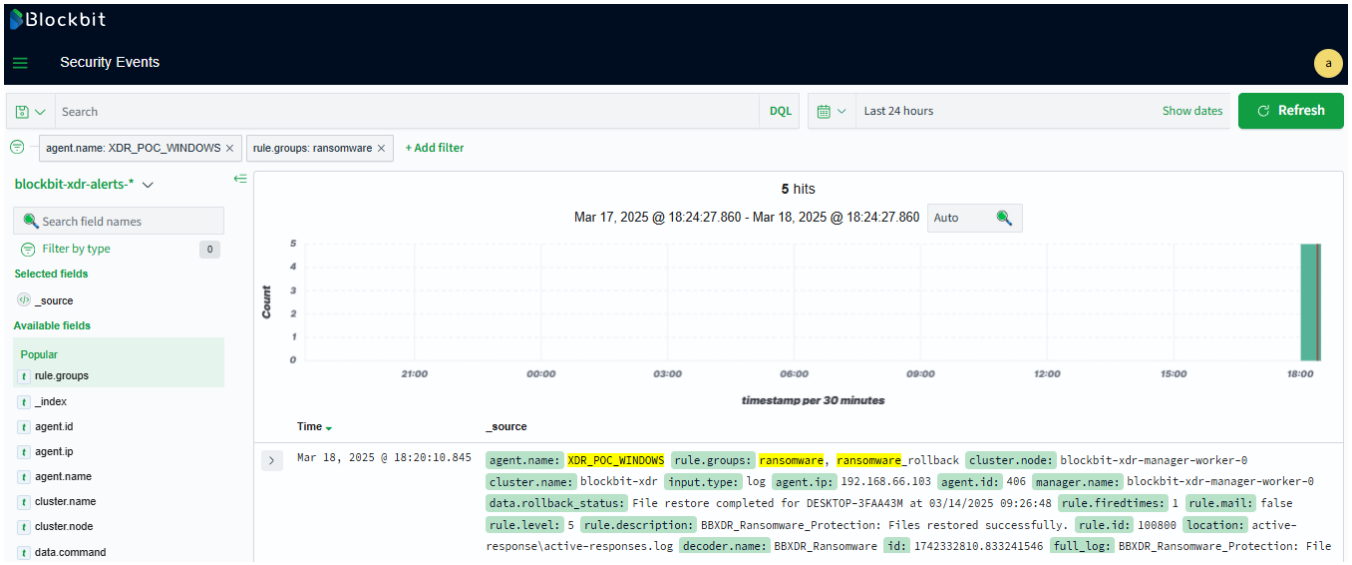
O Blockbit XDR é capaz de desfazer qualquer modificação realizada por um ataque, restaurando configurações do sistema, edições de registro e permissões de arquivos comprometidos.

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 admininstração.

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 Rolllback 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

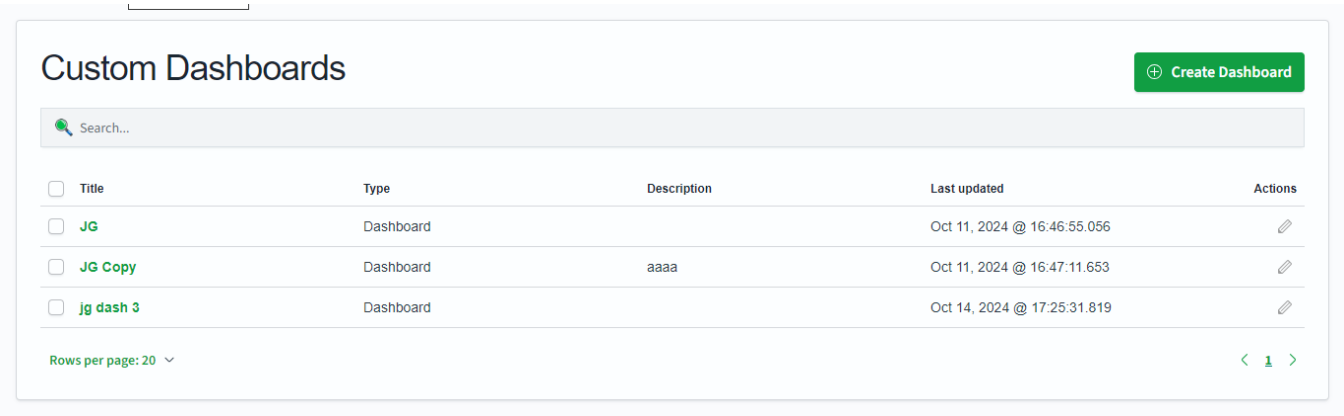
Essas funcionalidades garantem que o Blockbit XDR não apenas detecte, mas também responda e mitigue ameaças de forma automatizada, reduzindo o tempo de resposta e minimizando impactos operacionais.

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.



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;

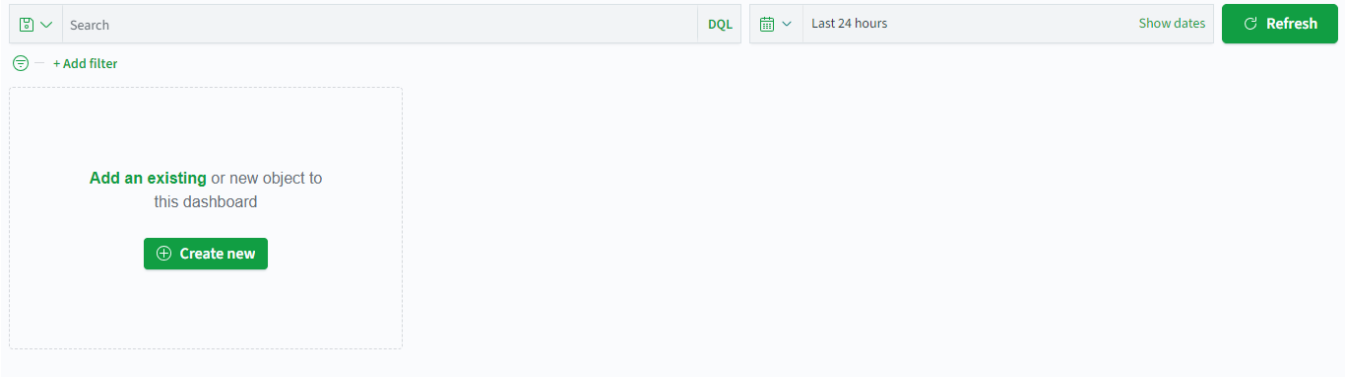
Description: descrição do dashboard;

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.

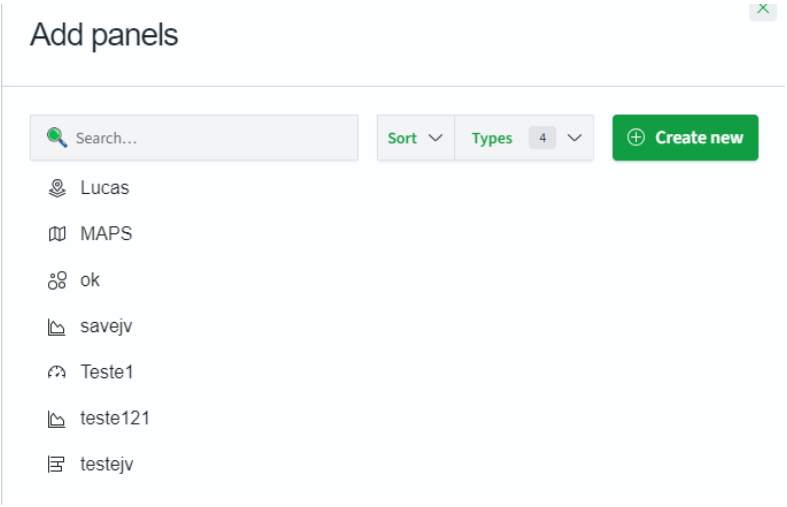


Search

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.

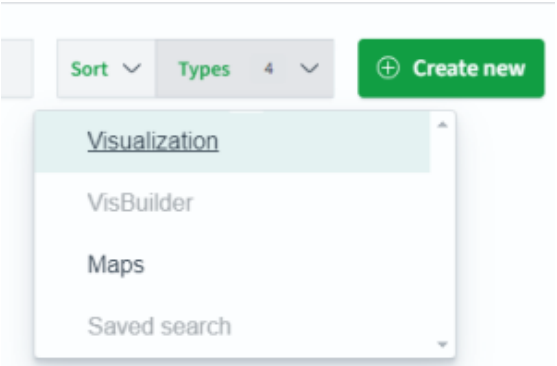
Um modal irá se abrir com uma lista de visualizações já criadas:



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 descendente.

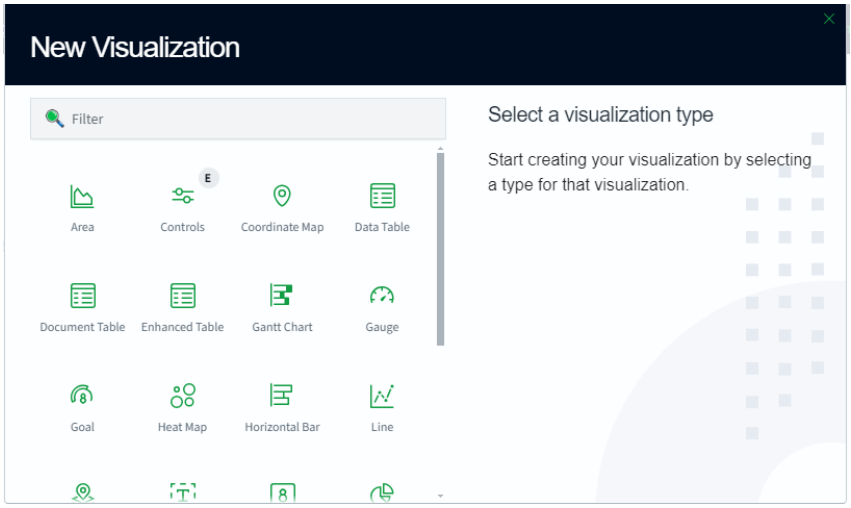
Em types, você pode selecionar as visualizações por tipo.



Para criar uma nova visualização, clique em **Create new** (

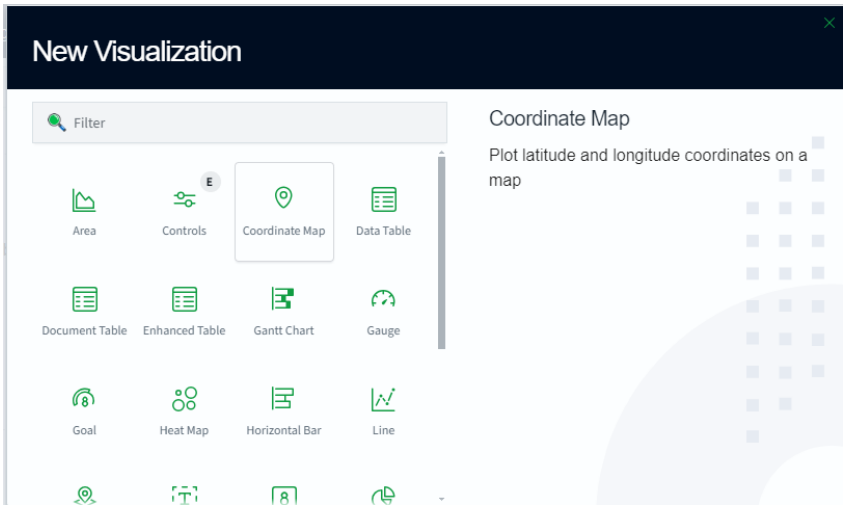
).

Um modal com as visualizações disponíveis irá abrir:



XDR - Custom Dashboards - Create Visualization

Ao clicar em Create new, um modal irá aparecer:

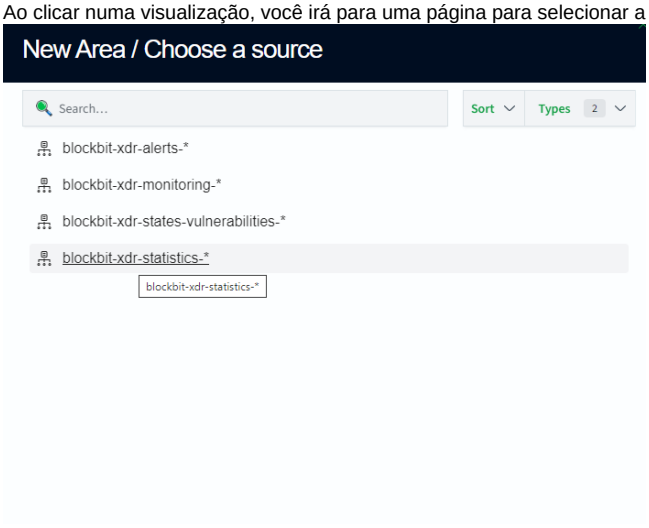


Este modal contém os tipos de visualizações suportados pelo Blockbit XDR.

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.

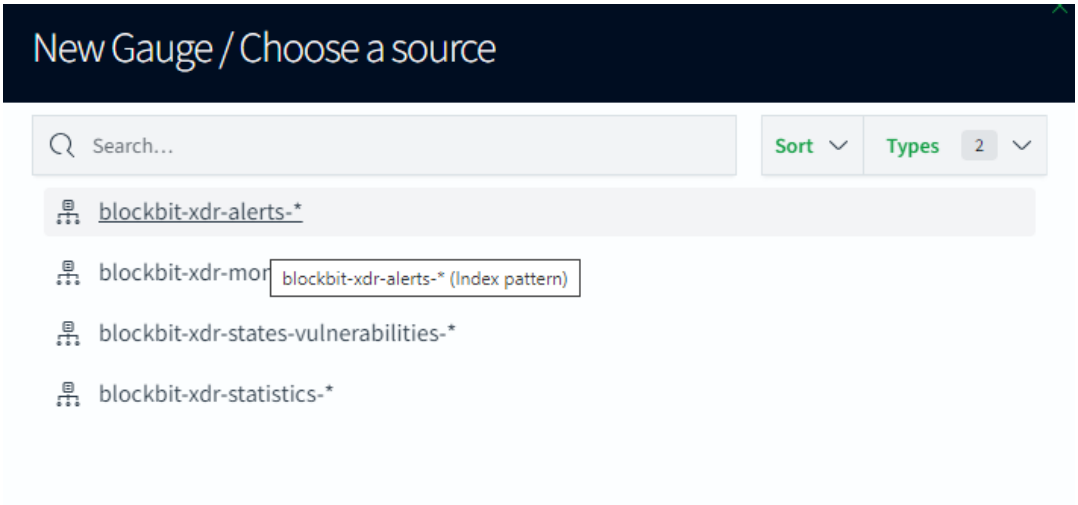
Para conferir todas as visualizações, acesse Visualizações Disponíveis.

XDR - Custom Dashboards - How to - Criar visualização

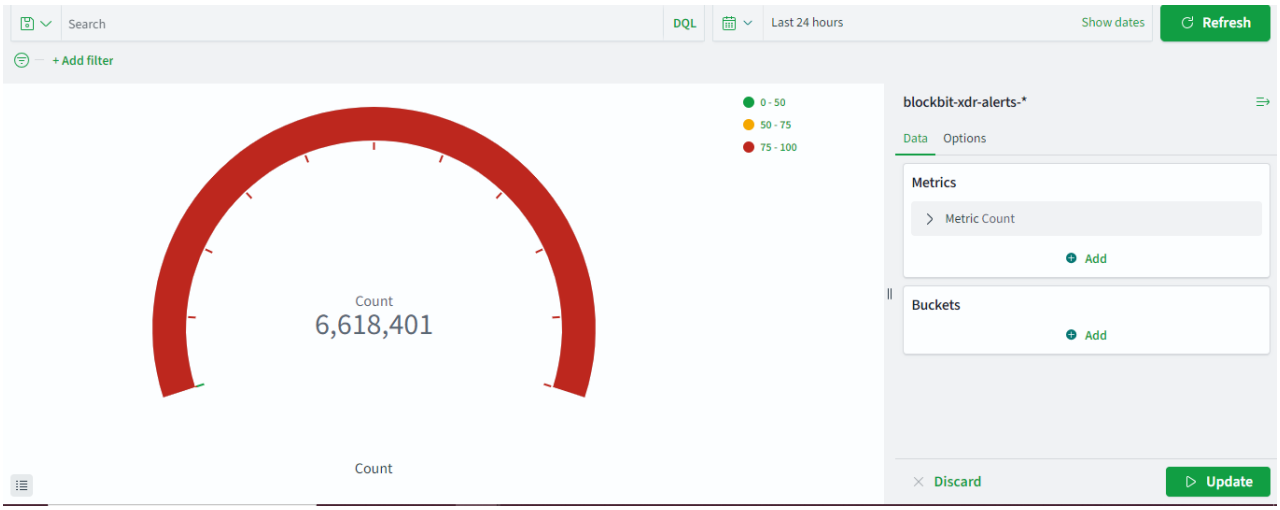
Neste how to você irá aprender a criar uma visualização tipo **Gauge** para o dado **rule.frequency**.

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:

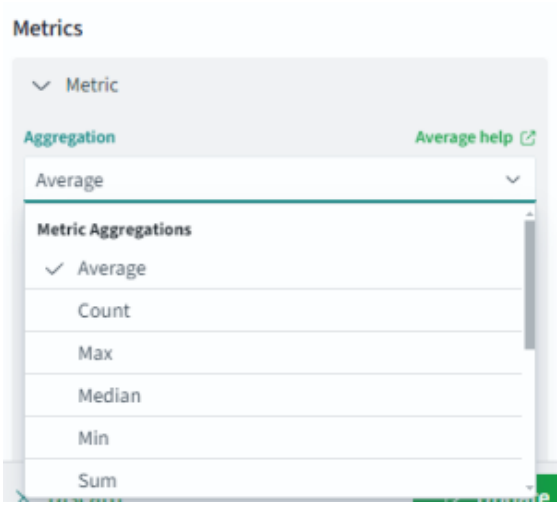


O gráfico em questão conta todos os dados da fonte.

Clique em Metric count.

Um submenu irá abir.

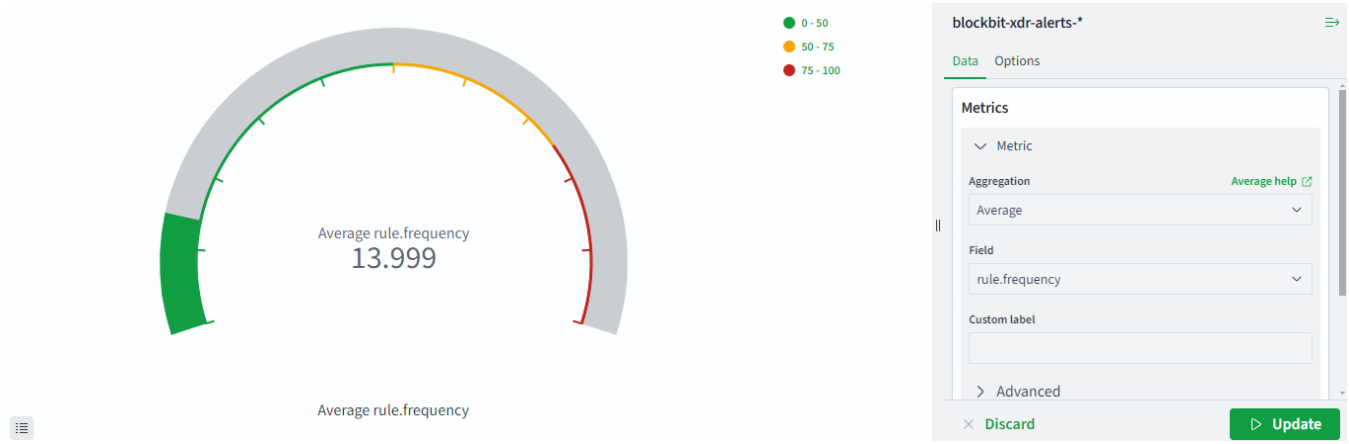
Em **Aggregation**, selecione **Average**.



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

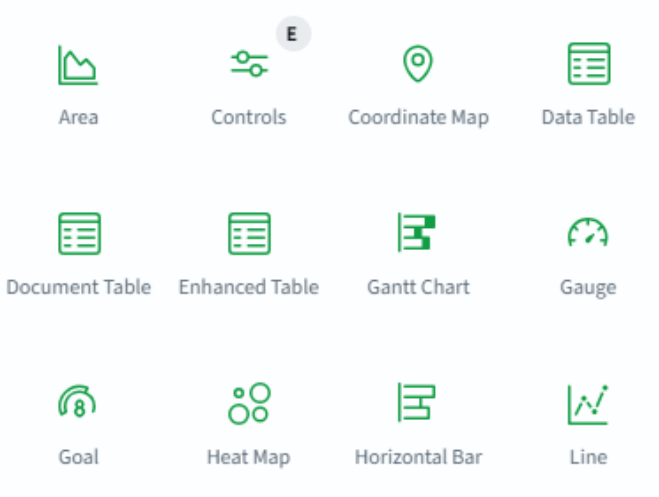
Clique em Update.

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

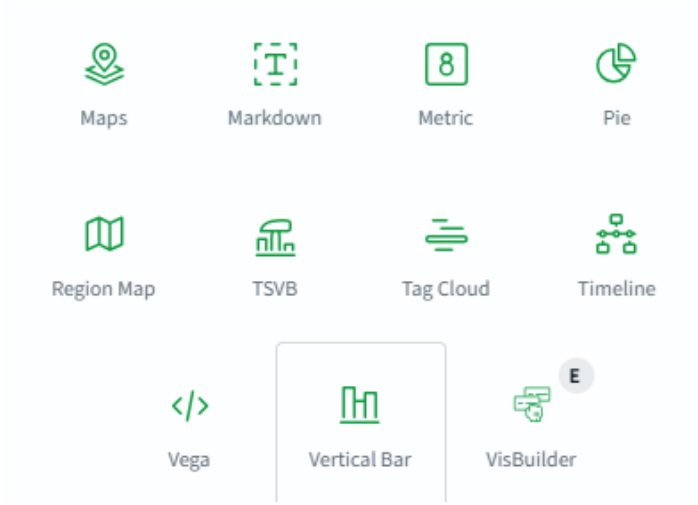
Gráfico que mostra a frequência de um evento ao longo do tempo.

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.

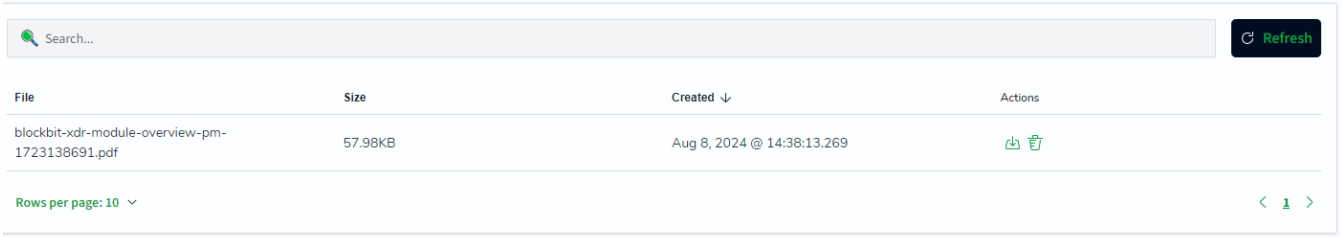
VisBuilder

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.



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:

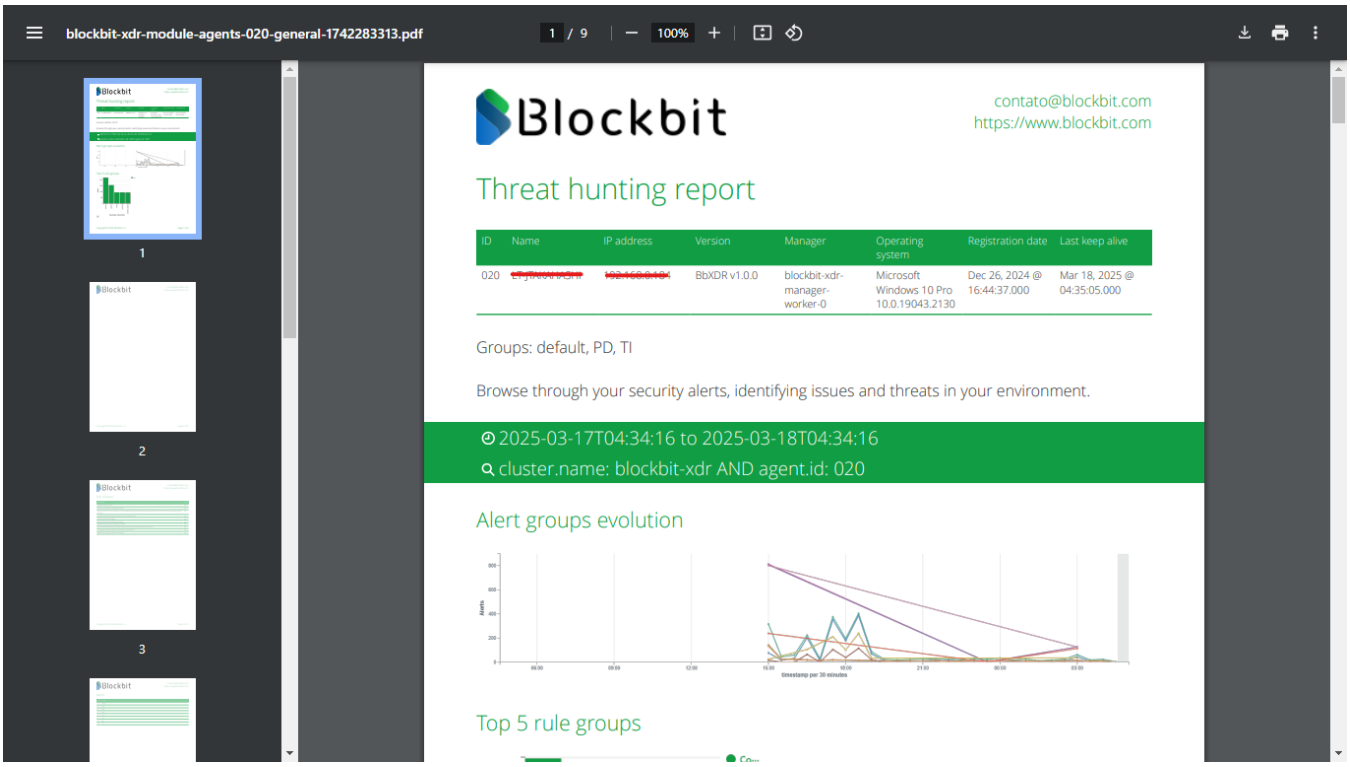
Arquivo (**File**): nome do arquivo do relatório.

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.**



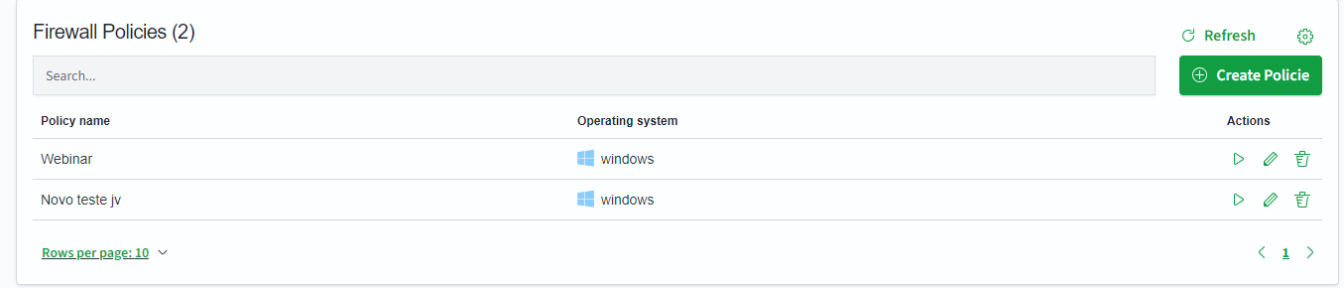
XDR - Endpoint Control Center

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.

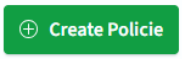
Principais Funcionalidades

- 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.



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

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

Para criar uma política, clique em **Create Policie (** ).

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

Os campos da lista são:

ID: código identificador da política;

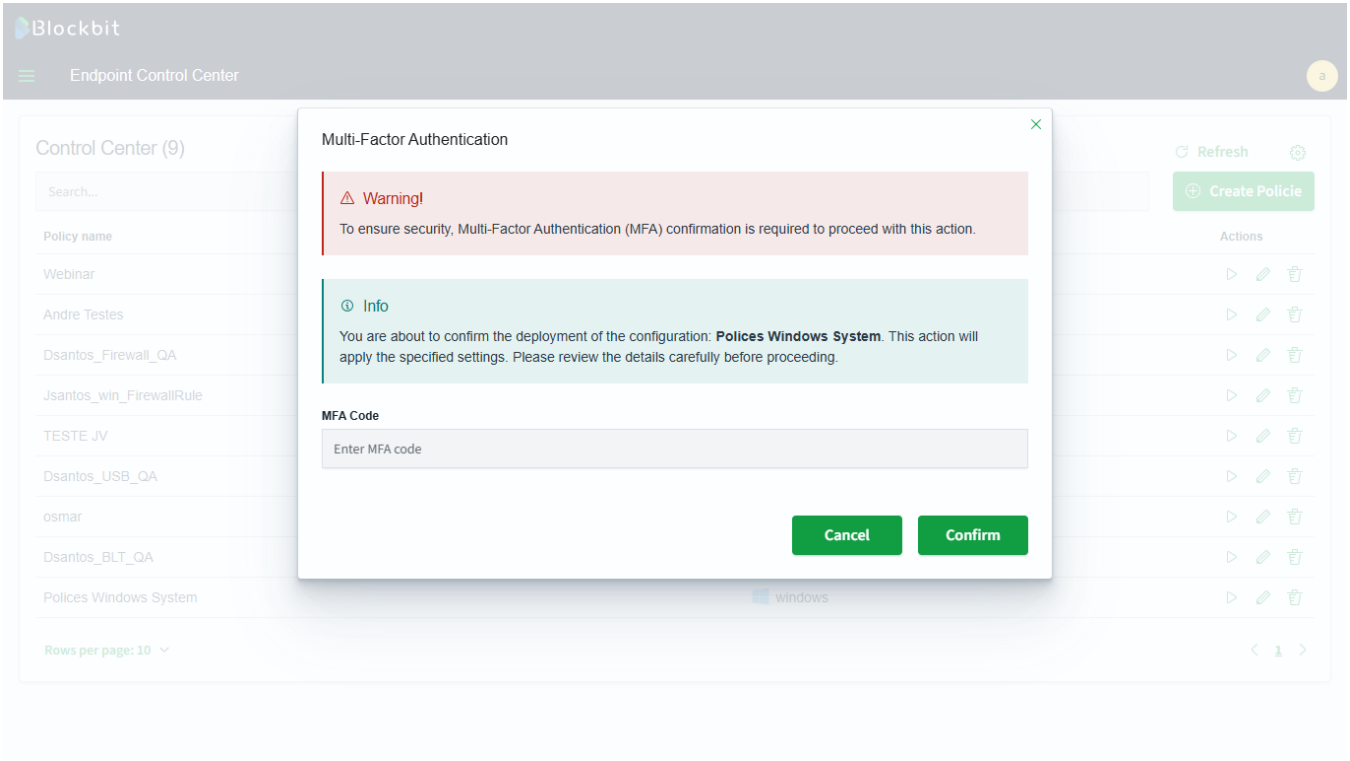
Policy name: nome da política;

Operating system: sistema operacional onde a política será aplicada;

Actions: ações disponíveis:

Deploy commands ( **)**: aplicar a politica. 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.

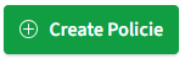


Edit ( ): editar a política;

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.

Policy Name: determine o nome da política;

Select Operating System: selecione o sistema operacional;

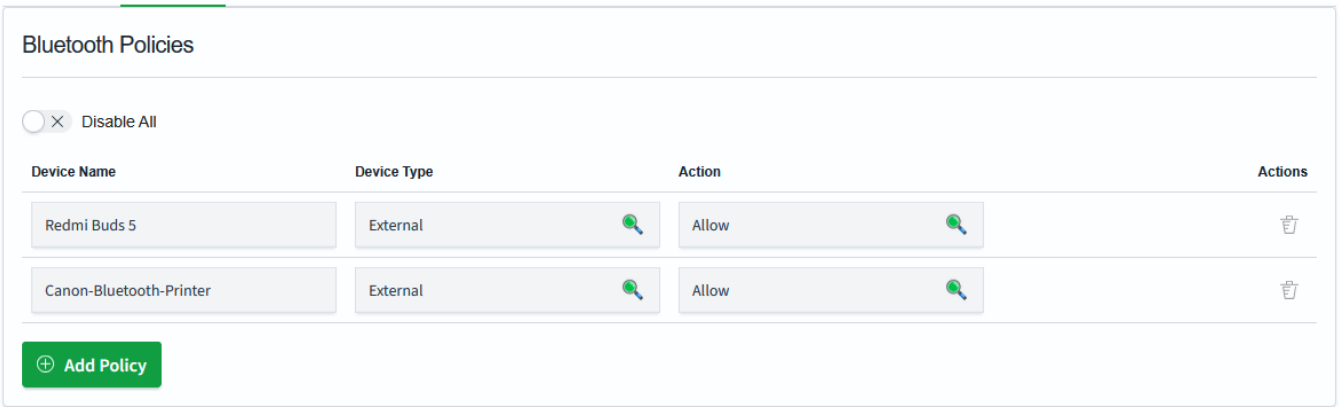
Select Agents: Selecione um ou mais agentes específicos para a aplicação da política, permitindo configurações personalizadas e envio de programações individuais diretamente do console de administração.

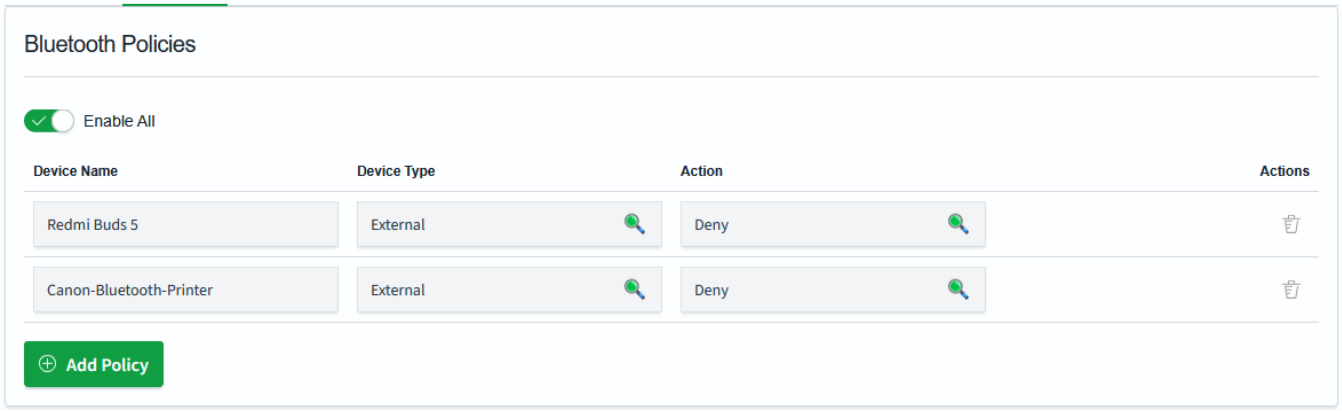
Select Group: Selecione um grupo de endpoints para aplicação da política de forma massiva, permitindo a **distribuição de configurações em lote** e a orquestração eficiente de múltiplos dispositivos simultaneamente.

General

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

Exemplos:

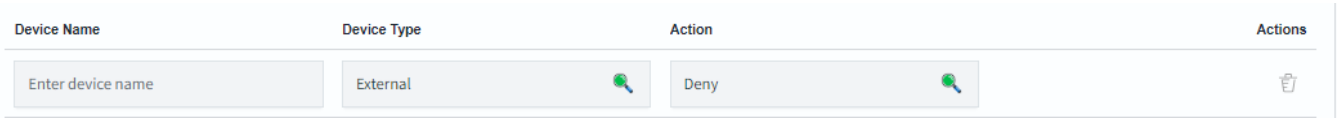




Em **Bluetooth Policies**, você cria políticas específicas para conexões via bluetooth.

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 (**  **).**

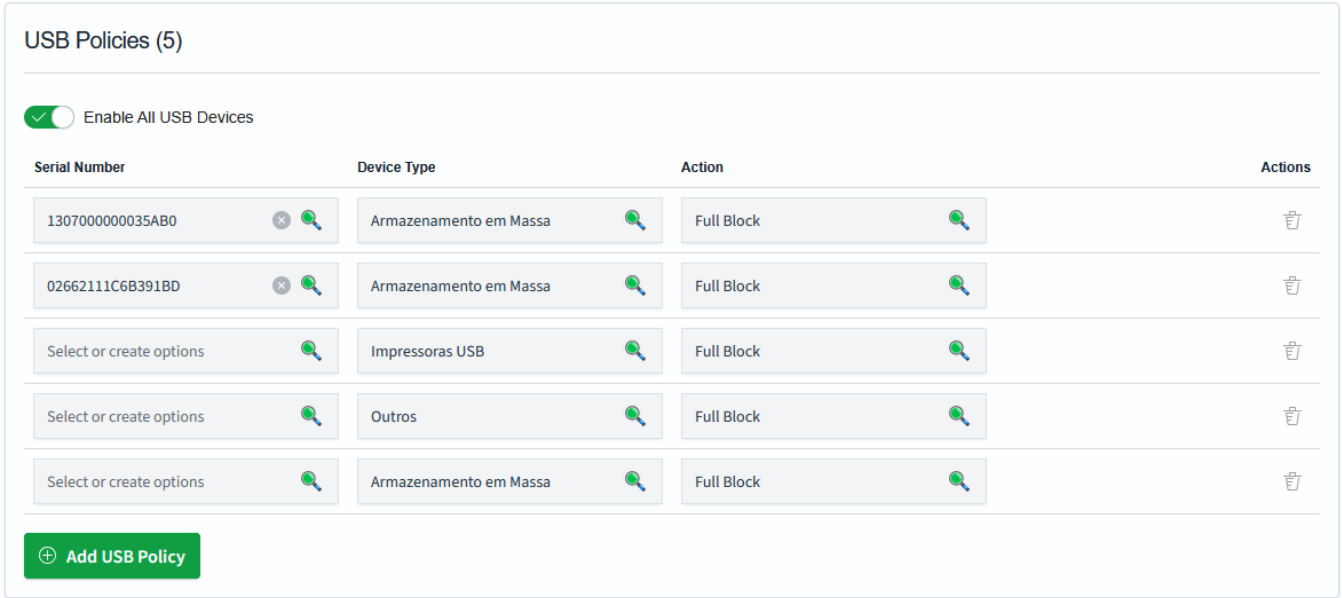


Insira o nome do periférico em **Device Name**;

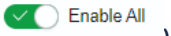
Selecione o tipo do periférico em **Device Type**. São 2 tipos: **Internal** (interno) e **External** (externo);

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 ().



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

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 USB Policy (**  **).**

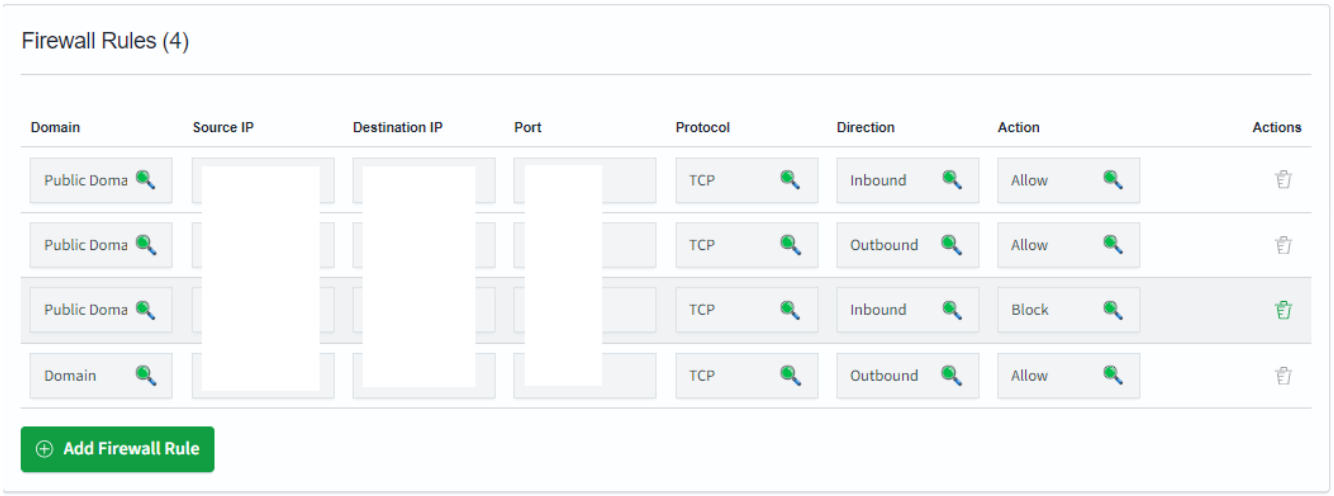
Insira o número de série do periférico em **Serial Number**;

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

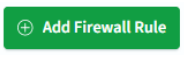
Os tipos de periférico são determinados pelo sistema operacional.

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 ().



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.**

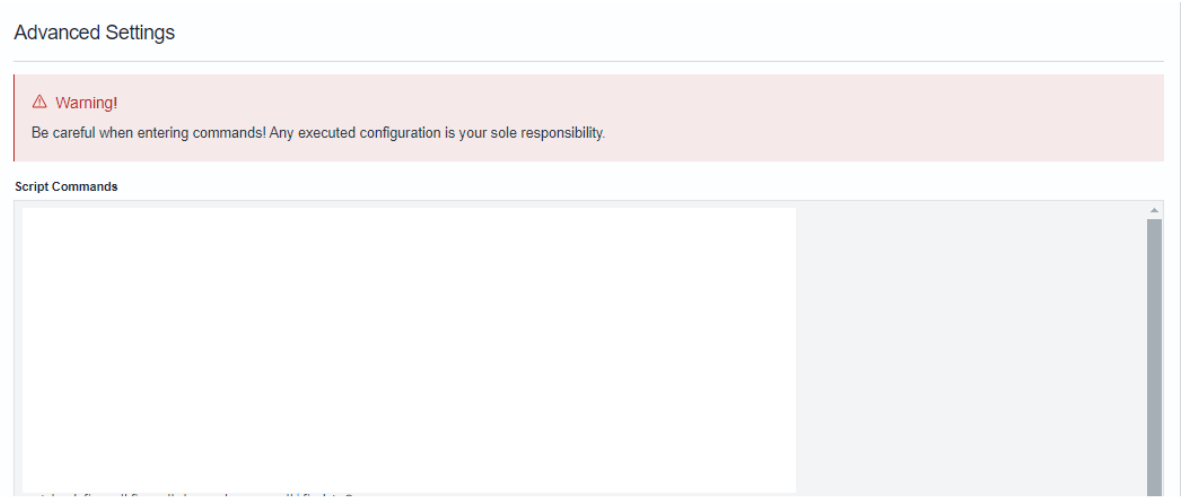
Selecione a direção em **Direction**. Pode ser **Inbound** (chegando) ou **Outbound** (saindo).

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

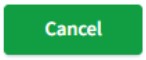
Em **Actions,** você pode deletar a política ao clicar na lixeira ( ).

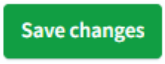
As regras de firewall configuradas pelo Blockbit XDR sempre terão prioridade sobre quaisquer outras regras criadas localmente no firewall do endpoint, garantindo um controle centralizado e eficaz da segurança da rede.

Advanced Settings



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

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

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

Exemplos da capacidade do Advanced Settings:

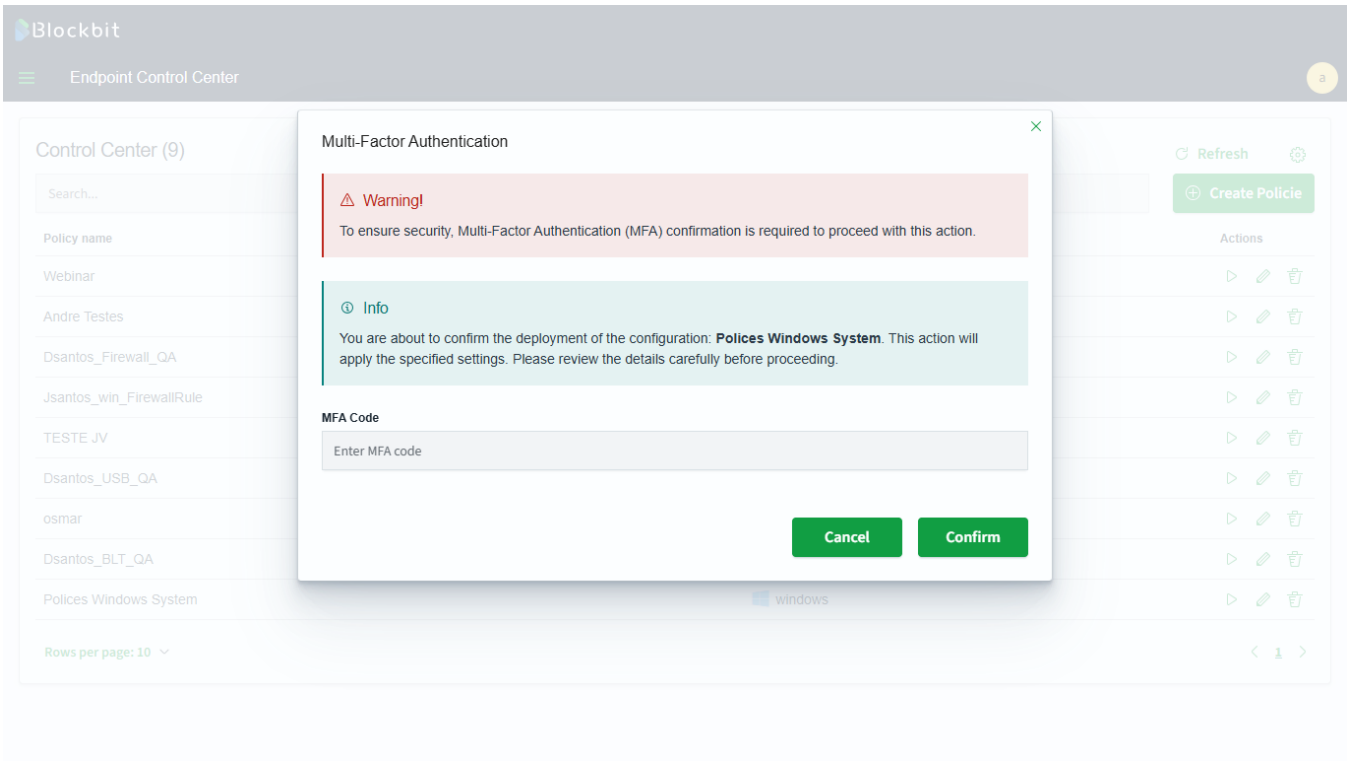
1. Script PowerShell - Atualização do Agente Blockbit XDR

```
# 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

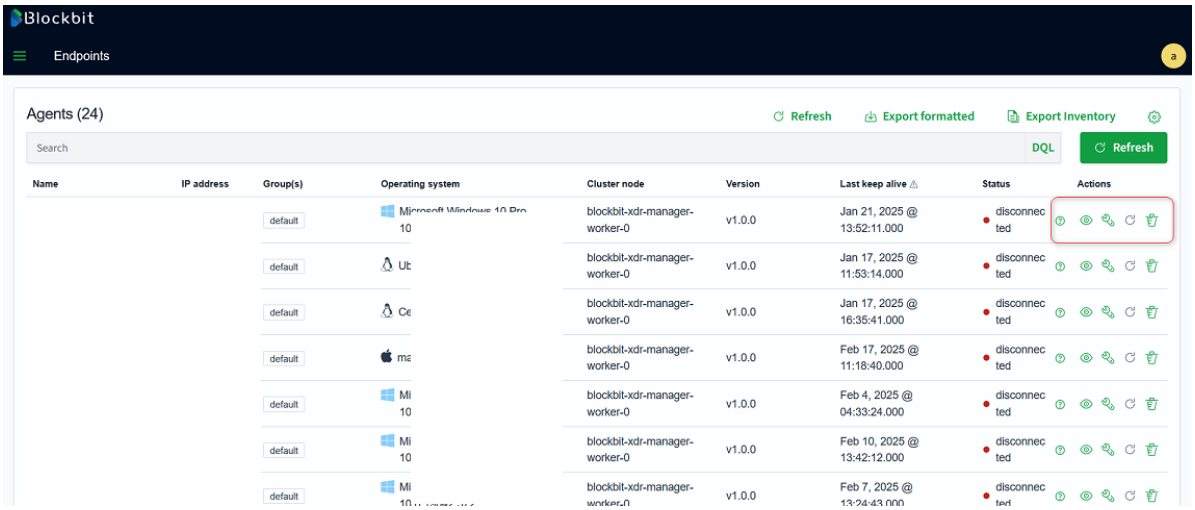
```
# Nome do serviço do agente Blockbit XDR
$ServiceName = "Blockbit XDR"

# 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.

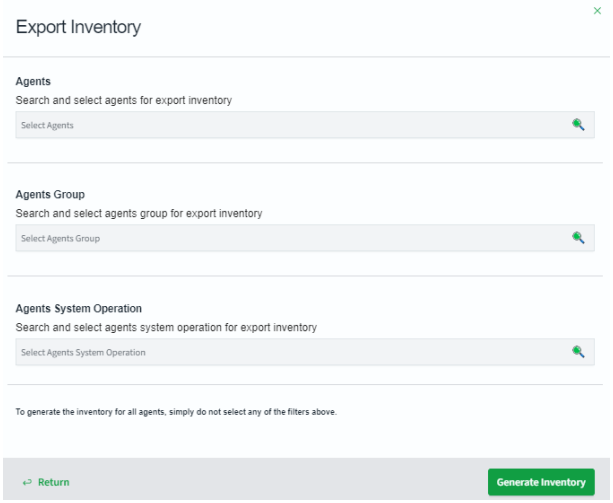


Para procurar por um agente específico, utilize a barra de buscas (**Search**), onde você pode montar uma query para procurar por agentes.

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.



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.

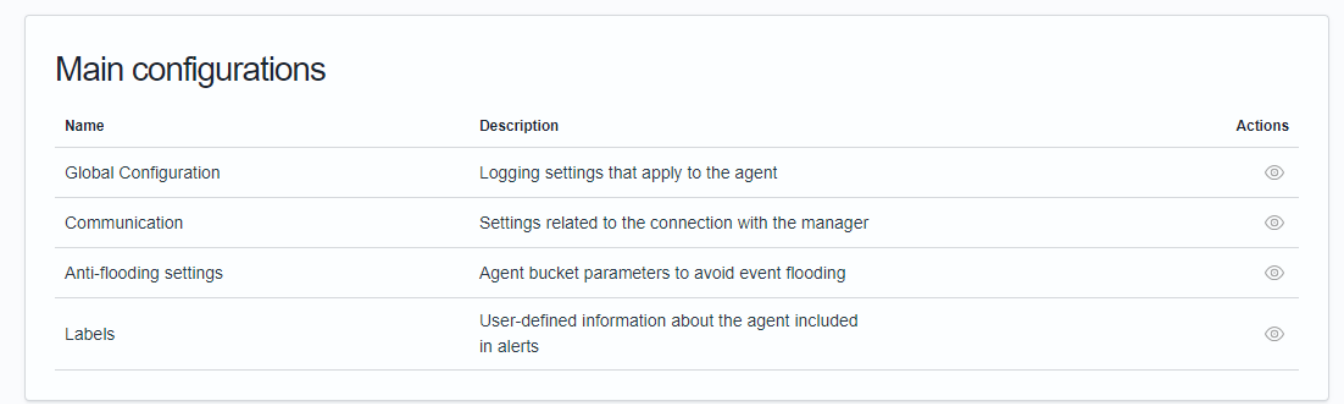
XDR - Endpoints Summary - Configurações

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

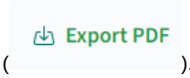
Configurações não suportadas pelo sistema operacional do agente aparecem como desabilitadas.

Configurações principais

Para acessar às configurações, clique no olho ( ).

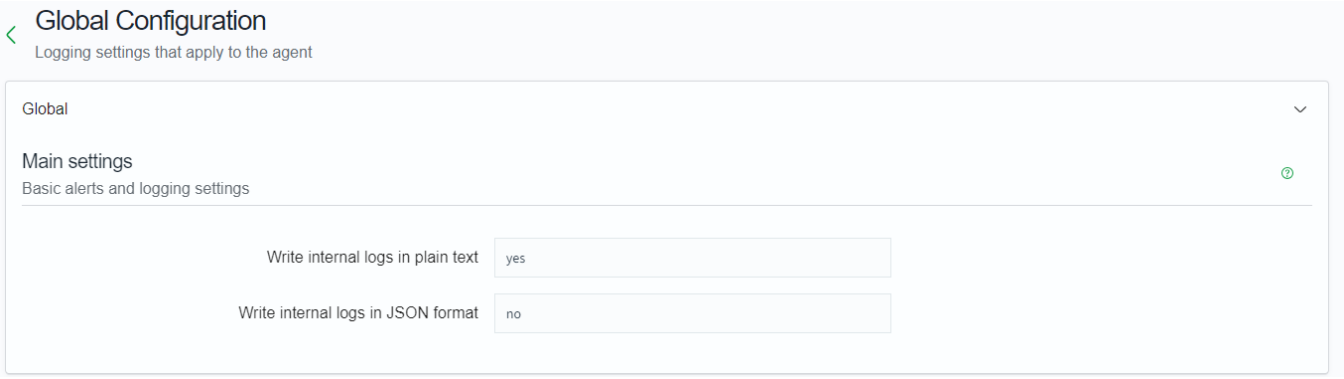


Para exportar as configurações em PDF, clique em **Export PDF** ( ).



Configurações globais (Global Configuration)

São configurações para logs internos.

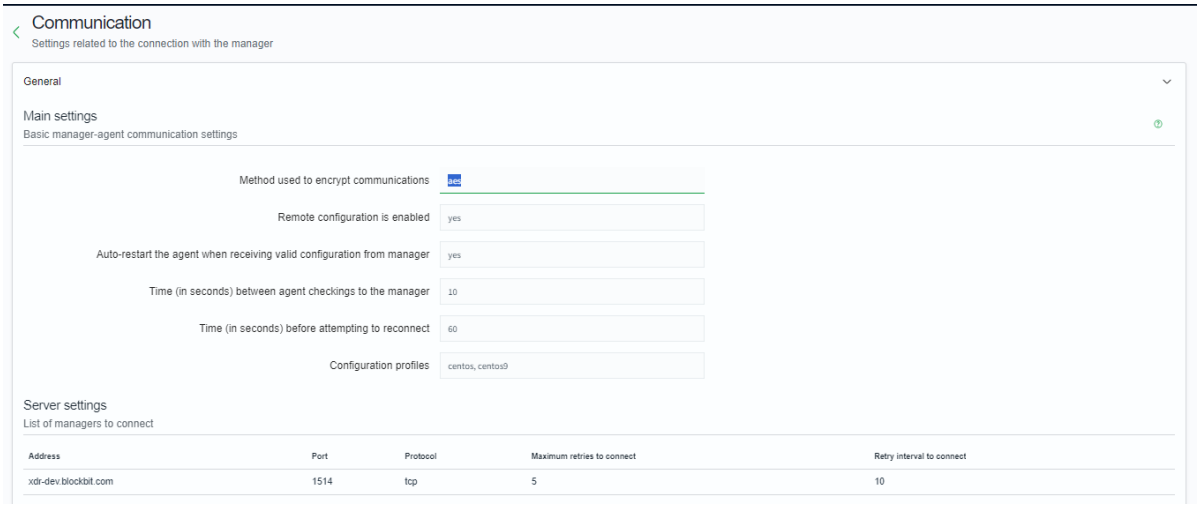


Write internal logs in plain text: permite a criação de logs em plain text;

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

Communication

São configurações relacionadas à comunicação do agente com o manager.



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;

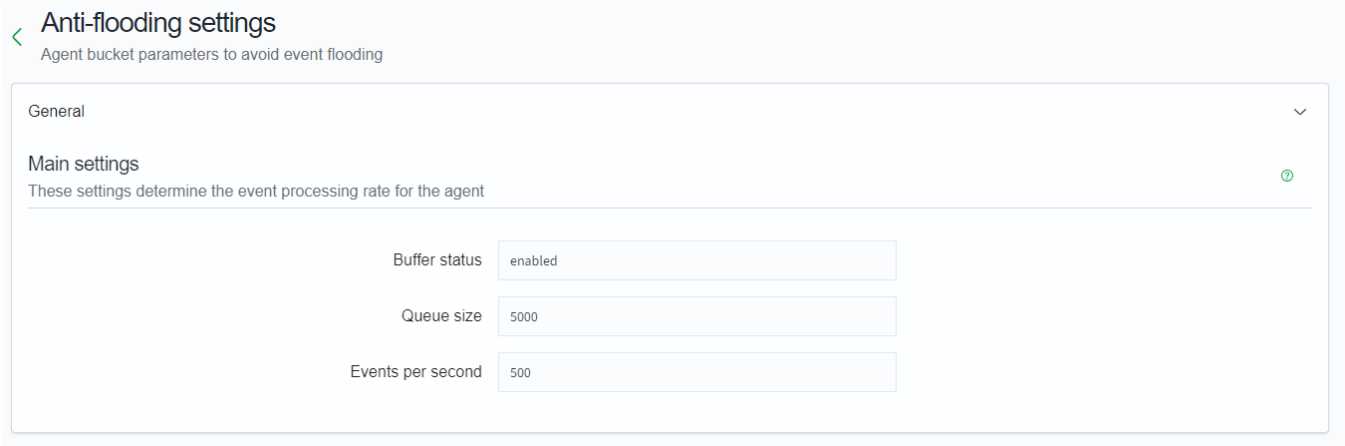
Protocol: protocolo do manager;

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.



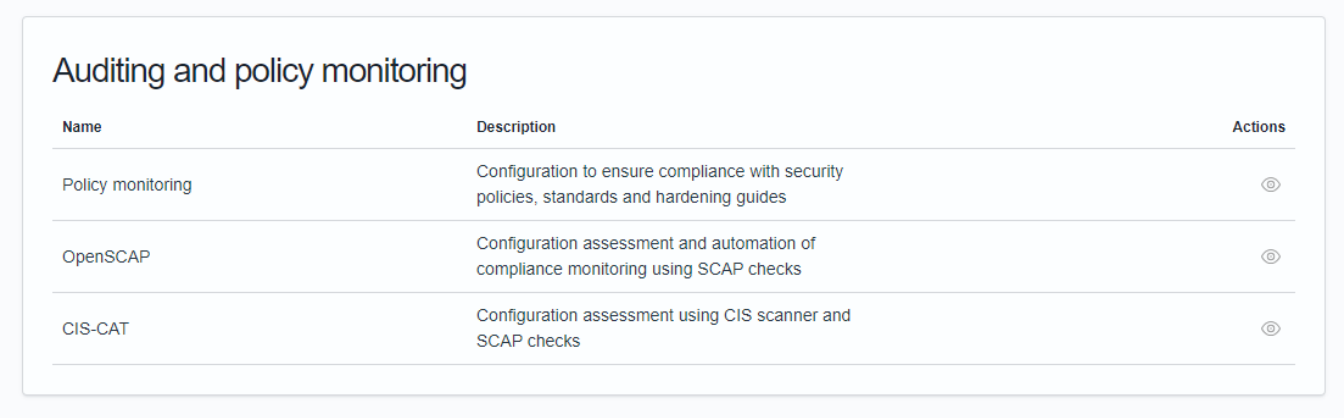
Buffer status: permite informar a quantidade de dados em espera;

Queue size: define o máximo de requisições em espera;

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

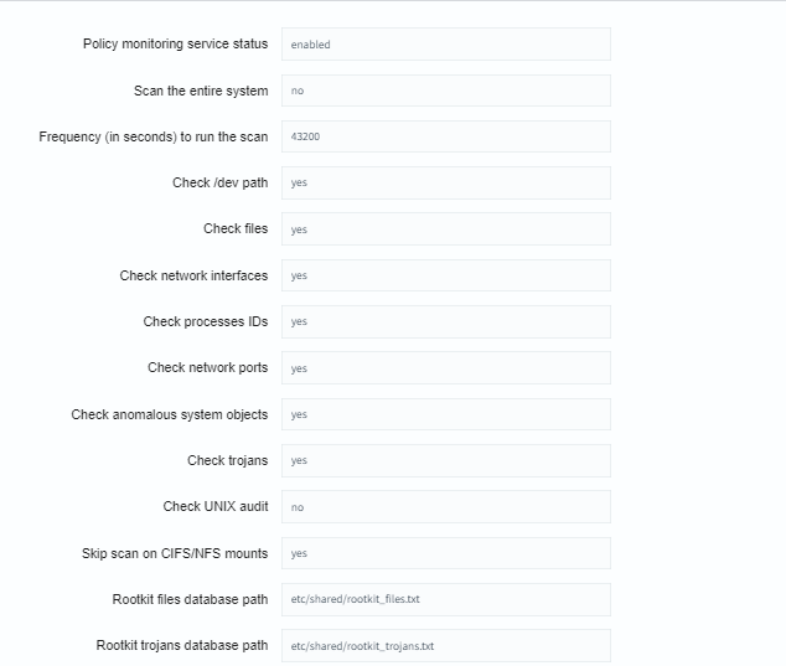
Auditing and policy monitoring

Aqui estão as configurações de auditoria e monitoramento de políticas.



Policy monitoring

Aqui estão as configurações de políticas.



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 conectadosl;

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;

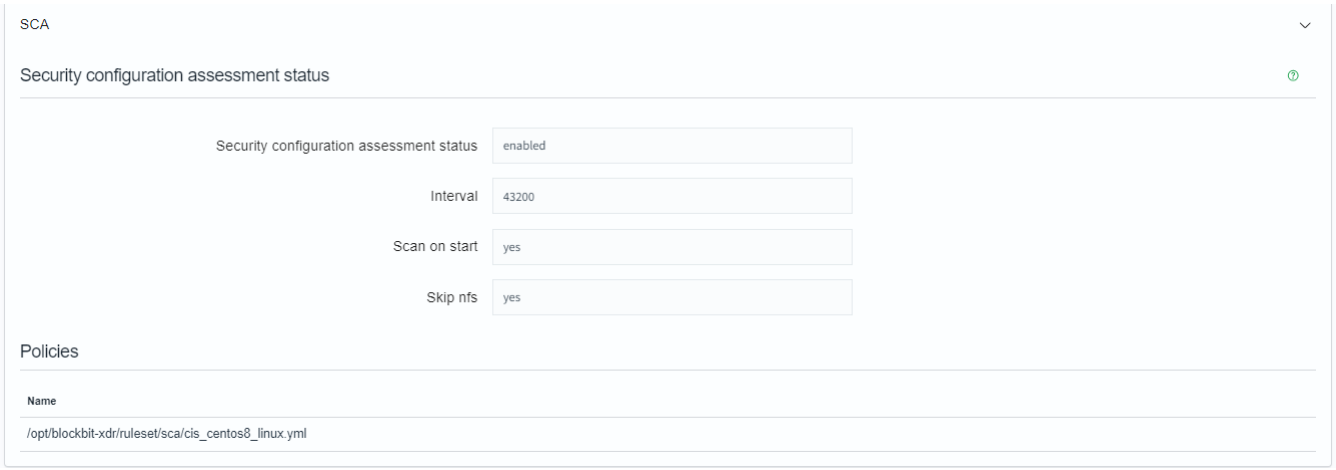
Check trojans: permite checar o sistema para detectar trojans;

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

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

Rootkit files database path: determina o diretório do rootkit;

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



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

Interval: determina o intervalo entre os escaneamentos;

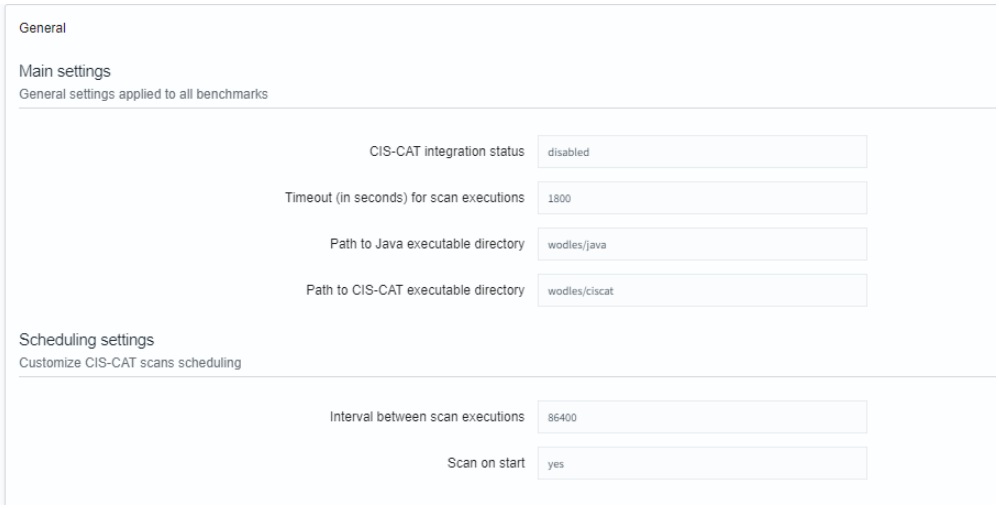
Scan on start: habilita o escaneamento quando o sistema é iniciado;

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.



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;

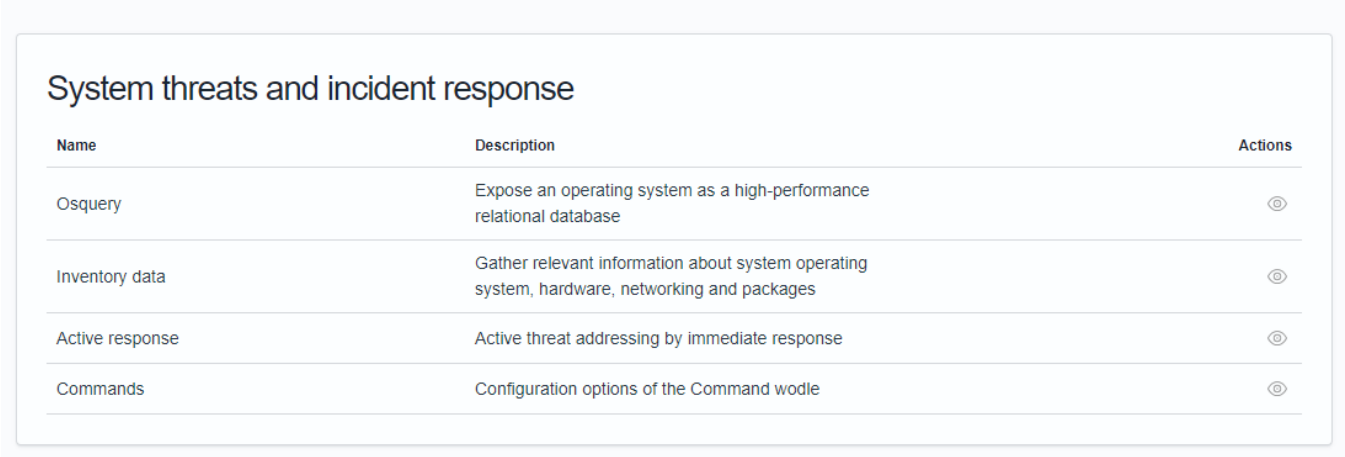
Path to CIS-CAT executable directory: localização do diretório executável CIS-CAT;

Interval between scan executions: intervalo entre escaneamentos;

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

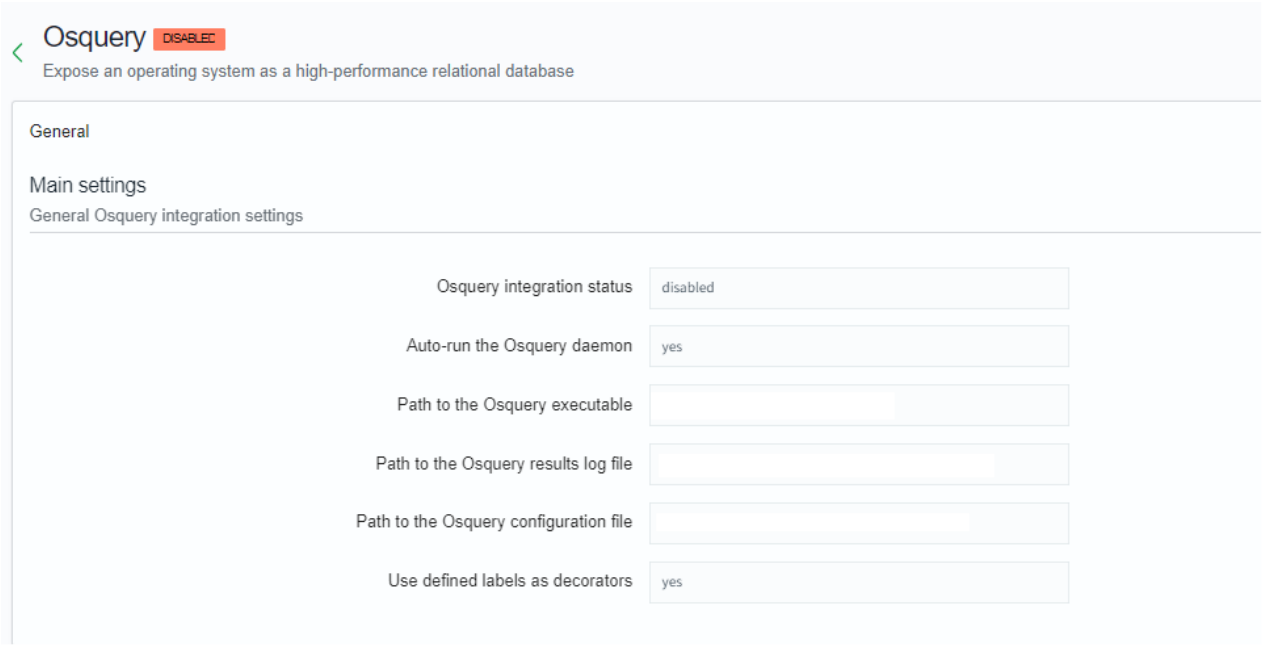
System threats and incident response

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



Osquery

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



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;

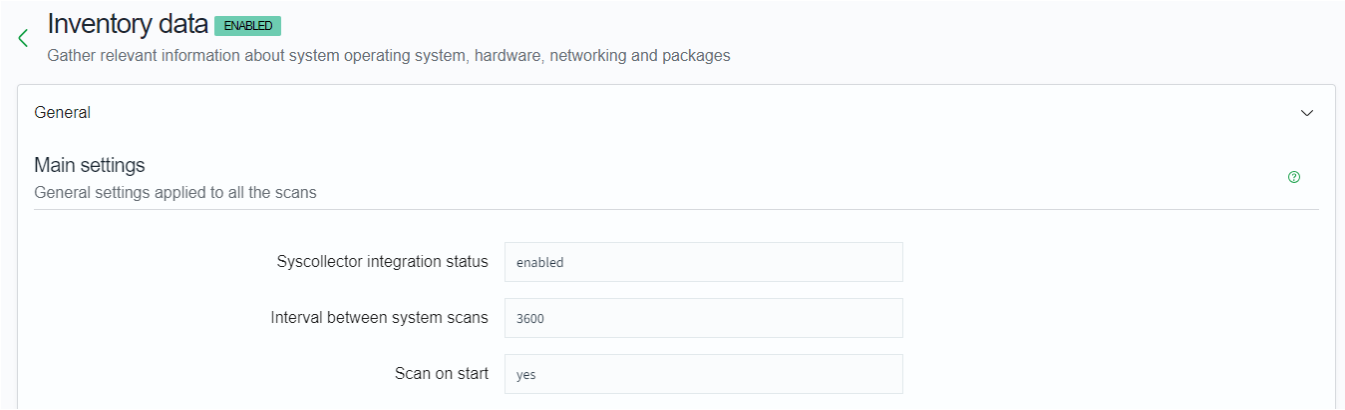
Path to the Osquery results log file: caminho do diretório do arquivo de logs do Osquery;

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.

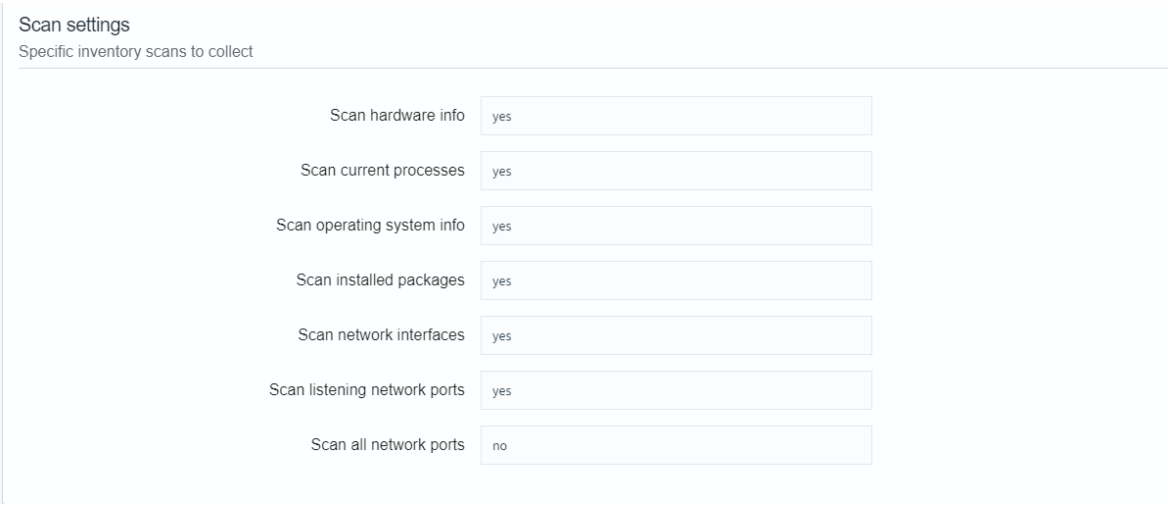


Main settings: configurações gerais do escaneamento;

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: 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;

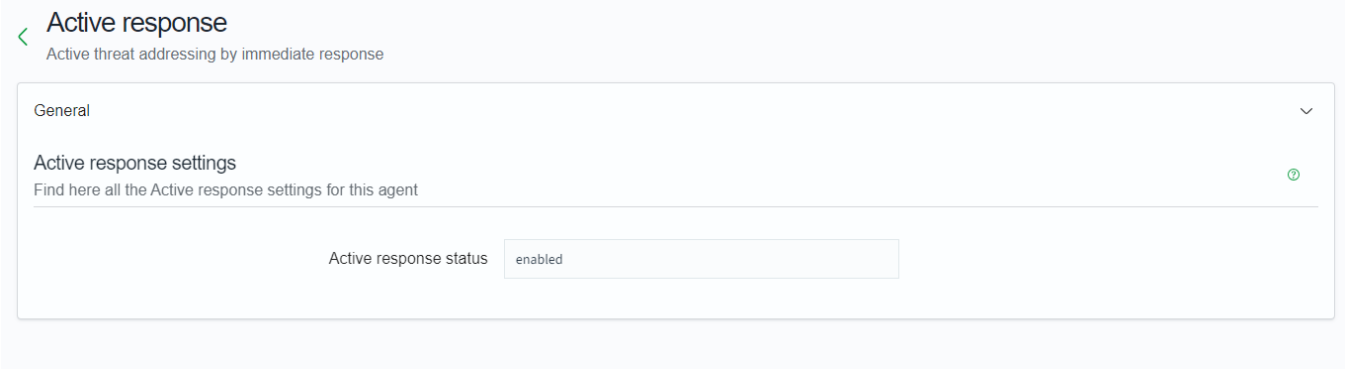
Scan network interfaces: permite escanear interfaces de rede;

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.

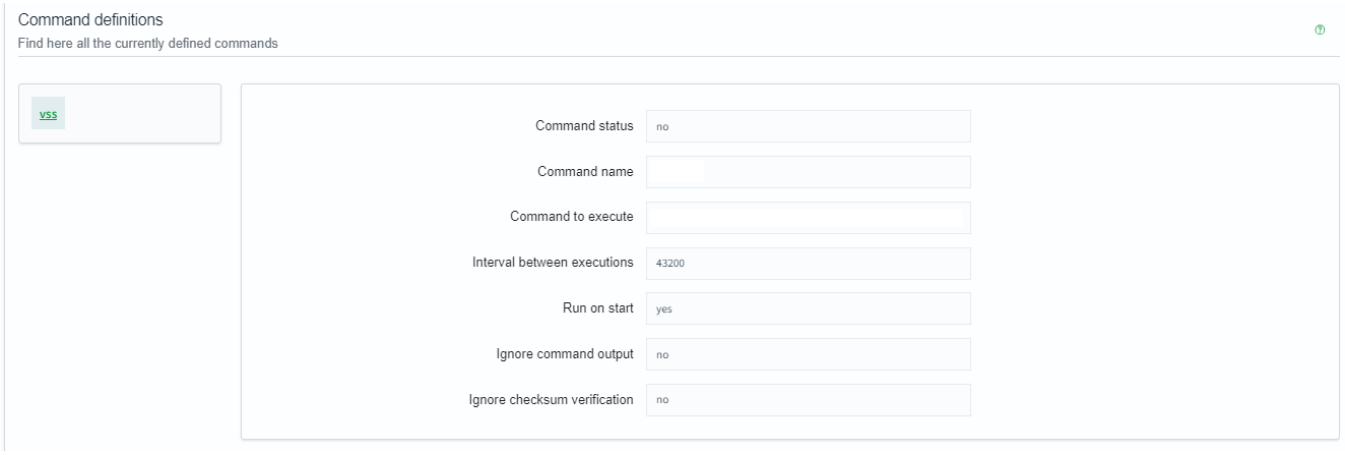


Active response status:

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

Commands

Aqui são configurados os comandos.



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;

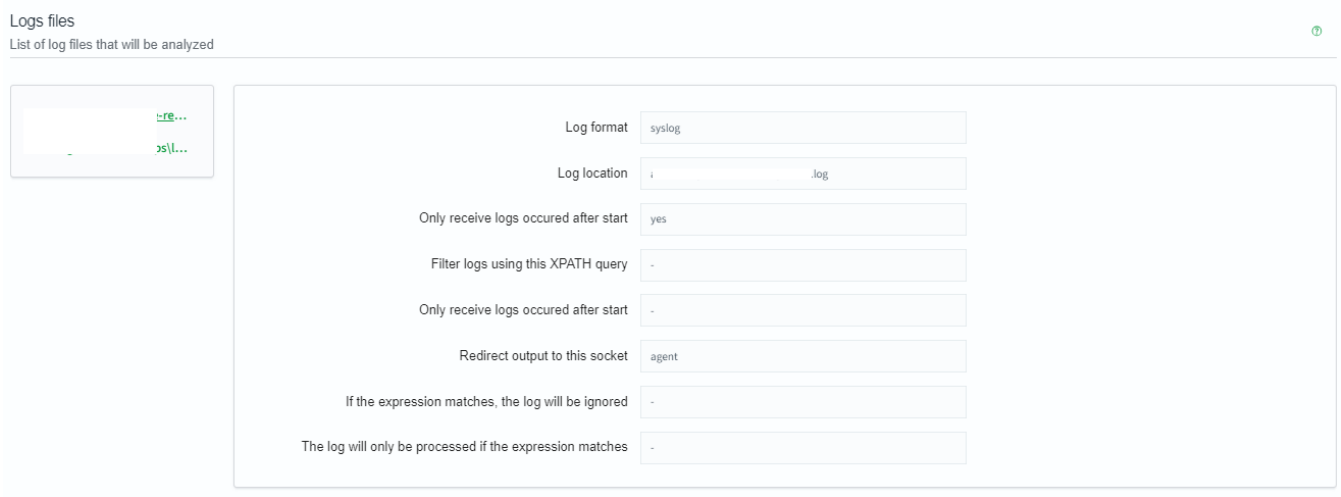
Ignore checksum verification: ignorar a verificação de checksum.

Log collection

Exibe as configurações de logs.

Logs files

Exibe configurações de arquivos de logs.



À esquerda, estão listados os arquivos de logs.

Log format: formato do log;

Log location: diretório do log;

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

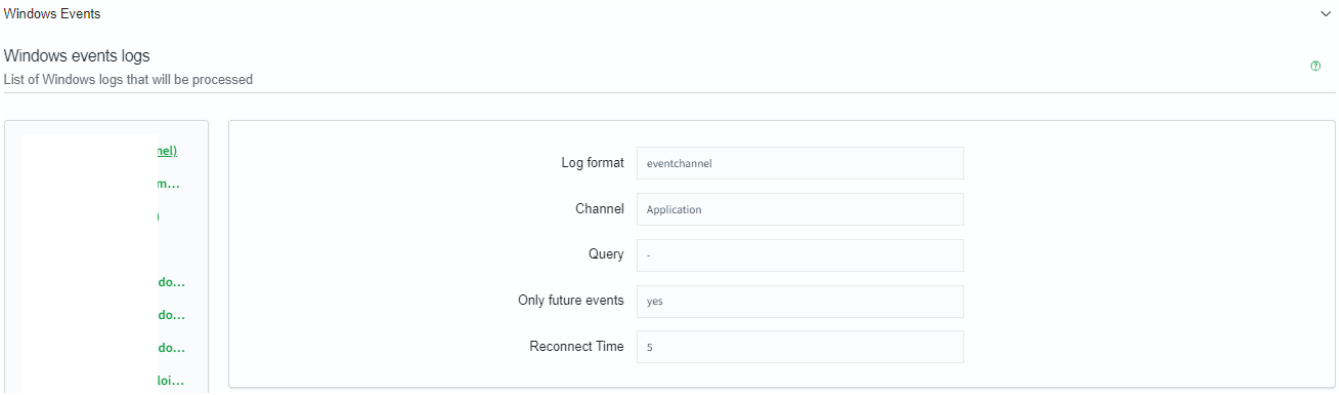
Redirect output to this socket: permite redirecionar resultados ao socket selecionado;

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.



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

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

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 escaneanento de arquivos CIFS/NFS;

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

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

Skip scan of /proc directory: permite pular o escaneanento 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;

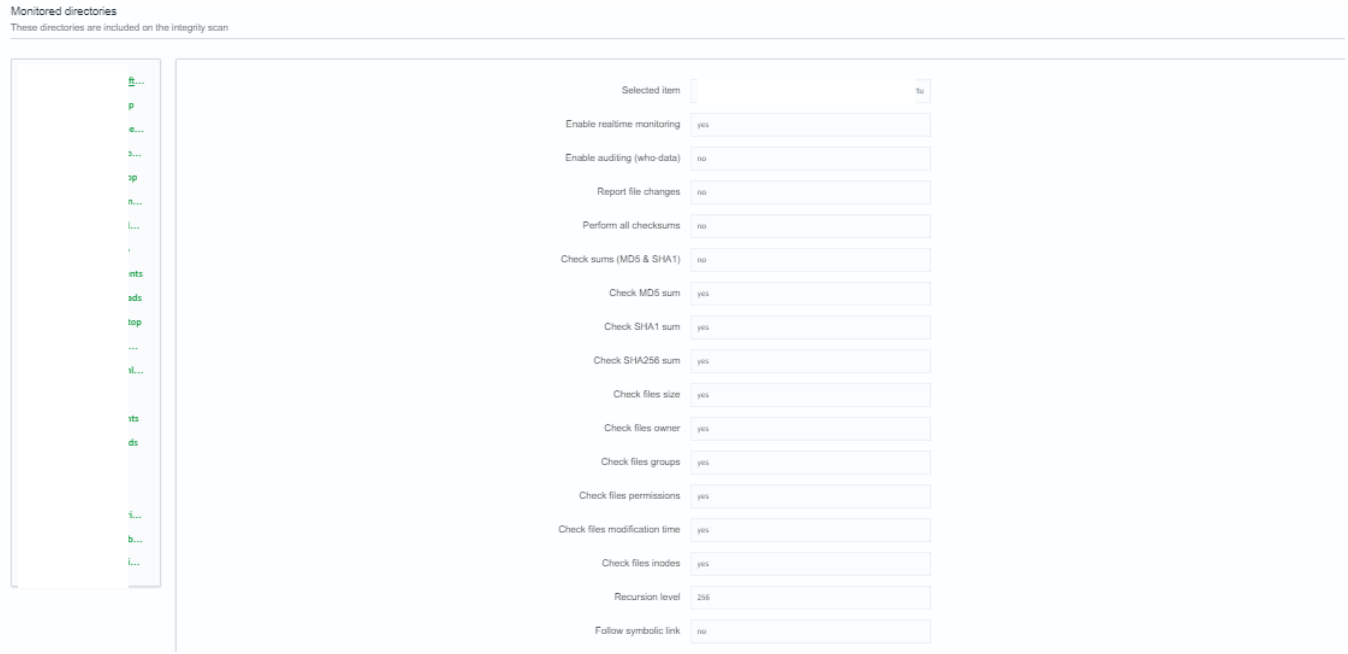
Maximum event reporting throughput: throughput máximo para relatar eventos;

Process priority: prioridade do processo;

Database type: tipo da base de dados.

Monitored

Configurações dos diretórios monitorados.



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 cts	32bit
H	32bit
H	32bit
H	64bit

Ignored

É a lista de registros ignorados.

Path
ini

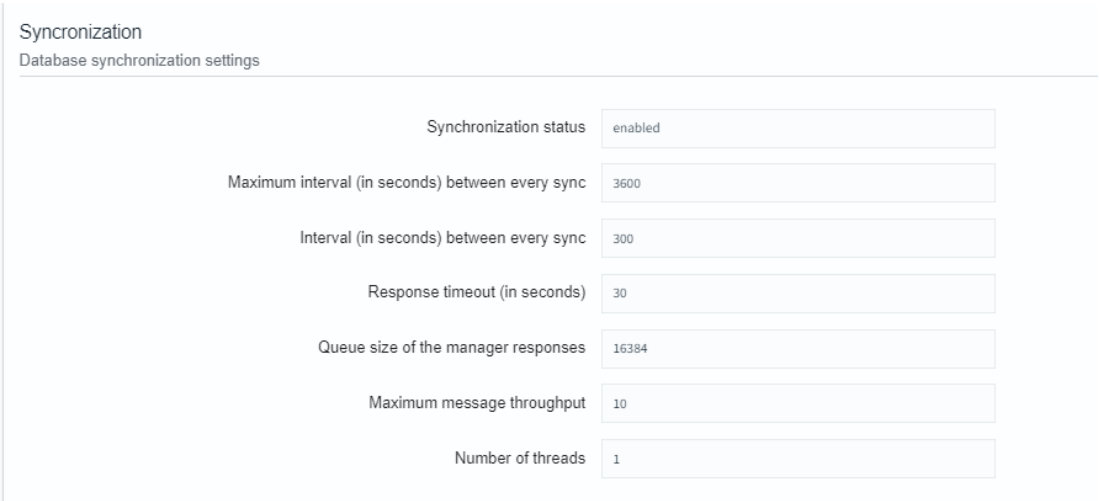
Sregex
5

Path: diretório do registro a ser ignorado;

Sregex: expressões regulares a serem ignoradas.

Synchronization

Configurações de sincronização de bases de dados.



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;

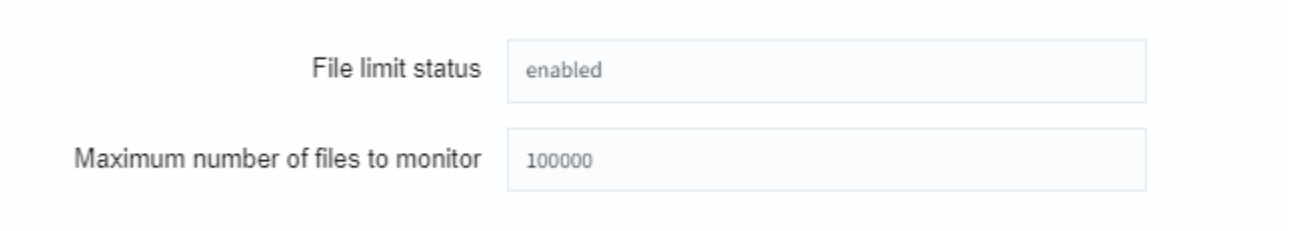
Queue size of the manager responses: tamanho da fila de respostas do manager;

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: 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

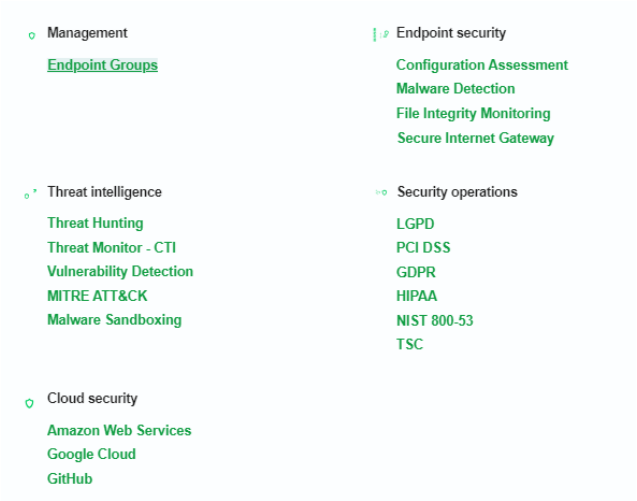
O Blockbit XDR integra o **Sysmon** no Windows e o **auditd** no Linux, permitindo o monitoramento detalhado de atividades do sistema. A solução registra eventos críticos, como execução de processos, modificações em arquivos e alterações no registro, proporcionando uma visão abrangente e forense das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

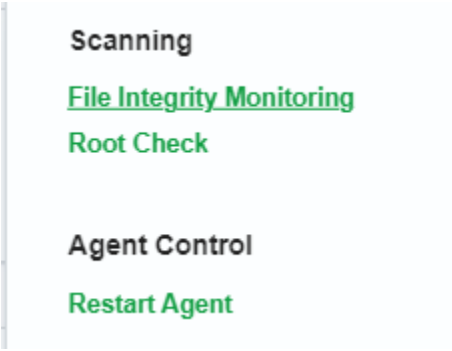
Esse recurso possibilita a detecção proativa de ameaças, investigação detalhada e resposta automatizada a incidentes, garantindo maior controle sobre a segurança do ambiente.

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:



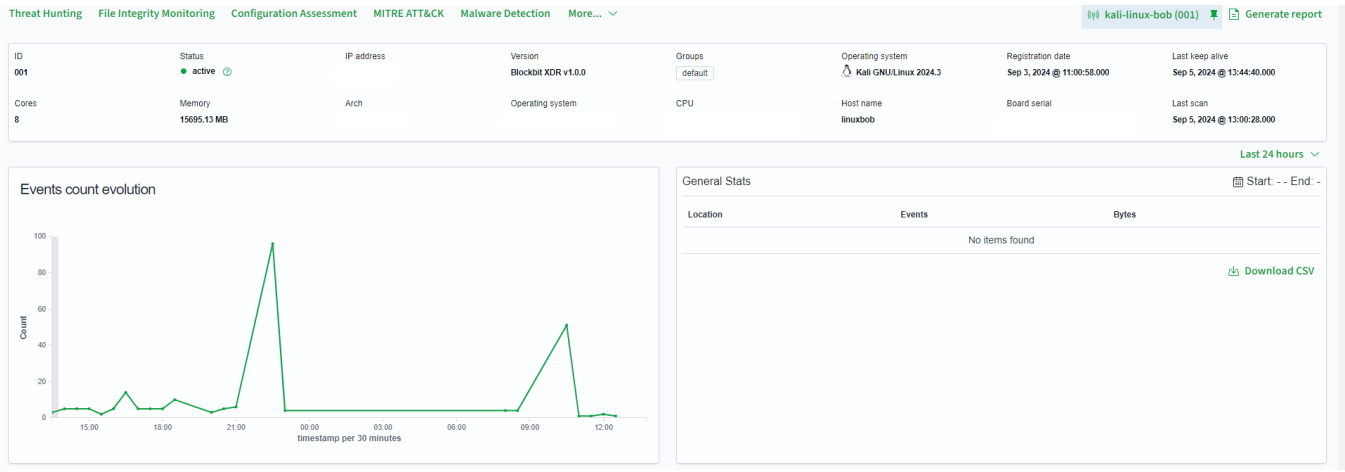
File Integrity Monitoring: escanear o agente utilizando o **File Integrity Monitoring** do Blockbit XDR;

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;

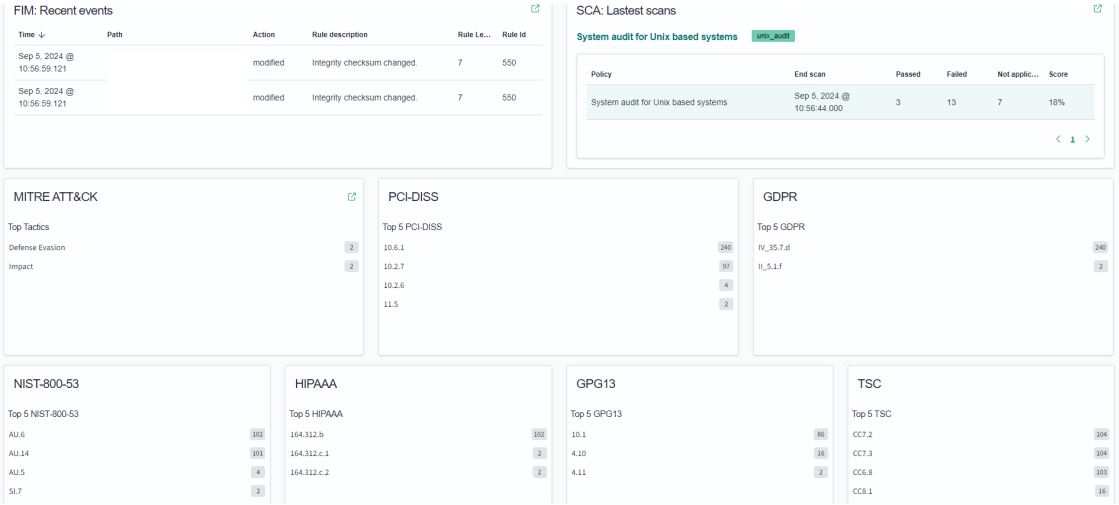
Host name: nome do servidor;

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: 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;

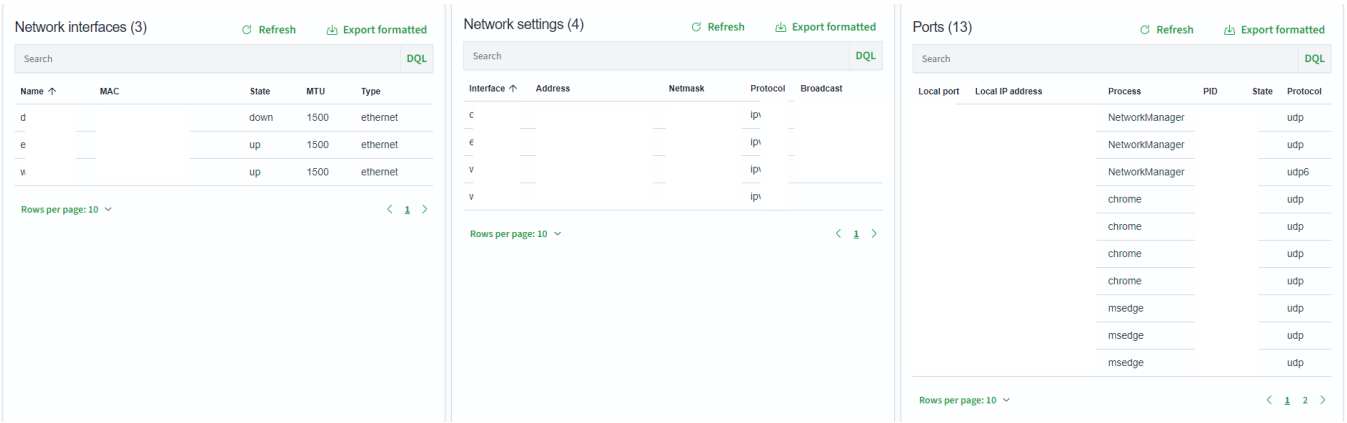
GDPR: estatísticas de GDPR específicas do agente;

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: 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;

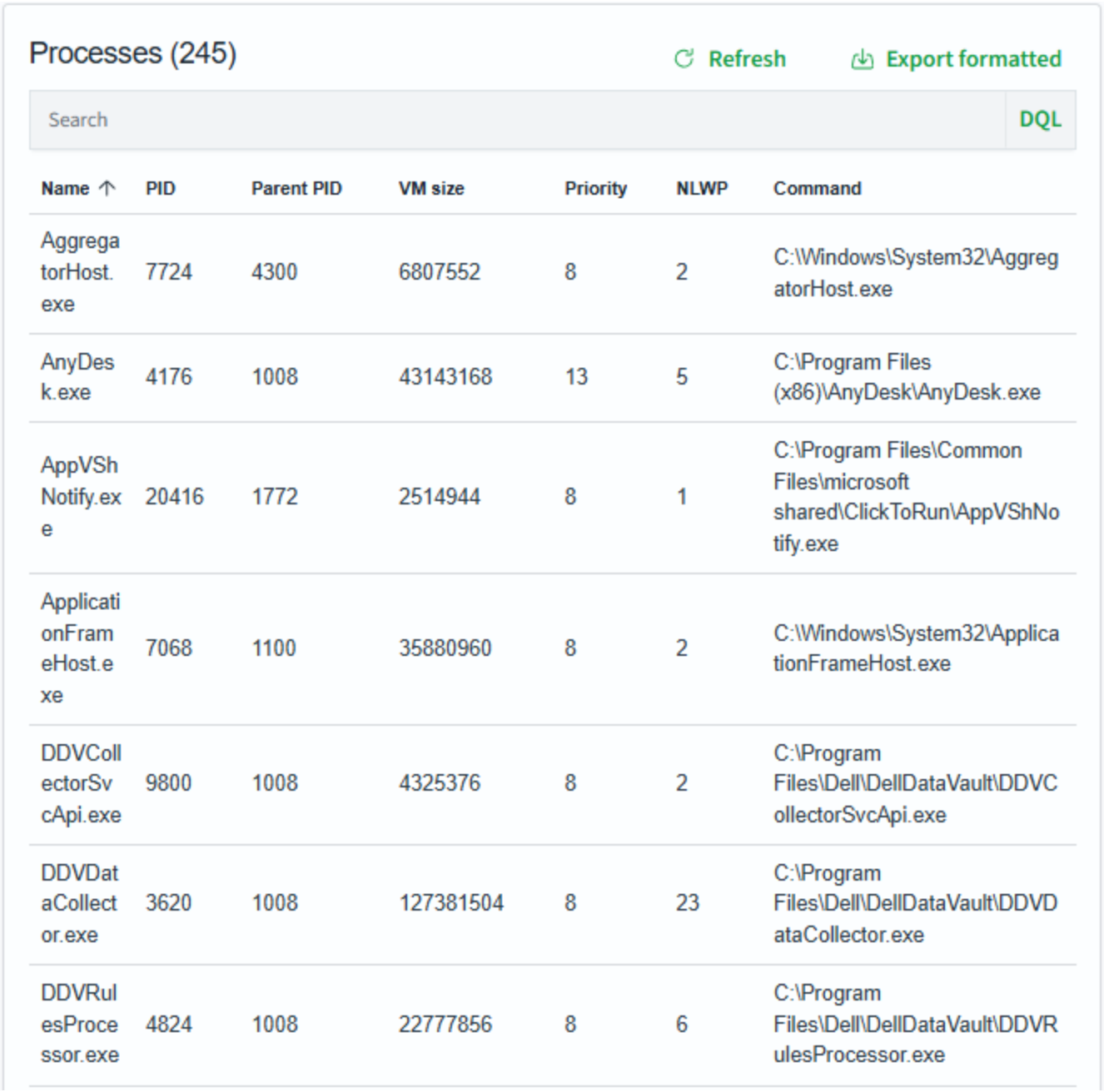
Process: serviço executado;

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
AggregatorHost.exe	7724	4300	6807552	8	2	C:\Windows\System32\AggregatorHost.exe
AnyDesk.exe	4176	1008	43143168	13	5	C:\Program Files (x86)\AnyDesk\AnyDesk.exe
AppVShNotify.exe	20416	1772	2514944	8	1	C:\Program Files\Common Files\microsoft shared\ClickToRun\AppVShNotify.exe
ApplicationFrameHost.exe	7068	1100	35880960	8	2	C:\Windows\System32\ApplicationFrameHost.exe
DDVCollectorSvcApi.exe	9800	1008	4325376	8	2	C:\Program Files\Dell\DellDataVault\DDVCollectorSvcApi.exe
DDVDataCollector.exe	3620	1008	127381504	8	23	C:\Program Files\Dell\DellDataVault\DDVDataCollector.exe
DDVRulesProcessor.exe	4824	1008	22777856	8	6	C:\Program Files\Dell\DellDataVault\DDVRulesProcessor.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.

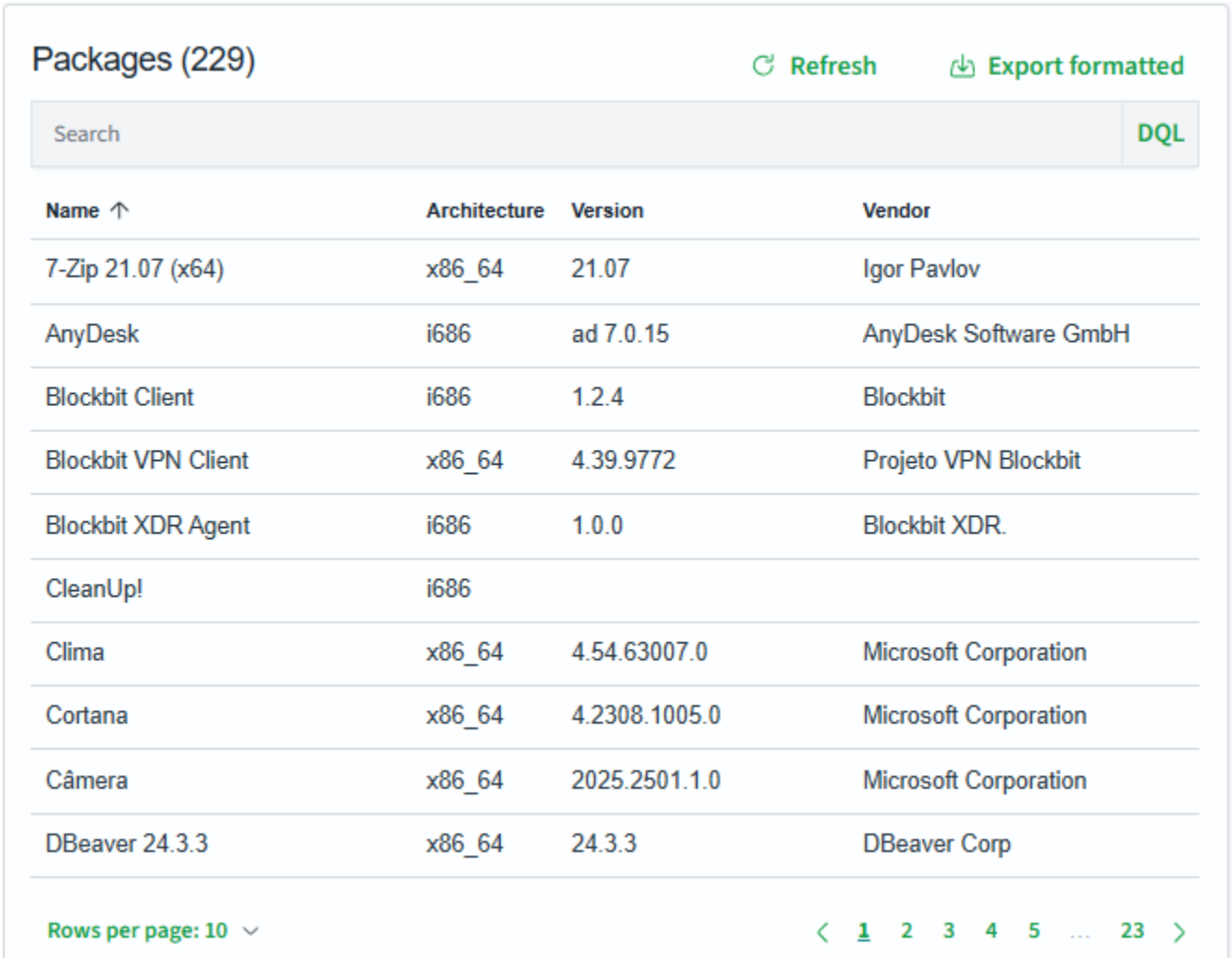
Parent PID (ID do Processo Pai): Indica o processo que originou a execução do processo atual. A partir desse identificador, é possível visualizar a árvore hierárquica dos processos, facilitando a análise de comportamentos suspeitos, como injeção de código e execução de malware.

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:



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:

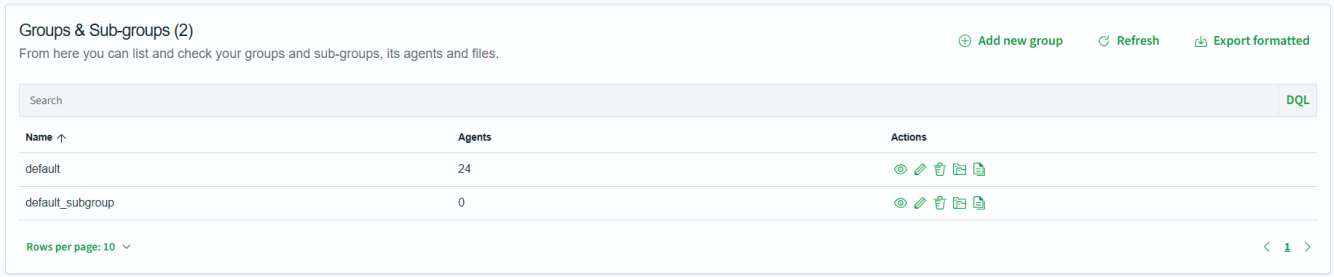
O Blockbit XDR suporta herança de políticas, permitindo que regras definidas em um nível superior sejam aplicadas automaticamente a subgrupos e endpoints associados.
Os administradores podem definir configurações globais para a empresa e permitir que unidades individuais ajustem parâmetros específicos conforme necessário.

Políticas Baseadas em Grupos para Segurança e Monitoramento:

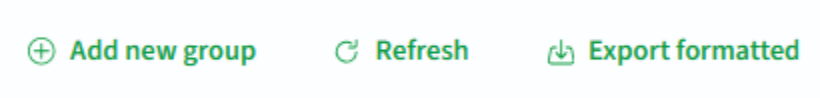
- Isolamento de Endpoints comprometidos, garantindo contenção de ameaças.
- Bloqueio de processos maliciosos e resposta automatizada a incidentes.
- Correção automática de configurações alteradas por malwares ou ataques.
- Definição de regras para prevenção de novas ameaças e mitigação de riscos.

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.

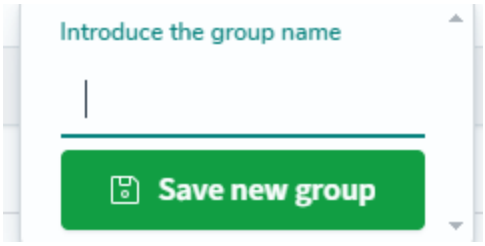


As ações disponíveis:



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.

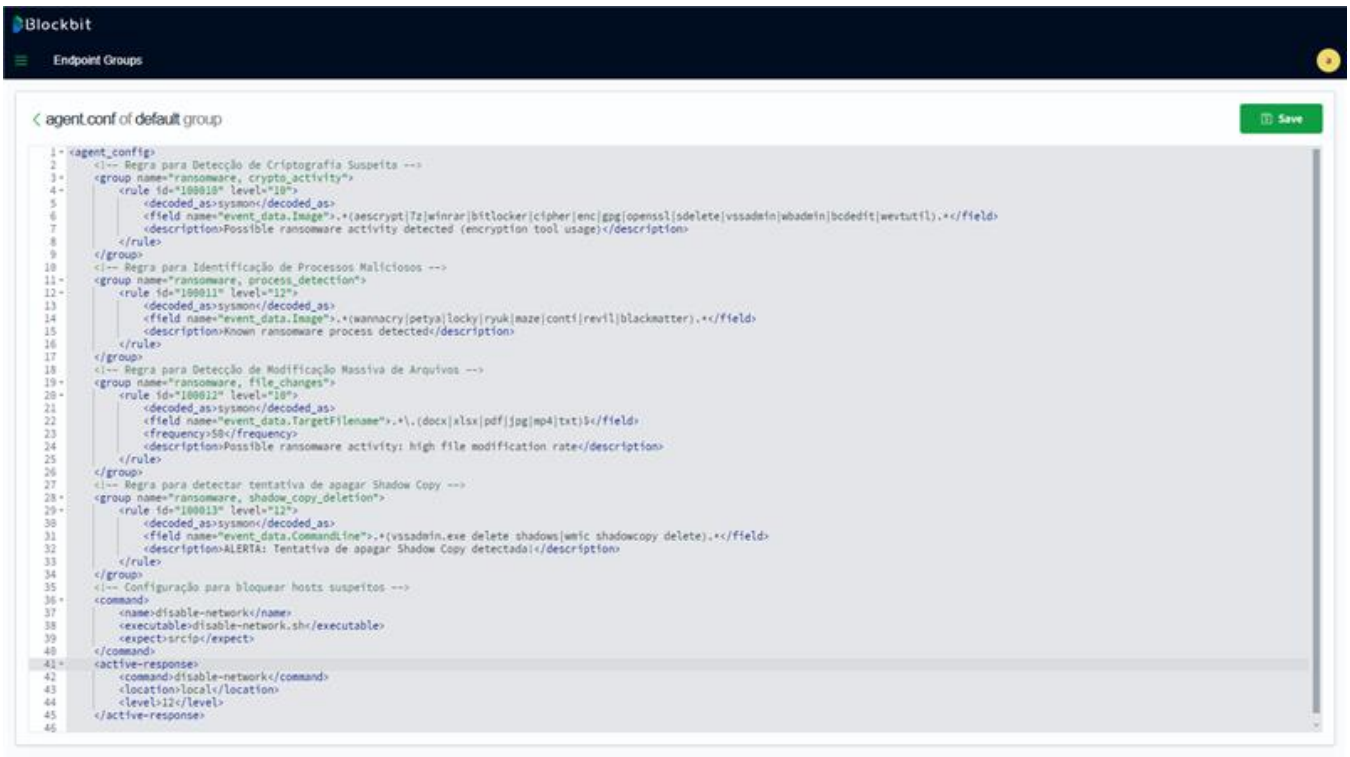
Ao clicar em **Export formatted**, será criado um arquivo .csv com informações dos grupos.

Para cada grupo, há **cinco** ações:

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

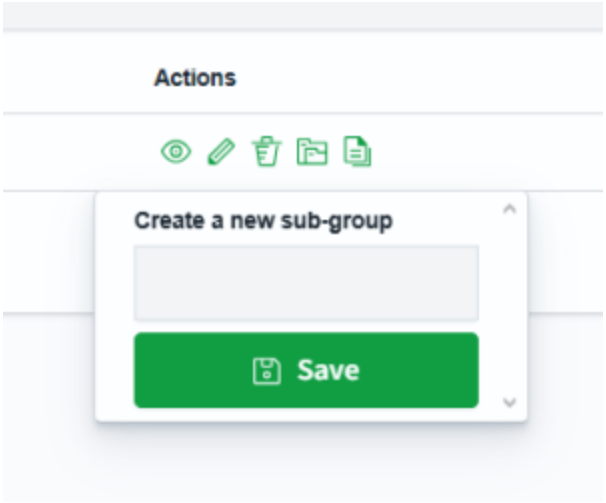
Editar grupo (**Edit group configuration**) ( ): abre um editor com informações do grupo. Permitindo personalizar as configurações, regras e exceções dos endpoints pertencentes a esse Grupo ou Sub-grupo, para ativar as detecções automaticamente.

Exemplo:

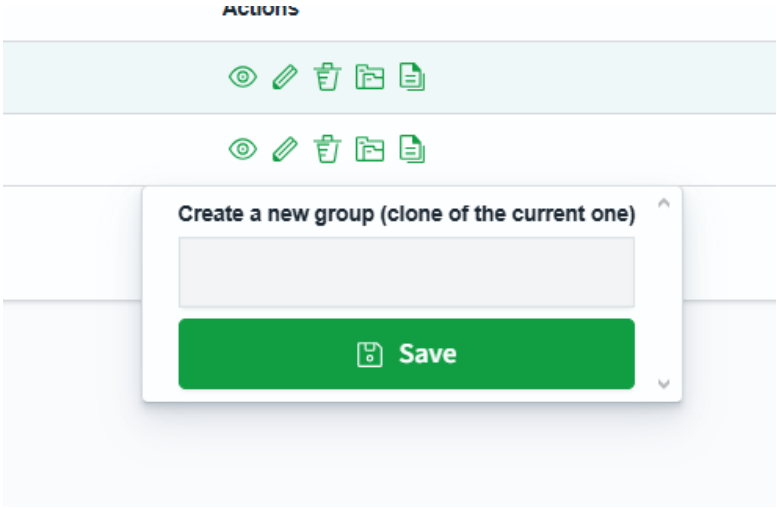


Deletar grupo (**Delete**) ( ): apaga o grupo ou subgrupo.

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.

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.

```
    <if_sid>61603</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)bcdedit\s\s\/set\s{default}\srecoveryenabled\sNo</field>
    <description>System recovery disabled. Possible ransomware activity detected.</description>
    <mitre>
      <id>T1059</id>
    </mitre>
  </rule>

  <rule id="100621" level="12">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)wbadmin\s\sdelete\scatalog\s-quiet</field>
    <description>System catalog deleted. Possible ransomware activity detected.</description>
    <mitre>
      <id>T1059</id>
    </mitre>
  </rule>

  <rule id="100622" level="12">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)bcdedit\s\s\/set\s{default}\srecoveryenabled\sNo</field>
    <description>System recovery disabled. Possible ransomware activity detected.</description>
    <mitre>
      <id>T1059</id>
    </mitre>
  </rule>

  <rule id="100623" level="12">
    <if_sid>92032</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)wevtutil.*cl</field>
    <description>Windows event logs deleted. Possible malicious activity detected.</description>
    <mitre>
      <id>T1070.001</id>
    </mitre>
  </rule>

<!-- Ransom note file creation -->


  <rule id="100626" level="10" timeframe="50" frequency="3" ignore="300">
    <if_matched_sid>554</if_matched_sid>
    <same_field>md5</same_field>
    <different_field>file</different_field>
    <description>The file $(file) has been created in multiple directories in a short time. Possible ransomware activity.</description>
  </rule>

  <rule id="100627" level="7" timeframe="30" frequency="10" ignore="300">
    <if_matched_sid>550</if_matched_sid>
    <field name="file" type="pcre2">(?i)C:\\Users</field>
    <description>Multiple Files modified in the User directory in a short time.</description>
  </rule>

  <rule id="100629" level="7" timeframe="300" frequency="2" ignore="300">
    <if_matched_sid>63104</if_matched_sid>
    <field name="win.system.message" type="pcre2">(?i)log file was cleared</field>
    <description>Windows Log File Cleared.</description>
    <mitre>
      <id>T1070.001</id>
    </mitre>

  </rule>

</group>
```

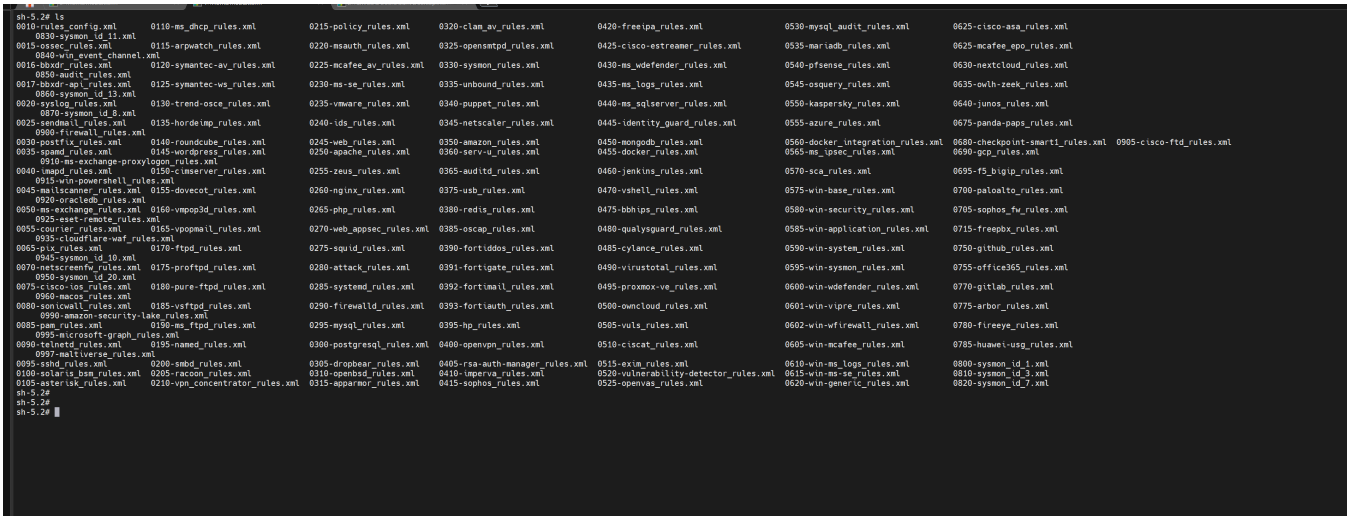
```
<group name="ransomware,ransomware_detection">
  <rule id="100628" level="12" timeframe="300" frequency="2" ignore="300">
    <if_matched_group>ransomware_pre_detection</if_matched_group>
    <if_sid>100626,100627,100615,100616,100617,100618,100619</if_sid>
    <description>Ransomware activity detected.</description>
  </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.



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.

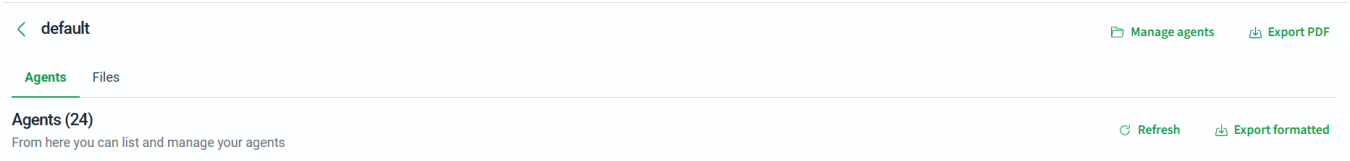
Por que Enumerar Arquivos

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.

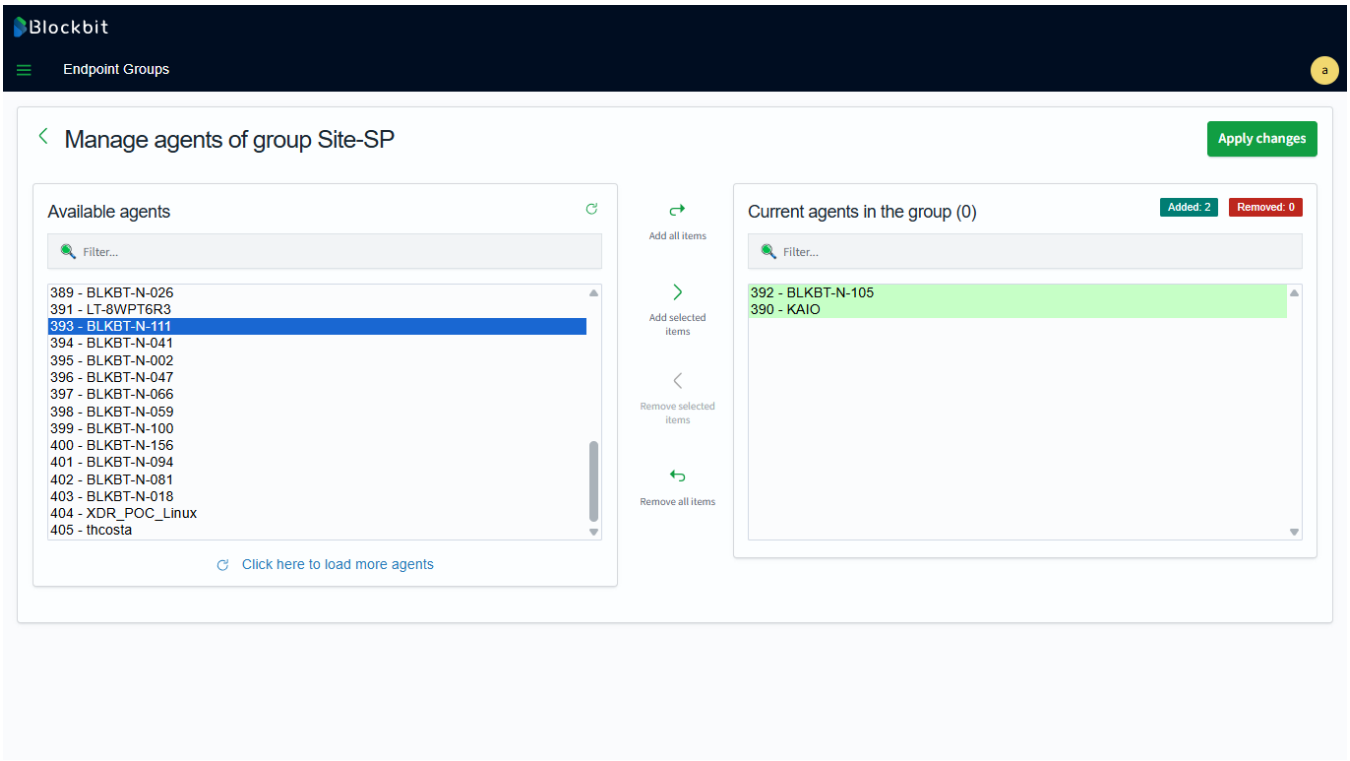
XDR - Endpoint Groups - View details

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

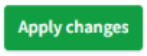


Em **Export PDF (**  **),** você pode exportar um PDF com as configurações e/ou os agentes do grupo.

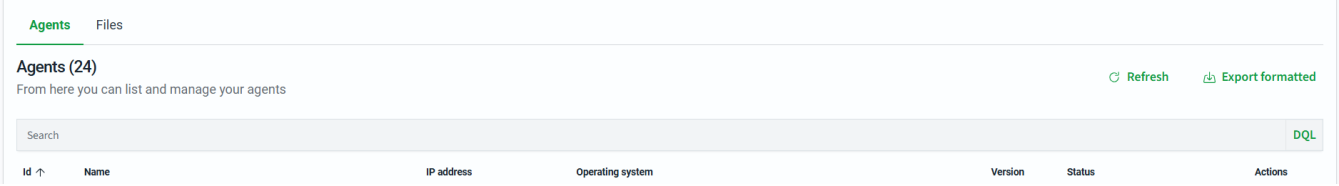
Em **Manage agents,** você pode adicionar ou remover agentes do grupo.



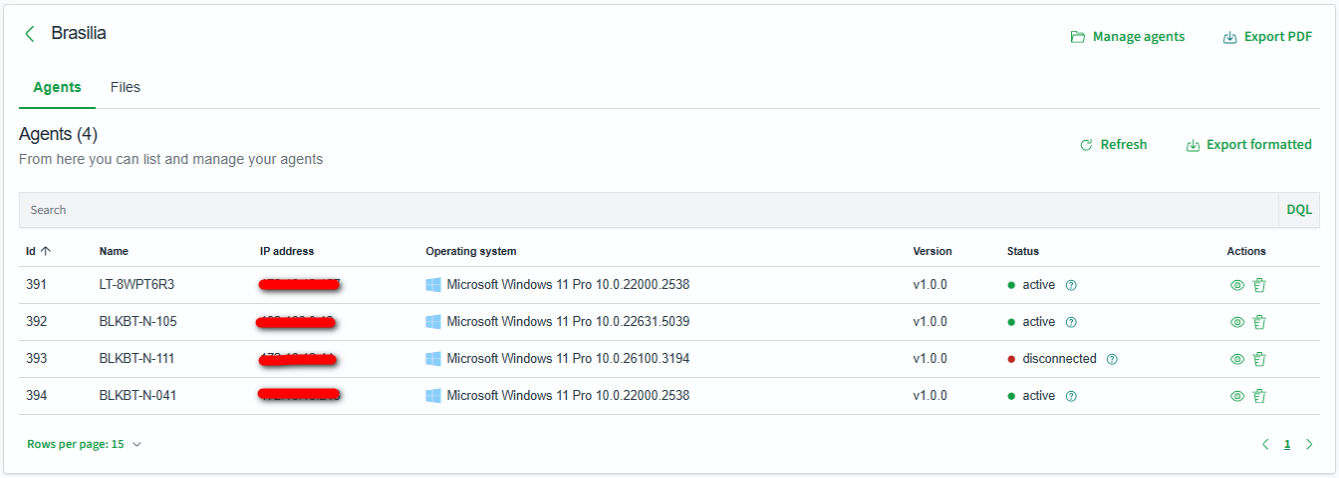
Para adicionar ou remover agentes, utilize os botões entre as listas.

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

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



Agents

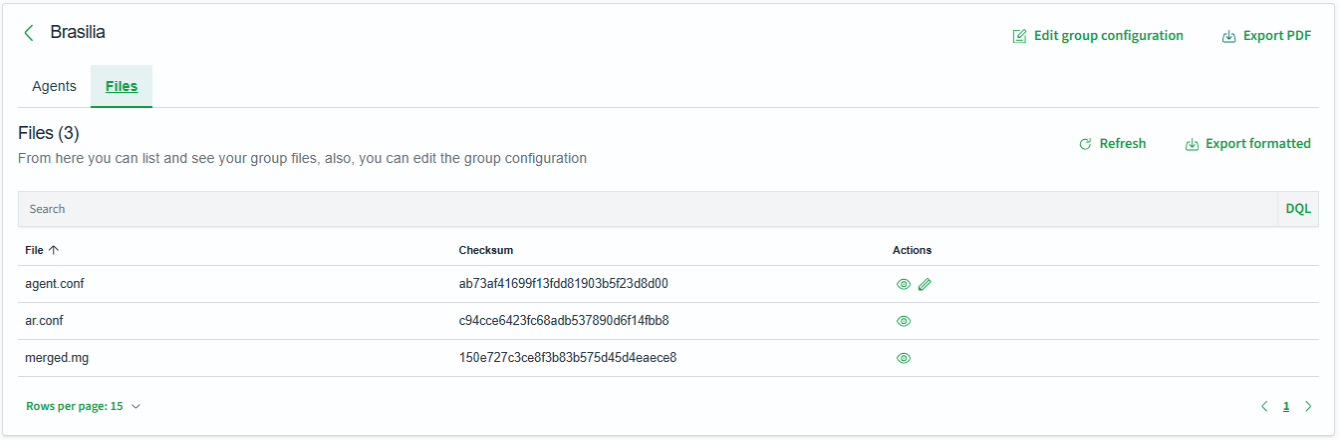


Para cada agente, há as seguintes características.
O **Id** é o número identificador do agente.
Name é o nome do agente.
IP address é o endereço IP do agente.
Operating system é o sistema operacional do agente.
Version é a versão do agente.
Status é o status do agente. São dois status: ativo (**active**) e desconectado (**disconnected**).

Actions: ações sobre o agente:

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

Files

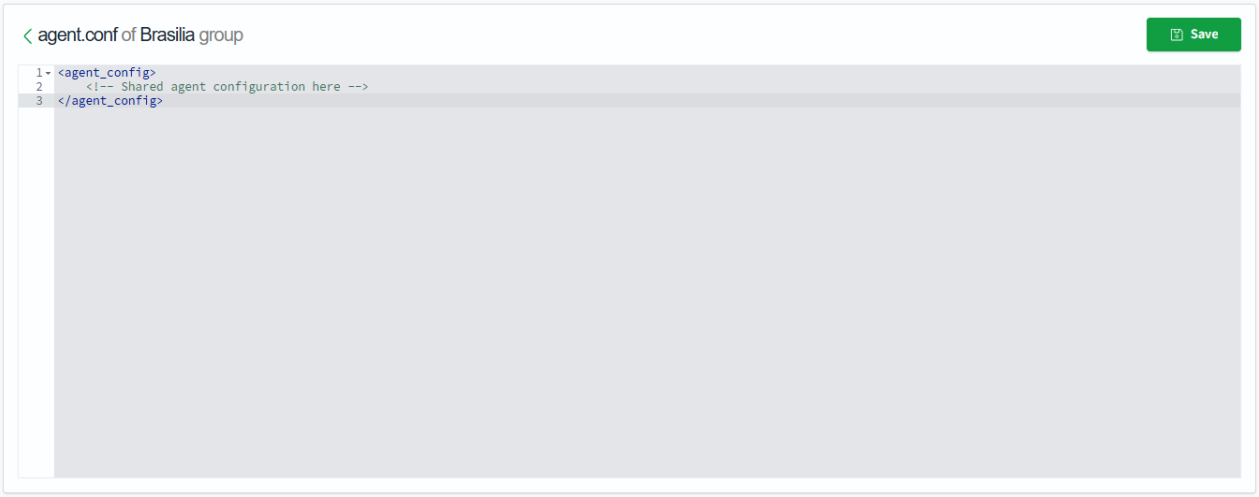


Para cada arquivo, há as seguintes características:

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 Brasilia group
Save
<agent_config>
<!-- Shared agent configuration here -->
</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/disabilita 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/disabilita 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**;

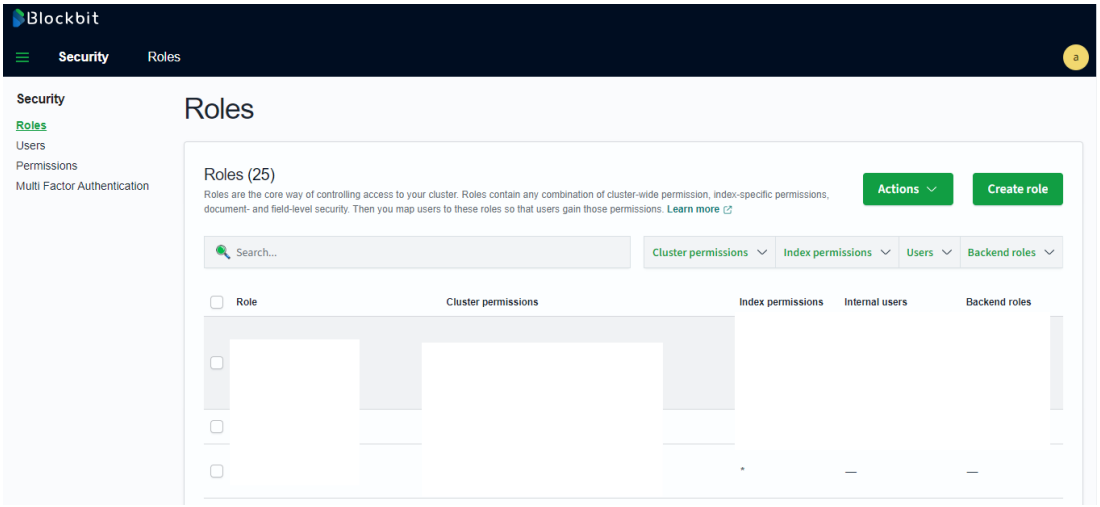
XDR - Security - Roles

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;

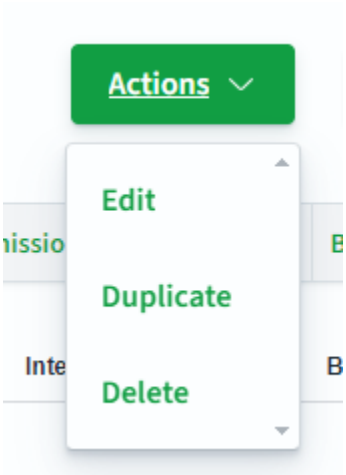
Index permissions: permissões de acesso aos recursos do index;

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.

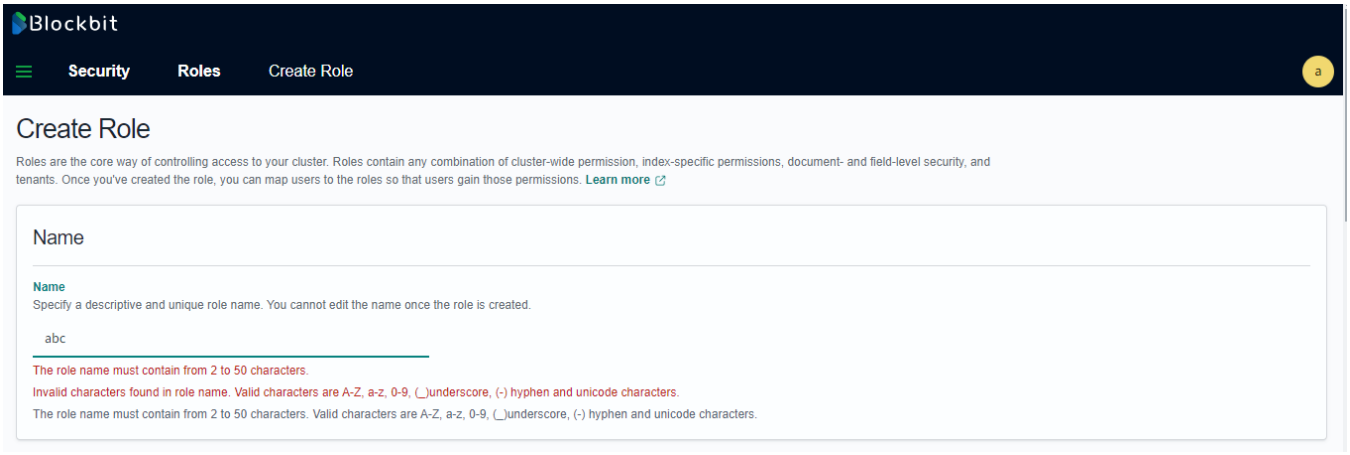
Delete: deletar regra. Você pode deletar mais de uma regra.

Para criar uma regra, clique em **Create role**.

XDR - Security - Create role

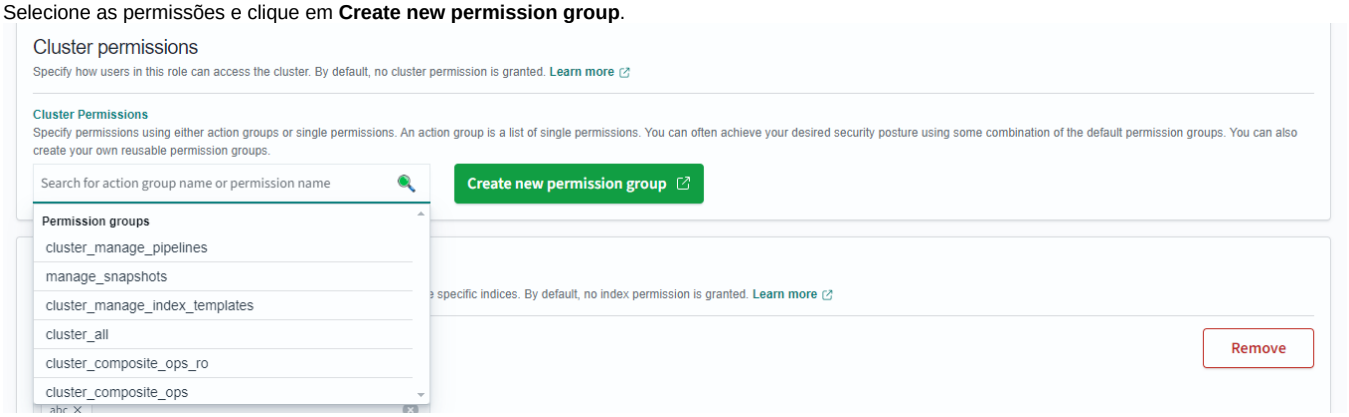
Neste artigo, a **Role** é referida como **Papel**.

Para criar um papel, primeiro dê um nome.



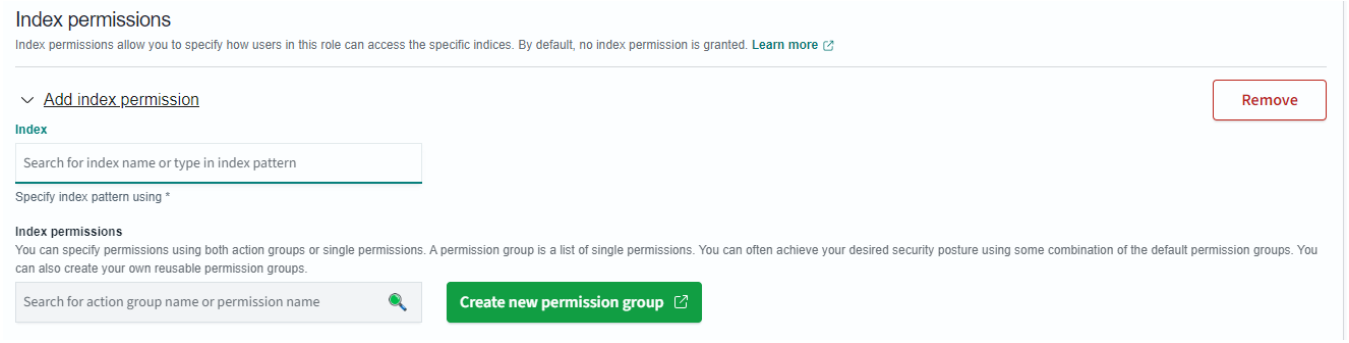
Depois, determine quais permissões este papel vai ter ao acessar o cluster.

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

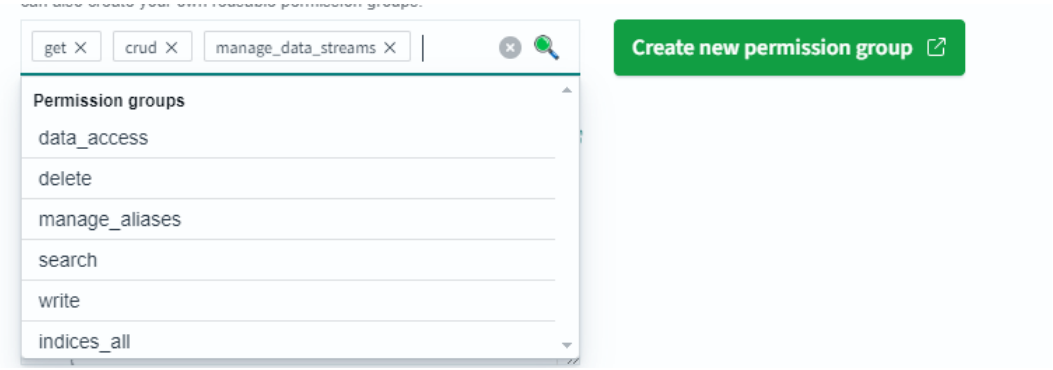


Depois, determine quais as permissões este papel vai ter ao acessar os **Indexes:**

Selecione os **indexes.**



Depois, especifique permissões dentro deles



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).

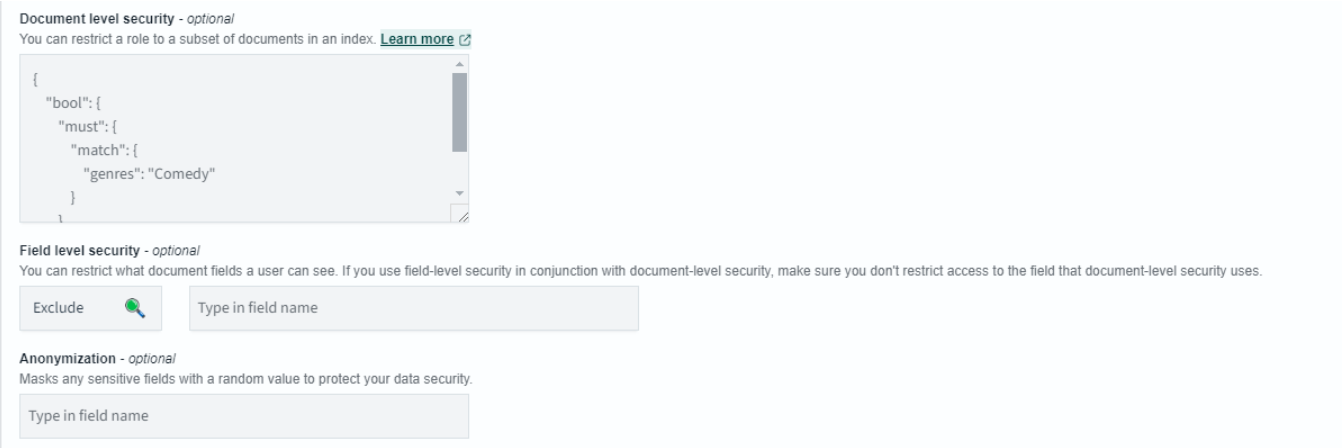
Exemplo:

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

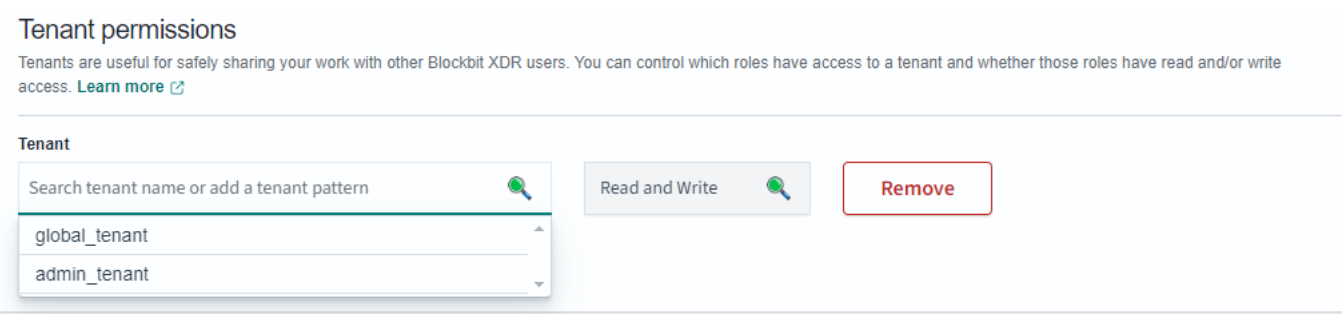
Em **Field level security**, você pode restringir o acesso a certos campos de documentos.

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.



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



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

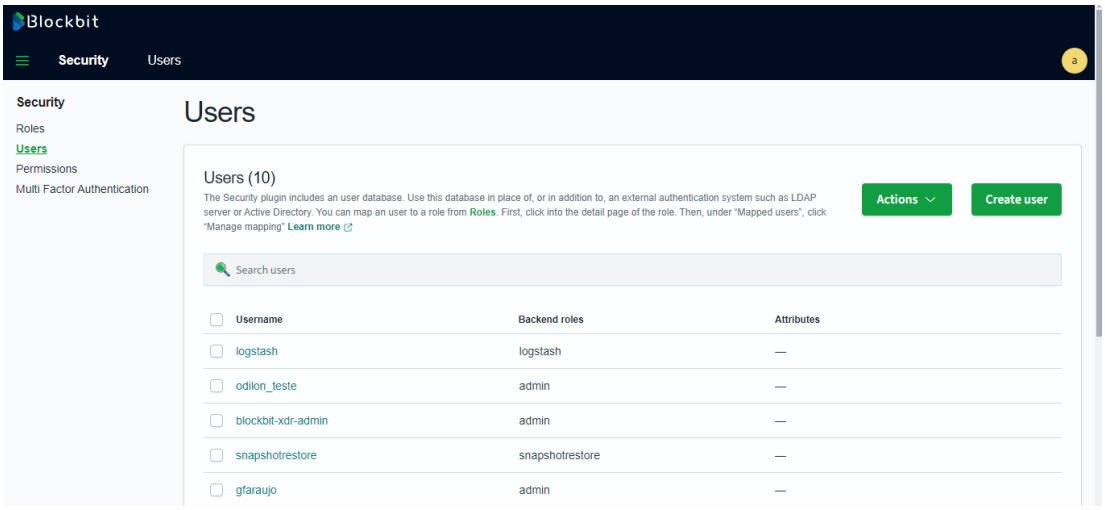
Quem acessa e administra o XDR são os usuários, ou pessoas autenticadas e com permissão para acessar a plataforma.

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;

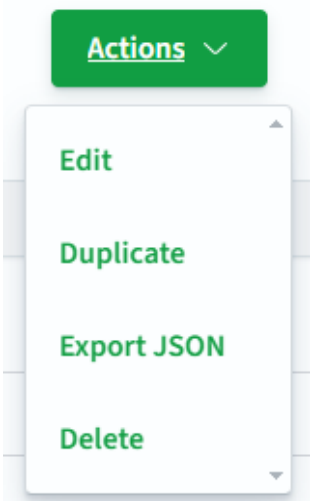
Backend role: grupo de permissões padrão de um usuário;

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.

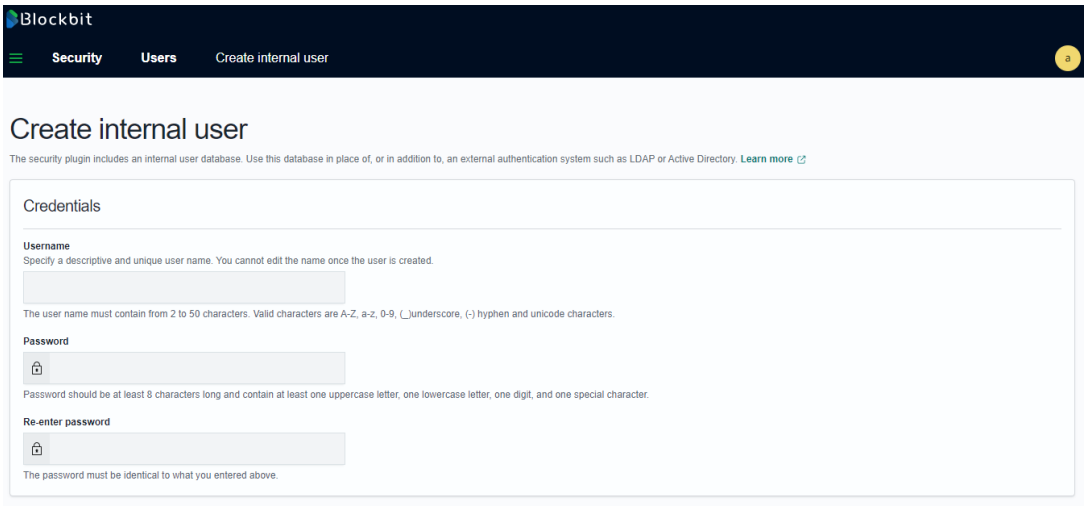
Delete: deletar usuário. Você pode deletar mais de um usuário.

Para criar um usuário, clique em **Create user**.

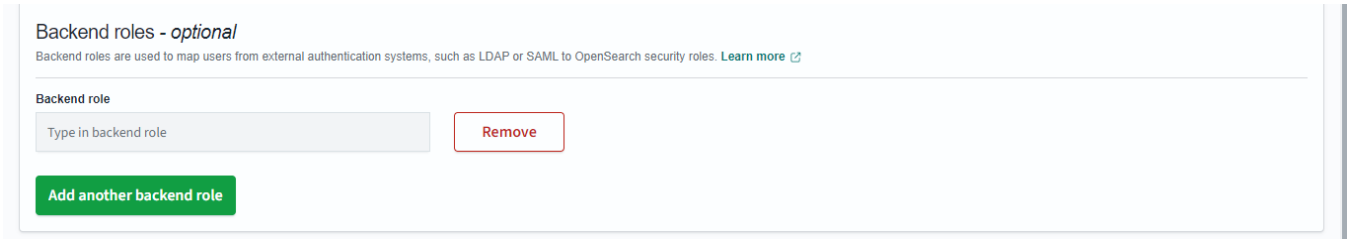
XDR - Security - Create User

Para editar um usuário, o processo é o mesmo.

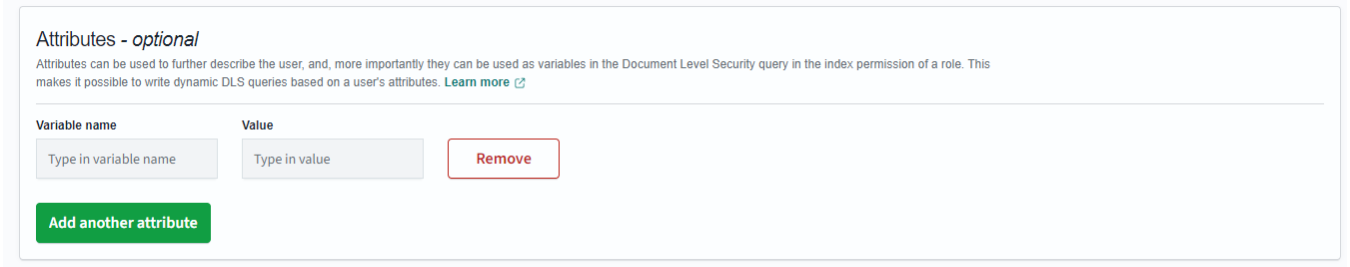
Para criar um usuário, primeiro crie um nome e uma senha:



Depois, defina os papéis:



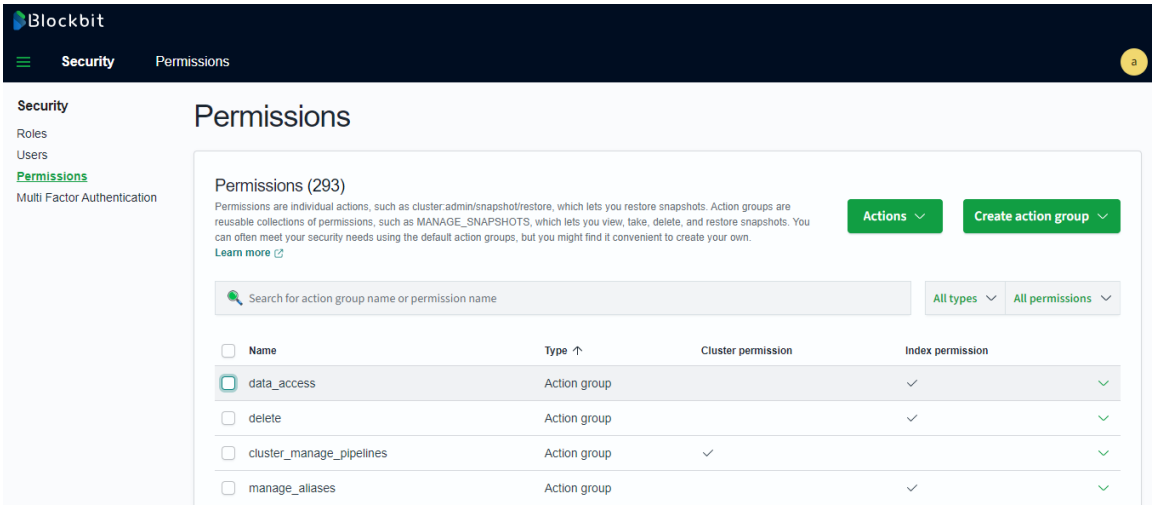
No final, defina os atributos:



Para criar o usuário, clique em **Create**.

XDR - Security - Permissions

Permissões são ações específicas que um usuário é autorizado a tomar.



As permissões são classificadas por:

Name: nome da permissão;

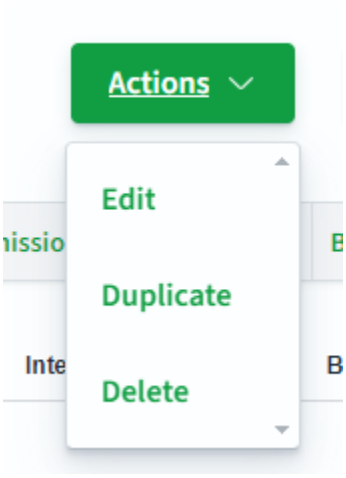
Type: tipo da permissão;

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:

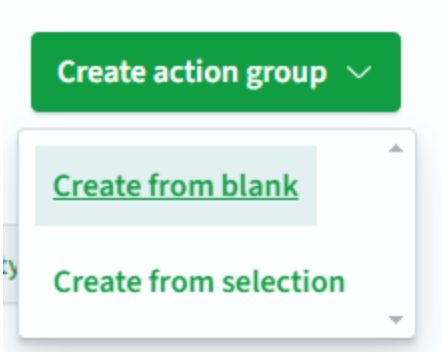


Edit: editar permissão. Esta opção é habilitada quando uma permissão é selecionada.

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

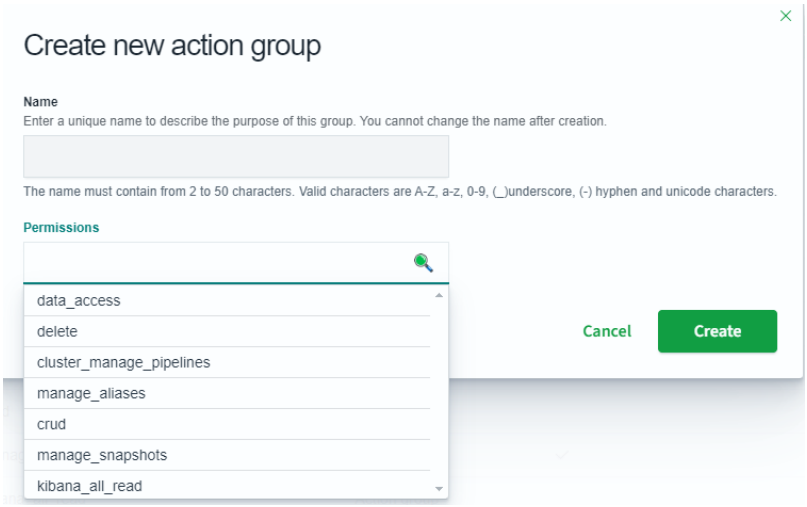
Delete: deletar permissão . Você pode deletar mais de uma permissão .

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;

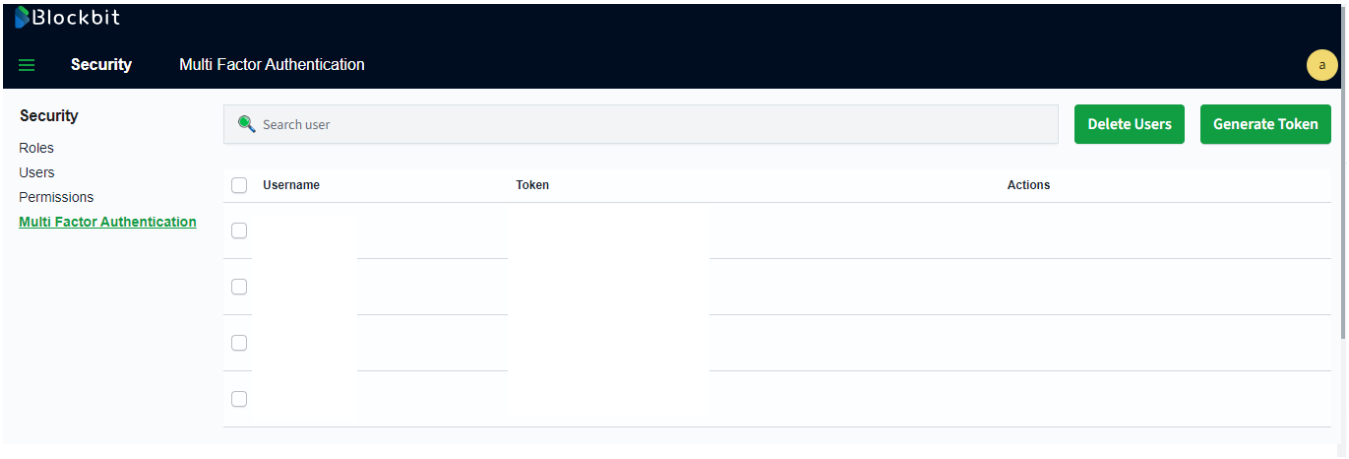
Create from selection: criar um grupo de ações a partir de permissões pré-selecionadas.



Para criar um grupo de ações, dê um nome e selecione as permissões.

XDR - Security - Multi Factor Authentication

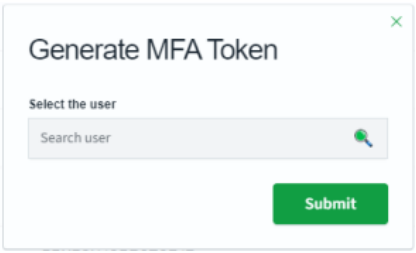
A autenticação multi fator é uma forma de aumentar a segurança do acesso ao exigir mais de um fator para garantir a identidade de um usuário.



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.**



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:

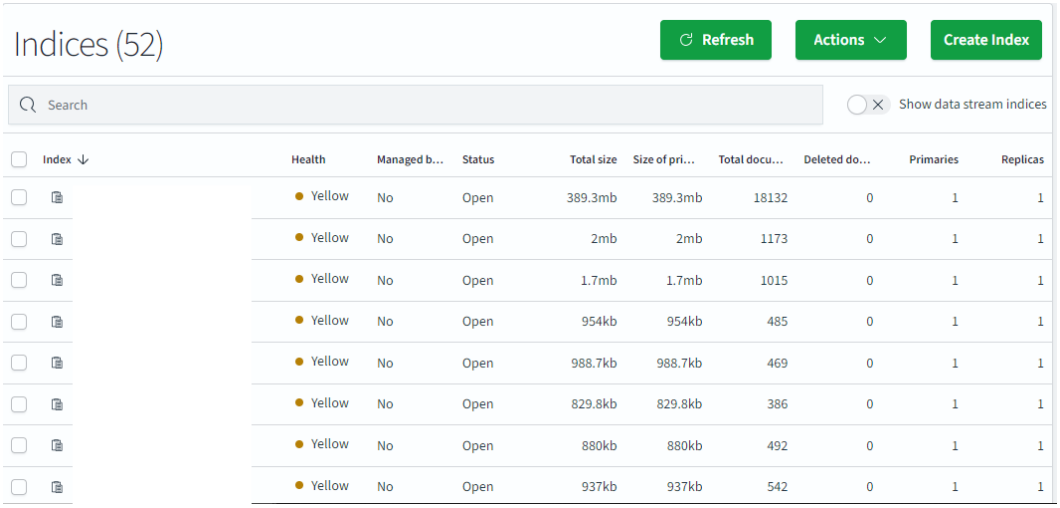
State Management Policies
Indices

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 **índex**.

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 indices na aba **Indices**.



Para buscar um index específico, utilize a barra de pesquisa (**Search**).

Para mostrar indices em data stream, ou que utilizam dados contínuos, clique em **Show data stream indices**.

Os indices são classificados por:

Index: nome do index;

Health: saúde do índex. 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;

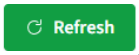
Total documents: número total de documentos;

Deleted documents: número de documentos deletados;

Primaries: shards primários;

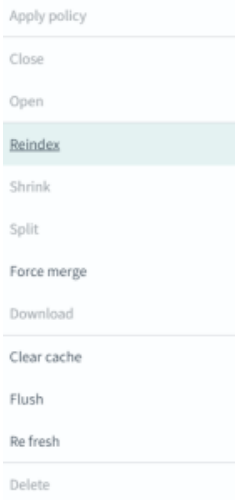
Replicas: shards replicados.

Ao clicar num index, você também poderá configurá-lo.

No botão **Refresh** (

), os indices são atualizados;

No botão **Actions** (Actions), são apresentadas as seguintes ações;



Apply policy: aplicar política aos indices selecionados;

Close: fechar os indices selecionados;

Open: abrir os indices selecionados;

Reindex: reindexar os indices selecionados;

Shrink: comprimir os indices selecionados;

Split: dividir os indices selecionados;

Force merge: fundir os indices selecionados;

Download: baixar os indices selecionados;

Clear cache: limpar o cache;

Flush: remover permanentemente;

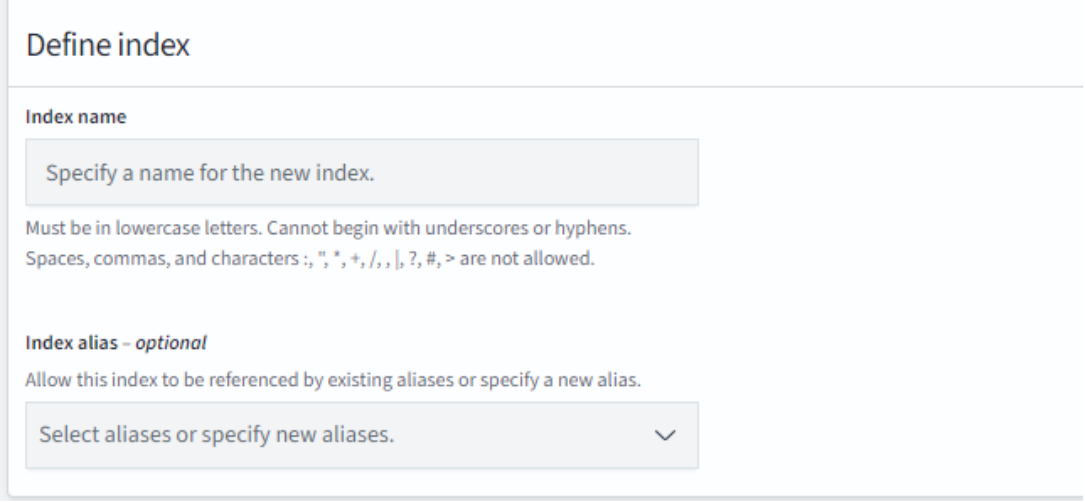
Refresh: atualizar;

Delete: apagar.

Para criar um index, clique em **Create index** (Create Index).

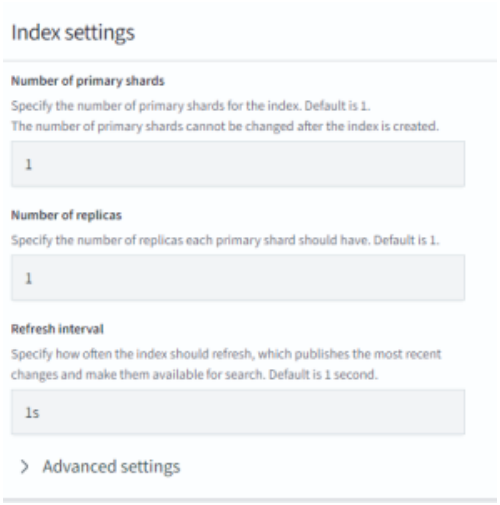
XDR - Indices - Indices - Create index

Para criar um index, primeiro, você define o nome dele.



Em **Index name**, insira o nome do index;

Em **Index alias**, você pode definir um **alias**, ou um grupo de indices.



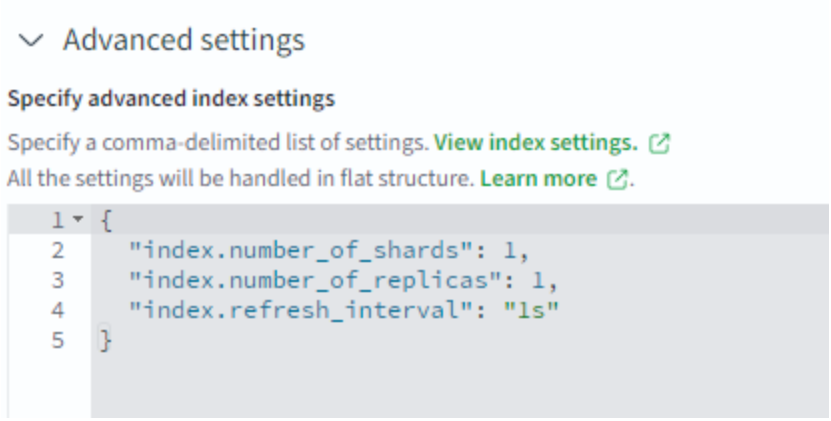
Depois, defina as configurações do index em **Index Settings**.

Determine o número de shards primárias em **Number of primary shards**;

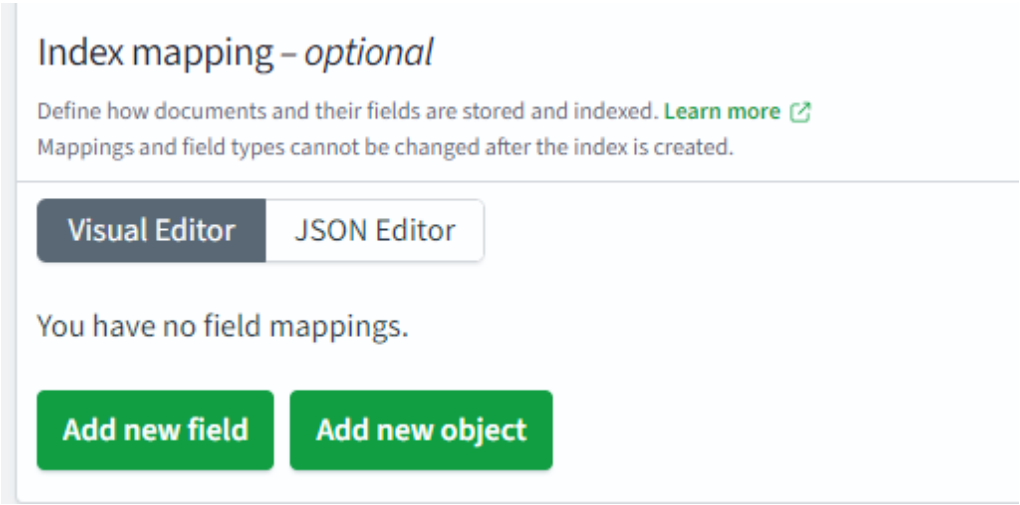
Determine o número de réplicas em **Number of replicas**;

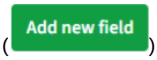
Determine os intervalos de atualização do index em **Refresh interval.**

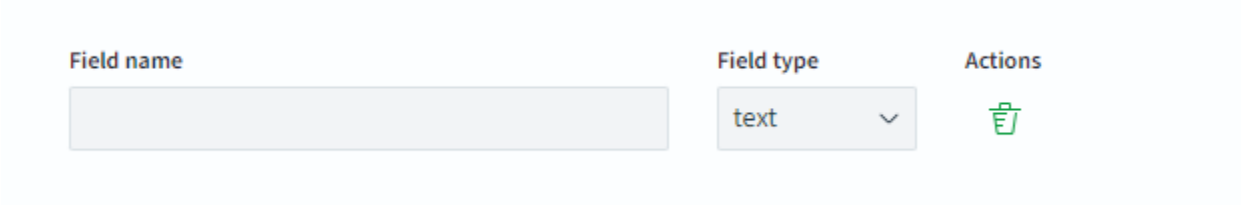
Em **Advanced settings**, você pode modificar configurações avançadas por meio de um JSON.



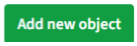
Para definir como um documento será armazenado num index, vá em **Index mapping.**



Em **Add new field** (), adicione uma categoria de dados.

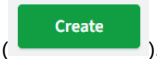


Dê um nome para a categoria e determine o seu tipo em **Field type**. Para deletar, clique em **Delete** ()

Em **Add new object** (), adicione um objeto JSON.

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.

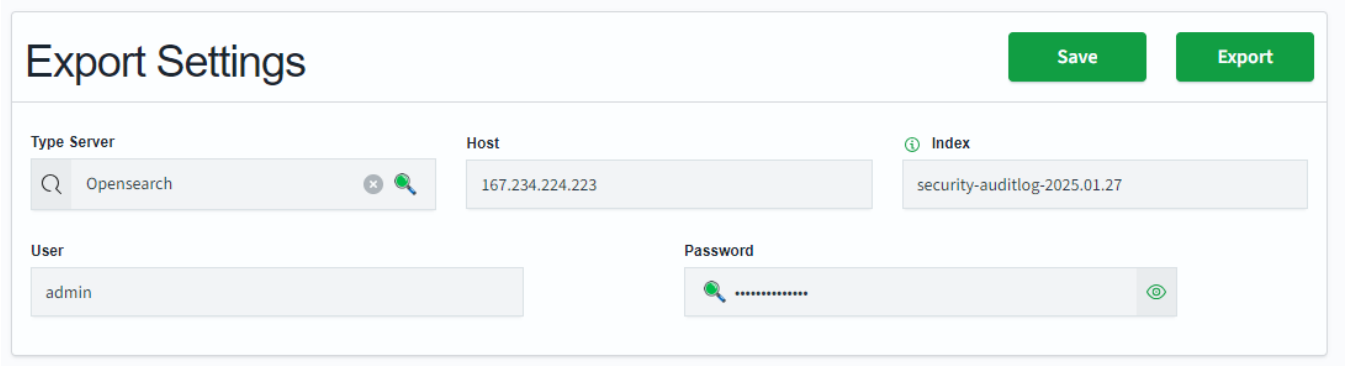
Para deletar, clique em **Delete** ().

Para criar o index, clique em **Create** (

).

XDR - Indices - Settings

O Blockbit XDR permite exportar logs de auditoria em formato JSON e/ou Syslog.



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.

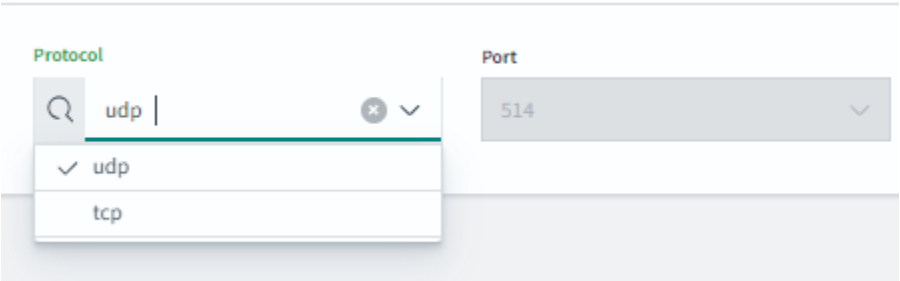
Para exportar uma categoria de índices, utilize um asterisco (*****) para selecionar tudo que foi digitado antes dele. (exemplo: **auditlog-2025*** exporta todos os índices de 2025. **auditlog-2025.01*** exporta todos os índices de janeiro de 2025, ou de eventos blockbit-xdr-alerts-1.x-2025.01*);

Quando o servidor é **Opensearch**, o sistema irá pedir as credenciais do administrador.

User: usuário que irá exportar o log;

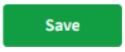
Password: senha do usuário que irá exportar o log.

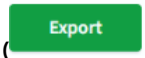
Quando o servidor é **SysLog**, o sistema irá pedir para configurar o protocolo de rede.



Protocol: protocolo de rede. São suportados **UDP** (porta 514) e **TCP** (porta 601).

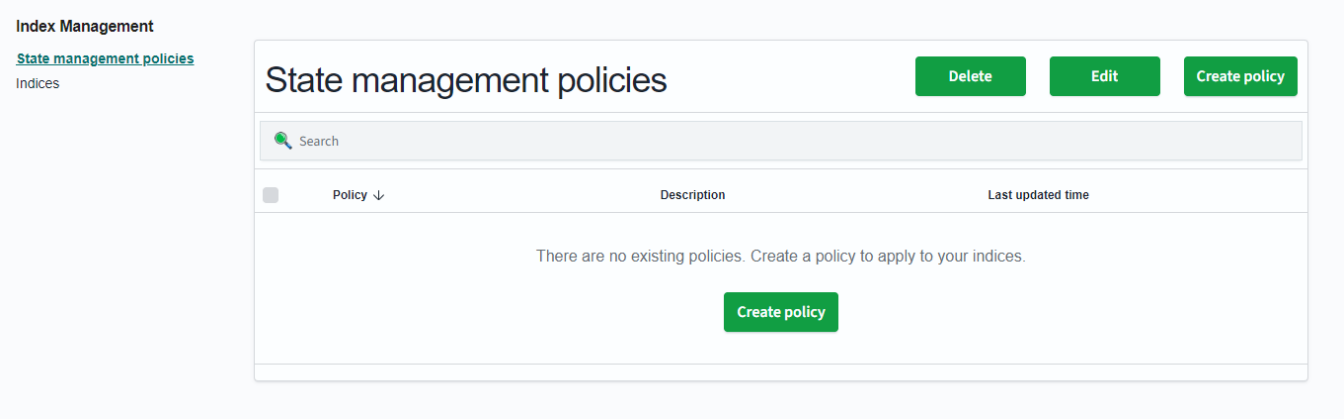
Port: porta.

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:

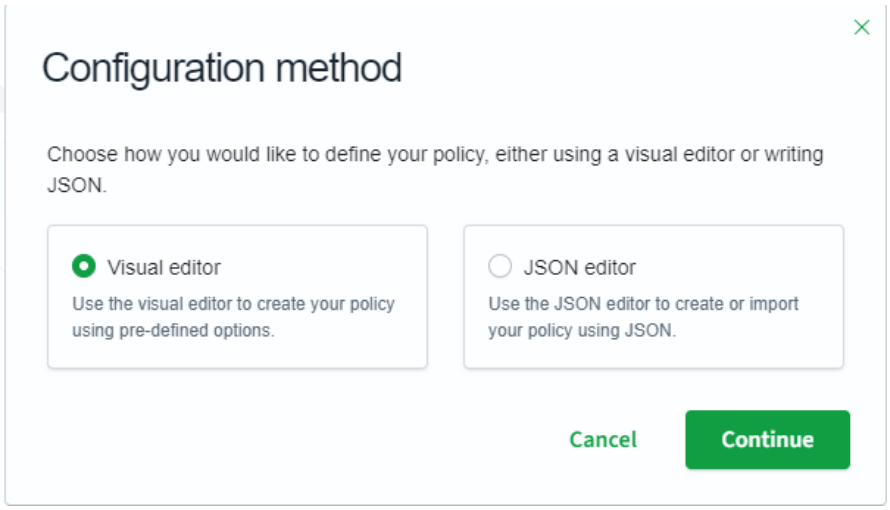
Policy: nome da política;

Description: descrição da política;

Last updated time: horário da última atualização da politica.

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:

Para criar uma política, primeiro dê um nome em **Policy ID**.

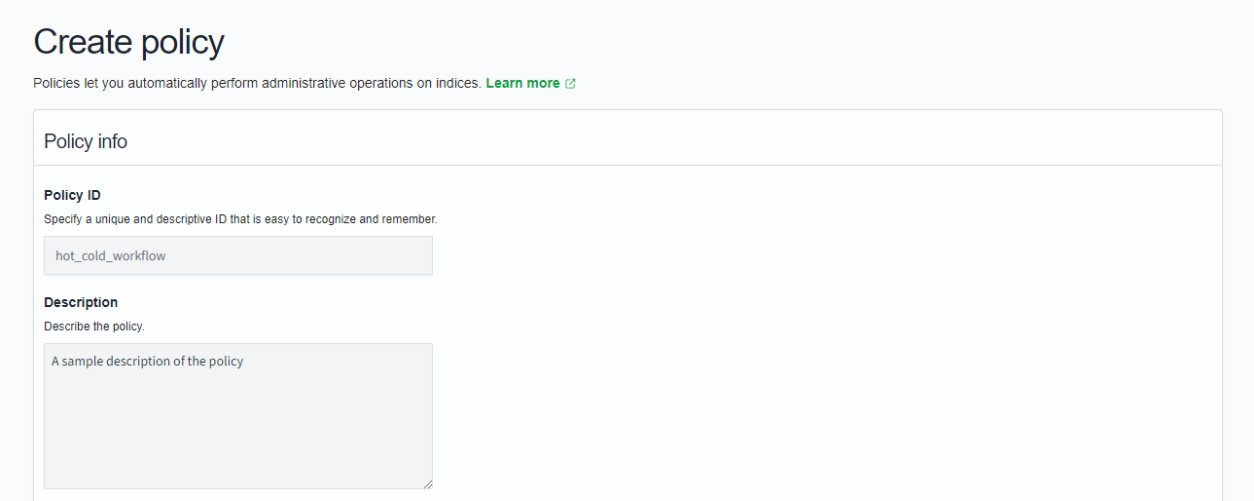
Depois, em **Define policy**, você pode criar ou colar um JSON com as definições da política.

Clique em **Copy** para copiar o JSON.

Clique em **Auto indent** para indentar automaticamente o JSON.

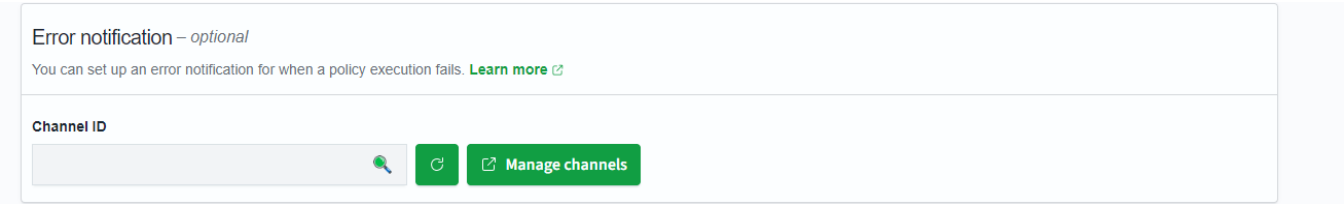
XDR - Indices - State Management Policies - Visual editor

Ao selecionar o Visual editor, você irá para esta página:



Para criar uma política, primeiro dê um nome em **Policy ID**.

Você pode adicionar uma descrição em **Description**.

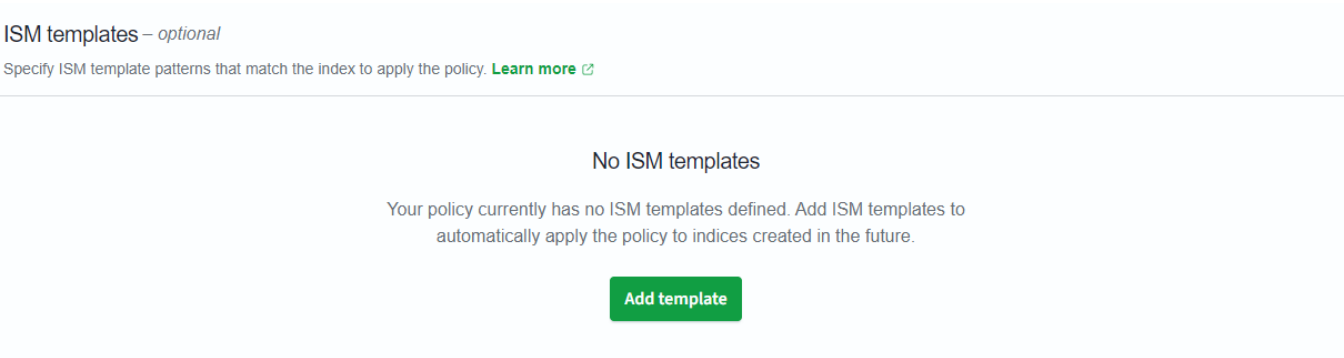


Em Error notification, você pode gerenciar as notificações de erro

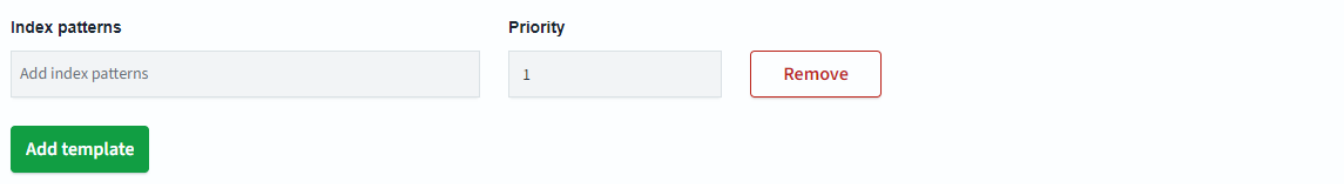
Insira o canal onde a notificação será apresentada em **Channel ID.**

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.

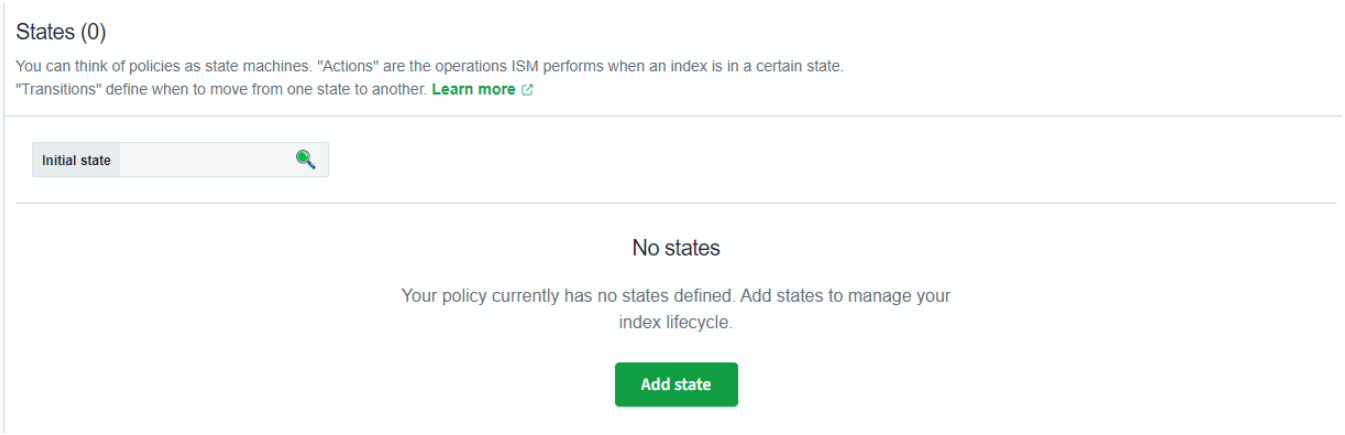


Para adicionar um template, clique em **Add template**.



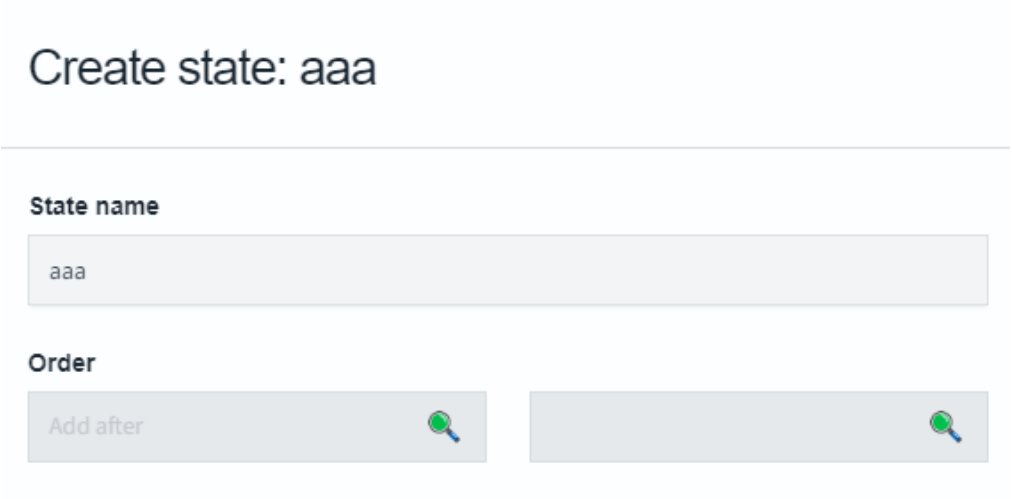
Insira o Index pattern (ID de referência do índex) e defina a prioridade. Depois, clique em Add template. Para deletar, clique em Remove.

Em **States**, você pode determinar os estados que cada **índex** irá passar. Em cada estado, o ISM template irá realizar ações específicas.



Em **Initial state**, você pode buscar por um estado inicial.

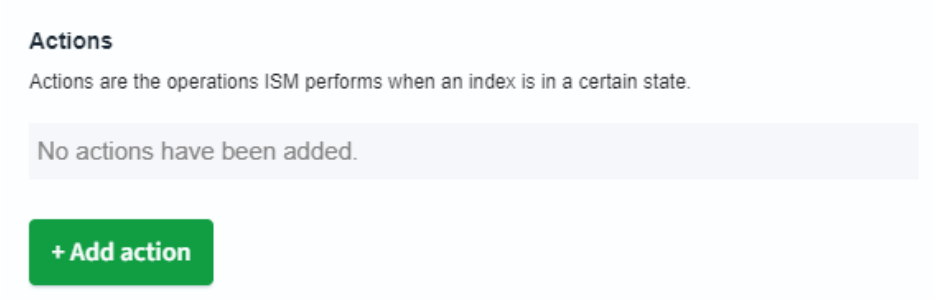
Para criar um estado, clique em **Add state**.



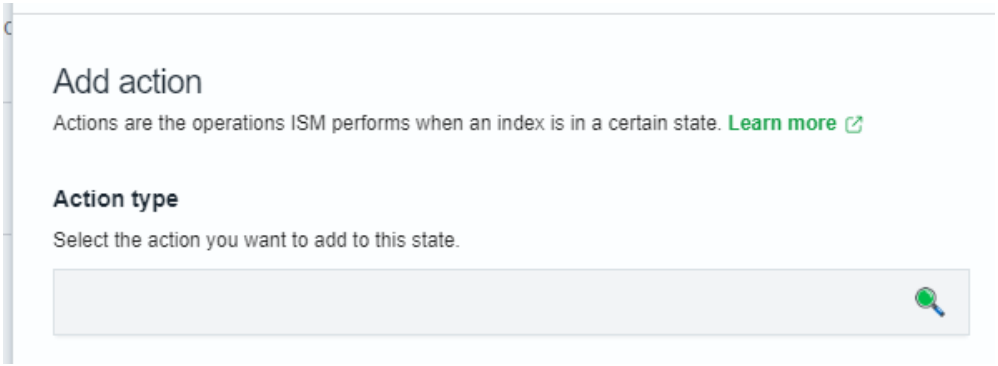
Nomeie o estado em **State name.**

Em **Order**, você define a aplicação do estado entre outros estados.

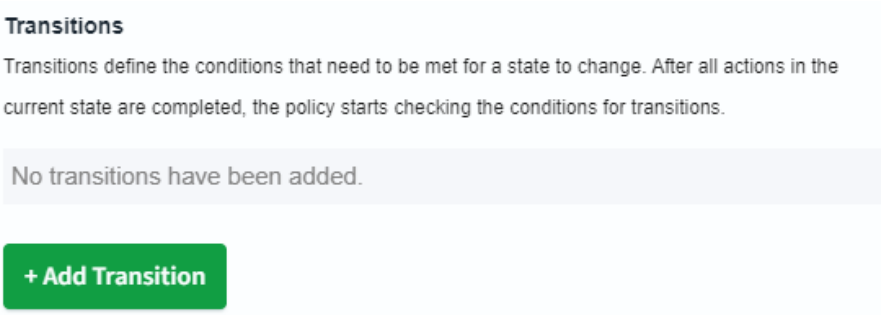
Clique em **Add action** para adicionar uma ação.



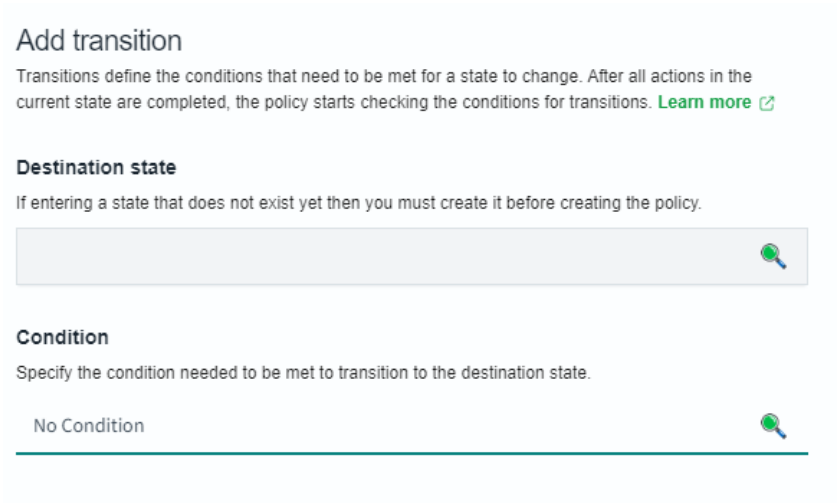
Para criar uma ação, defina o tipo:



Clique em **Add transition** para definir as condições de mudança de estado.



Para adicionar uma transição, defina o estado anterior e as condições:



XDR - Audit

O Blockbit XDR permite gerar logs de auditoria, que rastreiam acessos ao cluster

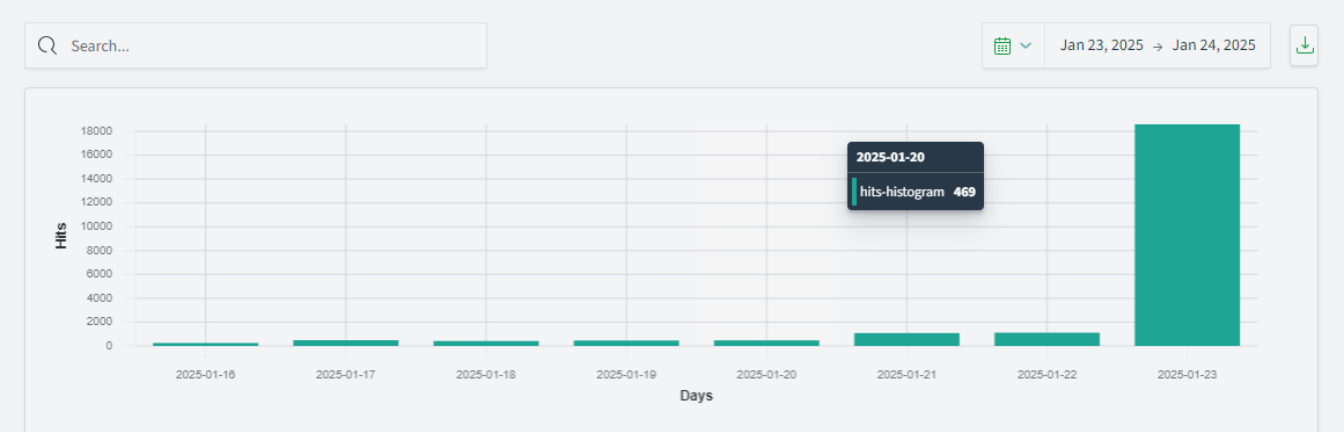
Ao clicar em Audit, você poderá acessar:

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.

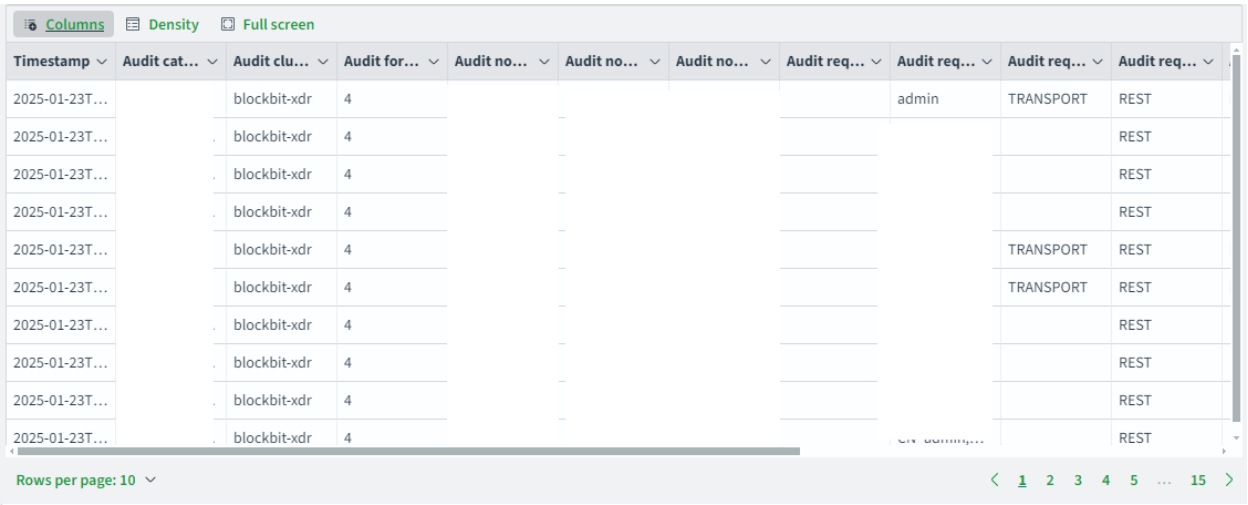


Para pesquisar, use a barra de busca.

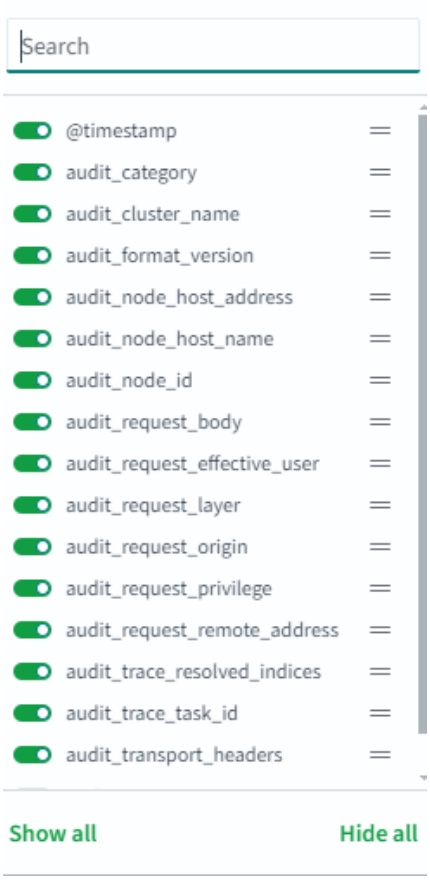
Para definir o intervalo, use o calendário. Mais informações em sistema de buscas.

Para baixar um arquivo CSV com os logs de auditoria, use o botão de download ( ).

Abaixo do gráfico, há uma lista de logs gerados.



O botão **columns** permite definir quais categorias serão mostradas.



@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 indices resolvidos afetados pela requisição;

audit_trace_task_id: identificação da requisição;

audit_transport_headers: o header da requisição;

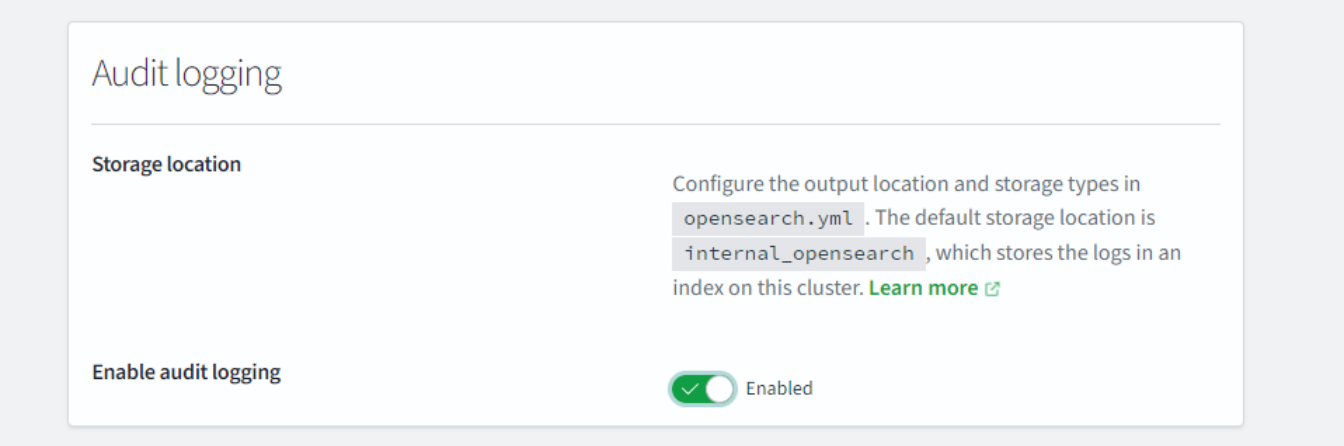
audit_transport_request_type: o tipo da requisição.

O botão **Density** permite aumentar ou diminuir a densidade da lista;

O botão **Full screen** coloca a lista em tela inteira.

XDR - Audit - Settings

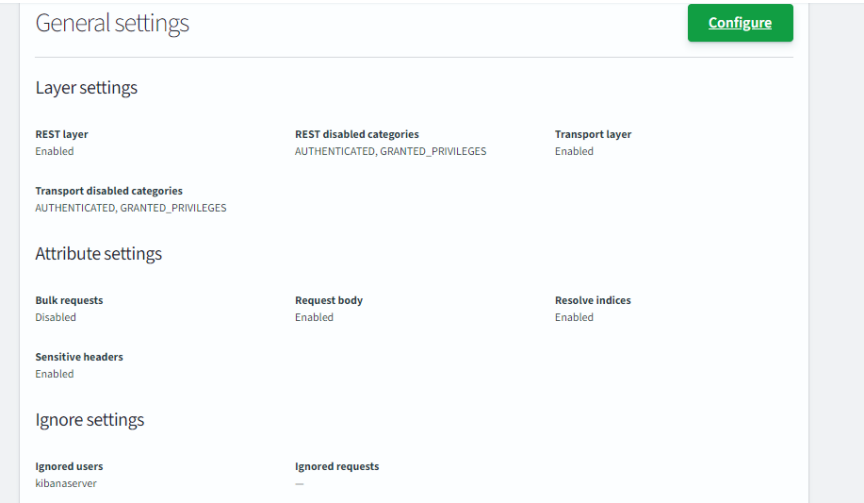
Em Settings, você pode definir as configurações dos logs de auditoria.



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 definí-las, clique em **Configure** (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.

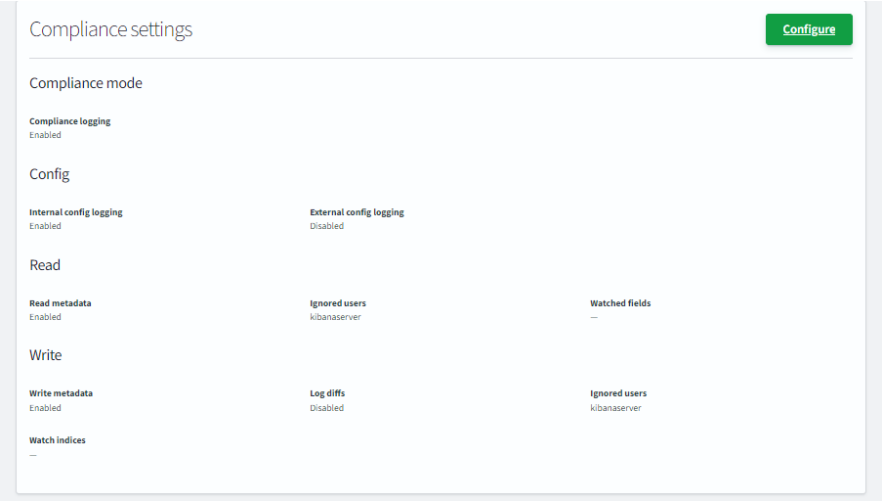
Resolve indices: resolver indices na auditoria;

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 definí-las, clique em **Configure** (Configure).



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 indices 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;

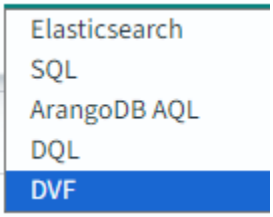
Watched indices: listar indices a ser observados durante eventos tipo **write**. Ao adicionar um index, será gerado **1 log por documento**.

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.

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:

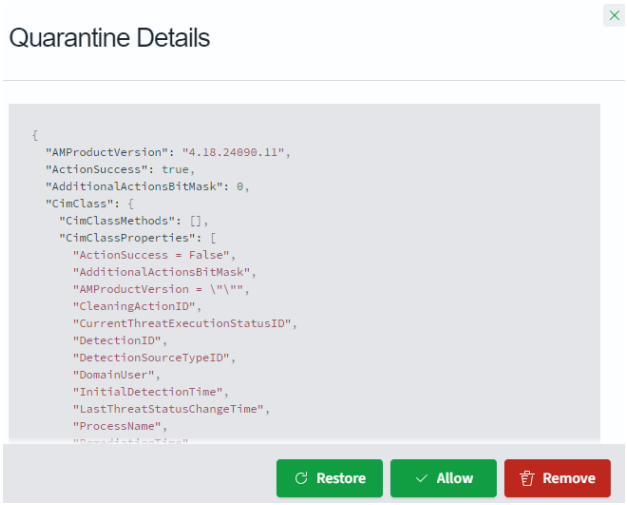
Detection ID: identificador dado ao arquivo pelo Blockbit XDR;

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 disponiveis:

View threat details (**)**: abre um modal com detalhes do arquivo. No modal, você pode administrar o arquivo.



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**.**

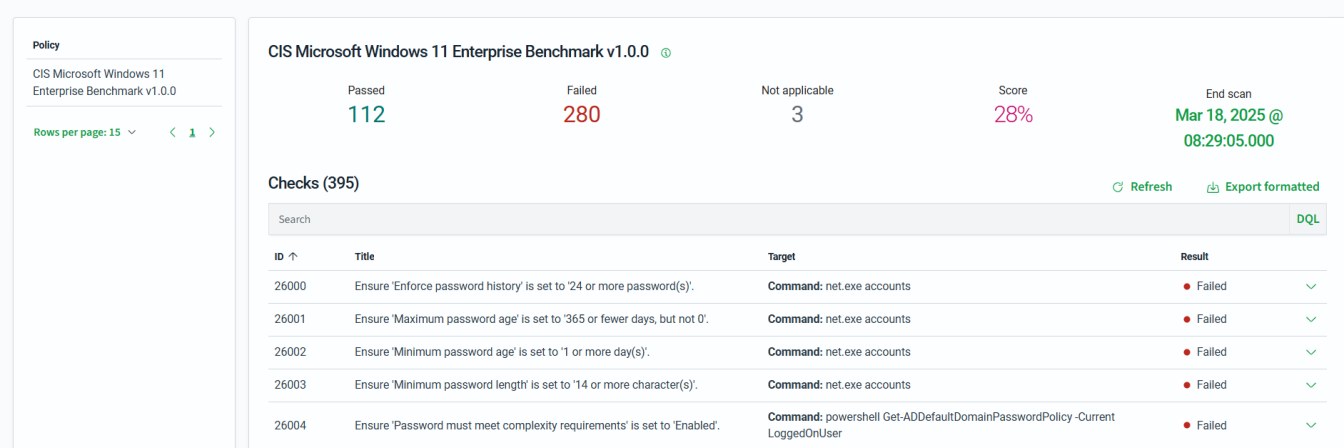
Restore ( **)**: Restaura o arquivo para o seu local original, permitindo que seja carregado, acessado e executado no endpoint. Essa ação só deve ser realizada caso o arquivo tenha sido verificado e considerado seguro.

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.



Ao clicar em **Export formatted**, será criado um arquivo **.csv** com informações da checagem.

No começo da tela, são listados os resultados da checagem :

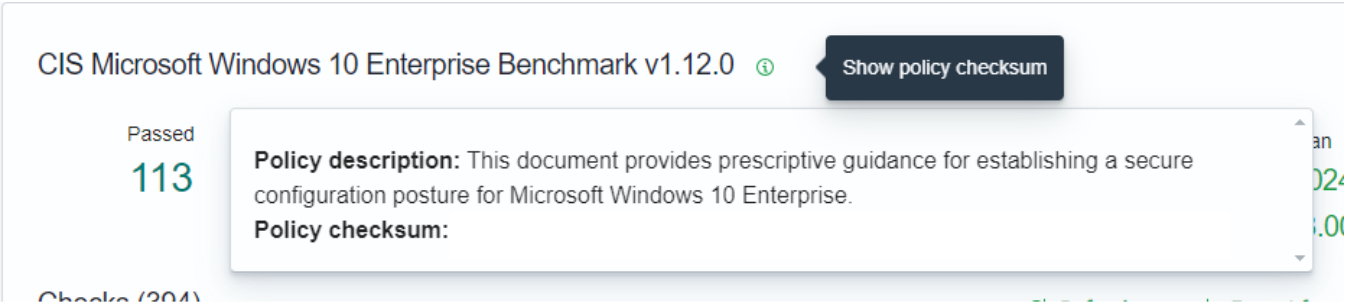
Passed: configurações consideradas satisfatórias;
Failed: Configurações consideradas insatisfatórias;

Not applicable: Configurações que não foram consideradas no escaneamento;

Score: Porcentagem das configurações consideradas satisfatórias;

End scan: Momento do fim do escaneamento.

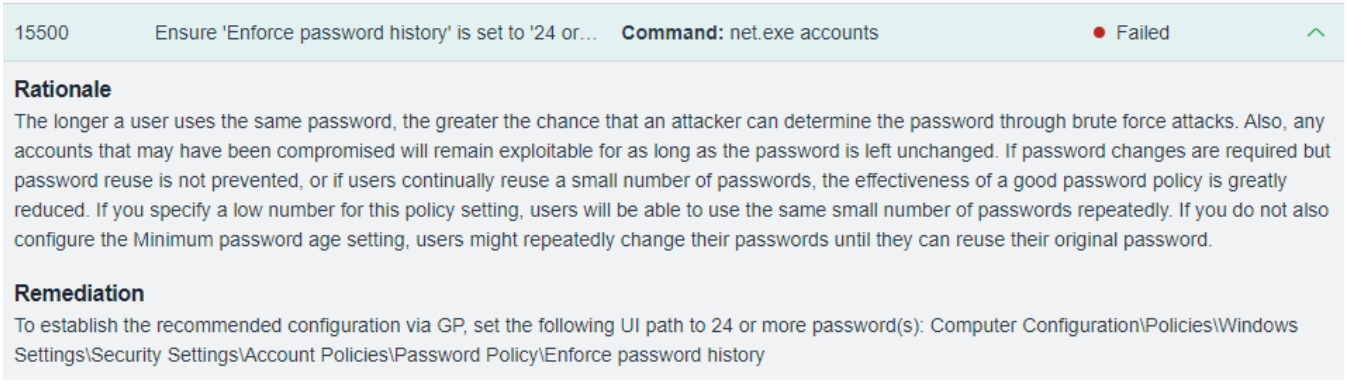
Você pode conferir a descrição e o checksum do agente ao clicar no informacional.



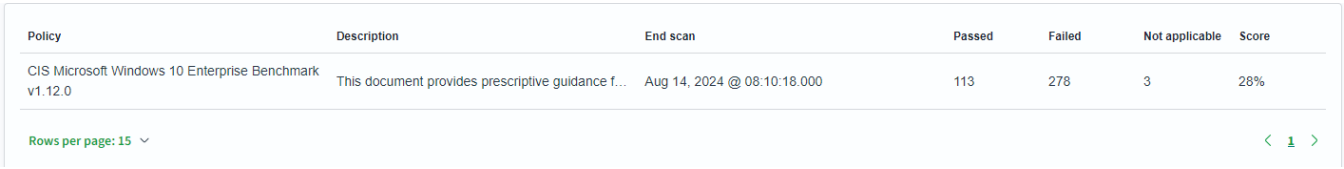
Abaixo, serão apresentadas as checagens individuais com:
ID: identificador da checagem;
Title: Título da checagem;

Target: alvo da checagem;

Result: resultado da checagem.
Ao clicar no resultado, são apresentadas mais informações sobre o teste.



Ao clicar em Inventory, você pode conferir a lista de agentes que foram testados.



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.

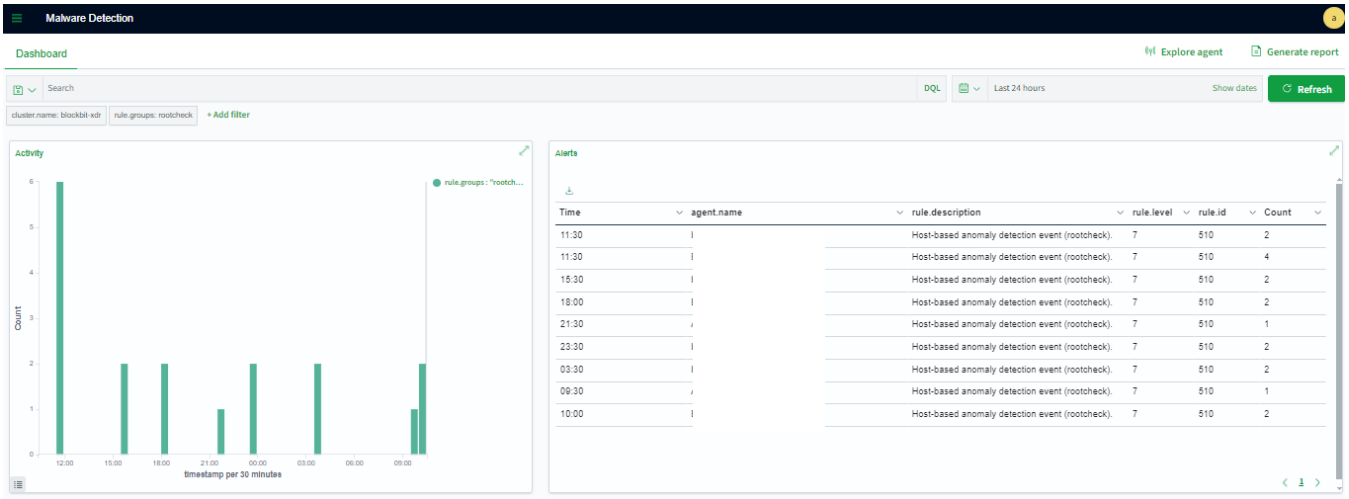
Análise Multi-Motor com VirusTotal e Threat Intelligence:

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

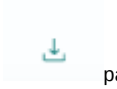
A barra permite buscar por eventos específicos. Para mais informações, confira Sistema de buscas.

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.

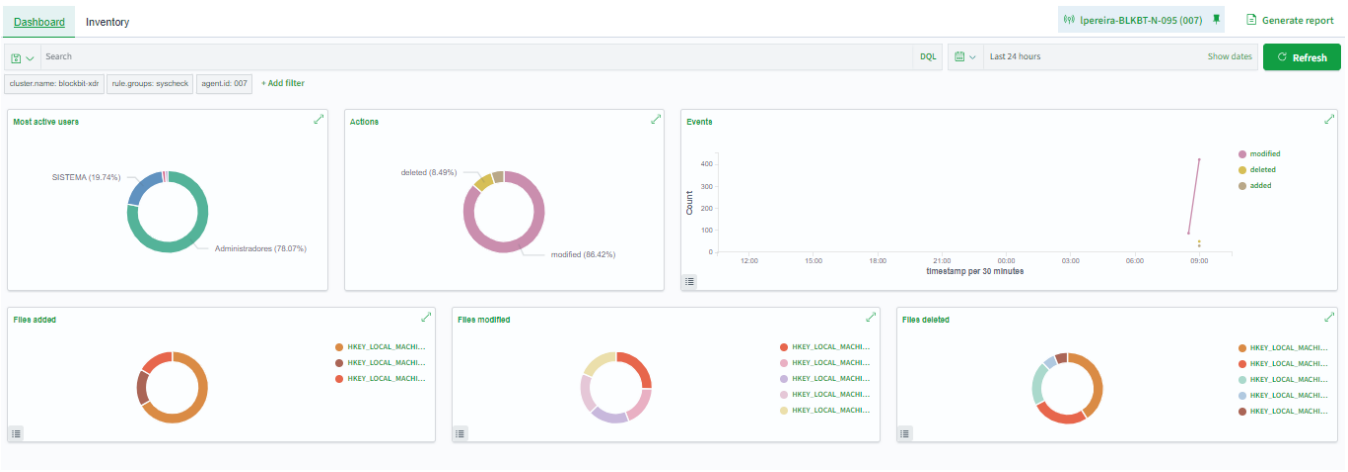
O **File Integrity Monitoring** suporta:

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;

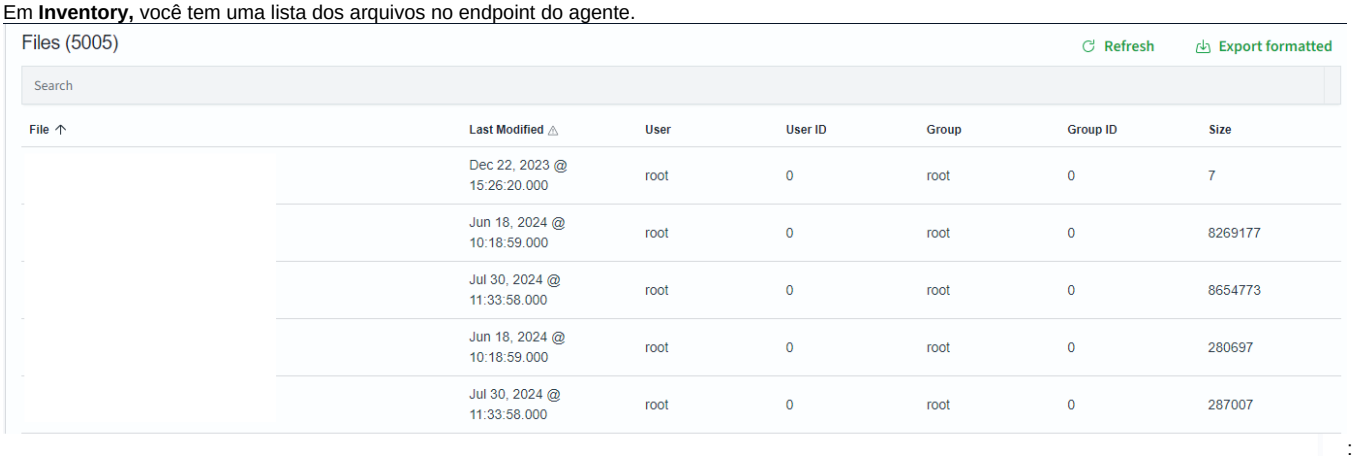
- **Delete:** apagar arquivo.

Events: número de eventos contados a cada 30 minutos.

Files added: Nomes dos últimos arquivos adicionados.
Files modified: Nomes dos últimos arquivos modificados.

Files deleted: Nomes dos últimos arquivos apagados.

Em **Inventory,** você tem uma lista dos arquivos no endpoint do agente.



:

São mostradas as seguintes informações de cada arquivo.

File: nome do arquivo;

Last modified: última modificação;

User: usuário do arquivo;

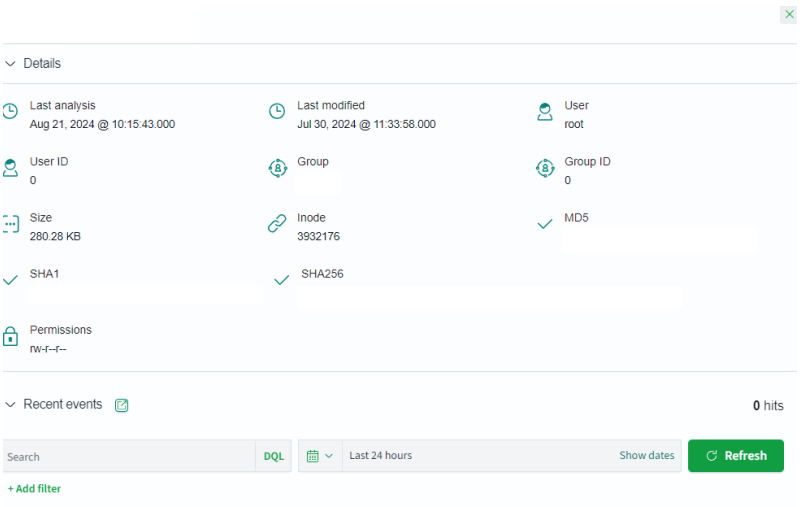
User ID: identificador do usuário;

Group: grupo do arquivo;

Group ID: identificador do grupo do 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:

Inode: informações sobre a localização do arquivo na rede;

MD5: código de verificação do arquivo;

SHA1: algoritmo de segurança de 160 bits do arquivo;

SHA256: algoritmo de segurança de 256 bits do arquivo;

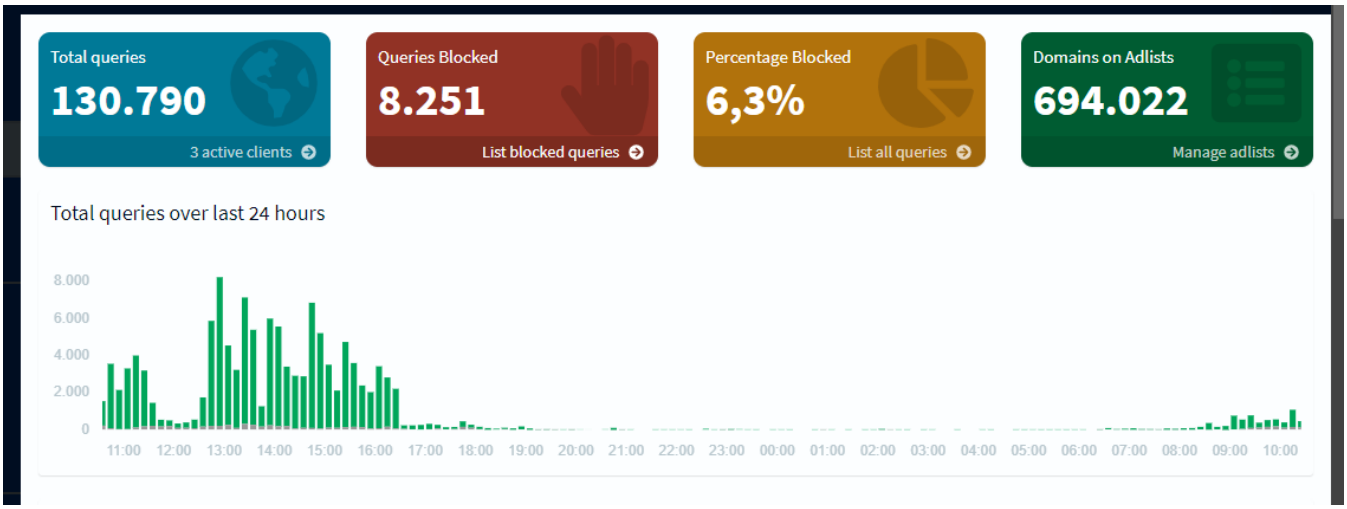
Permissions: permissões do arquivo.

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.

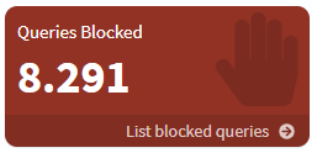


O dashboard do Secure Internet Gateway é divivido em:

Total queries

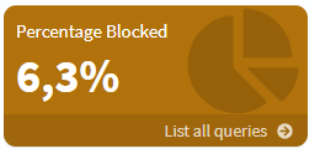
É o total de consultas na rede. Você também pode checar os clientes ativos no momento. Ao clicar, você irá para a lista de clientes.

Queries Blocked



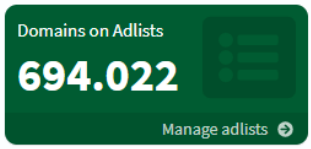
É o número de consultas bloqueadas. Ao clicar, você irá para a lista de consultas bloqueadas.

Percentage Blocked



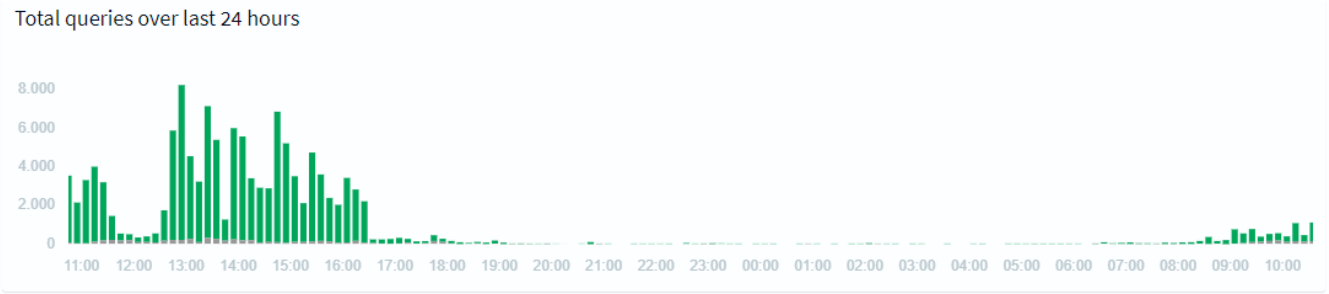
É a porcentagem de consultas bloqueadas. Ao clicar, você irá para as consultas mais recentes.

Domains on Adlists



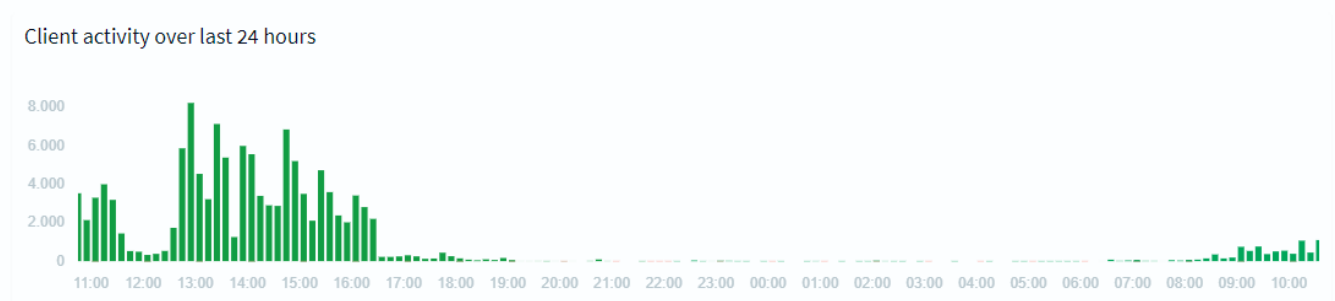
É o número de domínios na Adlist (lista de domínios bloqueados pelo bloqueador de anúncios). Ao clicar, você irá para a lista de dompinios.

Total queries over last 24 hours



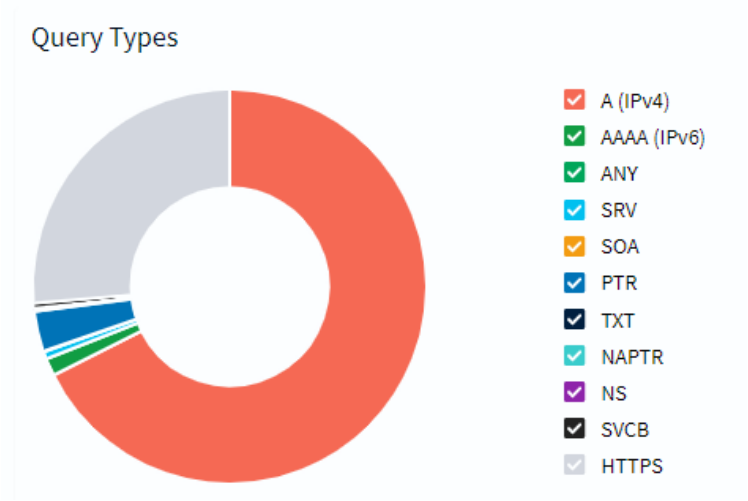
O gráfico mostra o número de chamados nas últimas 24 horas separados por intervalos de 10 minutos.

Client activity over last 24 hours



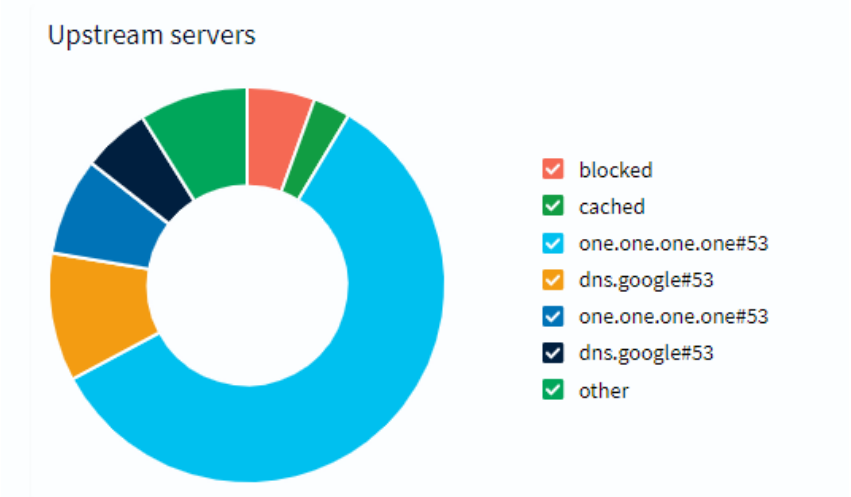
O gráfico mostra a atividade dos clientes nas últimas 24 horas separados por intervalos de 10 minutos.

Query types



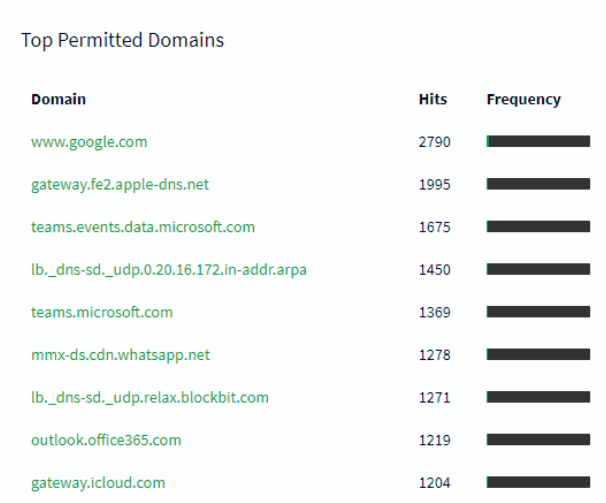
O gráfico separa as consultas por tipo. Ao passar o mouse, você confere a porcentagem de cada tipo de consulta.

Upstream servers



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



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

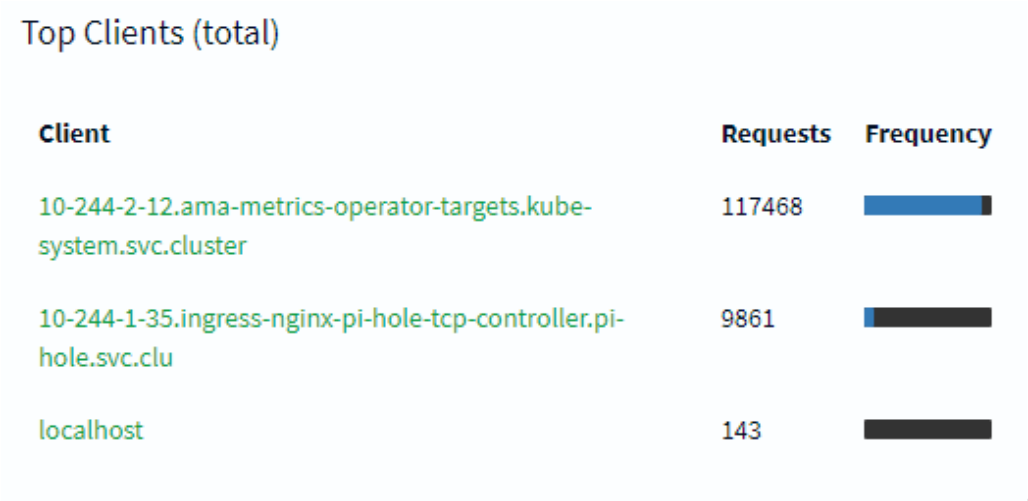
A lista mostra os domínios bloqueados mais acessados. Ela é separada em:

Domain: URL do domínio;

Hits: número de acessos;

Frequency: frequência de tentativas.

Top Clients (total)



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)

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.

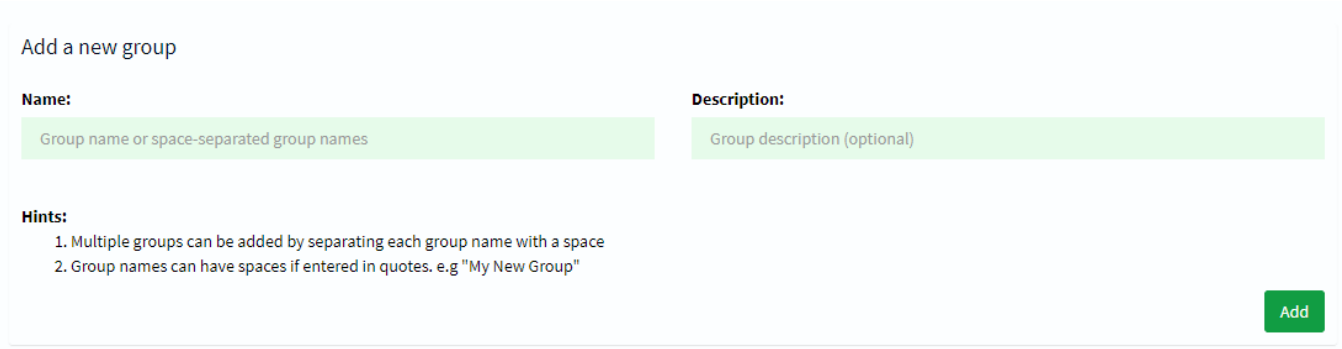
XDR - Secure Internet Gateway - Groups

O Secure Internet Gateway permite a criação de grupos de clientes ou domínios.

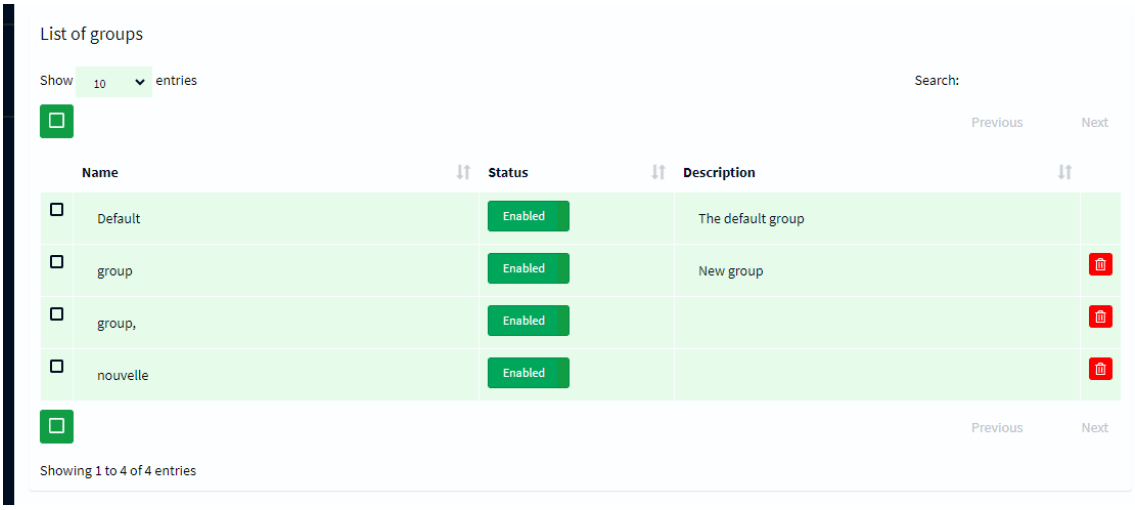
Com eles, você pode habilitar ou desabilitar o bloqueio de DNS simultaneamente em todos os elementos do grupo.

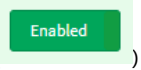
Para criar um grupo, dê um nome, descreva e aperte Add (

).
Para criar mais de um grupo, insira os nomes e separe por espaço.
Para utilizar espaços, coloque o nome do grupo entre aspas (" ").

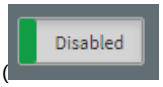


Abaixo, há um lista de grupos.



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 ().

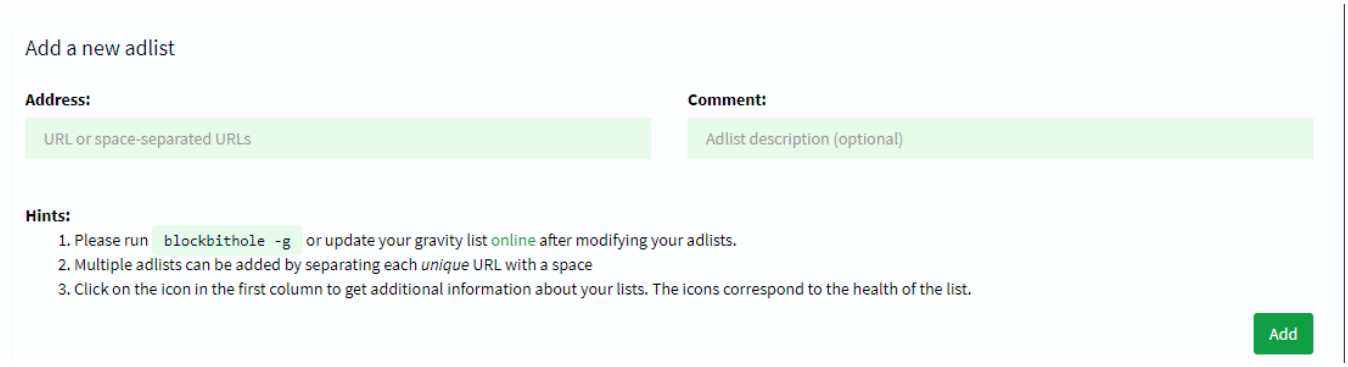
Para selecionar todos os grupos, clique na caixa verde escura () sem nenhum grupo selecionado ou no + () com pelo menos um grupo selecionado.

XDR - Secure Internet Gateway - Groups - Adlists

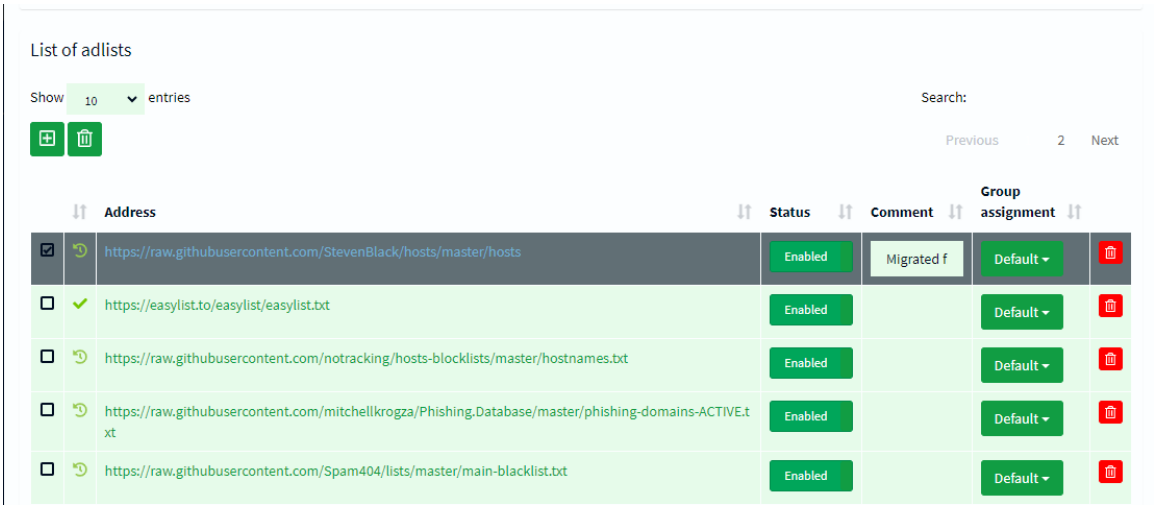
Uma **Adlist** é uma lista de domínios conhecidos por entregar publicidade. Ao bloquear as consultas de DNS desses domínios, o conteúdo de publicidade de uma página não é carregado.

Nesta página, você pode adicionar adlists e separá-las em grupos.

Após atualizar uma adlist, atualize o Gravity (lista de domínios bloqueados).



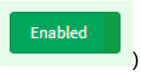
Para adicionar uma adlist, insira a URL em **Address** , descreva em **Comment** aperte Add (Add).
Para inserir mais de uma URL, separe por espaço.

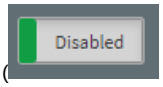


Em **List of adlists** há uma lista de adlists.

Em **Address**, estão listadas as URLs das adlists.

Ao clicar nos ícones  e  , você tem informações adicionais da adlist.

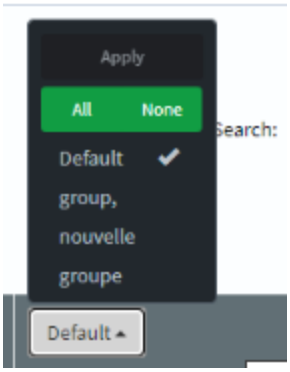
As adlists são inseridas como habilitadas por padrão. Em **Status**, Clique em Enabled() para desabilitar.

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( ).

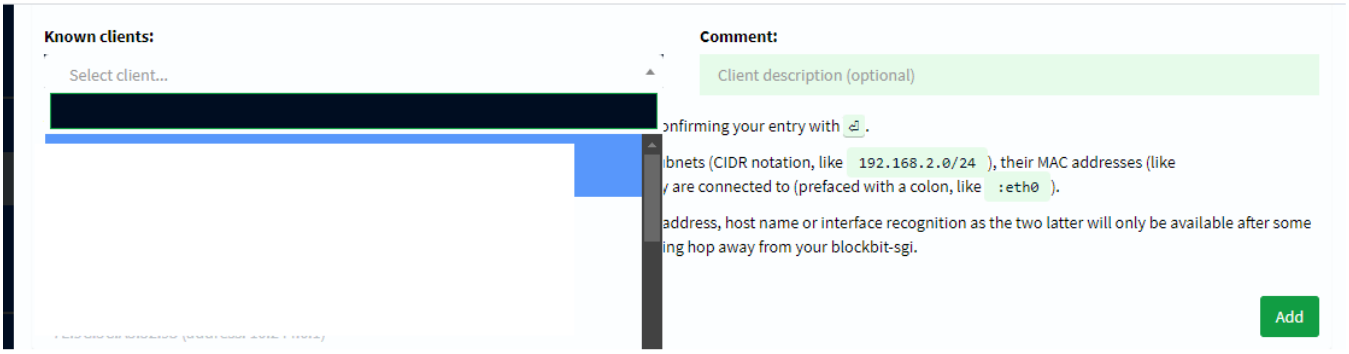
Você pode apagar mais de uma adlist simultaneamente. Para isso, selecione as adlists e clique em apagar todos ( ).

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 Add (

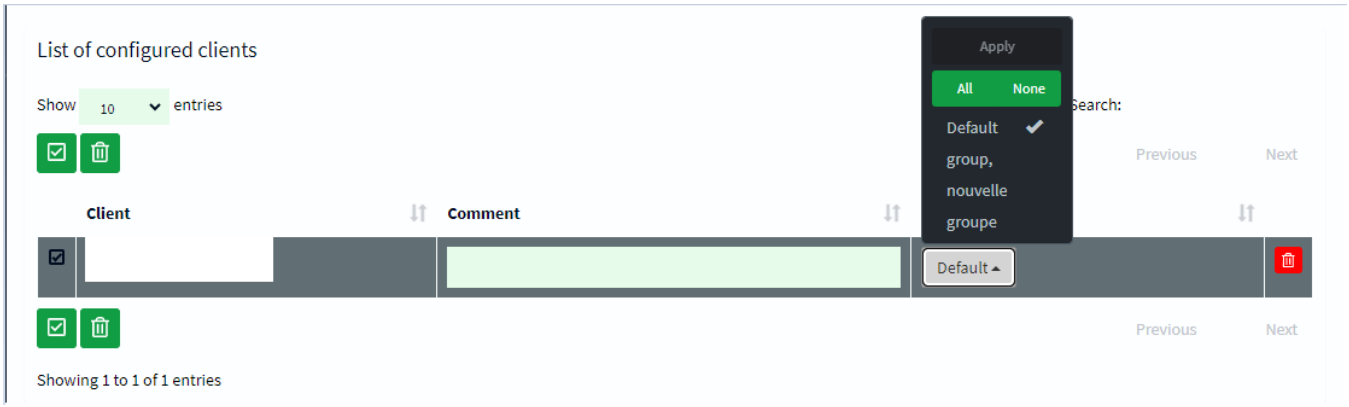
) ou aperte **enter**.



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.



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.

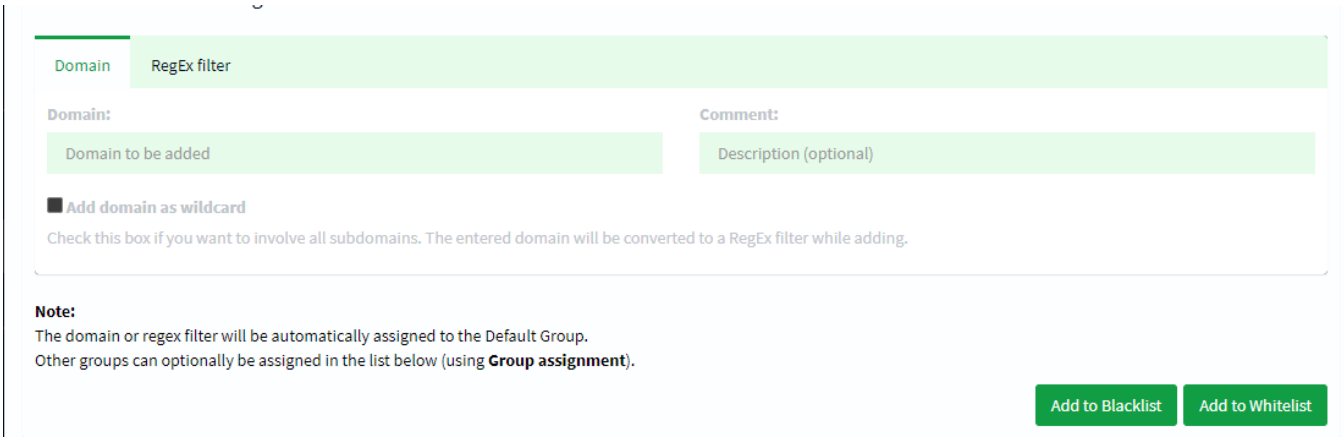
XDR - Secure Internet Gateway - Groups - Domains

O Secure Internet Gateway tem duas listas de domínios:

Whitelist: lista de domínios aceitáveis;

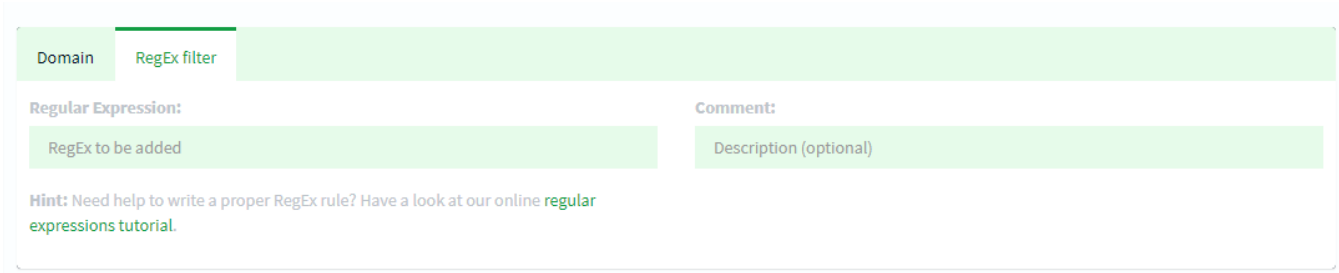
Blacklist: lista de domínios inaceitáveis.

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**.

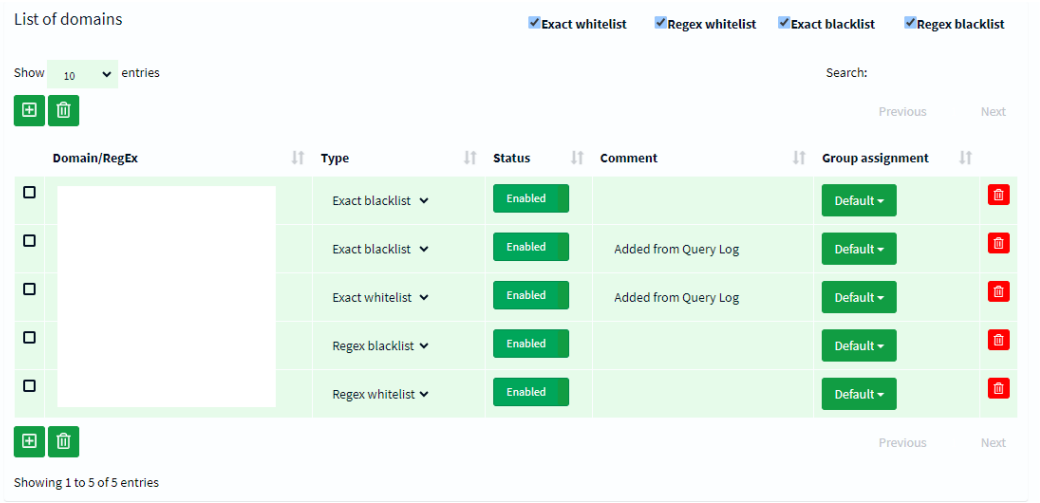
Para adicionar à Blacklist, clique em Add to Blacklist (

).

Para adicionar à Whitelist, clique em Add to Whitelist (

).

Em **List of domains**, há uma lista dos domínios ou RegEx e seus grupos.



Em **Type,** você pode mudar o tipo de registro do domínio.

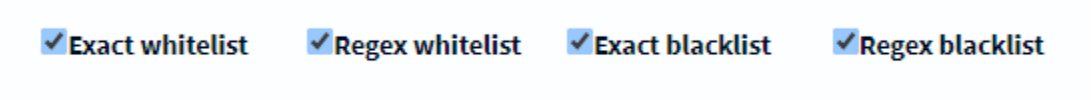
Exact whitelist: coloca o domínio exato na Whitelist.

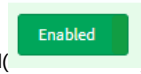
RegEx whitelist: aplica a regra determinada pela RegEx para colocar na Whitelist.

Exact blacklist: coloca o domínio exato na Blacklist.

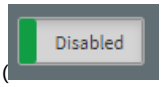
RegEx blacklist: aplica a regra determinada pela RegEx para colocar na Blacklist.

Você pode filtrar os registros por tipo no canto superior direito.



Os domínios entram na lista com o bloqueio de DNS habilitado por padrão. Em **Status**, Clique em Enabled(

) para desabilitar.

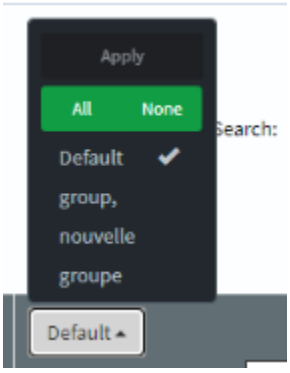
Para habilitar, clique em disabled (

).

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 selecionar todos os domínios ou RegEx, clique na caixa verde escura () sem nenhum domínio ou RegEx selecionado ou no + () com pelo menos um domínio ou RegEx selecionado.

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.

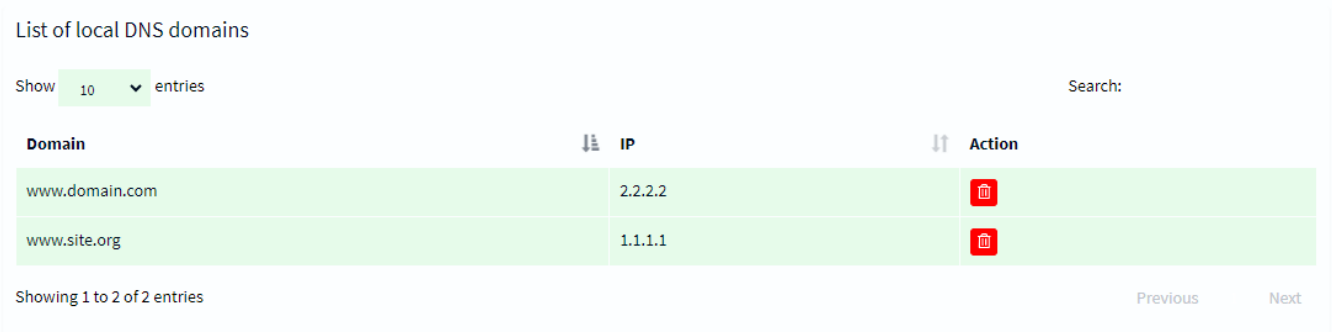
Você pode os servidores por pares domínio/IP ou CNAME.

DNS Records

Esta opção lista pares domínio/IP.

Para adicionar um par, insira o domínio em **Domain** e o endereço IP associado a ele em **IP Address.** Depois, clique em Add ()

Em **List of local DNS domains,** há uma lista de pares domínio/IP.



Domain é o domínio;

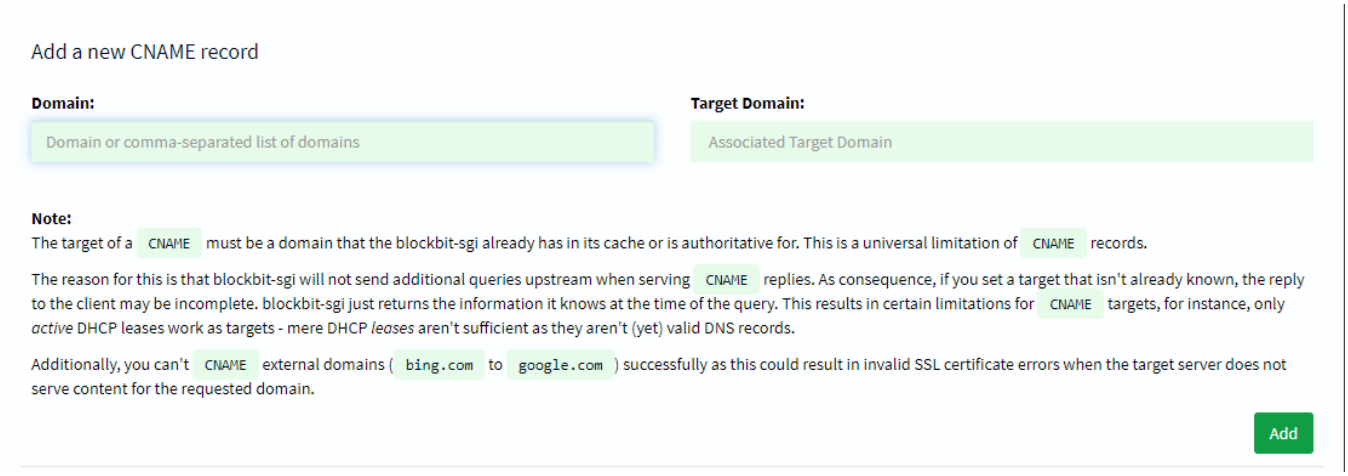
IP é o IP associado ao domínio.

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.



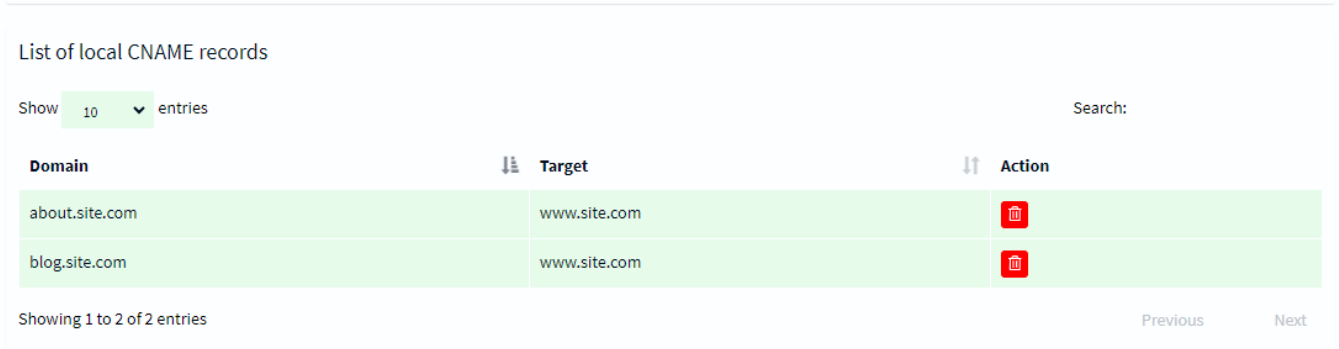
Em **Domain,** insira o domínio alias.

Em **Target Domain,** adicione o domínio canônico.

Para adicionar, clique em Add (

).

Em **List of local CNAME records,** há uma lista de pares **Domain** e **Target.**



Domain é o domínio alias;

Target é o domínio canônico.

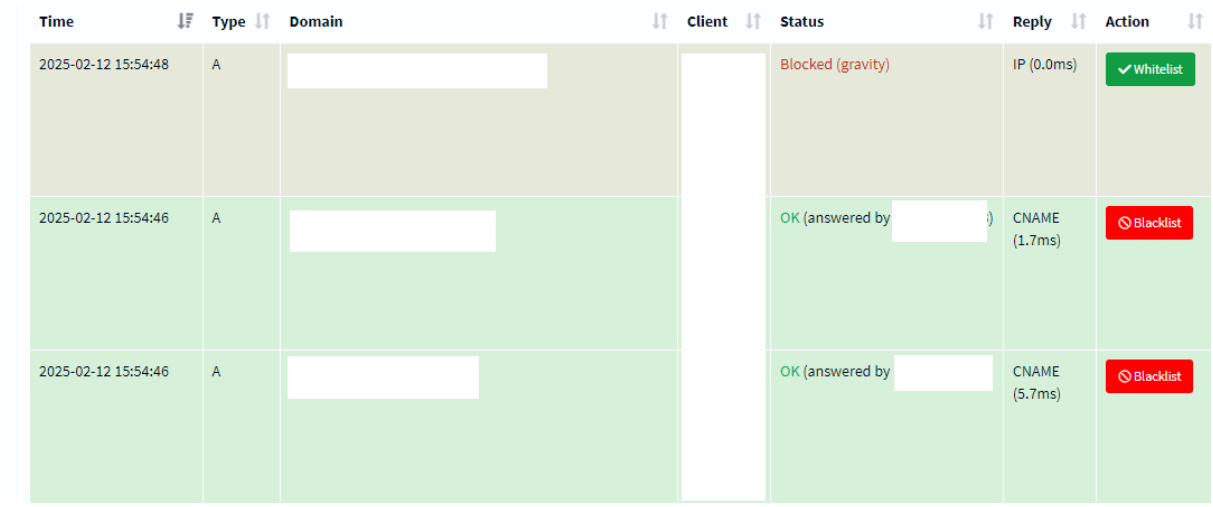
Para apagar o par, clique na lixeira().

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: 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 (Blacklist);
- Se uma consulta foi bloqueada, ela pode ser liberada e ir para a lista branca (Whitelist).

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.

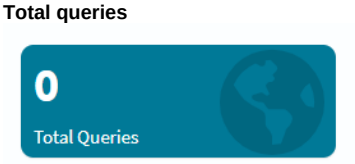
Graphics

Esta página mostra número de consulta ao longo do tempo em forma de gráfico.

Query log

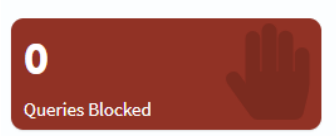
Esta página lista as consultas no intervalo selecionado.

Total queries



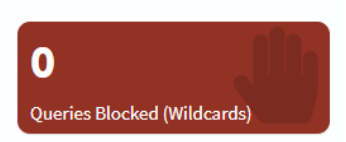
É o total de consultas na rede.

Queries Blocked



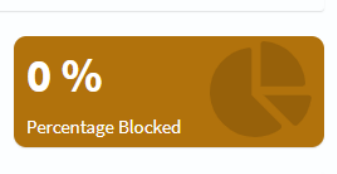
É o número de consultas bloqueadas.

Queries Blocked (Wildcard)



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;

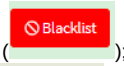
Domain: domínio que a consulta espera uma resposta;

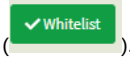
Client: cliente que a consulta espera uma resposta;

Status: estado da consulta. Pode ser Blocked (consulta bloqueada) ou OK (consulta respondida);

Reply: tempo e tipo da resposta;

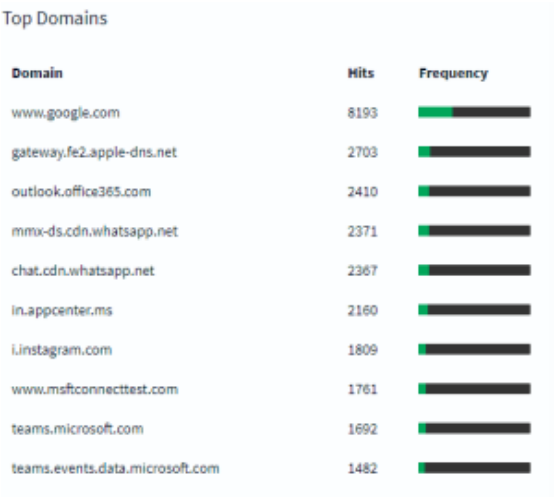
Action: ações possíveis.

- 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



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

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)

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.

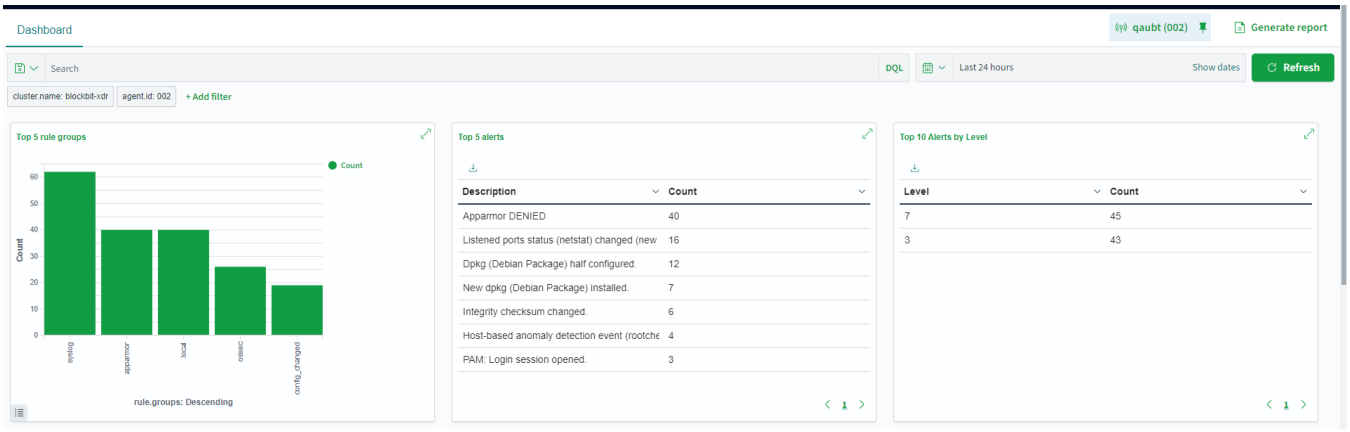
O Blockbit XDR oferece fluxos de trabalho completos para pesquisa e investigação de ameaças, unindo automação, inteligência artificial e análise manual. Por meio de uma linha do tempo interativa, é possível conduzir análises forenses aprofundadas, visualizando toda a sequência de eventos e processos 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.

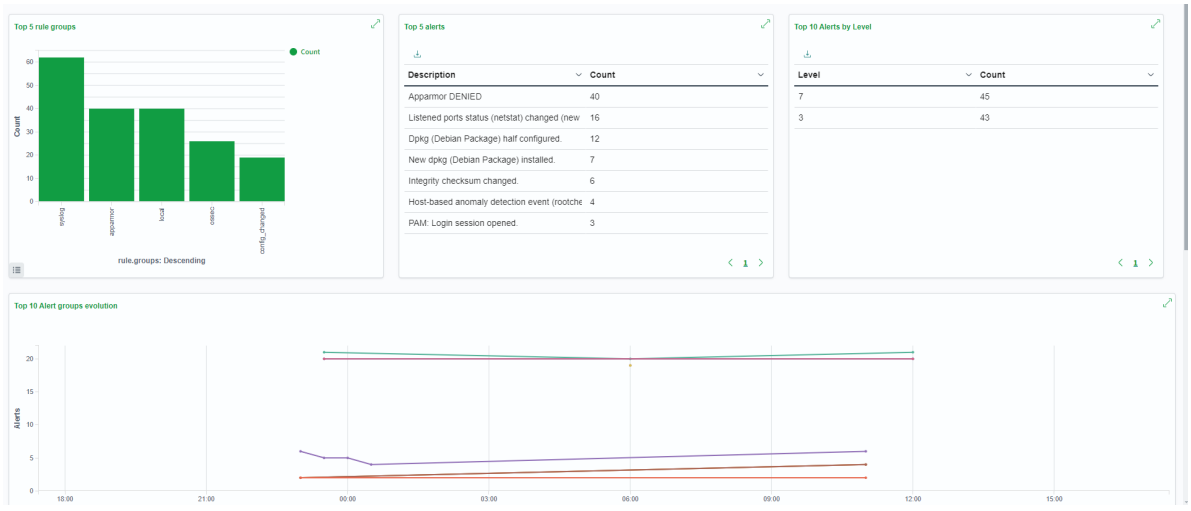


Search

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:

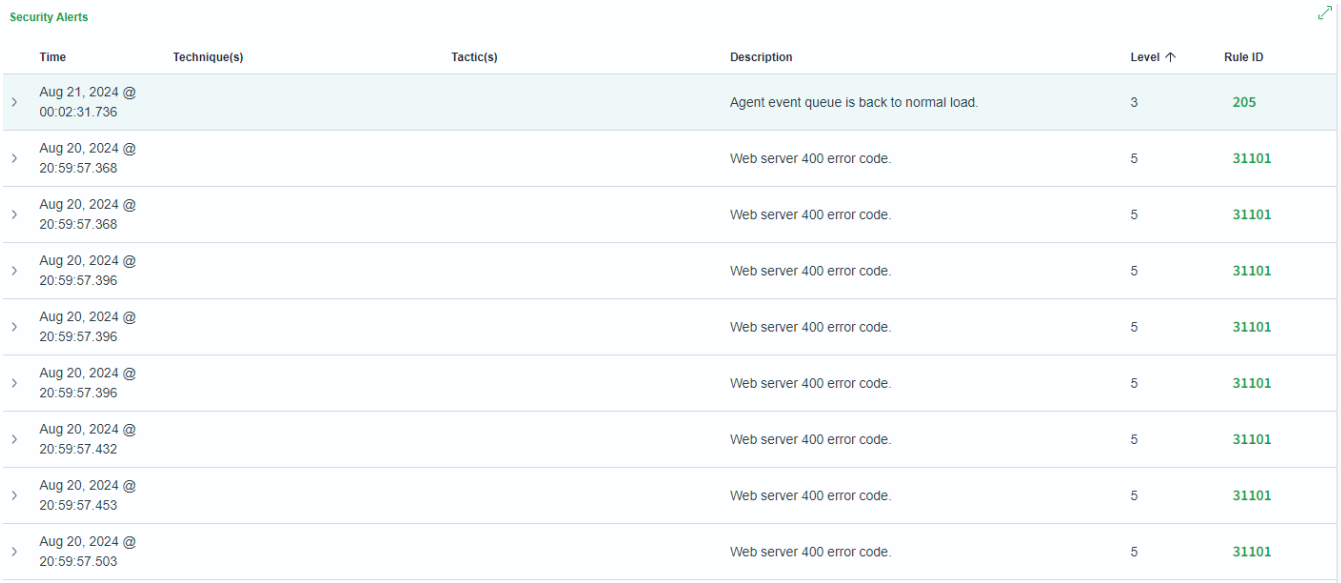
Top 5 rule groups: grupos de regras que mais geraram alertas;

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.



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: operação que gerou a notificação;

Message: mensagem da notificação;

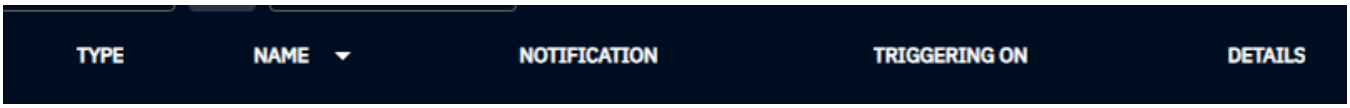
Original creation date: data da notificação;

Trigger: gatilho responsável pela notificação.

Triggers (): gatilhos.

Aqui você pode conferir os gatilhos que geram notificações.

São classificados por:



Type: tipo do gatilho;

Name: nome do gatilho:

Notification: notificação gerada pelo gatilho;

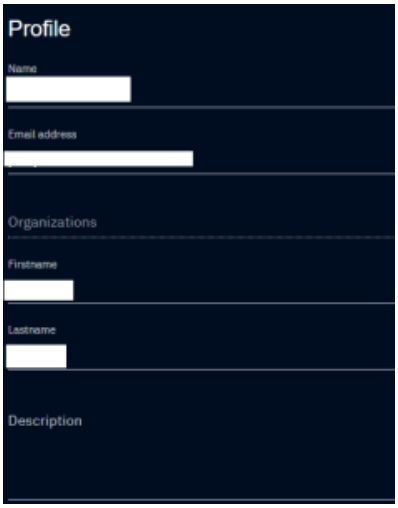
Triggering on: o que gerou o gatilho;

Details: detalhes do gatilho.

Profiles (): perfis.

Aqui você pode administrar o usuário.

Profile



Aqui você pode mudar os dados do usuário como nome, email, organização e descrição.

User experience

Aqui você pode mudar;
Theme: tema do CTI (modo claro ou escuro);

Language: língua do CTI;

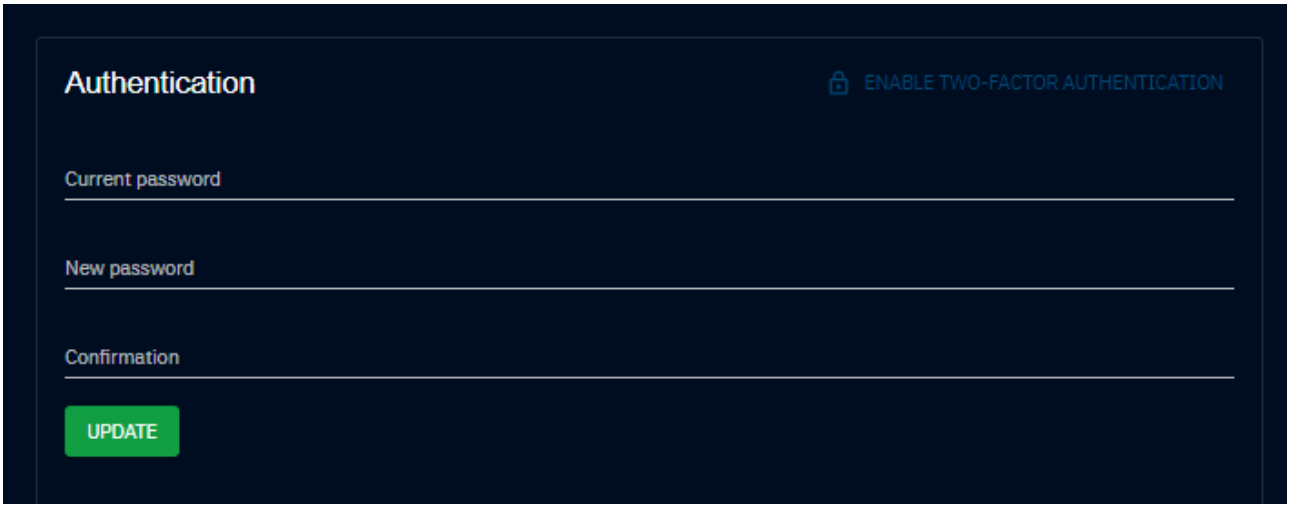
Unit system: sistema de medidas (métrico ou imperial).

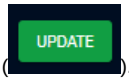
Show left navigation submenu icons: mostrar ícones do submenu à esquerda;

Auto collapse submenu in left navigations: minimizar automaticamente o submenu à esquerda.

Abaixo, há um espaço para tags sobre interesses de notificação.

Authentication

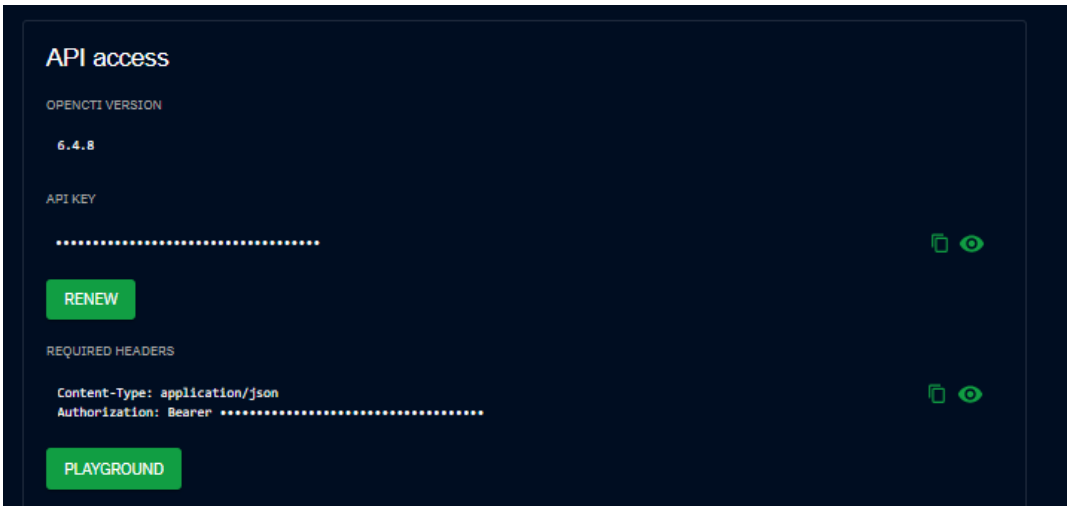


Aqui você pode mudar a sua senha. Insira a senha atual, a nova senha e repita a nova senha. Para mudar, clique em **Update** (

).

Para habilitar a autenticação em dois fatores, clique em **Enable two-factor authentication.**

API access



Aqui você pode administrar o acesso à API.

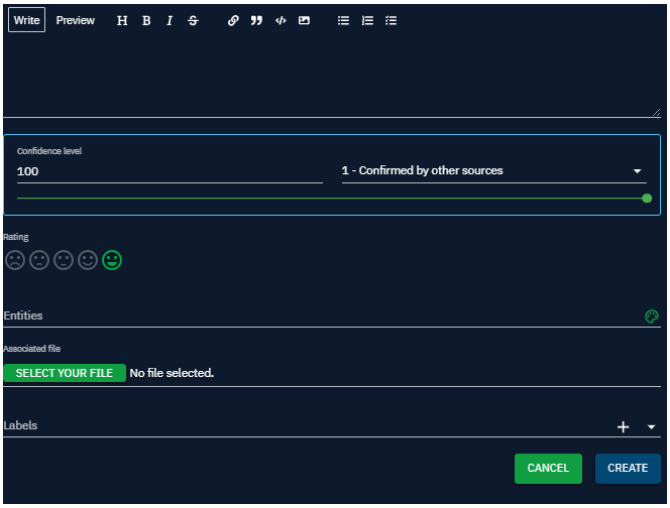
Para renovar a chave da API, clique em **Renew (** 

);

Para acessar o ambiente, clique em **Playground (** 

).

Feedback



Aqui você pode criar um feedback da plataforma.

Determine:

Description: descrição do feedback,

Confidence level: insira o nível de confidência 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;

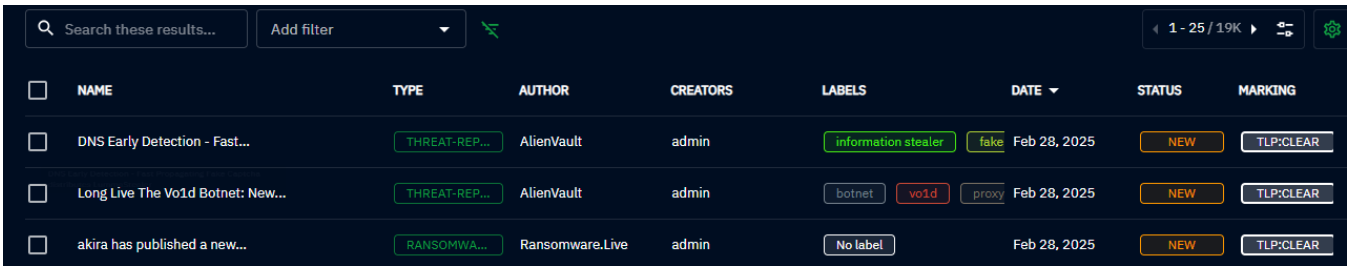
Enrichment ( ): buscar novos dados;

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.



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;

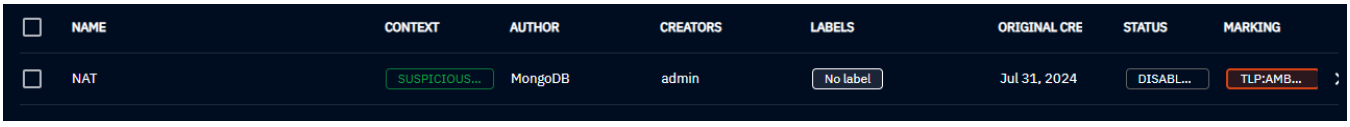
Date: data da ameaça;

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.



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;

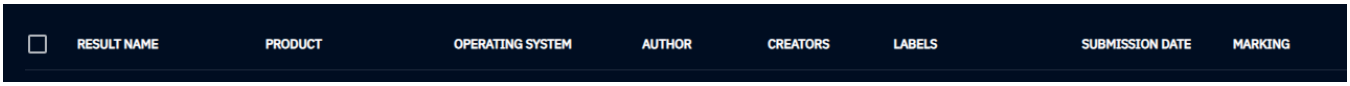
Original creation: criação da ameaça;

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.



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.

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;

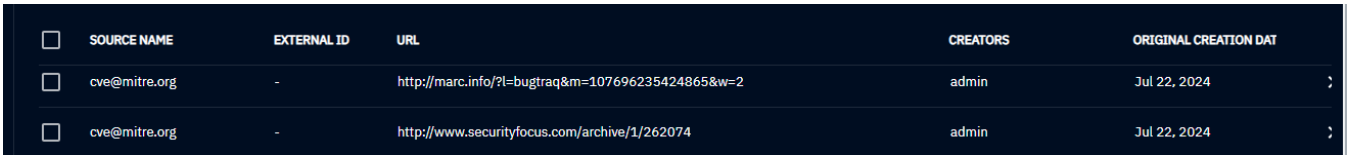
Original creation date: data de criação da nota;

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.



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 rescan ( ): escanear novamente a regra;

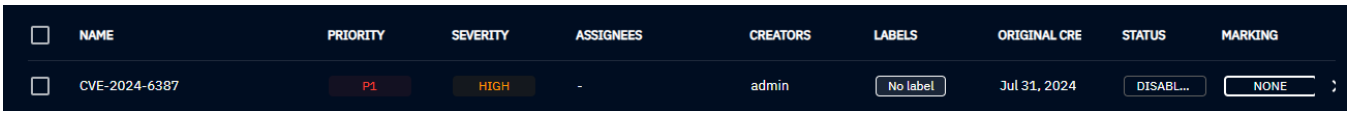
Enrichment ( ): buscar novos dados;

Merge ( ): fundir dados;

Add in container ( ): adicionar dados a um contêiner.

Incident Responses

Aqui estão agrupadas as respostas a incidentes.



Name: 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: 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: 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 distribuidas.

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.

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 (): atualizar;

Rule rescan (): escanear novamente a regra;

Enrichment (): buscar novos dados;

Merge (): fundir dados;

Add in container (): adicionar dados a um contêiner.

Observables

Aqui estão listados os objetos observáveis, ou elementos imutáveis.

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: 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: tipo de padrão de busca. Este padrão serve para identificar ameaçascpotenciais;

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: 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:

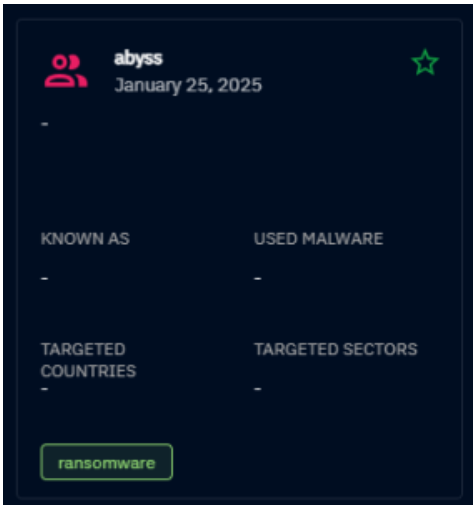
Threat actors (groups): grupos conhecidos por ataques.

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

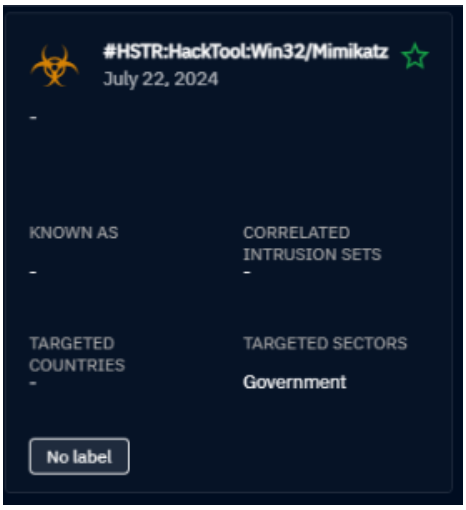
Esta aba é parte da biblioteca do CTI. Aqui estão listados os elementos para um ataque.

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.



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: 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: 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: 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;

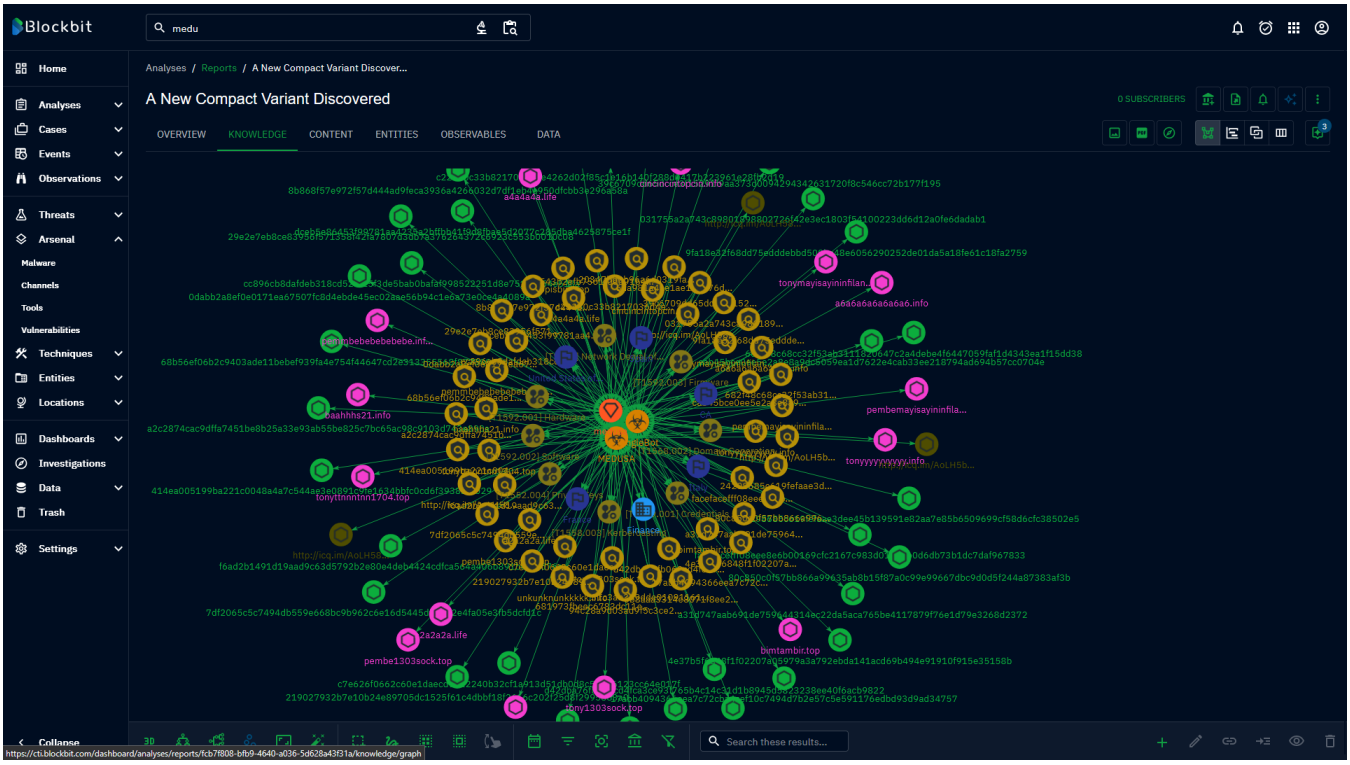
Creators: quem criou o verbete da vulnerabilidade.

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.


Blockbit
medu
Home
Analyses
Cases
Events
Observations
Threats
Arsenal
Malware
Channels
Tools
Vulnerabilities
Techniques
Entities
Locations
Dashboards
Investigations
Data
Trash
Settings
Collapse
Analyses / Reports / A New Compact Variant Discover...
A New Compact Variant Discovered
0 SUBSCRIBERS
OVERVIEW
KNOWLEDGE
CONTENT
ENTITIES
OBSERVABLES
DATA
Search these results...
https://cti.blockbit.com/dashboard/analyses/reports/fcb7f808-bfb9-4640-a036-5d628a43f31a/knowledge/graph

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: 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: 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;

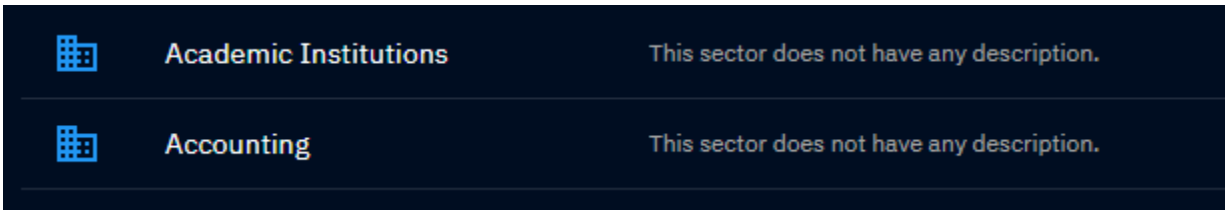
XDR - Threat Monitor - CTI - Entities

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.



São listados por **Tipo** e uma descrição.

Events

Aqui estão listados eventos no mundo real.

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: 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: 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: 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 localidadesdo mundo real.

Para buscar um resultado, utilize a barra de buscas. Você pode filtrar as buscas em **Add filter.**

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;

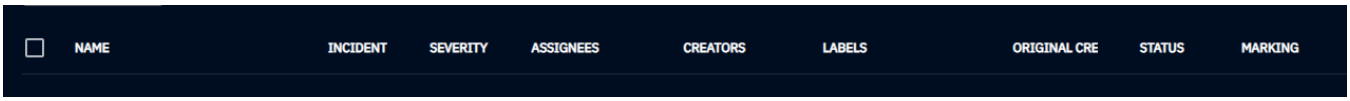
Enrichment ( ): buscar novos dados;

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: 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;

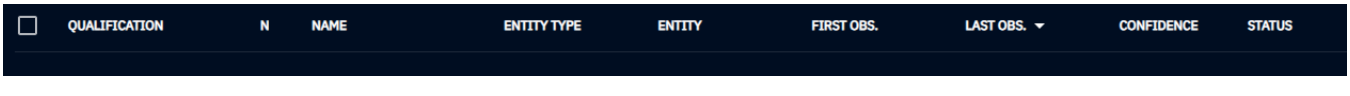
Original creation date: data da criação do incidente;

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: 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: 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: tipo da entidade;

Name: nome de entidade;

Author: autor da entidade;

Creators: criador da entidade;

Labels: etiquetas recebidas pela etndiade. 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.

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;

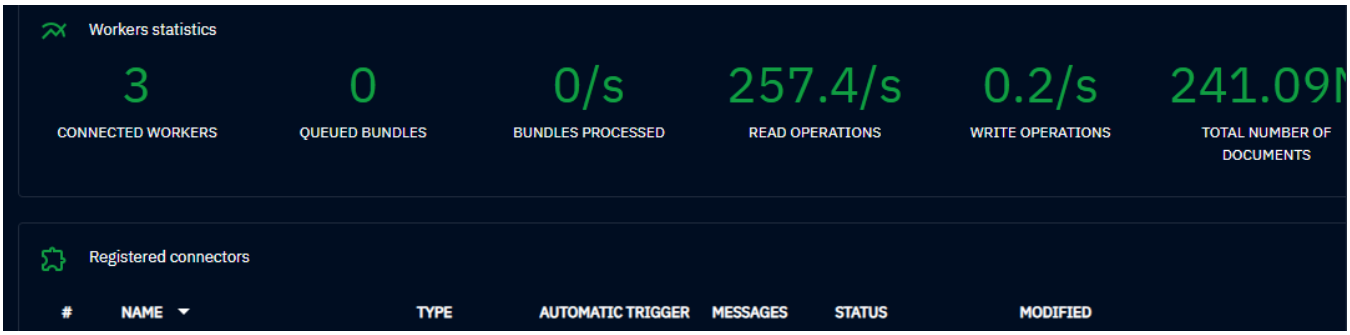
Creators: criador da relação;

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: 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);*

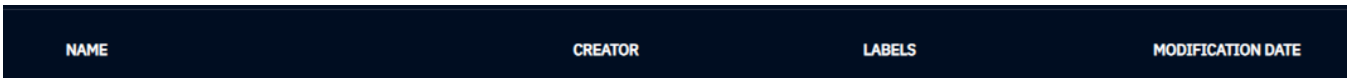
CSV feeds: *feeds criados usando o formato CSV (comma-separated value).*

Import

Aqui, você pode importar arquivos.

Para importar um arquivo, clique na nuvem ()

Para copiar e colar os conteúdos do arquivo, clique neste ícone:  .



Os arquivos são classificados em:

Name: nome do objeto;

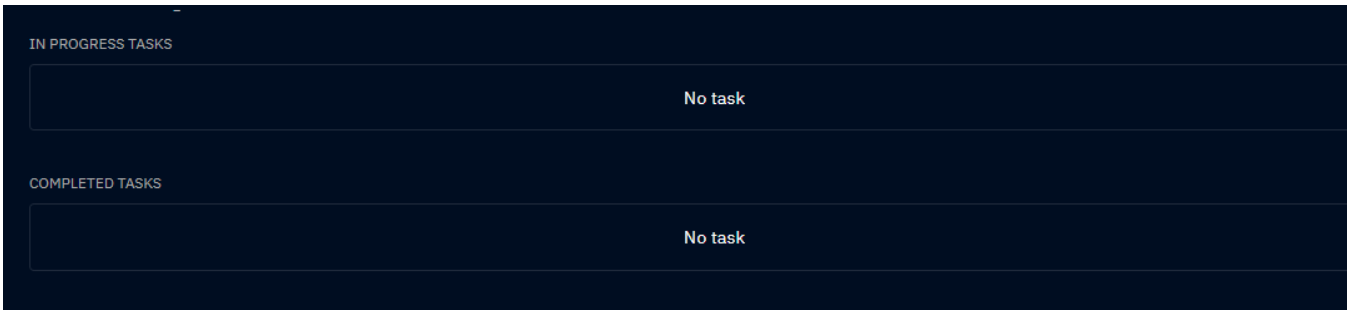
Creators: criador do objeto;

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.



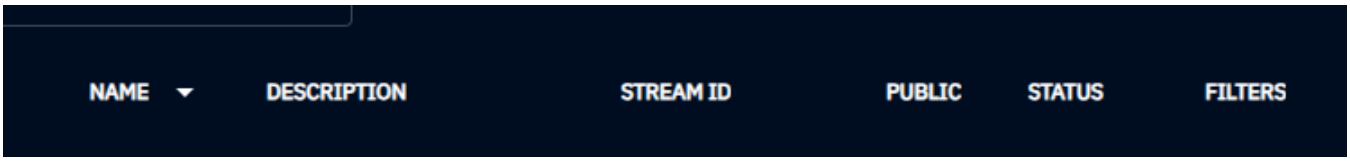
In progress tasks: tarefas em andamento;

Completed tasks: tarefas completas.

Data sharing

Aqui estão listados os streams e feeds RSS e TAXII.

RSS



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: 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: 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.

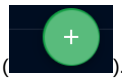
Type: tipo da etiqueta;

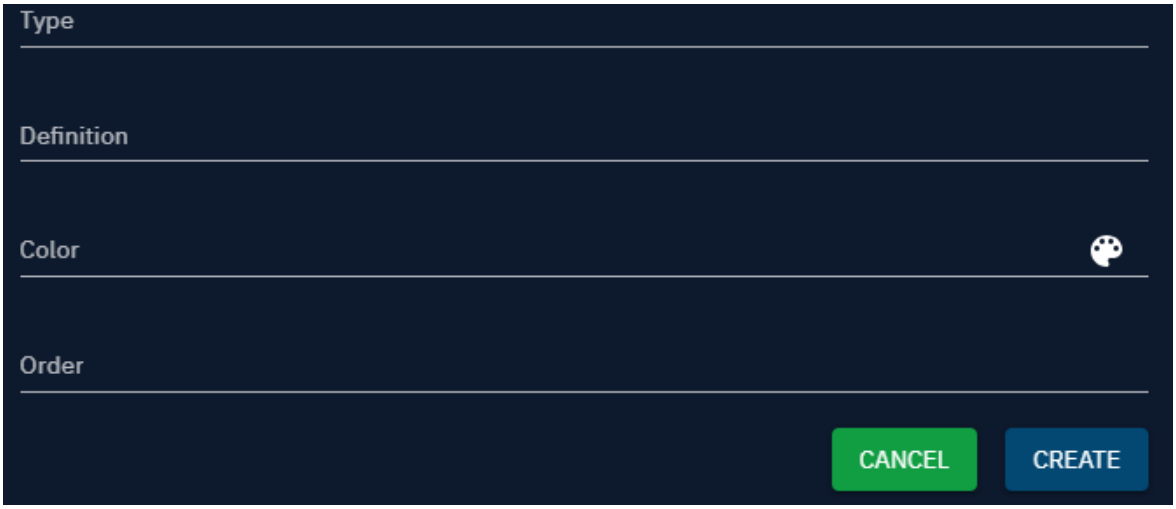
Definition: definição da etiqueta;

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 ().



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 (**  **).**

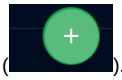
Taxonomies

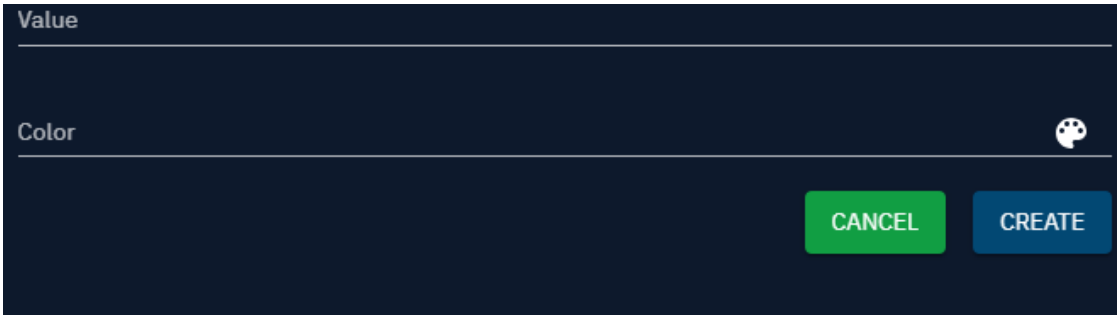
Aqui estão listadas as etiquetas de taxonomia.

Value: 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 ().



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

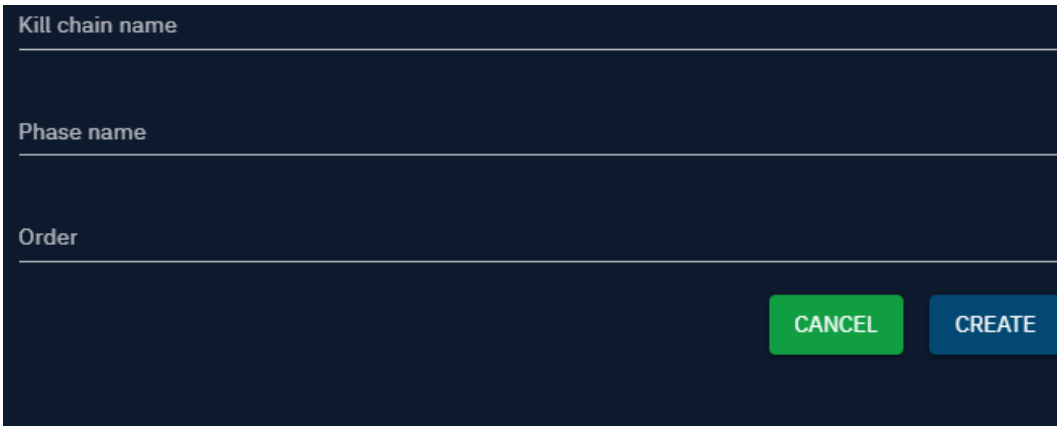
Kill chain name: nome da fase no MITRE ATT&CK;

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 ().



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: 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: 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.

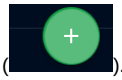
Status templates

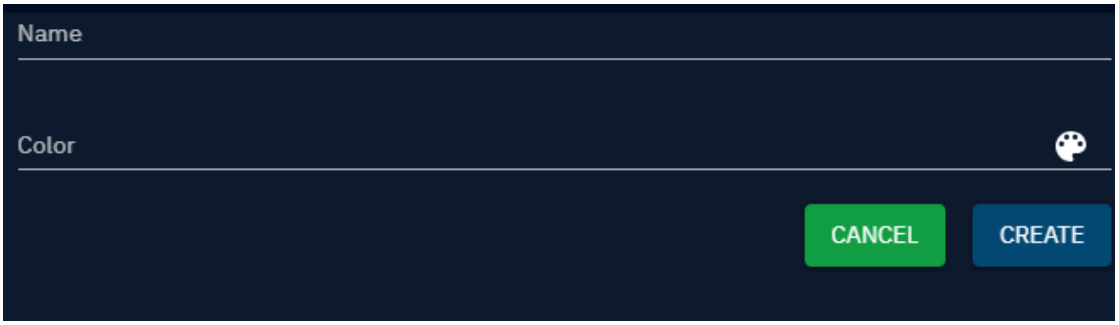
Aqui estão listadas etiquetas de status.

Name: 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 (
).



Determine:

Name: nome da etiqueta de status;

Color: cor da etiqueta de status;

Para criar, clique em **create (** 

).

Para cancelar, clique em **cancel (** 

).

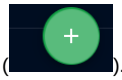
Case templates

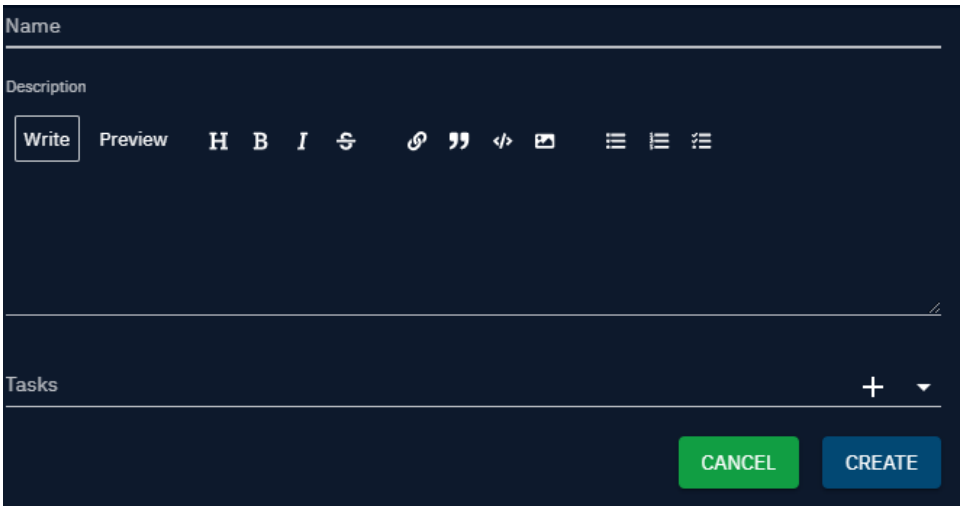
Aqui estão listadas etiquetas de casos.

Name: 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 ().



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: nome do usuário;

Email: e-mail do usuário;

First name: primeiro nome do usuário;

Last name: último sobrenome do usuário;

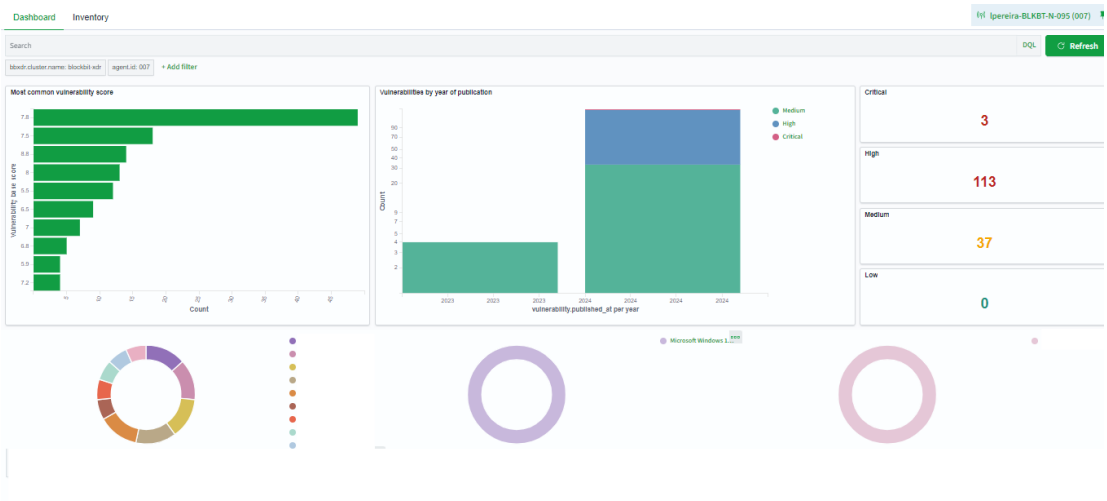
Max confidence: confiança máxima do usuário;

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.

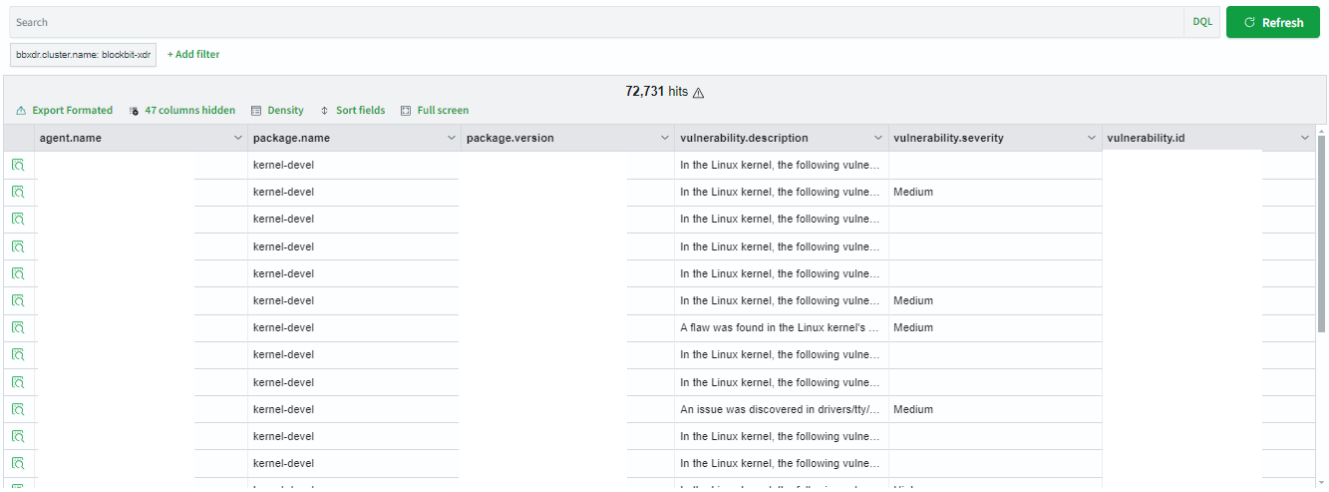
Most common vulnerability score: mostra a classificação de severidade mais comum das vulnerabilidades detectadas. Vai de 0 (baixa) a 10 (crítica);

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.



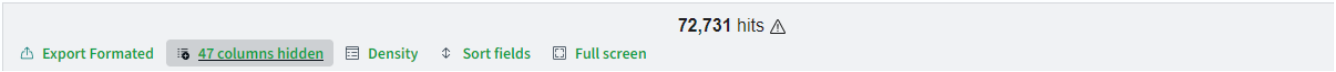
Search

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.



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.

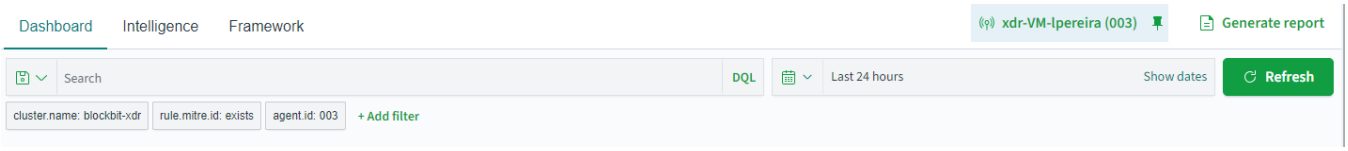
XDR - MITRE ATT&CK

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.

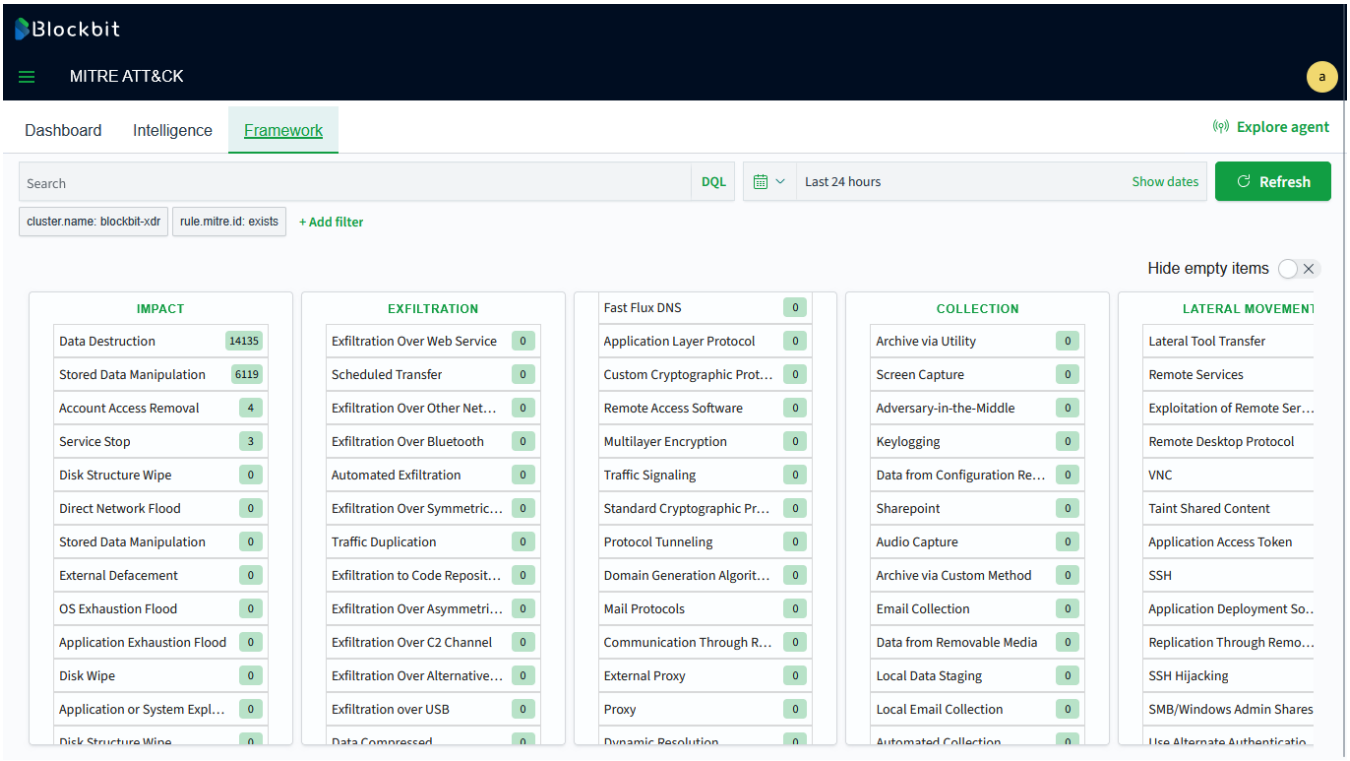
Em **Top tactics**, são elencadas as táticas que mais geraram alertas;

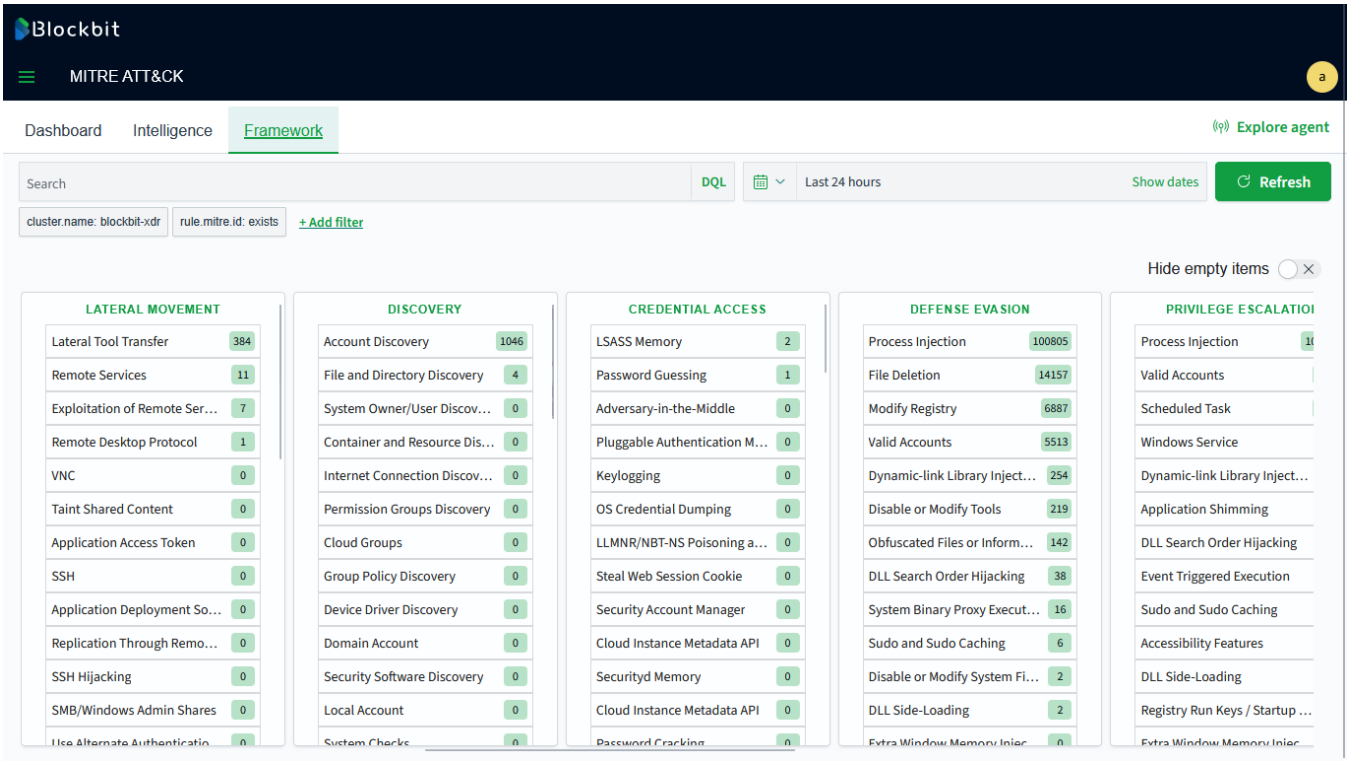
Em **Top techniques**, são elencadas as técnicas que mais geraram alertas;

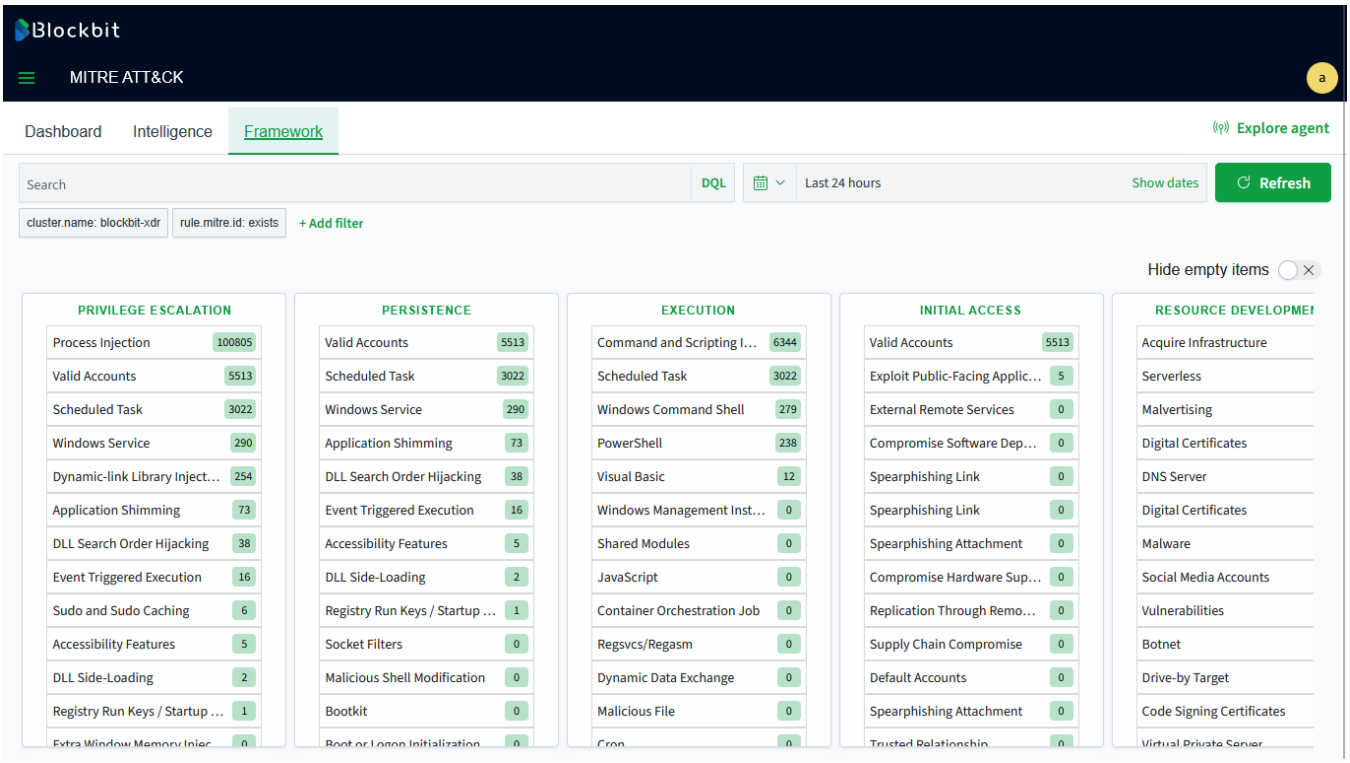
Em **Alerts evolution over time**, são mostrados alertas por tipo em intervalos de 30 minutos.

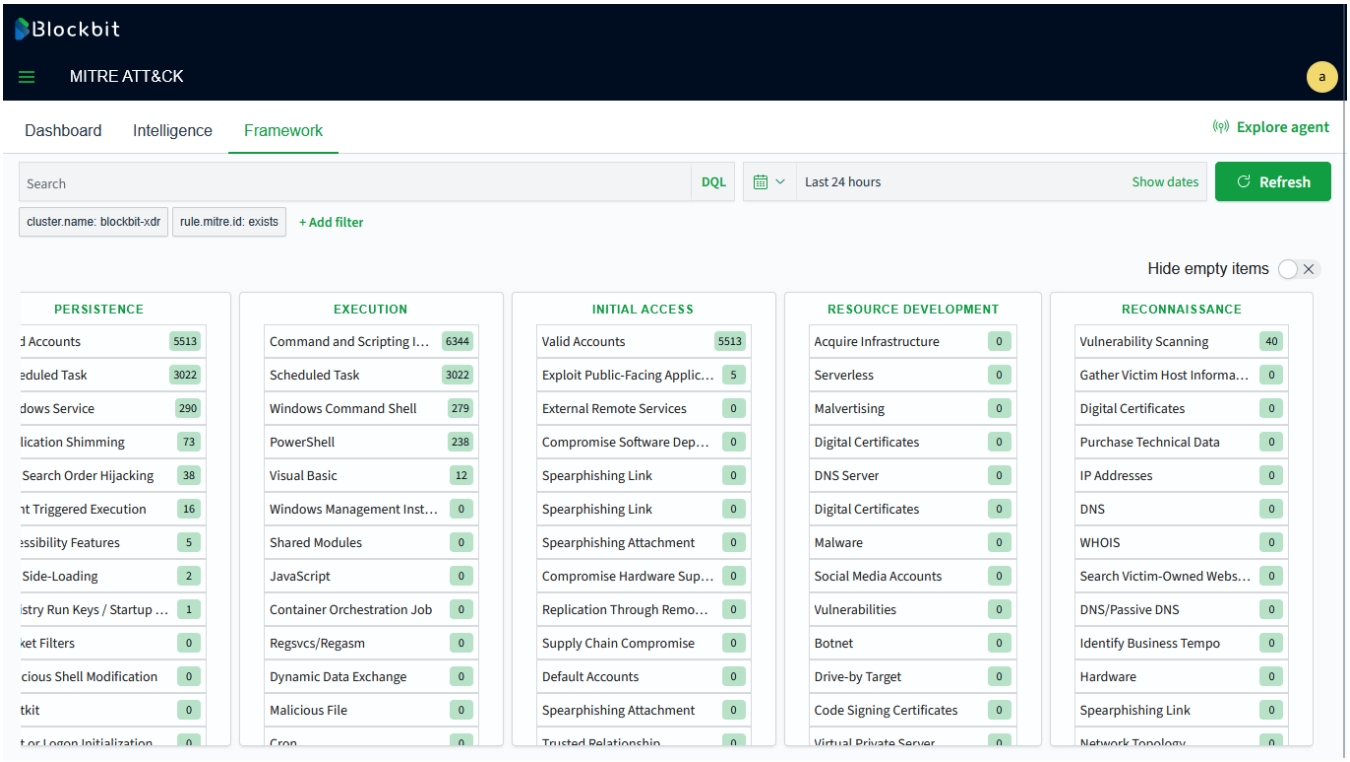
XDR - MITRE ATT&CK - Framework

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.









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

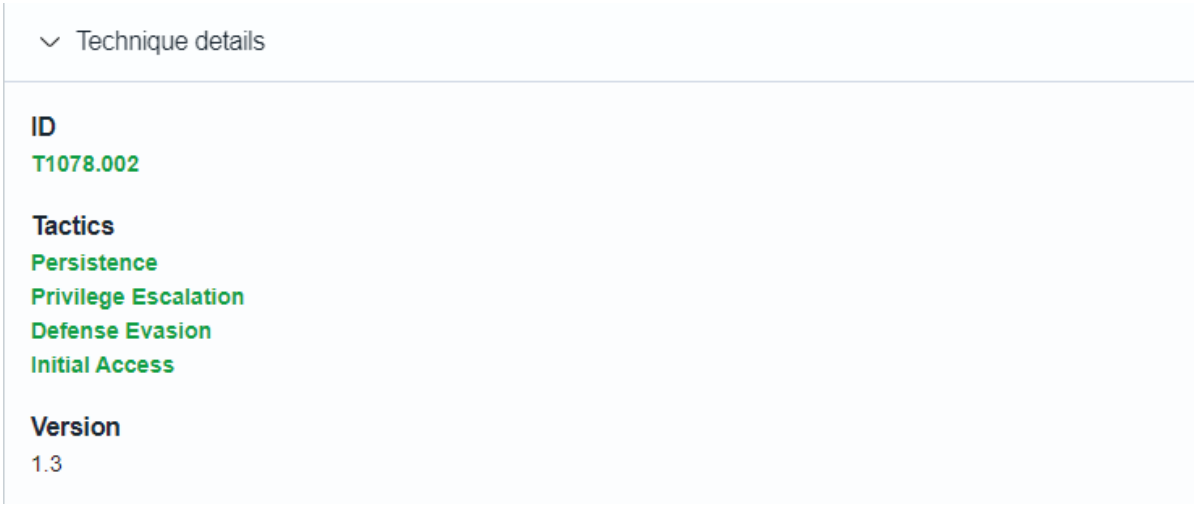
Nesta página, os alertas são classificados automaticamente por táticas e técnicas, permitindo que os analistas compreendam o padrão e o comportamento da ameaça. Cada técnica agrupa as táticas relacionadas, proporcionando uma visão estruturada da evolução do ataque.

- 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.

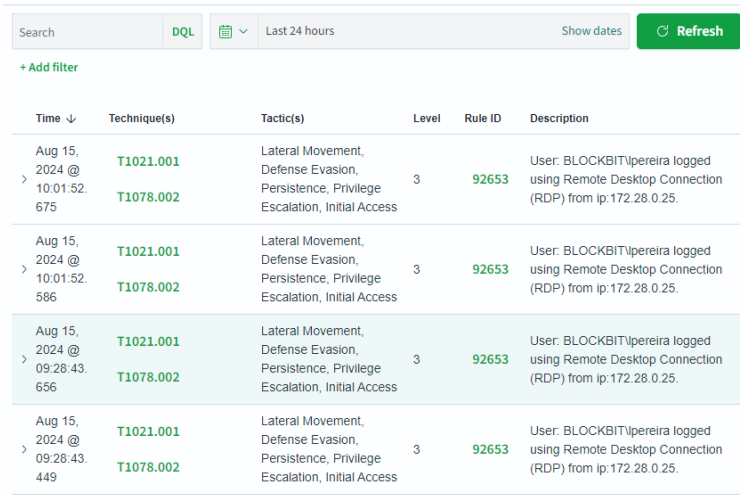
Show in dashboard ( ): irá criar um dashboard específico para esta técnica.

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.



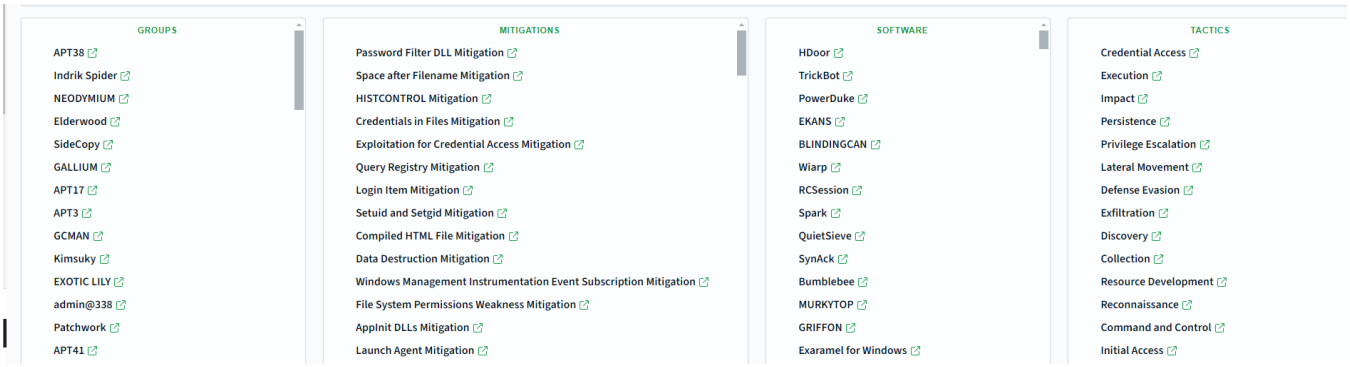
No topo, há o ID da técnica e as táticas a ela associada.



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.



As informações são divididas por assuntos:

Groups: grupos que empreendem ataques maliciosos;

Mitigations: técnicas de mitigação de ataques;

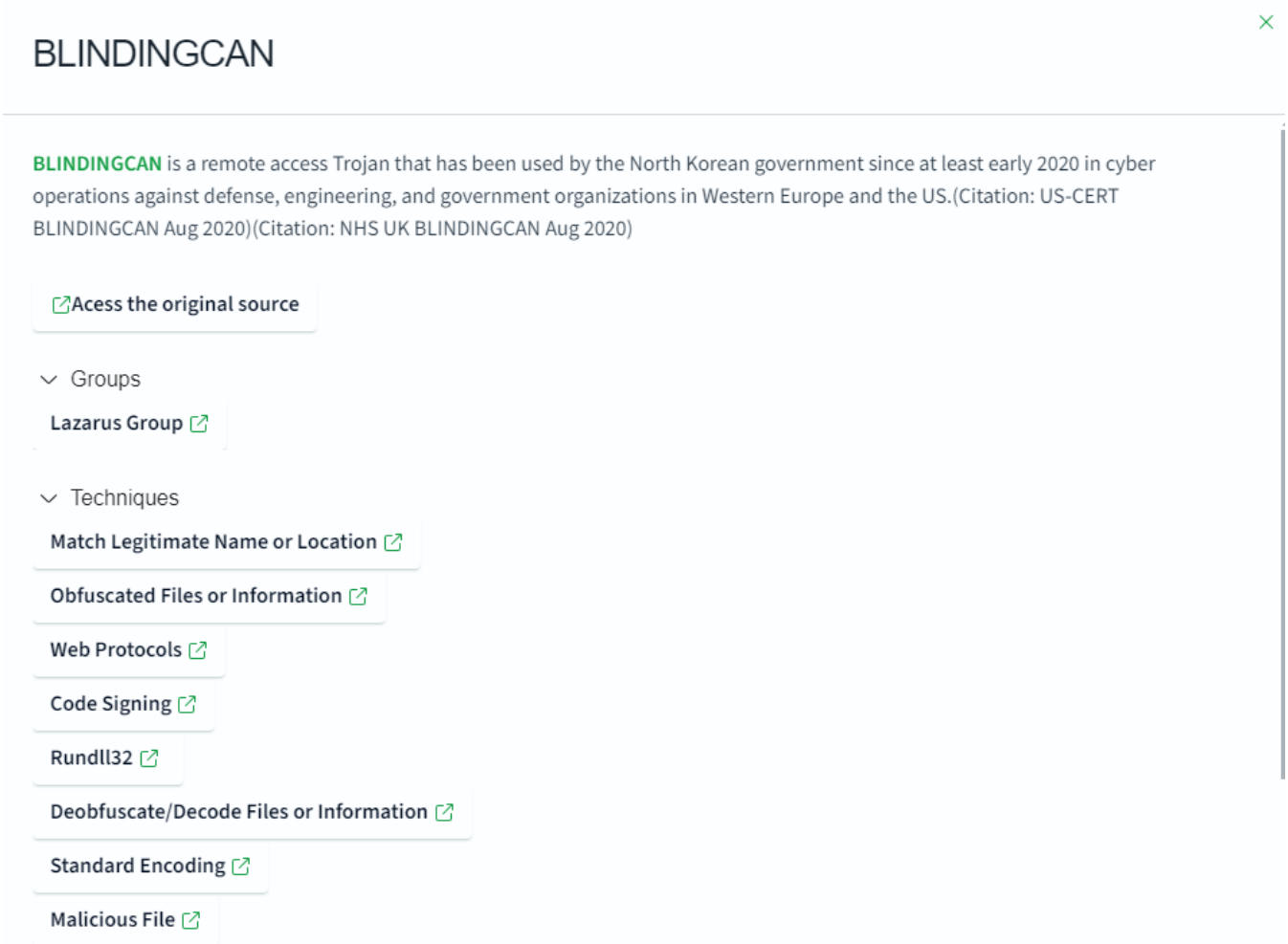
Software: softwares utilizados em ataques maliciosos;

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")



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.

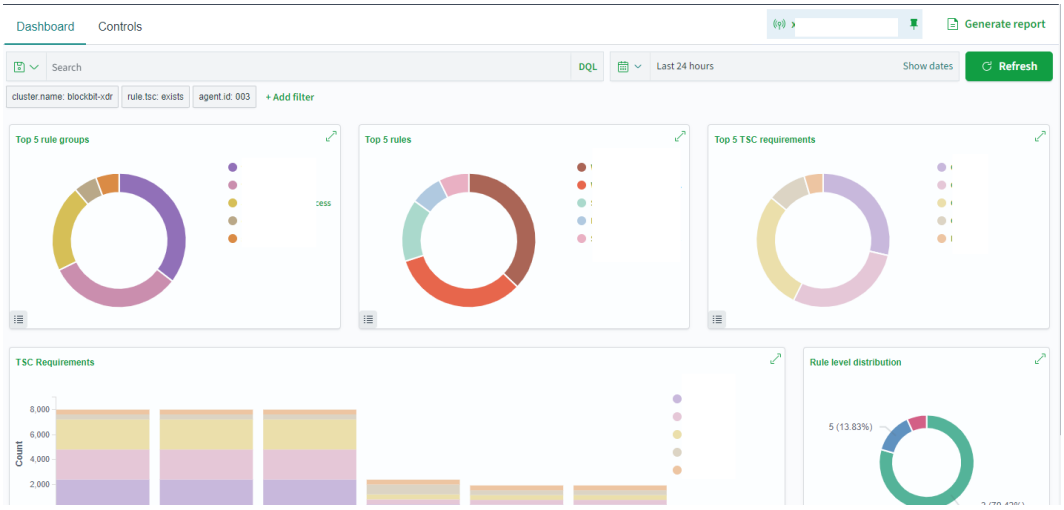
PCI DSS (**Payment Card Industry Data Security Standard):** Padrão de segurança de dados do setor de cartões de pagamento.

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

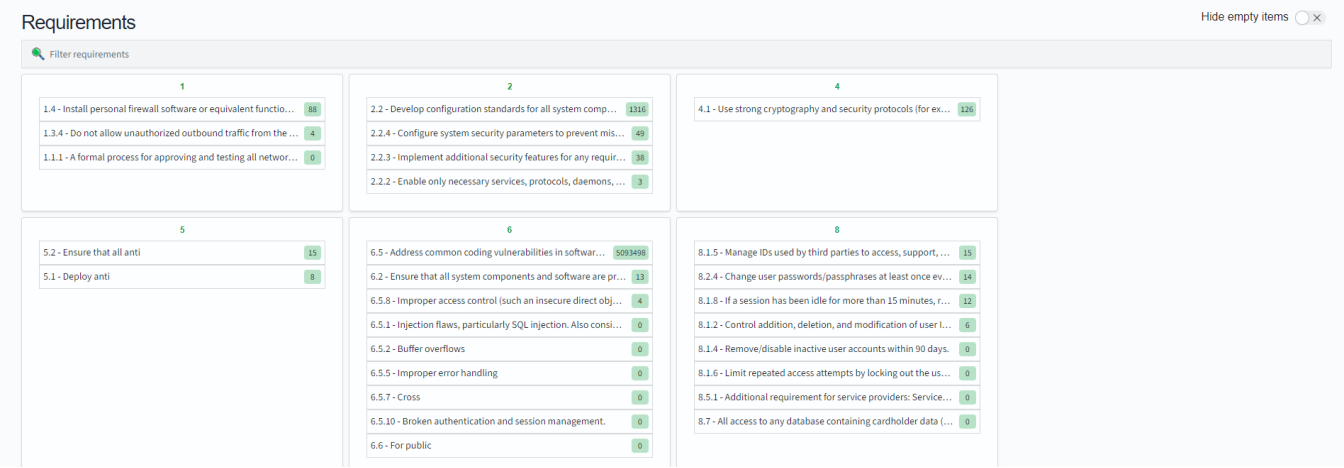
NIST 800-53

PCI DDS

TSC

Controls

Nesta página, você pode conferir os alertas separados por requerimento.

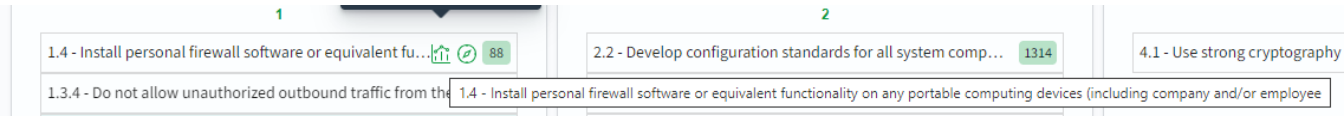


Para mostrar apenas requerimentos com alertas, clique em **Hide requirements with no alerts**.

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.

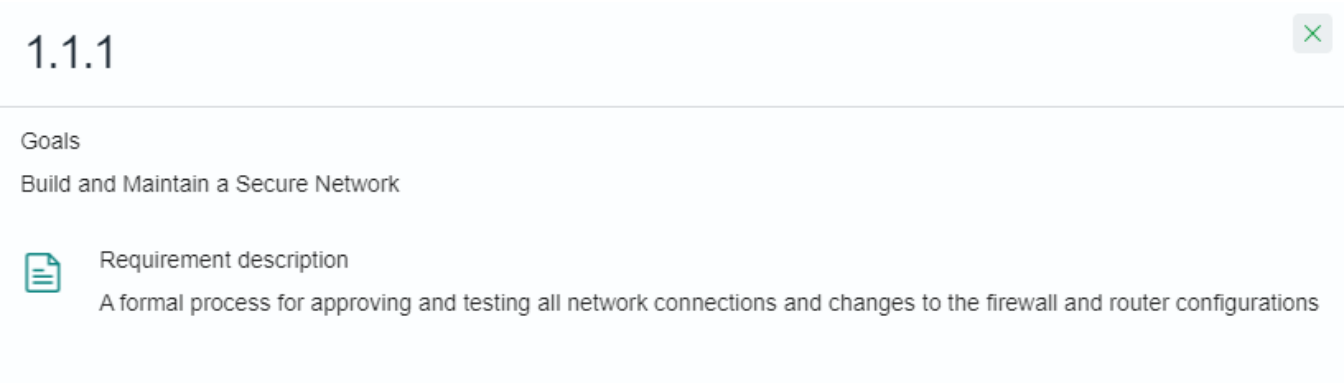
Ao passar o mouse sobre um requerimento, aparecerá uma breve descrição dele e dois botões:



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.

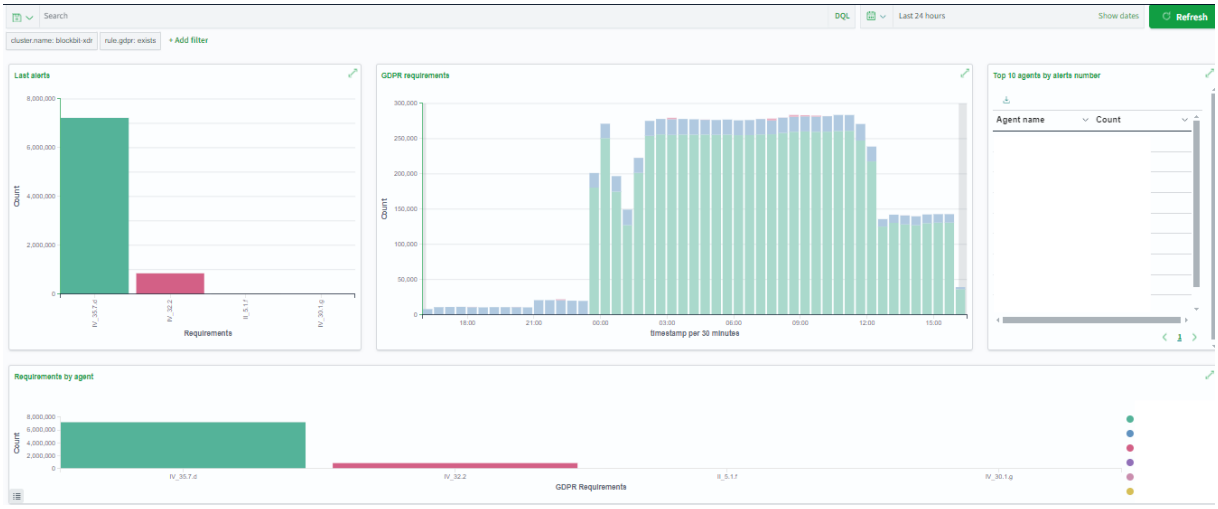


XDR - Security Operations - GDPR

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;

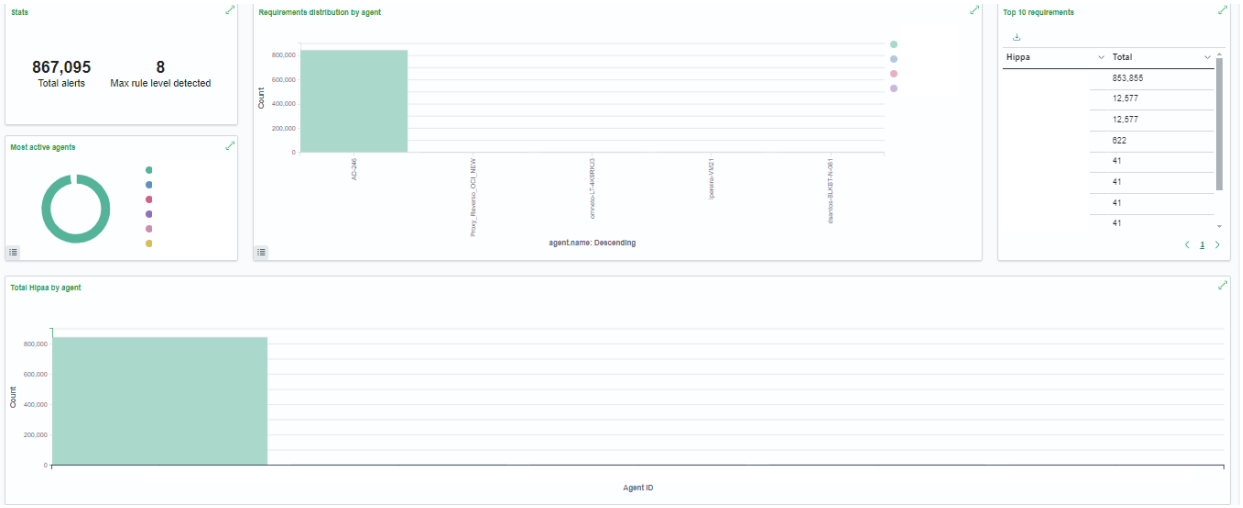
Top 10 agents by alerts number: agentes com mais alertas vintulados;

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.

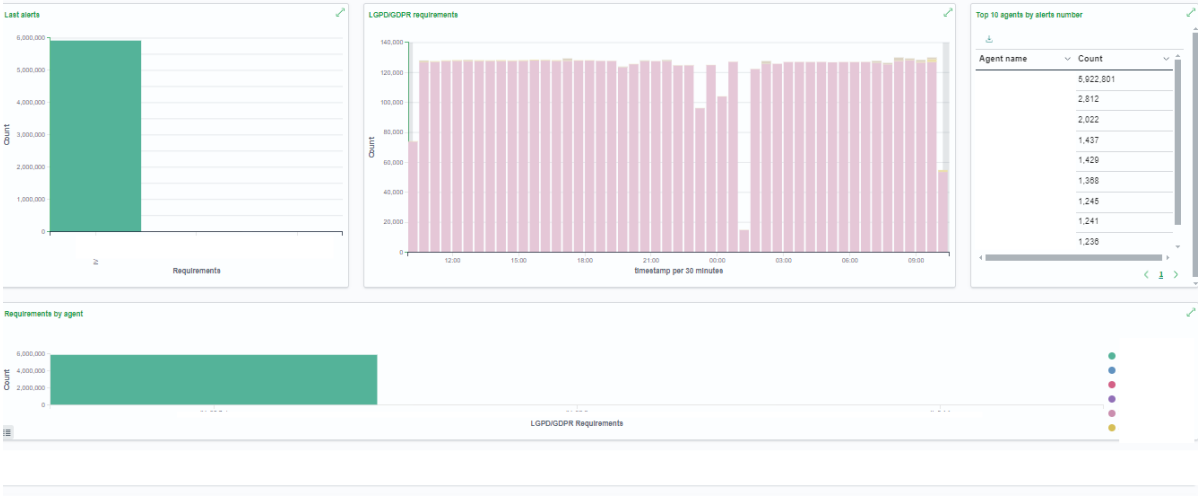
Requirements distribution by agent: violações distribuídas por agentes;

Top 10 requirements: requerimentos com mais violações;

Total HIPAA by Agent: violações por agente ao longo do tempo.

XDR - Security Operations - LGPD

A LGDP (**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;

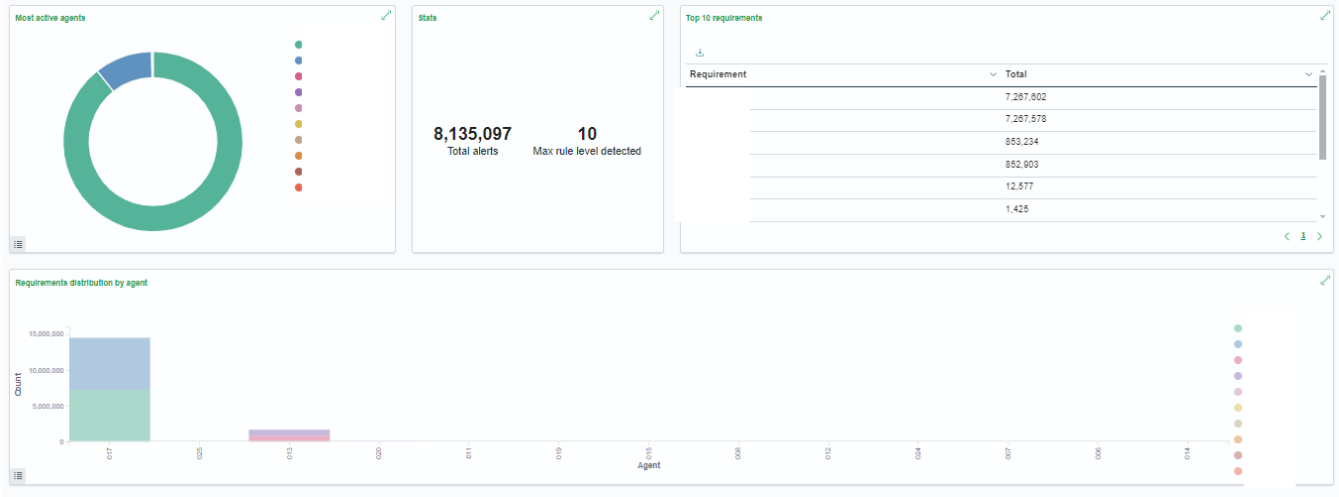
Top 10 agents by alerts number: agentes com mais alertas vintulados;

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.

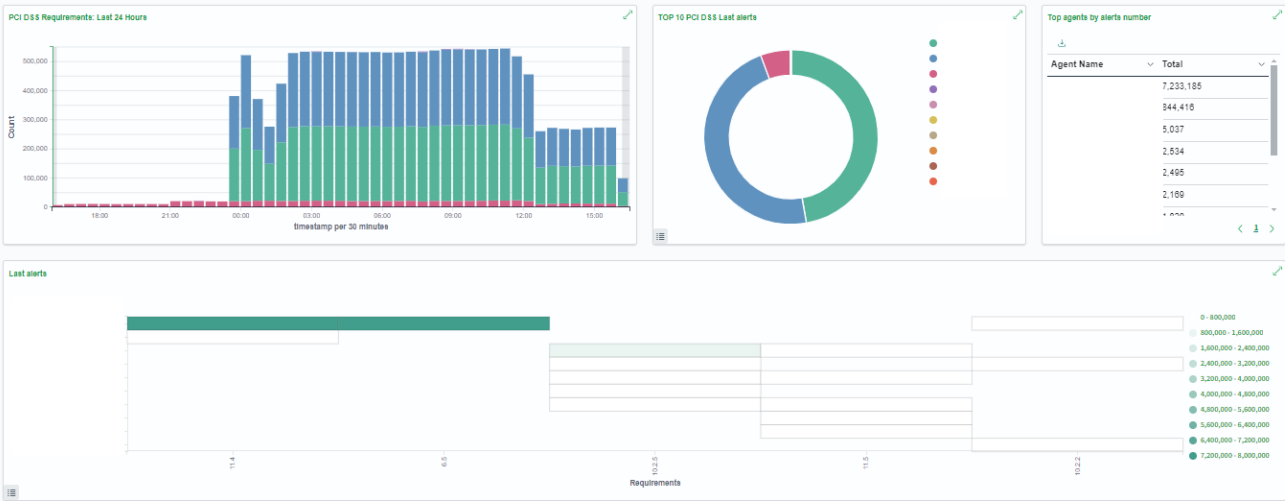
Top 10 requirements: requerimentos com mais violações;

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

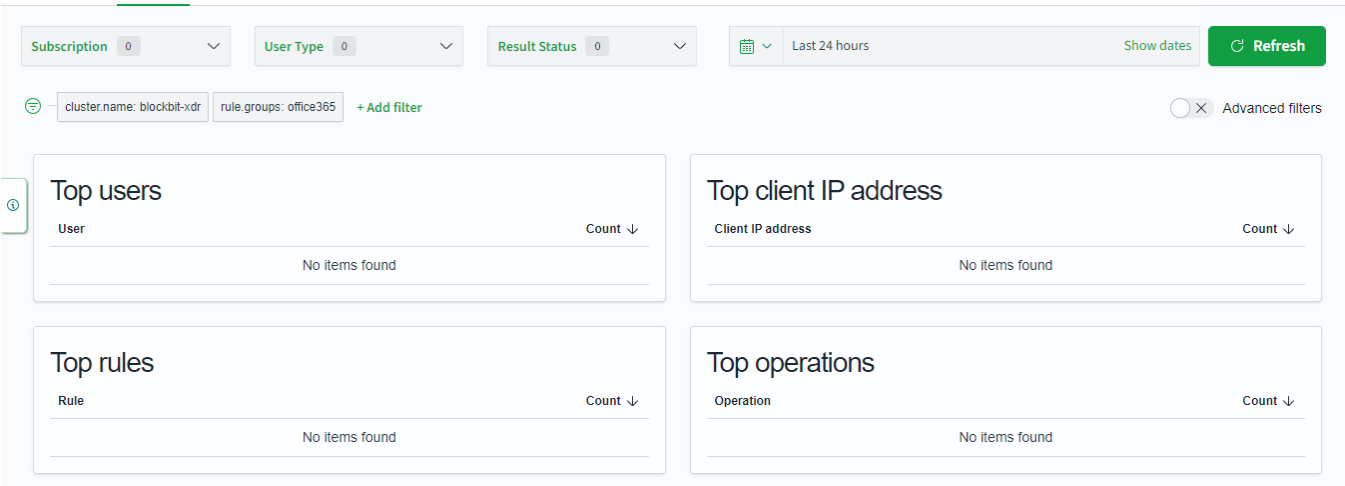
Os agentes utilizam o **AWS Instance Metadata Service (IMDS)** para coletar informações como **ID da instância, tipo de máquina, região, VPC e tags associadas**. Com esses dados/metadados, a solução ajusta automaticamente as políticas de segurança conforme o perfil da instância na nuvem AWS.

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.



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

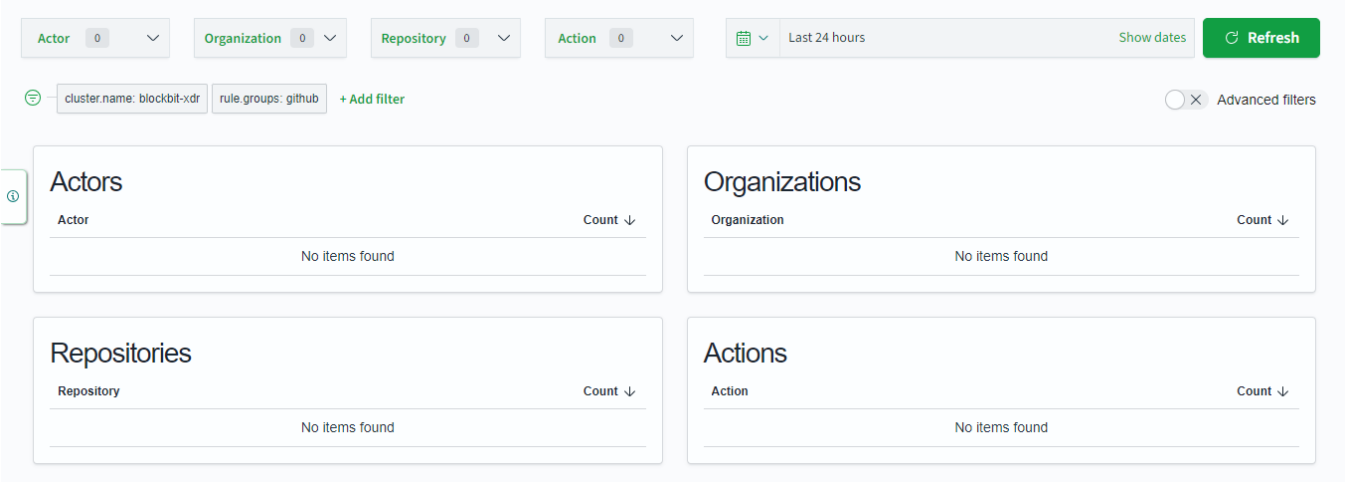
Para ambientes baseados em **Docker e Kubernetes**, os agentes do **Blockbit XDR** acessam **variáveis de ambiente e configurações da infraestrutura de orquestração**, como **ID do contêiner, namespace, labels, volume mounts e configurações de rede**. Isso permite que a segurança seja aplicada com base 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.



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:

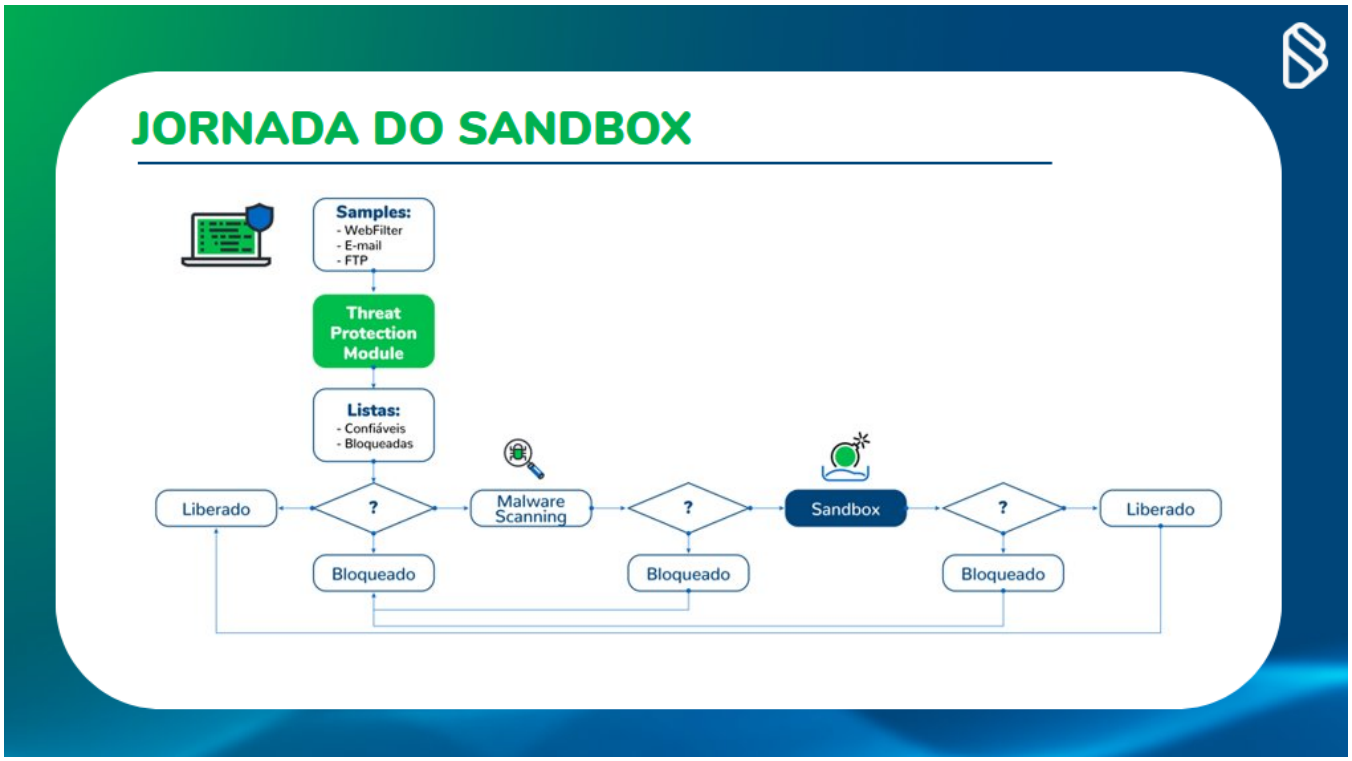
Zero-day Identification: É a possibilidade de identificar ameaças sem assinatura baseado em seu comportamento e pontuação no sistema de *Machine Learning*.

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.

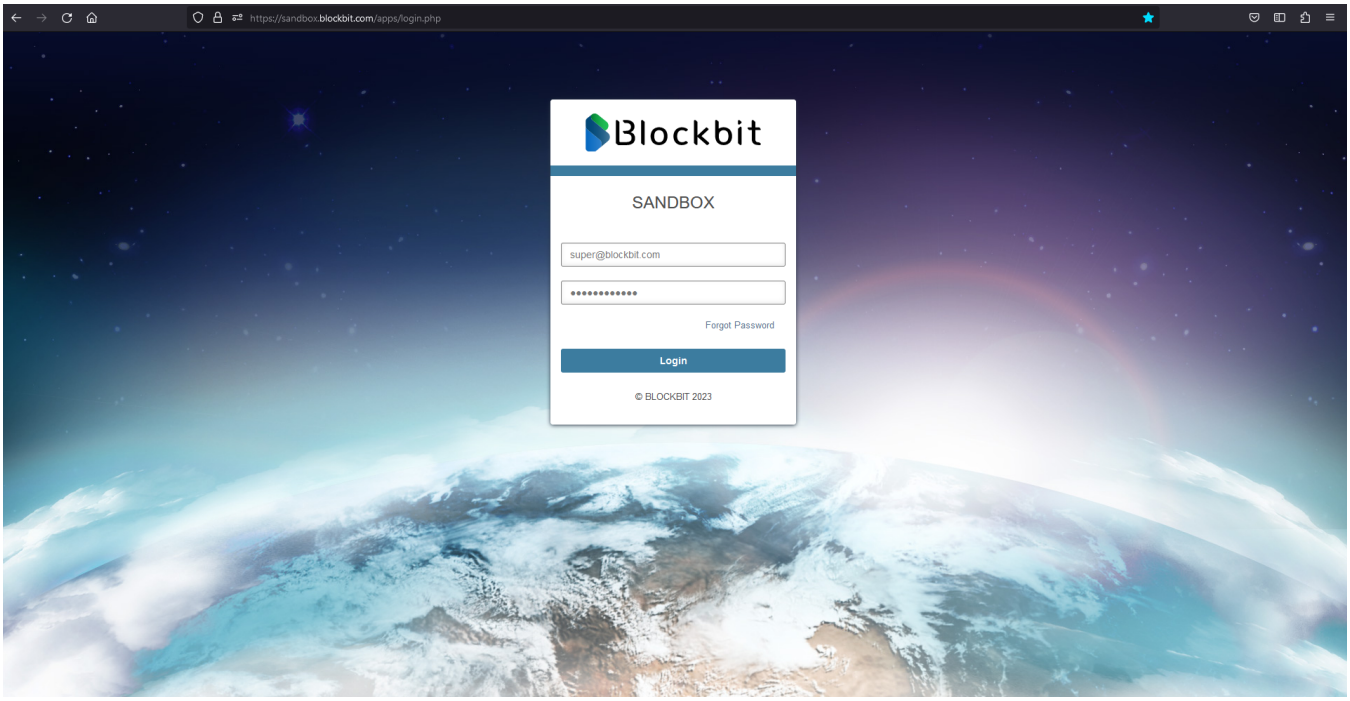
Abaixo, podemos ver o fluxo de processos do Sandbox:



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 detalhe 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.

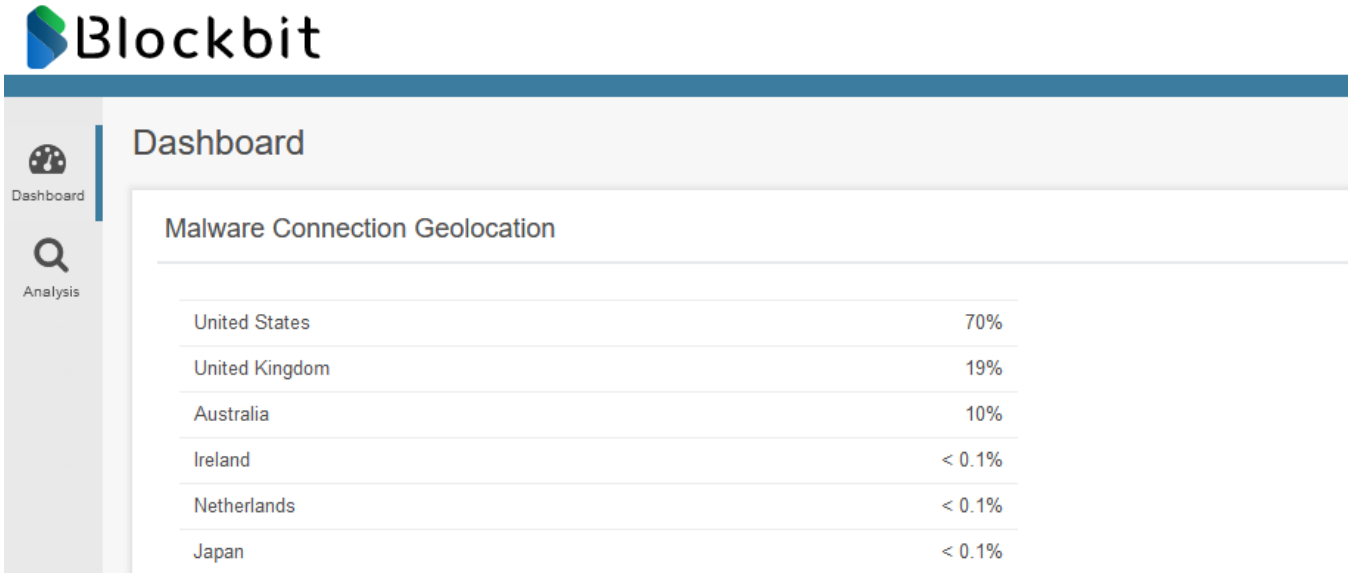
Caso a senha seja perdida, é possível ser recuperada clicando em "Forgot Password" e seguindo os passo subsequentes para registrar uma nova senha.

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.



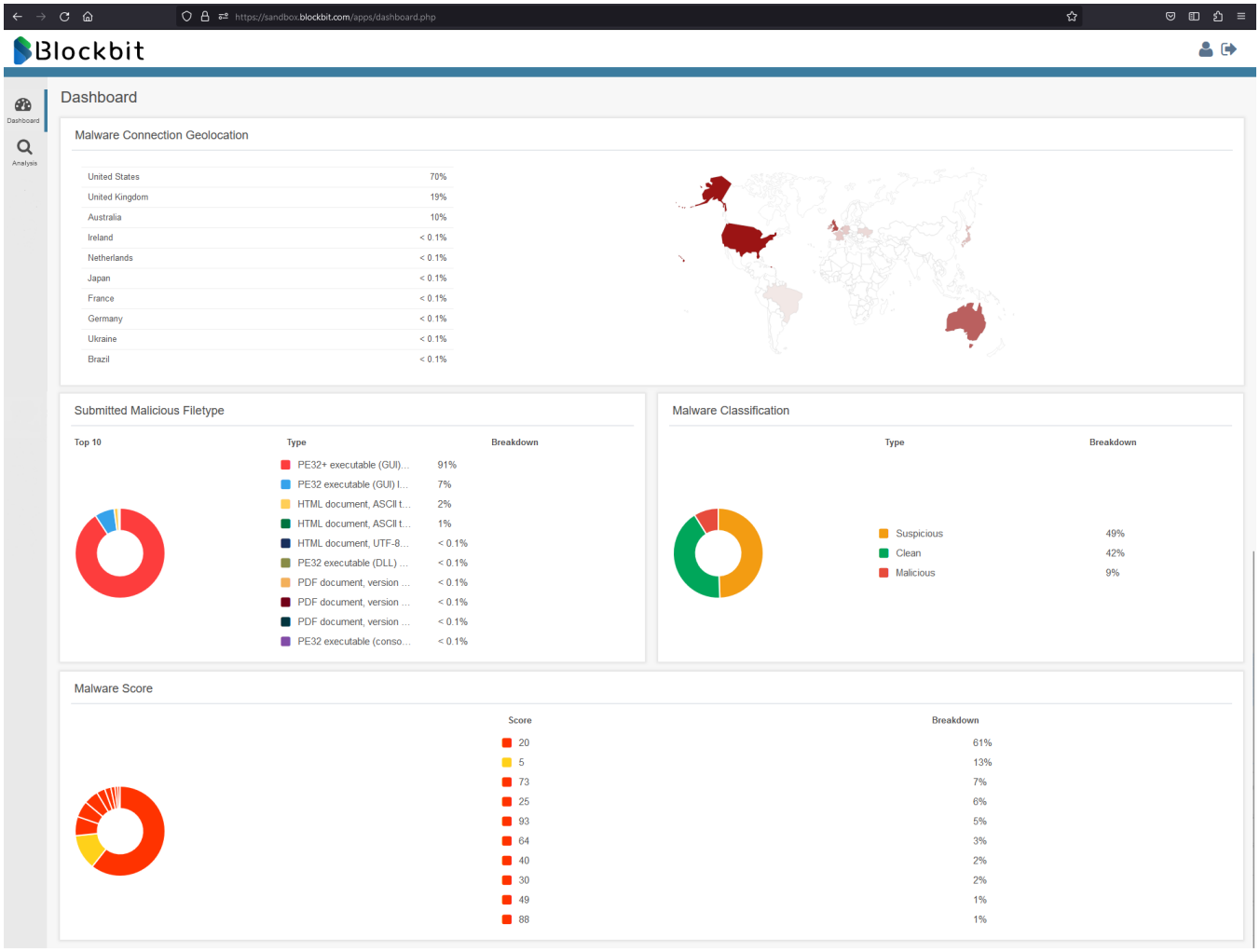
Sandbox - Dashboard e Analysis

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.

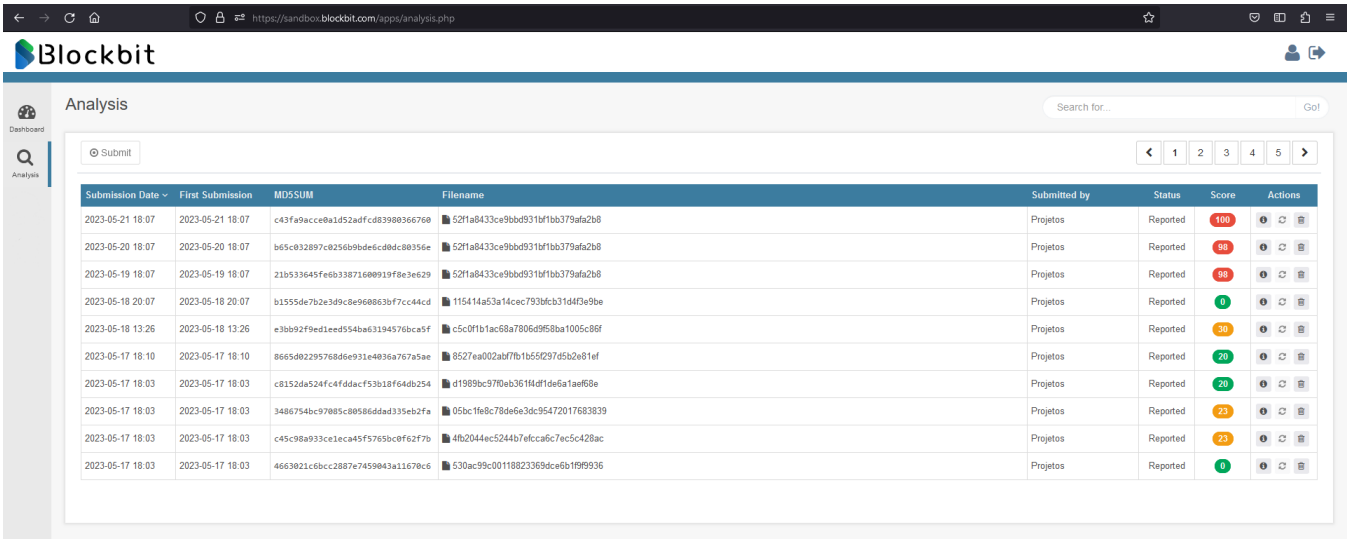
Submitted Malicious Filetype: Em um top 10, mostra os tipos mais comuns de arquivos maliciosos, submetidos para análise.

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:

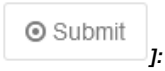


Analysis

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:

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:

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.

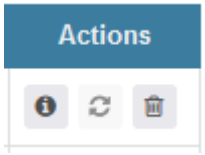
Filename: Nome original do arquivo.

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.

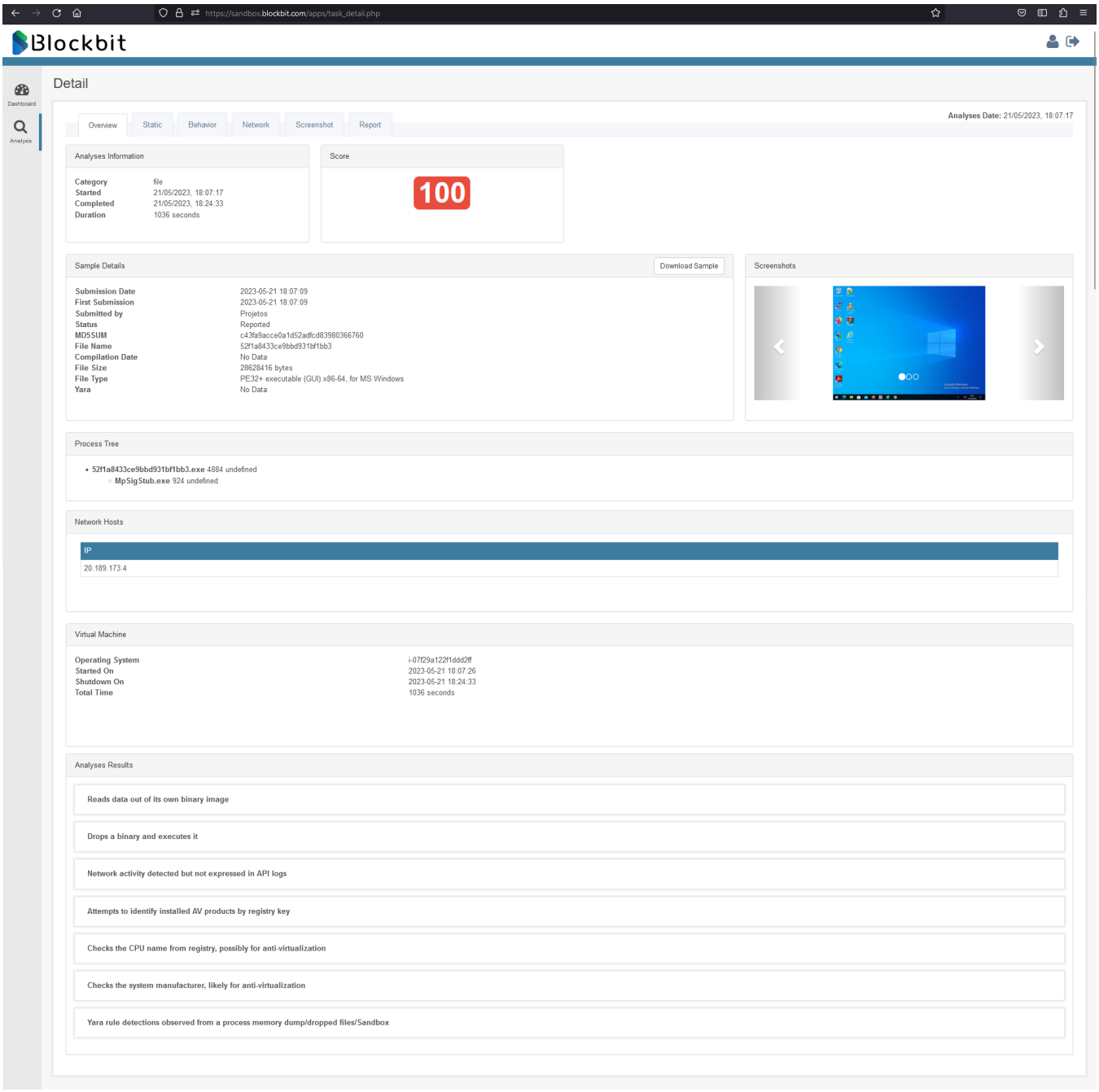
Apagar: Apaga a assinatura selecionada.

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.

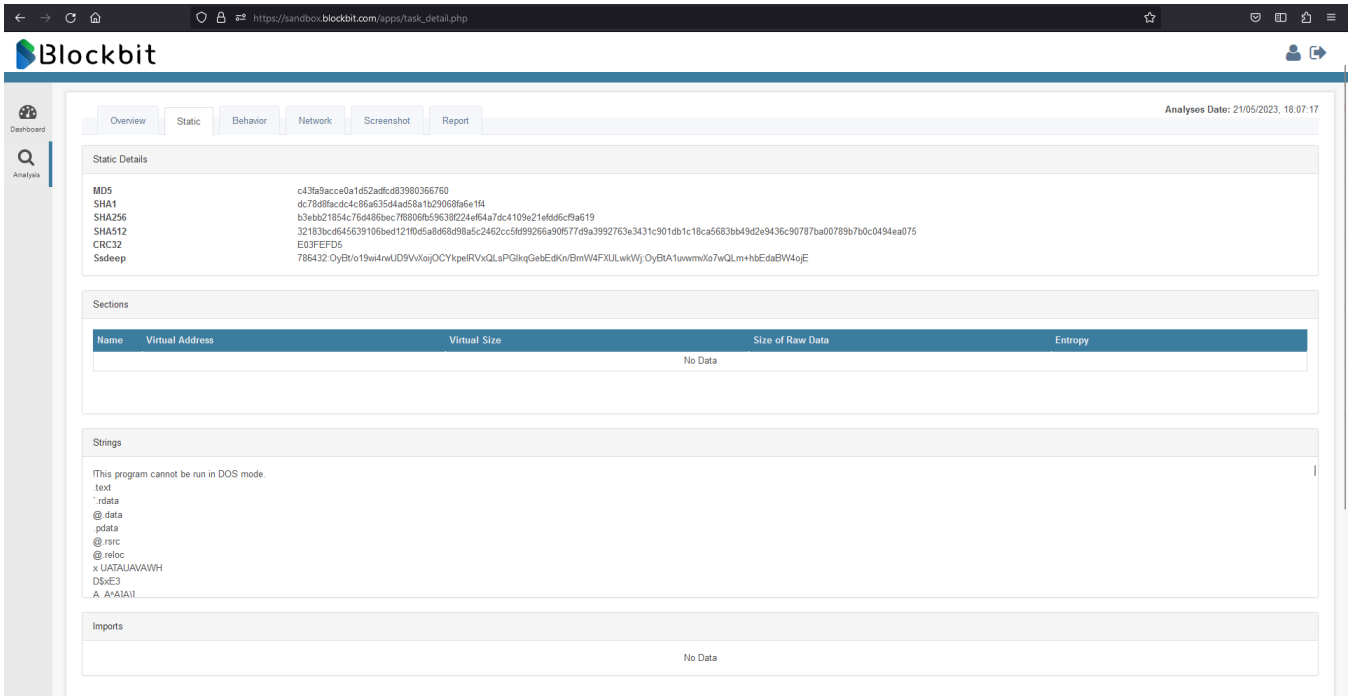
Network Hosts: Mostra o IP do ambiente virtual no qual a aplicação foi executada.

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:



Aba Static

Static details: Nesta painel podemos ver detalhes sobre as chaves de criptografia utilizadas na assinatura, e o arquivo MD5 do arquivo.

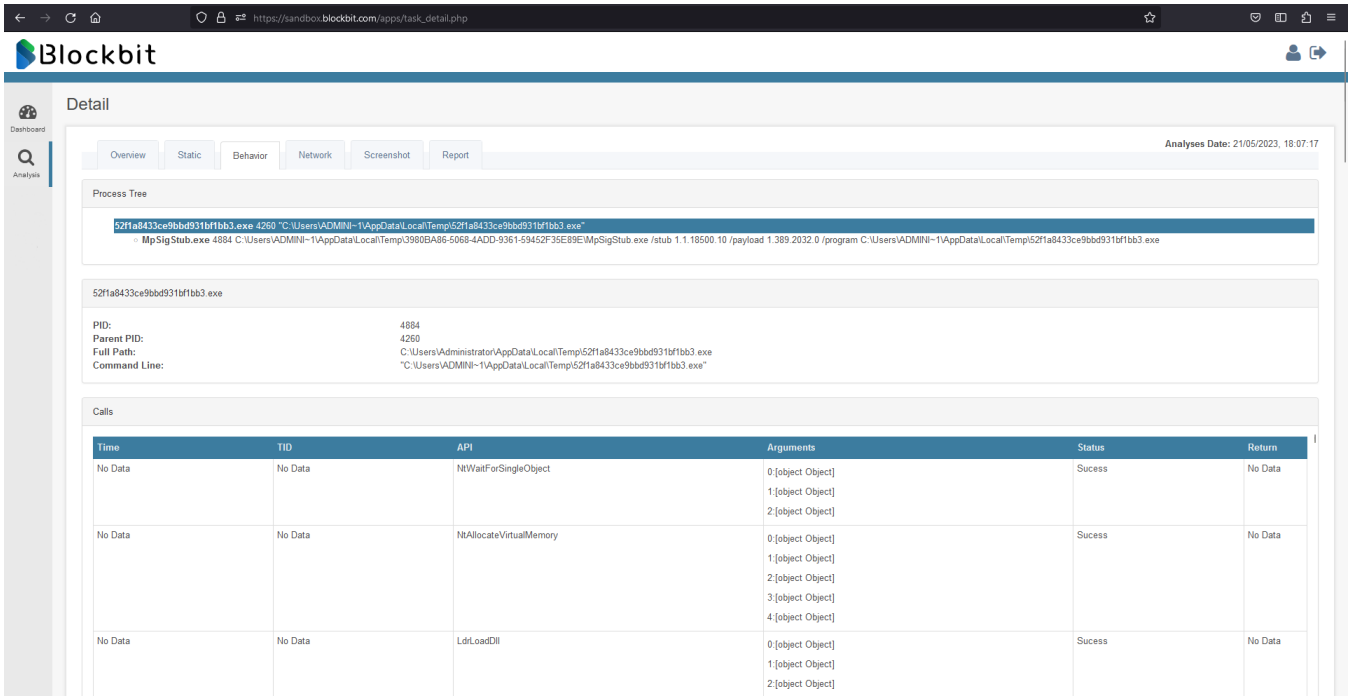
Sections: Este campo exibe detalhes sobre a máquina virtual utilizada na análise, tais como o nome, endereço virtual, tamanho utilizado em disco, tamanho dos dados utilizados e também o nível de entropia (aleatoriedade) presente na codificação do arquivo malicioso.

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:



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:

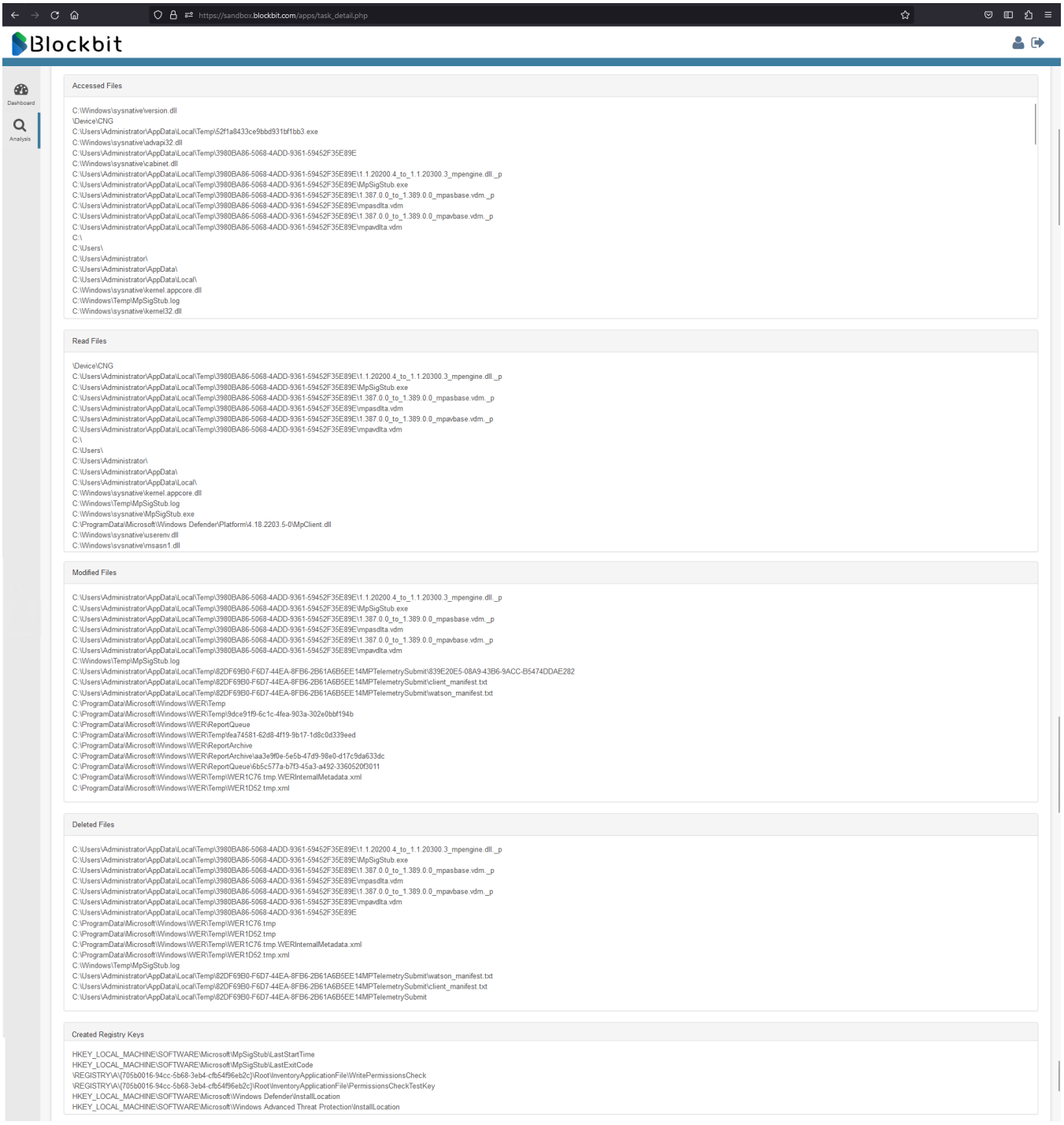
- PID (Process ID): Identificador do processo em execução.
- Parent PID: Indica qual processo pai originou a execução do arquivo analisado.
- Full Path: Caminho completo do arquivo executado no sistema.
- Command Line: Comando exato usado para iniciar o processo, o que pode revelar técnicas como argumentos 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.

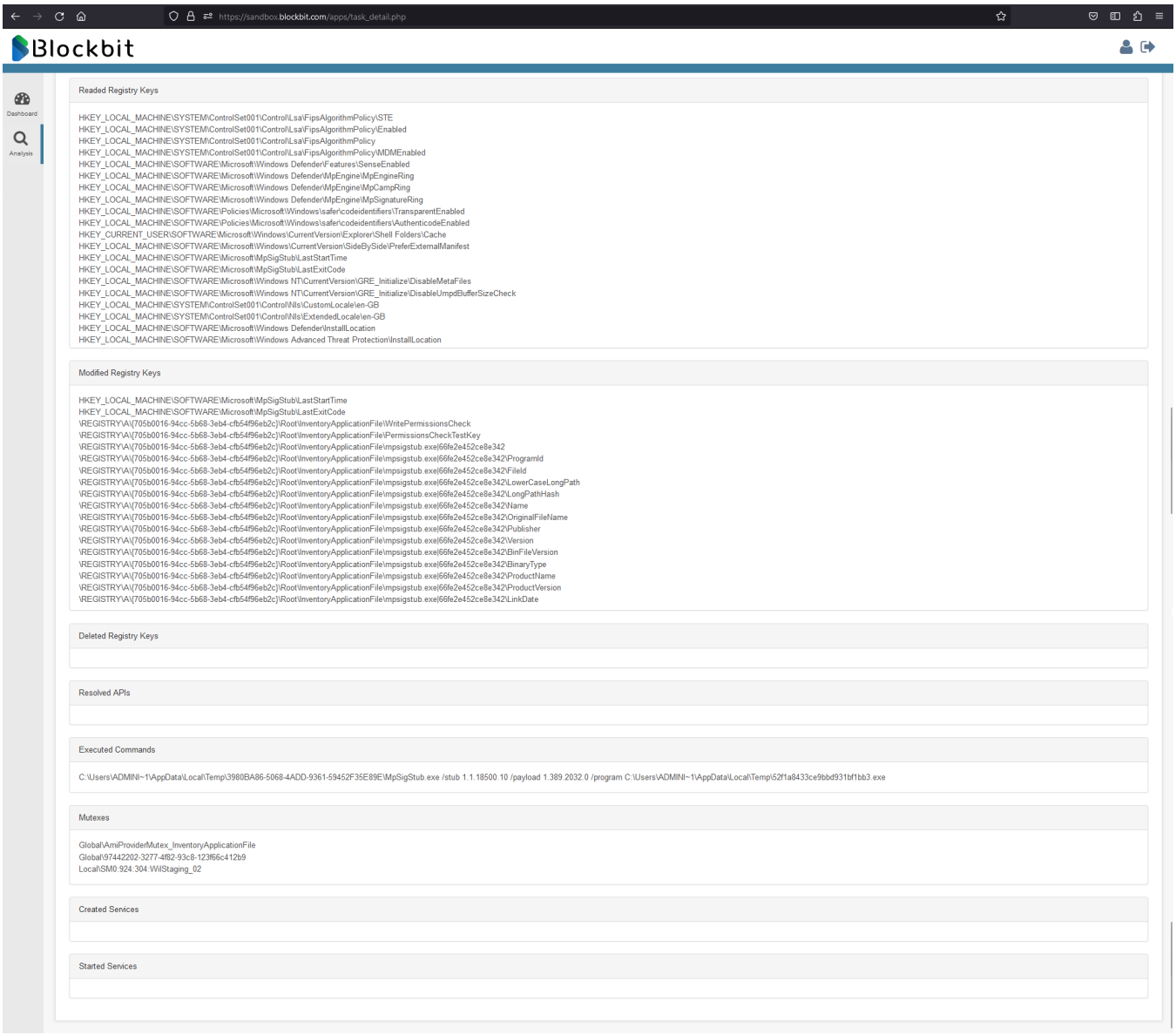
Permite entender exatamente como o malware interage com o sistema, ajudando a detectar táticas de exploração, roubo de credenciais e ataques de injeção de código.



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.*

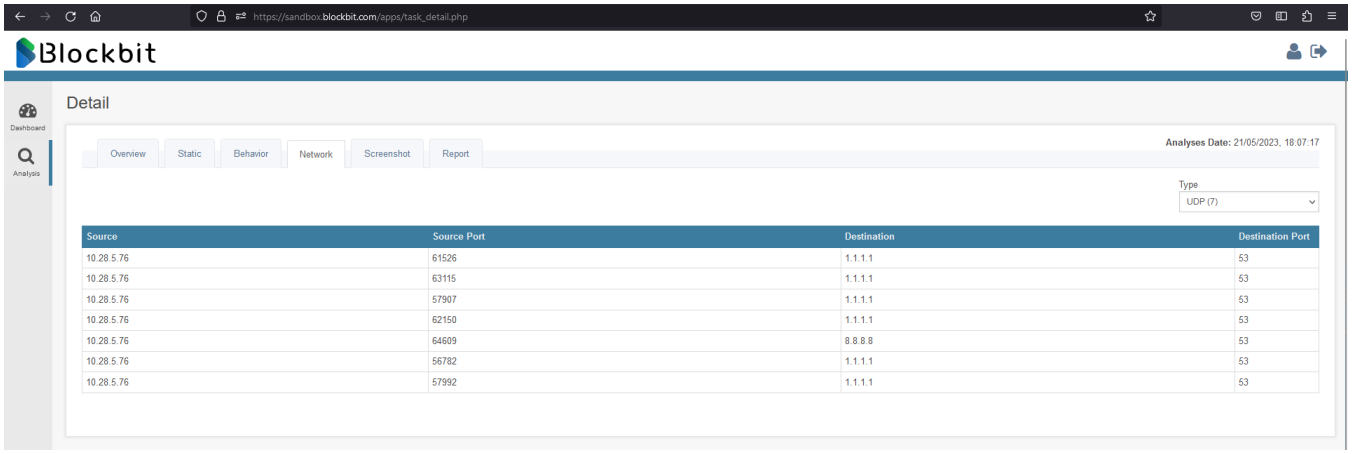


Dados sobre as chaves de registro que a assinatura maliciosa tentou acessar

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:



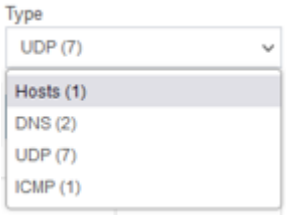
Aba Network

Source: O IP fonte.

Source Port: As portas fonte pelas quais tentativas de comunicação ocorreram.

Destination: O gateway de destino.

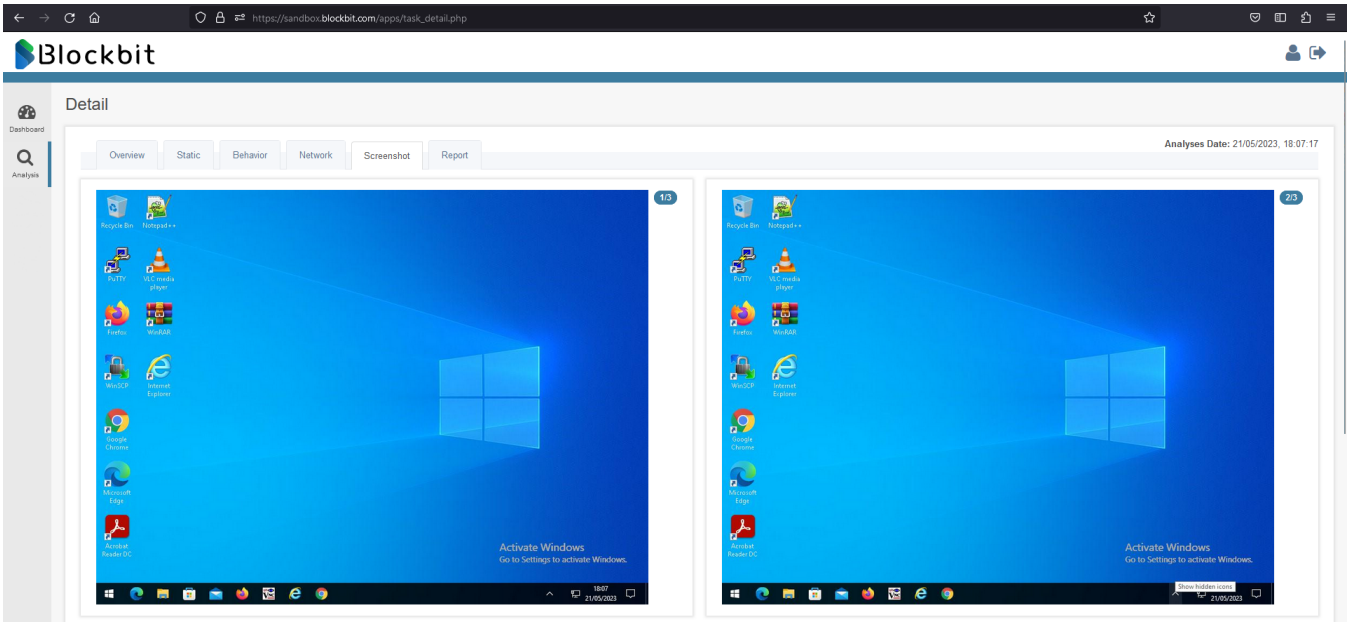
Destination Port: A porta destino para qual a tentativa de comunicação da assinatura maliciosa ocorreu.



Tipos de protocolo de rede

Blockbit ATP Sandbox - Screenshot

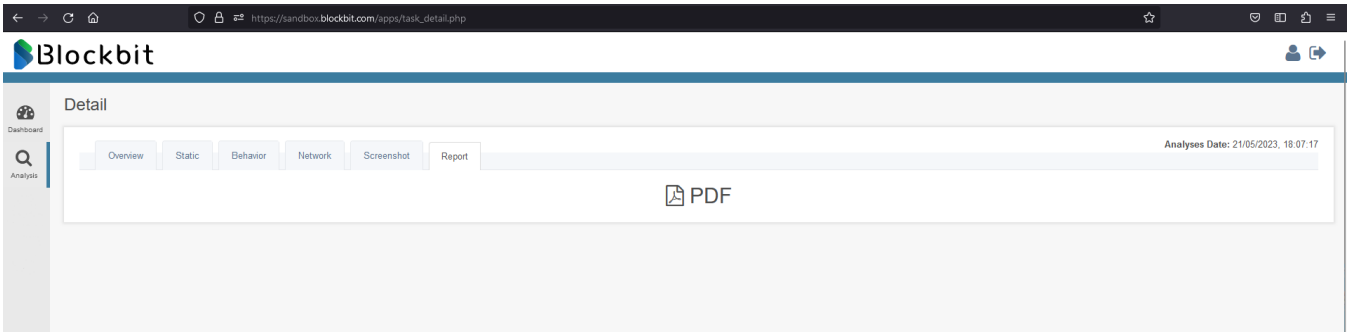
A seção screenshot mostra imagens do ambiente virtual no qual a analise foi realizada:



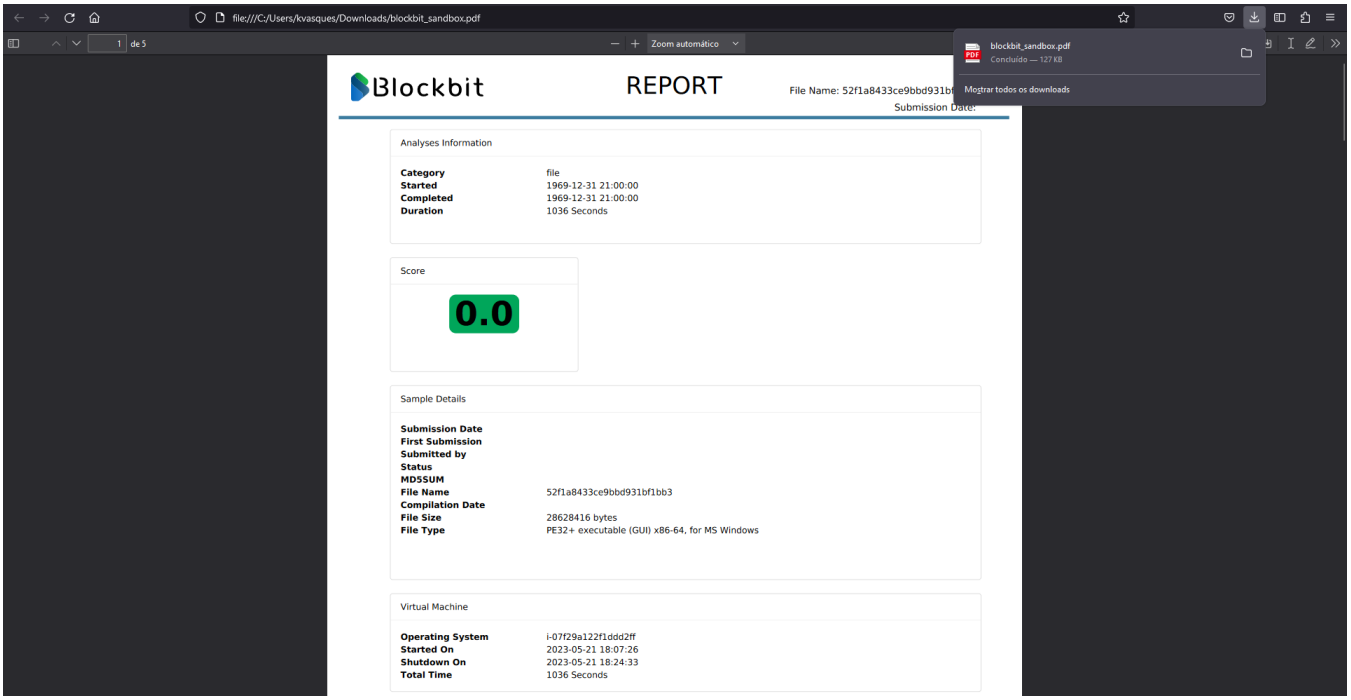
Seção Screenshot

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