

Resource Center

Documentation



1

1. Blockbit XDR - Administrator's Guide	5	
1.1 XDR - Introduction	6	
1.2 XDR - Minimum requirements	7	
1.3 XDR - Architecture	8	
1 4 XDR - API	q	
1.4.1 XDR - API - Configuration	11	,
1.4.2 XDR - All - Doordivating on agont	17	,
	17	
1.4.3 ADR - API - Role Based Access Control	10	5
1.4.3.1 XDR - API - RBAC Reference	19	,
1.4.4 XDR - API - Updating an agent		4
1.5 XDR - Collected Data	24	ł
1.6 XDR - Agents	26	5
1.6.1 XDR - Agents - Communication via web proxy	28	3
1.6.2 XDR - Agents - Installing an Agent on an Endpoint	30)
1.7 XDR - Search System	33	3
1.8 XDR - First access	35	5
1.9 XDR - Dashboard	37	7
1.9.1 XDR - Dashboard - Graphics	38	3
1.9.2 XDR - Dashboard - Mitre ATT&CK	39)
1.9.3 XDR - Dashboard - Overview	40)
194 XDR - Dashbard - Techniques	Δ1	í
1 10 XDR - Security Events	42	,
1 10 1 XDR - Security Events - Event list	Δ ⁻	ł
1 10 2 XDR - Security Events - Hits		í
1 10 2 XDR - Security Events - Notifications		
1 10 4 Zh - Geounity Evonts - Nouncatoris -	۰۰۰۰ 4C	
111 VDP - Custom Dashboarde		,
111 1 ZDL - Custom Dashboards - Craste Dashboard		,
11111 XDK - Custom Dashboards - Greate Dashboard		1
1.11.1.1 ADA - Custom Dashboarda, Viewelizationa		r 2
1.1.1.1.2 ADK - Custoffi Dashboards - Visualizations		ر د
1.12 XDR - Reports		5
1.13 XDR - Endpoint Control Center		,
1.13.1 XDR - Endpoint Control Center - Create policy	61	-
1.14 XDR - Endpoints Summary	65)
1.14.1 XDR - Endpoints Summary - Configurations	66	5
1.14.2 XDR - Endpoints Summary - Summary Panel)
1.15 XDR - Endpoint Groups & Sub-groups	74	ł
1.15.1 XDR - Endpoint Groups - Inheritance	77	1
1.15.2 XDR - Endpoint Groups - View details	80)
1.15.3 XDR - Endpoints Groups - Active Response	81	I
1.16 XDR - Security	83	3
1.16.1 XDR - Security - Roles	84	ł
1.16.1.1 XDR - Security - Create role	86	5
1.16.2 XDR - Security - Users	88	3
1.16.2.1 XDR - Security - Create User	90)
1.16.3 XDR - Security - Permissions	91	J
1.16.4 XDR - Security - Multi Factor Authentication	93	3
1.17 XDR - Indices	94	ł
1.17.1 XDR - Indices - Indices	95	5
1.17.1.1 XDR - Indices - Indices - Create index	97	7
1.17.2 XDR - Indices - Settings	99)
1.17.3 XDR - Indices - State Management Policies	10)(
1.17.3.1 XDR - Indices - State Management Policies - JSON editor	10)1
1.17.3.2 XDR - Indices - State Management Policies - Visual editor	10)2
1.18 XDR - Audit	10)5
1.18.1 XDR - Audit - Overview	10)6
1.18.2 XDR - Audit - Settings	10) <u>o</u>
1.19 XDR - Quarantine	11	1
1.20 XDR - Configuration Assessment		13
1 21 XDR - Malware Detection	11	15
1.22 XDR - File Integrity Monitoring	11	17
1 23 XDR - Secure Internet Gateway	11	0
1 23 1 XDR - Secure Internet Gateway - Groups	12	24
1 23 1 1 XDR - Secure Internet Gateway - Groups - Adlists	12	26
123 1 2 XDR - Secure Internet Gateway - Groups - Clients	12	2
123.1.3 XDR - Secure Internet Gateway - Groups - Domains	12	20
1 23 2 XDR - Secure Internet Gateway - Local DNS	11	32
1 23 3 XDR - Secure Internet Gateway - Query Log	11	,∠ ₹∕\
1 23 3 1 XDR - Secure Internet Gateway - Query Log - Long Term Data	11	,- ~
1 24 XDR - Threat Hunting	11	رب در
1.25 ADA - Theat Monitor - CTI	IC 47	10
125 ADIC TITIGAL WOTING COT		rU 14
1.25.1 ADIX - Tilled Widilitor - CTL Dashibudiu	14	11 10
1.22.1.1.ADK - THIERALMONITO - CTT - DASHDOAID - ACTIONS		⊧∠ 1.⊏
1.20.2 ADK - Thileau Monitor - CTL - AntalySes	14	+0 1 7
1.2J.5 ADR - THIERI MUNITUH - CTI - Cases	14	+/ 10
1.20.4 AUK - Infeat Monitor - CTI - UDServations	14	18
1.20.5 ADK - Integat Monitor - CTI - Integats	15	1 כרב
1.20.0 AUK - Infeat Monitor - CII - Arsenal	15	2
ו.בס. / אטא - Infeat Monitor - 11 - Lecnniques	15	4כ

1.25.8 XDR - Threat Monitor - CTI - Entities	155
1.25.9 XDR - Threat Monitor - CTI - Locations	157
1.25.10 XDR - Threat Monitor - CTI - Events	158
1.25.11 XDR - Threat Monitor - CTI - Data	160
1.25.12 XDR - Threat Monitor - CTI - Trash	163
1.25.13 XDR - Threat Monitor - CTI - Settings	164
1.26 XDR - Vulnerability detection	168
1.26.1 XDR - Vulnerability detection - Inventory	169
1.27 XDR - MITRE ATT&CK	170
1.27.1 XDR - MITRE ATT&CK - Dashboard	171
1.27.2 XDR - MITRE ATT&CK - Framework	172
1.27.3 XDR - MITRE ATT&CK - Intelligence	174
1.28 XDR - Security Operations	175
1.28.1 XDR - Security Operations - GDPR	177
1.28.2 XDR - Security Operations - HIPAA	178
1.28.3 XDR - Security Operations - LGPD	179
1.28.4 XDR - Security Operations - NIST 800-53	180
1.28.5 XDR - Security Operations - PCI DDS	181
1.28.6 XDR - Security Operations - TSC	182
1.29 XDR - Cloud Security	183
1.29.1 XDR - Cloud Security - Amazon Web Services	184
1.29.2 XDR - Cloud Security - Azure/Microsoft 365	185
1.29.3 XDR - Cloud Security - Docker	186
1.29.4 XDR - Cloud Security - GitHub	187
1.29.5 XDR - Cloud Security - Google Cloud	188
1.30 XDR - Download	189

Blockbit XDR - Administrator's Guide

Blockbit XDR (eXtended Detection and Response) is a cloud-based solution that uses machine learning to detect, prioritize, and respond to threats. It utilizes data from various endpoints and, with Artificial Intelligence based on the Mitre ATT&CK standard, provides the shortest path between detection and response.

XDR - Introduction

Hello! Thank you for choosing Blockbit XDR.

This guide will assist you with the installation, configuration, and operation of the solution.

Blockbit XDR (eXtended Detection and Response) is a solution that combines various technologies to detect, prioritize, and respond to threats.

The XDR technology collects data from various network points such as servers, email, cloud environments, and endpoints. This data is analyzed and contextualized, allowing for threat detection. With this information, it's possible to discover the scope and impact of threats, how they entered the system, and what may be affected. These threats are then analyzed, contextualized, and prioritized so they can be addressed according to their level of risk.

How Blockbit XDR works: Identity Cloud Endpoints E-mail 1. Data entry Web Network 2. Detection Firewall **Threat Intelligence** Data correlation Analytics Prioritization 3. Responses **Response** and Event Automatization investigation administration

XDR is superior to previous technologies, such as Endpoint Detection and Response and Network Detection and Response, due to its proactive approach to threat detection and management, as well as its telemetry from multiple sources.

The Blockbit XDR features advanced mechanisms for reverting malicious changes, allowing the system to be restored to its state prior to an attack. The solution performs regular backups and maintains detailed logs of modifications, ensuring resilience against ransomware, accidental deletions, and unauthorized changes.

System Change Reversal

Blockbit XDR is capable of undoing any modifications made by an attack, restoring system configurations, registry edits, and permissions of compromised files.

Recovery of Encrypted Files and Data

For Windows systems, the solution can reverse destructive events, restoring files deleted or encrypted by ransomware through the central administration console.

Device Isolation and Containment on the Network

Blockbit XDR can place a device in quarantine, restricting its communication with the network to prevent the spread of threats.

It also allows for automatic policies to isolate compromised machines (Host Isolation), preventing attacks from advancing within the organization. These features ensure rapid response, effective mitigation, and operational continuity, minimizing the impact of cyberattacks.

XDR - Minimum requirements

- Supported Operating Systems
- Windows
 - 1. Windows Server 2008 (todas as versões), 2011, 2012, 2012 R2, 2016, 2019, 2022, 2025 or higher;
 - 2. Windows 7 (all versions), 8.1, 10, 11 or higher;
- macOS (amd/arm)
- Big Sur, Monterey, Ventura, Sonoma, Sequoia or higher;;
 Linux
 - 1. Ubuntu, Debian, Raspbian, Fedora, CentOS, Red Hat Enterprise Linux (RHEL), Rocky Linux, AlmaLinux, SUSE Linux Enterprise or OpenSUSE;
 - 2. Nuvens públicas, como AWS Linux, Oracle Linux, Azure Linux or Google Cloud Ubuntu Pro;
- Solaris
- HP-UX
- AIX.
- Agent Size: Between 50 and 100 MB
- Memory Requirement: Between 10 and 50 MB
- Disk Requirement: Between 50 and 100 MB
- Network Requirement: 10 KB/sec
- Connectivity Requirement Between Agents: Ports 1514/TCP and 1515/TCP must be open to the Internet.

All the operating systems mentioned above are supported on native installations on physical hardware, in on-premises virtualization environments such as VMware, KVM, among others, as well as on public and private cloud infrastructures like AWS, Azure, Google, Oracle, among others, ensuring flexibility and compatibility for various IT architectures.

XDR - Architecture

The architecture of Blockbit XDR uses a scalable and modular approach deployed in a Kubernetes environment. This facilitates the orchestration of components in a distributed manner, allowing for high availability, scalability, and flexibility.

Components



1. Endpoints: PCs, Notebooks, Servers, Virtual Machines, and Cloud Instances: these are the source points where Blockbit XDR agents are installed, tasked with collecting security data such as logs, events, and suspicious activities directly from the monitored devices. For more information, refer to Agents.

Agent Registration: Each endpoint registers its agents with the central Blockbit XDR cluster. These agents are configured to send security data for processing.

- Agent Data: After registration, the agents transmit the collected data to the cluster for processing and analysis.
- Blockbit XDR Cluster: Blockbit XDR Master: the central component of the cluster, responsible for communication within the cluster, workload management, and coordination of the various services distributed by Kubernetes.
 - Blockbit XDR Worker: responsible for collecting, initially processing, and sending data to other system components.
- 3. Blockbit XDR Indexer: Responsible for receiving and indexing the processed data from the Worker.
- 4. Blockbit XDR Dashboard:
 - It is the visualization interface. It receives the indexed data from the Indexer and presents this information in graphs, alerts, and customizable dashboards.
 - Kubernetes allows for distributed access, ensuring that the interface is always available, even in high user demand scenarios.
- 5. Security Operations Center (SOC):
 - The SOC team uses the Dashboard for analysis and decision-making, viewing processed and organized security data to identify threats and respond to incidents in real-time.

Kubernetes in the Architecture of Blockbit XDR:

- Container Orchestration and Management: Each component of Blockbit XDR (Master, Workers, Indexer, Dashboard) can be packaged as a container and orchestrated by Kubernetes, facilitating automatic scaling, restarting in case of failure, and load balancing among different nodes.
- High Availability: Kubernetes allows deployments with multiple replicas of services, which can run to ensure system resilience.
- Configuration Management: Kubernetes dynamically manages the configurations of each Blockbit XDR component, allowing adjustments as needed without downtime.

XDR - API

The Blockbit XDR API is a RESTful API that enables interaction between the Blockbit XDR Manager and any script or program capable of making requests.

Authentication

The Blockbit XDR API requires authentication. Every request must include a JSON Web Token (JWT). JWT is an open standard (RFC 7519) that allows secure transmission of information as a JSON object.

To obtain a JWT, call basicAuth for POST /security/user/authenticate.

JWTs have a default validity of 900 seconds. To change this, call PUT /security/config. Tokens issued before the change are automatically revoked.

Login with Username and Password:

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

Use the previous' response token to any requisition at the endpoint:

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

Access

To access the API:

If SSL (HTTPS) is enabled and the API is using a self-signed certificate, you need to add the -k parameter to bypass server communication verification.

1. Send a User Authentication Request via POST

Use the following command:

```
Replace <BLOCKBITXDR_API_USER> and <BLOCKBITXDR_API_PASSWORD> with your credentials. Substitute the TOKEN variable with the JWT response.
```

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

2. Verify the Generated TOKEN

The response should look like this:

eyJhbGciOiJFUzUxMiIsInR5cCI6IkpXVCJ9.

```
eyJpc3MiOiJ3YXplaClsImFlZCl6IldhenVoIEFQSSBSRVNUIiwibmJmIjoxNzA3ODk4NTEzLCJleHAiOjE3MDc4OTk0MTMsInN1Yi16IndhenVo
IiwicnVuX2FzIjpmYWxzZSwicmJhY19yb2xlcyI6WzFdLCJyYmFjX21vZGUiOiJ3aGl0ZSJ9.ACcJ3WdV3SnTOC-
PV2oGZGCYH3GpStSOul61UHHT7w6eUm_REOP_g8SqqIJDDW0gCcQNJTEECortIuI4zj7nybNhACRlBrDBZoG4Re4HXEpAchyFQXwq0SsZ3HHSj7e
JinBF0pJDG0D8d1_LkcoxaX3FpxpsCZ4xzJ492CpnVZLT8qI4
```

3. Send a Request

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

The response should look like this:

```
{ "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 }
```

Accessing Endpoints

After logging in, you can access any endpoint using the structure below:

Replace <METHOD> with the desired method and <ENDPOINT> with the desired endpoint.

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

Requests and Responses

The Blockbit XDR API has three main components:

- Request Method: GET, POST, PUT, or DELETE
- URL: Specifies the endpoint
- Authorization Header: Includes the JWT token

Example cURL Command

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

Breakdown of the cURL Command:

- -X GET/POST/PUT/DELETE: Specifies the request method.
- http://<BLOCKBITXDR_MANAGER_IP>:55000/<ENDPOINT> or https://<BLOCKBITXDR_MANAGER_IP>:55000/<ENDPOINT>: Specifies the endpoint URL.
- -H "Authorization: Bearer <YOUR_JWT_TOKEN>": Specifies the JWT authorization.
- -k: Suppresses SSL errors.

Response Structure

Field	Subfields	Description
data		
	affected_items	Lists affected items.
	total_affected_items	Shows the total affected items.
	failed_items	Lists failed items.
	total_failed_items	Shows the total failed items.
message		Description of the result.
error		Description of the error.

API Responses

Code	Description
200	Everything is fine.
400	Bad request. Request rejected due to an error.
401	Unauthorized. No valid API key provided.

402	Request failed. Valid parameters but failed.
403	Forbidden. API key lacks permission.
404	Not found. The requested resource does not exist.
409	Conflict. The request conflicts with another.
429	Too many requests. API rate limit exceeded.
500+	Server error. Blockbit XDR server encountered an issue.

Example Response:

```
{ "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 - Configuration

Accessing the XDR API Configuration

The XDR API can be configured on the Blockbit XDR server. By default, all options are commented out. To apply a configuration, uncomment and edit the desired settings.

If the XDR API is running in a cluster, any configuration changes made on the master node must be manually replicated on other nodes.

Example Configuration

```
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
```

Restarting the API

After making configuration changes, restart the API with the following command:

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

Configuration Options

General Settings

- host: List of valid IPs or hostnames where the API is running. Default: ['0.0.0.0', ':::'].
- port: Port for the API to listen on. Range: 1-65535. Default: 55000.
- drop_privileges: Run the blockbit-xdr-api process as a non-root user. Default: yes.
- experimental_features: Enable development features. Default: no.
- max_upload_size: Maximum body size (in bytes) the API accepts. Default: 10485760 (10 MB).

HTTPS Configuration

- enabled: Enable SSL (HTTPS). Default: yes.
- key: Private key filename. Default: server.key.
- cert: Certificate filename. Default: server.crt.
- use_ca: Use a CA-signed certificate. Default: no.
- ssl_protocol: SSL protocol allowed. Default: auto.
- **ssl_ciphers**: Specific SSL ciphers to use. Default: none.

Access Control

- max_login_attempts: Maximum login attempts before blocking. Default: 50.
- **block_time**: Block duration in seconds. Default: 300.
- max_request_per_minute: Max requests per minute. Default: 300.

Security Configuration Endpoints

The API allows querying and modifying security configurations via specific endpoints:

Get Current Security Config:

GET /security/config

• Update Security Config:

```
PUT /security/config
```

• Restore Default Security Config:

```
DELETE /security/config
```

Generating SSL Certificates

The SSL certificate ensures secure communication between the Blockbit XDR server API and its clients. Certificates are stored in /var/ossec/api /configuration/ssl/.

Steps to Generate Certificates:

a. Generate a key and certificate signing request:

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

1. (Optional) Protect the key with a password:

ssh-keygen -p -f server.key

Key Configuration Parameters

Option	Description	Default
auth_token_exp_timeout	Token expiration time in seconds.	900
rbac_mode	Role-Based Access Control mode: black (allow all) or white (deny all).	white

Cluster Configuration Endpoints

GET /cluster/api/config: Get Configuration for All Cluster Nodes;

GET /manager/api/config: Get Local Configuration

Security Configuration Endpoints

GET /security/config: Retrieve the current security configuration.

Modify Configuration

PUT /security/config: Modify the security configuration.

Restore Configuration

DELETE /security/config: Restore the default security configuration.

SSL Certificate

This process is automatically executed the first time the Blockbit XDR server API runs.

The SSL certificate ensures secure communication between the Blockbit XDR server API and its clients. Certificate files are stored in the directory /var /ossec/api/configuration/ssl/.

Generating New Certificates for the Blockbit XDR API

By default, the password for the key must be entered every time the server starts. If the key was generated by the Blockbit XDR server API or using the command above, it will not have a password.

1. Generate the key and certificate signing request (requires the openssl package):

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

2. (Optional) Protect the key with a password:

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

You will be prompted to enter and confirm the new password

XDR - API - Deactivating an agent

To deactivate an agent via API, run the following commands:

To disconnect an agent temporarily:

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

The agent will restart and stop communicating with the XDR Manager temporarily.

To force an agent to reconnect:

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

XDR - API - Role Based Access Control

The Blockbit XDR API offers Role-Based Access Control (RBAC). It enables access control to endpoints and resources based on user privileges.

For more information, go to Security.

RBAC Policies

RBAC policies control API permissions using three elements: actions, resources, and effect.

 Actions represent a hierarchy of tasks that a user can perform. Example: Restart agent.

```
agent:restart
```

• Resources are any entities subject to an action. The set of resources is dynamic, but their types are static. Example:

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

• Effect can only be "allow" or "deny."

RBAC Modes

In the Blockbit XDR API, there are two RBAC modes: blacklist and whitelist. These modes determine how user actions are handled and the administrator's responsibilities.

- Blacklist (black): Allows all actions by default. The administrator specifies which actions are prohibited.
- Whitelist (white): Prohibits all actions by default. The administrator specifies which actions are allowed.

XDR - API - RBAC Reference

On this page, you can find the actions, resources, and effects of RBAC policies in the Blockbit XDR API.

Resources

- agent:group: Reference to agents by group name. Example: agent:group:web
- agent:id: Reference to agents by agent ID. Example: agent:id:001
- group:id: Reference to agent groups by group ID. Example: group:id:default
- node:id: Reference to cluster nodes by node ID. Example: node:id:worker1
- decoder:file: Reference to decoder files by filename. Example: decoder:file:0005-blockbit_xdr_decoder.xml
- list:file: Reference to list files by filename. Example: list:file:audit-keys
- rule:file: Reference to rule files by filename. Example: rule:file:0610-win-ms_logs_rules.xml
- policy:id: Reference to security policies by ID. Example: policy:id:1
- role:id: Reference to security roles by ID. Example: role:id:1
- rule:id: Reference to security rules by ID. Example: rule:id:1
- user:id: Reference to security users by ID. Example: user:id:1

Actions

For each action, the affected endpoints and necessary resources are specified using the structure: <Method> <Endpoint> (<Resource>)

active_response

The /active-response endpoint allows users to interact with the Active Response module.

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

agent

The /agents endpoint allows users to register and manage agents on the server.

- 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/group (agent:id, agent:group)
- DELETE /agents/{agent_id}/group (agent:id, agent:group)
 PUT /agents/group (agent:id, agent:group)
- agent:read GET /agents (agent:id, agent:group) GET /agents/{agent_id}/key (agent:id, agent:group)
- agent:restart 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)

cluster

The /cluster endpoint allows users to manage the configuration and health of master and worker nodes in the cluster.

 cluster:read GET /cluster/healthcheck (node:id) GET /cluster/nodes (node:id)
 cluster:restart PUT /cluster/restart (node:id)

decoders

The /decoder endpoint allows users to manage and retrieve information about decoders.

- decoders:read
- GET /decoders (decoder:file)
 decoders:update
 - PUT /decoders/files/{filename} (:)

event

The /event endpoint allows users to ingest security events for analysis.

```
• event:ingest
POST /events (:)
```

group

The /groups endpoint allows users to group agents for centralized configurations.

```
group:create
POST /groups (:)
group:read
GET /groups (group:id)
```

lists

The /lists endpoint allows users to manage CDB lists used for scanning malicious files.

```
• lists:read
GET /lists/files (list:file)
```

logtest

The /logtest endpoint allows users to test and validate new rules and decoders.

• logtest:run PUT /logtest (:)

manager

The /manager endpoint allows users to manage and retrieve information about the manager.

• manager:read GET /manager/info (:)

mitre

The /mitre endpoint retrieves MITRE ATT&CK framework data.

• mitre:read GET /mitre/tactics (:)

rootcheck

The /rootcheck endpoint allows users to interact with the rootcheck module.

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

rules

The /rules endpoint manages rules for analyzing events and generating alerts.

• rules:read GET /rules/files (rule:file)

syscheck

The /syscheck endpoint interacts with the File Integrity Monitoring module.

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

syscollector

The /syscollector endpoint gathers system information from monitored endpoints.

syscollector:read
 GET /syscollector/{agent_id}/hardware (agent:id, agent:group)

task

The $/ {\tt tasks}$ endpoint retrieves status information about tasks performed by the manager.

• task:status GET /tasks/status (:)

XDR - API - Updating an agent

O ChatGPT disse:

Before updating, check which agents are outdated. You can do this via API or the Blockbit XDR interface.

API

To list outdated agents via API, run the following command:

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

Replace <BLOCKBIT_XDR_MANAGER_IP> with your manager's IP.

Replace <YOUR_JWT_TOKEN> with your JWT token.

2. Manually Updating Agents

To update a specific agent, use the following command:

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

To update all agents, use the following command:

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

3. Updating Agents in Groups

To update agents in a specific group, use the following command:

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

Replace <GROUP_ID> with the ID of the group you want to update.

4. Restarting Agents After Updating

After updating, restart the agents with the following command:

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

5. Verifying if the Update Was Successful

To check the version of the running agent, use the following command:

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

XDR - Collected Data

The Blockbit XDR ensures the protection of data from managed devices through robust encryption, both at rest and during transmission. All information is automatically processed and correlated, resulting in the generation of real-time logs and alerts, ensuring integrity, confidentiality, and proactive threat detection.

1. Encryption at Rest (Storage)

Blockbit XDR uses encryption to store data collected from endpoints and security events in the Blockbit cloud.

Logs, alerts, and sensitive data are stored in the Blockbit cloud with AES-256 encryption.

Access to the information is restricted through Role-Based Access Control (RBAC). Only authorized users can view sensitive data. The retention period and/or storage capacity of data, including logs (processed and unprocessed), events, audits, and reports, are configured according to the terms set in the licensing and/or contract. This setting ensures proper retention of information, in line with operational needs and the organization's compliance requirements.

2. Encryption in Transit (Transmission)

All communications between agents and the Blockbit XDR console are protected using TLS 1.3 or higher.

The Blockbit XDR API requires secure communication via HTTPS (SSL/TLS) for all interactions with the console and agents.

Traffic between internal components, such as agents and the Blockbit XDR Manager, also follows secure protocols, preventing data interception.

3. Compliance

Blockbit XDR follows security best practices compatible with LGPD, GDPR, PCI DSS, ISO 27001, and NIST.

To enable operation, Blockbit XDR collects the following data:

Data	Description
@timestamp	Date and time of the event.
GeoLocation.country_name	Name of the country of origin of the event.
GeoLocation.location	Coordinates of the event's origin.
GeoLocation.region_name	Name of the subnational division of origin of the event.
_index	Name of the index where the data was stored.
agent.id	Unique identifier of the agent that collected or generated the event.
agent.name	Name of the agent that collected or generated the event.
cluster.name	Name of the cluster where the agent is located.
cluster.node	Location of the event within the cluster.
data.id	Identifier of the processed data.
data.protocol	Protocol of the event.
data.srcip	Source IP of the event.
data.url	URL of the resource involved in the event.
decoder.name	Name of the decoder that interprets the received data.
full_log	Log entry of the event.
id	Identifier of the event.
input.type	Type of input for the event.
location	Location of the event.
manager.name	Name of the system that supervises the agents.
rule.description	Description of the rule triggered when generating the event.
rule.firedtimes	Number of times the mentioned rule has been triggered.
rule.gdpr	Compliance indicator of the rule with GDPR.
rule.groups	Group of the rule.
rule.id	Identifier of the rule.
rule.level	Severity level associated with the rule.
rule.mail	Indicates if the rule sends modifications via email.

rule.nist_800_53	Compliance indicator of the rule with NIST SP 800-53.
rule.pci_dss	Compliance indicator of the rule with PCI-DSS.
rule.tsc	Compliance indicator of the rule with TSC.

XDR - Agents

In XDR, the central component is the Agent.

The agent is a service of the XDR installed on an endpoint (PC, laptop, virtual machine, cloud instance). It will protect the endpoint and respond to threats.

Combining the features of EPP (Endpoint Protection Platform) and EDR (Endpoint Detection and Response), Blockbit XDR ensures a comprehensive approach to the prevention, detection, and response to cybersecurity incidents.

Real-Time Process Analysis

Before sending an alert to the administration console, the agent locally examines the process information, evaluating behavior, signatures, and characteristics of the executable.

If a process is identified as potentially malicious, the agent can take automatic remediation actions, such as blocking, terminating the process, or isolating the endpoint, reducing detection and attack mitigation time.

Artificial Intelligence and Machine Learning in File Analysis

The agent uses artificial intelligence and machine learning to analyze files before execution, preventing known and unknown threats (Zero-Day). During file execution, the agent monitors its behavior in real-time, detecting anomalies, exploit attempts, and lateral movement. If a file exhibits suspicious behavior, the agent can prevent its execution, quarantine it, or automatically apply corrective actions. With this proactive and intelligent approach, Blockbit XDR ensures advanced detection, rapid response, and reduced attack mitigation time, providing robust protection for endpoints in any environment.

Blockbit XDR Anti-Tamper Protection

Blockbit XDR features advanced anti-tamper protection, blocking any attempt to disable, modify, or remove the solution, even by local system administrators, domain admins, or threats, ensuring that only users authorized by Blockbit XDR have control.

1. Protection of Files, Processes, and Services

Prevents modification, deletion, or termination of Blockbit XDR services, blocking malicious actions from ransomware, rootkits, and other advanced threats. Ensures that even a user with local administrator credentials cannot deactivate or remove the agent, reinforcing security against both internal and external attacks.

2. Strict Permission Restrictions

Only properly authorized administrators can make changes to configurations or uninstall the agent. The Blockbit XDR agent prevents improper manipulations through reinforced internal controls and protection against unauthorized modifications to the system registry.

3. Kernel-Level Execution for Maximum Protection (Windows)

The Windows agent runs directly in the kernel space, ensuring the highest level of protection against tampering (anti-tamper). It operates at the operating system driver level, ensuring priority over common processes and blocking attempts to compromise by malware and advanced attacks.

)".

Continuous monitoring of the agent's status, with self-repair mechanisms that automatically restore any attempt to interrupt the essential services of Blockbit XDR.

In the list, each agent corresponds to an endpoint.

An agent can only be uninstalled or modified by a XDR administrator's user, password and MFA.

(o) Explore agent

The method for selecting an agent is standardized in Blockbit XDR.

To select an agent, click on "Explore agent (

A modal with the list of agents will open.

Explore agent

Search					
ID 个 OI	Name	Group	Version	Operating system	Status
001	bb-xdr-proxy-geo	default	v1.0.0	👌 CentOS Linux 7.9	• active 💿
003	xdr-VM-Ipereira	default	v1.0.0	Microsoft Windows 10 Pro 10.0.19042.631	• active 💿
004	AD-BB-246	default	v1.0.0	Microsoft Windows Server 2019 Standard 10.0.17763.6054	• active ⑦
006	Ipereira-note	default	v1.0.0	Microsoft Windows 10 Pro 10.0.19045.4529	• disconnected ⑦
007	lpereira-note1	default	v1.0.0	Microsoft Windows 10 Pro 10.0.19045.4529	• active ⑦
009	qaubt	default	v1.0.0	👌 Ubuntu 22.04.4 LTS	• active ⑦

To search for a specific agent, use the search bar (Search).

Click on the agent to select it.

For each agent, there are the following characteristics:

- Id: The identifying number of the agent.

- Id: The Identifying number of the agent.
 Name: The name of the agent.
 IP address: The IP address of the agent.
 Operating system: The operating system of the agent.
 Version: The version of the agent.
 Status: The status of the agent, which can be either active or disconnected.

XDR - Agents - Communication via web proxy

1. Configure the Agent to Use a Proxy

The agent configuration file is located at:

- Linux: blockbitxdretc.conf
- Windows: blockbitxdr/ossec.conf

Before modifying the file on Windows, pause the agent using this command:

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

In the <remote> section, add the following configuration:

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

After modifying the file on Windows, restart the agent with this command:

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

2. Restart the Agent to Apply the Configuration

After modifying the configuration file, restart the agent service:

o For systems using systemctl:

systemctl restart blockbit-xdr-agent

• For systems without systemctl:

/var/ossec/bin/ossec-control restart

3. Verify Communication Status

To ensure the agent is correctly communicating with the Manager/Workers through the proxy, use the following command:

• Linux:

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

• Windows:

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

XDR - Agents - Installing an Agent on an Endpoint

Blockbit XDR Agent Installation

The Blockbit XDR Agent can be manually installed on endpoints (Windows, Linux, and macOS) to ensure protection, monitoring, and real-time threat response. During installation, it is possible to specify the group to which the endpoint will be assigned using the parameter BBXDR_AGENT_GROUP.

Windows Installation

- 1. Open PowerShell as Administrator:
- Press Win + X and select PowerShell (Admin) or Windows Terminal (Admin).
- 2. Navigate to the directory where the installer was saved:

```
cd "C:\Path\to\file"
```

3. Install the agent and set the endpoint group: In PowerShell, execute the following command:

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

4. After installation, start the agent manually :

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

The agent is now active and in the configured group.

Automated and Mass Installation

The Blockbit XDR Agent can also be installed automatically and in bulk using PowerShell scripts, GPO (Group Policy Object) in Active Directory, SCCM (System Center Configuration Manager), or endpoint management tools, allowing remote distribution to multiple devices simultaneously, ensuring efficiency and standardization during deployment.

Linux Installation

The agent can be installed on Linux distributions using the .deb and .rpm package formats.

1. Access the terminal and locate the installation directory:

```
cd /path/to/file
```

2. Run the installer according to the distribution:

DEB Format:

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

RPM Format:

```
BBXDR_MANAGER="xdr-clientname.blockbit.com" BBXDR_REGISTRATION_PASSWORD="XXXX"
BBXDR_REGISTRATION_SERVER="xdr-clientname.blockbit.com" BBXDR_AGENT_GROUP="default" BBXDR_AGENT_NAME="
MACHINE_NAME_Linux" rpm -ihv bbxdr-agent-1.0.0-1.x86_64.rpm
```

3. Activate and start the agent:

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

The agent is now active and in the configured group.

macOS Installation

1. Create the Configuration File Open the terminal and execute:

cat <<EOF >/tmp/bbxdr_envs
BEXDR_MANAGER="xdr-clientname.blockbit.com"
BEXDR_REGISTRATION_PASSWORD="XXXX"
BEXDR_REGISTRATION_SERVER="xdr-clientname.blockbit.com"
BEXDR_AGENT_GROUP="default"
BEXDR_AGENT_NAME="MACHINE_NAME_macOS" EOF

2. Run the Installer:

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

The agent is now active and in the configured group.

Uninstallation of the Blockbit XDR Agent

To ensure security and full control of the environment, the uninstallation process for the Blockbit XDR agent requires authentication with Blockbit XDR administrator credentials, along with Multi-Factor Authentication (MFA).

This dual verification ensures that only users properly authorized by Blockbit XDR can remove the agent, preventing deactivation attempts by unauthorized users or threats seeking to compromise endpoint protection.



XDR - Search System

In Blockbit XDR, the search system is standardized.

In Search, you can look for specific elements. You can build simplified queries using the Dashboard Query Language.

In +Add filter, you can add filters to the search.

In Field, you can select the fields to be searched. In Operator, \boldsymbol{x}

By clicking on "create custom label?", you can create a specific name for the query.

In Edit as Query DSL, you can create a query via DSL.

Click on save () to save the query.

By clicking on the calendar (), a modal will open, and you will be able to select a time range to check security events.

In quick select, you can quickly choose a time range. You can determine whether the range applies to the last (Last) or upcoming (Next) moments, the amount, and the duration of the range. To apply, click on Apply.

Quick sele	ect				< >
Last	۵	24	hours	X	Apply
Last					
Next					

In Commonly used, you can use a pre-defined time range (e.g., last 15 minutes).

Commonly used	
Today	Last 24 hours
This week	Last 7 days
Last 15 minutes	Last 30 days
Last 30 minutes	Last 90 days
Last 1 hour	Last 1 year

In Recently used date ranges, you can reuse a time range.

Recently used date ranges

Aug 7, 2024 @ 10:30:30.820 to Aug 7, 2024 @ 10:30:30.840	1
Aug 7, 2024 @ 10:30:30.000 to Aug 7, 2024 @ 10:30:31.000	
Aug 7, 2024 @ 10:30:30.543 to Aug 7, 2024 @ 10:30:30.658	I
Aug 7, 2024 @ 10:30:30.000 to Aug 7, 2024 @ 10:31:00.000	l
Aug 7, 2024 @ 10:30:00.000 to Aug 7, 2024 @ 11:00:00.000	ļ
Last 6 dave	1

In Refresh every, you can set up automatic page refresh. You can determine the amount and duration of the interval. To apply, click on Start.

Refresh every



By clicking on the time field, you can select three ways to define the interval: Absolute: a specific date and time (e.g., 3:37 PM on October 15, 2023).

Absolute				Rel	ative	Now	
<	K Augu			st 2024			08:00
							08:30
SU	МО	TU	WE	TH	FR	SA	09:00
28	29	30	31	1	2	3	09:30
4	5	6	7	8	9	10	10:00
11	12	12	14	15	16	17	10:30
11	12	15	14	15	10	17	11:00
18	19	20	21	22	23	24	11:30
25	26	27	28	29	30	31	12:00

End date Aug 8, 2024 @ 10:55:07.878

Relative: a time interval relative to the present moment (e.g., 2 minutes ago).



Now: by setting the interval to "now," all updates will be made relative to the present moment. To refresh the page, click on Refresh.

XDR - First access

Blockbit XDR offers secure and flexible access for administrators and authorized users, ensuring enhanced protection through multiple authentication methods.

When accessing the platform, the user will be directed to the login screen, where they can authenticate using one of the following options:

- Local User + MFA: Uses credentials registered directly in Blockbit XDR, requiring a username, password, and a multi-factor authentication (MFA) token.
- SSO via LDAP + MFA: Allows integrated authentication with a corporate LDAP server, adding an extra layer of security with MFA.
- Authentication via SAML (Single Sign-On): Integrates with identity providers that support the SAML protocol (version 2.0 or higher), such as Microsoft Active Directory Federation Services (ADFS), Azure AD, Google Workspace, among others, enabling single sign-on with corporate credentials.

To log in, the user must enter their credentials in the form and, if configured, provide the MFA token. Alternatively, the "Log in with single sign-on" option can be used, which redirects to the SAML authentication flow.

This approach ensures greater security and compliance with corporate policies, facilitating access management and protecting against unauthorized access.

	je j
Blockbit	
Log in to Blockbit XDR	
R Username	
Password	
C MFA Token	
Log in	
Log in with single sign-on	

You will have to accept the terms and conditions (EULA) when accessing Blockbit XDR for the first time.

Terms of Service

CONTRATO DE LICENÇA PARA USUÁRIO FINAL

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

LICENCIAMENTO:

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

Accept

×

Click on Accept (

)to accept.

Accept
XDR - Dashboard

The **Blockbit XDR Dashboard** provides an intuitive and centralized interface, offering a comprehensive view of the environment's security in real-time. With interactive graphs, customizable panels, and prioritized alerts, administrators can monitor critical events, analyze threats, and make quick decisions. The structured workflow enables a swift response to incidents, including automated actions for risk mitigation, streamlining investigations, and ensuring efficient cybersecurity management.

This is the main space of Blockbit XDR. Here, you can monitor and manage threats and check the system status.

Overview

This section provides general information about ongoing threats. For more details, go to Overview.

Mitre ATT&CK



The Mitre ATT&CK is a framework of tactics (the reasons for an attack) and techniques (how an attack is conducted) and serves as the foundation of Blockbit XDR. All metrics are based on concepts from Mitre ATT&CK.

Each tactic or technique has a specific remedy, and Blockbit XDR has a reference database that can be consulted.

For more information, visit Mitre ATT&CK.

Graphics

Blockbit XDR provides visual representations of attack severity. For more information, go to Graphics.

Techniques

This section lists the main attack techniques and the associated events. An attack can use more than one technique simultaneously. For more information, go to Techniques.

XDR - Dashboard - Graphics

The Blockbit XDR features two charts divided into four sections. Each section represents 1/4 of a circle, with each segment showing attacks divided by severity. The closer to the center, the more severe the attacks.



It shows attacks point of entry:

- Network
- Files
- Application
- Operating System

World map



The sources of the attacks are displayed. The countries in red are the ones that originated attacks.

On the left, there is a ranking of the 15 countries that originated the most attacks.

To see the name of a country, hover over it. To zoom in, use the scroll wheel of your mouse.

XDR - Dashboard - Mitre ATT&CK

The Mitre ATT&CK is a framework of techniques and attack patterns. Each technique has a specific remedy. There are two concepts: **Technique:** how the attacker gains access to a system. **Tactic:** why the attacker enters a system.

For more information, visit Mitre ATT&CK.

In the Dashboard, attacks are classified according to severity and divided into 4 categories, which are further divided into 14 sublevels.

Pre-attack: preparation for the attack. Severity: **low**

- Reconnaissance: information gathering.
- · Resource development: establishing resources for future attacks.
- Initial access: attempting to breach the network.
- Execution: attempting to run malicious code.

Attack/Infection: attack attempts

Severity: medium

- Persistence: attempts to maintain the attack.
- Privilege escalation: attempts to gain higher-level permissions.
- Defense evasion: attempts to avoid defenses and go unnoticed.

Breach/Infestation: violation

Severity: high

- Credential access: attempts to steal usernames and passwords.
- Discovery: environment exploration.
- · Lateral movement: attempts to move through the environment.
- Collection: attempts to gather data.

Post-breach/Extraction: impact

Severity: Critical

- Command and control: attempts to communicate with compromised systems to control them.
- Exfiltration: attempts to steal data.
- Impact: attempts to manipulate, disrupt, or destroy a system or its data.

For more in-depth information about Mitre ATT&CK, visit attack.mitre.org.

XDR - Dashboard - Overview

Overview

Blockbit XDR offers an automatic alert correlation system, allowing events related to the same attack to be grouped and analyzed efficiently. This feature reduces response time and enhances the detection of complex threats, ensuring a unified view of the incident.

	AGEN	ITS		EVENTS	/ENTS - 24H 3 30D ALERTS - 24H 3 30D						
	Ager 48	nts		Tot 5	tal Events ,557,064	Total Alerts 5,557,040					
Active 37	Disconnected 11	Pending 0	Unrelated 0	Max EPS Current Storage (GB) 90 16.0		Critical 12	High 2	Medium 117,541	Low 5,439,486		

Agents

The agent is an XDR service installed on an endpoint (PC, notebook, virtual machine, cloud instance). It will protect the endpoint and respond to threats.

By clicking on the number of agents, you will go to their list. For more information, visit Agents.

- Active: active;
- Disconnected: disconnected;
- Pending: in the process of connecting;
- Unrelated: registered but not connected.

Events

Number of events in the selected period. In the switch, you can choose between 24 hours or 30 days.

- Total events: number of events in the selected period;
- Max EPS: events per second. The interval is 60 seconds;
- Current Storage: total logs of saved events.

Total alerts

Threats detected in the period. In the switch, you can choose between 24 hours or 30 days. Clicking on the alerts takes you to the Security Events page.

- Low: low severity;
- Medium: medium severity;
- High: high severity;
- Critical: critical severity.

XDR - Dashboard - Techniques

Here are the main attack techniques and the associated events. An attack can use more than one technique simultaneously.

			TECHNIQ	UES			
ІМРАСТ		EXFILTRATION		COMMAND AND CONTROL		COLLECTION	
T1565.001	8546	C There are no results.		D There are no results.		There are no results.	
T1485	1679					-	
T1531	56						
T1489	23						
LATERAL MOV	EMENT	DISCOVERY		CREDENTIAL ACCESS		DEFENSE EVASION	
T1021.004	57358	C There are no results.		T1110.001	78087	T1078.002	40650
T1550.002	40648			T1110	3043	T1550.002	40648
T1021.001	1648					T1078	13340
T1021	22					T1112	10123
						T1070.004	1679
PRIVILEGE ESCA	ALATION	PERSISTENCE		EXECUTION		INITIAL ACCESS	
T1078.002	40650	T1078.002	40650	There are no results		T1078.002	40650
T1078	13340	T1078	13340	-		T1078	13340
T1548.003	25	T1543.003	11				

The techniques are organized by decreasing severity and group associated tactics.

Hovering over any tactic will display a modal with more information.

Clicking will redirect you to the Security Events page with information on attacks using the selected tactic.

Only tactics associated with events are shown.

XDR - Security Events

This page provides a detailed view of all security events recorded by **Blockbit XDR**, allowing for in-depth analysis and facilitating real-time incident investigation.

When a threat is detected, the agent user receives a detailed notification, informing them of the action taken and the event details. This ensures transparency and a rapid response to incidents, enabling administrators to efficiently view and manage critical events.



Search

The bar allows you to search for specific events. For more information, see Search System.

Hits Chart

The hits chart shows how many security events (hits) occurred in the selected time frame. For more information, go to Hits.

Event List

Below the chart, the events are listed. For more information, go to Event List.

XDR - Security Events - Event list

Below the chart, the events are listed.

> Aug 7, 2024 @ 21:41:43.558	<pre>cluster.node: blockbit-xdr-manager-worker-0 cluster.name: blockbit-xdr input.type: log agent.ip: 192.168.2.10 agent.name: bb-xdr-proxy-geo agent.id: 002 data.protocol: POST data.srcip: 200.103.23.34 data.id: 403 data.url: /provisioning/checkProvisioning manager.name: blockbit-xdr-manager-worker-0 rule.firedtimes: 138,308 rule.mail: false rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.tsc: CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3 rule.description: Web server 400 error code. rule.groups: web, accesslog, attack rule.id: 31101 rule.nist_800_53: SA.11,</pre>
> Aug 7, 2024 @ 21:41:43.558	<pre>cluster.node: blockbit-xdr-manager-worker-0 cluster.name: blockbit-xdr input.type: log agent.ip: 192.168.2.10 agent.name: bb-xdr-proxy-geo agent.id: 002 data.protocol: POST data.srcip: 177.222.235.83 data.id: 403 data.url: /provisioning/checkProvisioning manager.name: blockbit-xdr-manager-worker-0 rule.firedtimes: 138,315 rule.mail: false rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.tsc: CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3 rule.description: Web server 400 error code. rule.groups: web, accesslog, attack rule.id: 31101 rule.nist_800_53: SA.11,</pre>
> Aug 7, 2024 @ 21:41:4:⊕ ∈	cluster.node: blockbit-xdr-manager-worker-0 cluster.name: blockbit-xdr input.type: log agent.ip: 192.168.2.10 agent.name: bb-xdr-proxy-geo agent.id: 002 data.protocol: POST data.srcip: 45.229.241.156 data.id: 403 data.url: /provisioning/checkProvisioning manager.name: blockbit-xdr-manager-worker-0 rule.firedtimes: 138,318 rule.mail: false rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.tsc: CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3 rule.description: Web server 400 error code. rule.groups: web, accesslog, attack rule.id: 31101 rule.nist_800_53: SA.11,

Clicking on an event will give you access to all its information in table or JSON format. For more information, visit Collected Data.

XDR - Security Events - Hits

The hits chart shows how many security events (hits) occurred in the selected time frame.



Hovering over a column will display the selected time interval and the number of hits.

Clicking on a column will divide the selected interval.

The interval divisions are as follows: Year - Month - Week - Day - Hour - Minute - Second - Millisecond.

XDR - Security Events - Notifications

On Windows, when a threat is detected, a notification will appear for the agent user where the event was detected.



This notification will describe the action taken by Blockbit XDR and display a message with the action the user should take.

The "More Information" button allows the user to access detailed information about the threat.

The "Close" button closes the notification.

XDR - Security Events - Ransomware Events

Blockbit XDR Administrator Guide: Detection, Correlation, and Response to Ransomware Incidents

1. Introduction

Blockbit XDR is an advanced security solution that enables the detection, correlation, and response to ransomware incidents using multiple analysis vectors and automated response. This guide is designed to assist administrators in investigating and mitigating attacks by filtering with rule.group and applying containment and recovery actions.

2. Identifying Ransomware-Related Events

2.1 Applying Filters

To begin analyzing a potential ransomware attack, use the rule.group="ransomware" filter in the Blockbit XDR event panel:

- 1. Access the Security Events interface.
- 2. In the search field, enter "ransomware" or use the filter rule.group=ransomware.
- 3. View the events related to ransomware detection in the environment.

Blockbit				
Security Events				a
♥ ransomware			DQL 🛗 🗸 Last 24 hours	Show dates C Refresh
agent.name: XDR_POC_WINDOWS ×	+ Add filter			
blockbit-xdr-alerts-* \checkmark			5 hits	
Search field names		Mar 17, 2025 @ 18:18:38.44	43 - Mar 18, 2025 @ 18:18:38.443 Auto 🔍	
Filter by type 0	5			
Selected fields	4			
ⓓ _source	3 3			
Available fields	Č 2			
t_index	1			
t agent.id	21:00	00:00 03:00	06:00 09:00	12:00 15:00 18:00
👔 agent.ip			timestamp per 30 minutes	
t agent.name	Time 🗸	_source		
t cluster.name	Mar 18, 2025 @ 18:18:11,806	A STATE AND DOC MENDONE Full last	blackbib udo antico anno 10 martin 0.1 Ma	aiainy. (yaaany yklaskii oo aaaaa oo ka
t cluster.node	, Mar 10, 2025 @ 10.10.11.000	<pre>o agent.name: XDR_POC_WINDOWS Tull_log:</pre>	add"."parameters":{"extra_args":["-title"."Ac\'	rigin":{"name":"DlockDit-xdr-manager-worker-
t data.command		action", "Bloqueio", "de", "rede", "efetua	ido.","-	
t data.extra_data		message","Caso","tenha","du\\x27vida,"	,"entre","em","contato","com","seu","administra	ador","de","rede."],"alert":{"timestamp":"2025-
t data.id		03-18T21:13:34.355+0000","rule":{"leve	el":12,"description":"Volume shadow copy deleted	d using VSSADMIN.EXE. Potential <mark>ransomware</mark>
t data.origin.module	Mar 18, 2025 @ 18:18:11.443	agent name: XDD DOC WINDOWS rule group	une, malware rancomware rancomware are detect	ion cluster node: blockbit_vdr_manager_worker_
t data.origin.name	, , ,	0 cluster.name: blockbit-xdr syscheck	<pre>k.mode: realtime syscheck.path: c:\users\xdr-pd</pre>	ac\desktop\antitamper_new\bkp\how to restore
t data.parameters.alert.agent.id		your files.txt syscheck.shal_after: al	bee599dc58c21a7cacf4bc6a727fee782df8b23 sysche	ck.uname_after: xdr-poc
t data.parameters.alert.agent.ip		syscheck.mtime_after: Mar 14, 2025 @ 0	09:20:27.000 syscheck.attrs_after: ARCHIVE sys	scheck.size_after: 1,475 syscheck.uid_after: S-
t data.parameters.alert.agent. name		1-5-21-1579519592-3895728182-791390580	-1002 syscheck.win_perm_after: { "allowed": ["DELETE", "READ_CONTROL", "WRITE_DAC",
t data.parameters.alert.cluster. name	> Mar 18, 2025 @ 18:18:07.610	<pre>agent.name: XDR_POC_WINDOWS rule.grou 0 cluster.name: blockbit-xdr svscheck</pre>	<pre>ups: malware, ransomware, ransomware_pre_detect <.mode: realtime syscheck.path: c:\users\xdr-po</pre>	<pre>ion cluster.node: blockbit-xdr-manager-worker- oc\downloads\how to restore your files.txt</pre>
t data.parameters.alert.cluster. node		syscheck.shal_after: abee599dc58c21a7	cacf4bc6a727fee782df8b23 syscheck.uname_after:	xdr-poc syscheck.mtime_after: Mar 14, 2025 @

Incident Start Logs

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

t data.win.eventdata. authenticationPackageName

Displays a pre-detection ransomware alert.

Blockbit										
Security Events										a
ତ ∽ Search					DQL	*	Last 24 hours		Show dates	ී <u>Refresh</u>
agent.name: XDR_POC_WINDOWS ×	rule.gro	oups: ransomware × + Add filte	r							
blockbit-xdr-alerts-* \checkmark					5 hi	ts				
Search field names			Mar	17, 2025 @ 18:24:27.860) - Mar 18, 2	025 @ 18:	24:27.860 Auto	C		
 Filter by type Selected fields 		5								
_source Available fields	Count	3								
Popular t rule.groups		0 21:00	00:00	03:00	06:00	2	09:00	12:00	15:00	18:00
t_index					timestamp ;	per 30 minu	ites			
t agent.id		Time 🚽	_source							
t agent.ip t agent.name	>	Mar 18, 2025 @ 18:20:10.8	45 agent.name: XDR_F cluster.name: blo	OC_WINDOWS rule.group	s: <mark>ransomwa</mark> log agent	are, ranso ip: 192.	omware_rollback cluste	r.node: blockbit 406 manager.name	-xdr-manager-worker-6	er-worker-0
t cluster.name			data.rollback_sta	tus: File restore comp le.description: BBXDR_	Ransomware	_Protection	FAA43M at 03/14/2025 0 on: Files restored suc	essfully. rule.fir	id: 100800 location:	active-
t data.command			response\active-r	esponses.log decoder.r	ame: BBXDR	_Ransomwa	re id: 1742332810.833	241546 full_log:	BBXDR_Ransomware_Pro	tection: File
t data.extra_data	>	Mar 18, 2025 @ 18:18:11.4	43 agent.name: XDR_F	OC_WINDOWS rule.group	s: malware	, <mark>ransomwa</mark>	are, <mark>ransomware</mark> _pre_de	tection cluster.	node: blockbit-xdr-ma	nager-worker-
t data.id			0 cluster.name: b	lockbit-xdr syscheck.	mode: real	time sysc	heck.path: c:\users\xc	r-poc\desktop\an	titamper_new\bkp\how	to restore
t data.origin.module			syscheck.mtime af	scheck.snal_atter: abe ter: Mar 14, 2025 @ 09	e599dc58c2	svscheck	<pre>c6a/2/Tee/820T8D23 System c.attrs after: ARCHIVE</pre>	svscheck.size a	fter: 1,475 syscheck	.uid after: S-
t data.parameters.alert.agent.id			1-5-21-1579519592	-3895728182-791390580-	1002 sysch	eck.win_p	erm_after: { "allowed"	: ["DELETE", "RE	EAD_CONTROL", "WRITE_	DAC",
t data.parameters.alert.agent.ip	>	Mar 18, 2025 @ 18:18:07.6	10 agent.name: XDR F	OC_WINDOWS rule.group	s: malware	, <mark>ransomw</mark>	are, <mark>ransomware</mark> pre de	tection cluster.	node: blockbit-xdr-ma	mager-worker-
t data.parameters.alert.agent. name			0 cluster.name: b	olockbit-xdr syscheck.	mode: real	time sysc fee782df8	heck.path: c:\users\xc	r-poc\downloads\	how to restore your f	files.txt
+ data narametere alert chieter										,e

Applying the rule.group="ransomware" filter.

3. Event Correlation

After identifying suspicious events, analyze the detailed logs to correlate malicious activities.

3.1 Log Analysis

• Identify alerts related to ransomware and malware.

- Check the origin of the event (agent.name, agent.ip, cluster.node).
- Analyze logs indicating suspicious activities, such as:
 - $^{\circ}~$ Mass creation and deletion of files.
 - Execution of suspicious commands (e.g., VSSADMIN.EXE deleting shadow copies).
 - ° Unknown processes making modifications to the system structure.

\$ Blockbit			^
Security Events		•	
tactic	<pre>t data.win.system.threadID</pre>	2596	-
t data.parameters.alert.rule.mitre. technique	t data.win.system.version	5	
t data.parameters.alert.rule. nist_800_53	t decoder.name	windows_eventchannel	
t data.parameters.alert.rule. pci_dss	e ् 🗉 🐻 t full_log	>	
t data.parameters.alert.rule.tsc		{"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-06f569 8ffbd9}" "eventTD":"!" "version":"5" "]evel":"4" "task":"!" "opcode":"8" "keywords":"4x88888888888888888888	
t data.parameters.alert.timestamp		ystemTime":"2025-03-14T12:20:42.7313626Z","eventRecordID":"190271","processID":"2112","threadID":"2596","ch	
t data.parameters.extra_args		annel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-3FAA43M","severityValue":"INFORMATION","m essage":"\"Process Create:\r\nRuleName: technique id=T1059.technique name=Command-Line Interface\r\nUtcTim	1
t data.parameters.program		e: 2025-03-14 12:20:42.727\r\nProcessGuid: {b6270aa7-1f1a-67d4-181a-000000001100}\r\nProcessId: 8476\r\nIma	
t data.protocol		GP ('''WINDAWE'''''VECENTRY/''VECENTRIA PVP'F'NFI PVPEEDAD' IN N IMMAI I WINKIIIA IMMINI MANNI'F'NDEEFFINTION'	
t data.rollback_status	t lu	1/423326/5.814518123	1
t data.sca.check.command	t input.type	log	
t data.sca.check.compliance.cis	t location	EventChannel	
t data.sca.check.compliance. cis_csc	t manager.name	blockhit-xdr-manager-worker-0	
t data.sca.check.compliance. gdpr_IV	t rule.description	Ransomware activity detected.	
t data.sca.check.compliance. gpg_13	# rule.firedtimes	1	
t data.sca.check.compliance. gpg13	<pre># rule.frequency</pre>	2	
t data.sca.check.compliance.hipaa			
t data.sca.check.compliance. nist_800_53	t rule.groups	<pre>ransomware, ransomware_detection</pre>	
t data.sca.check.compliance. pci_dss	t rule.id	100628	
t data.sca.check.compliance.tsc	# rule.level	12	
t data.sca.check.description	Q rule mail		
t data.sca.check.id	· Foreinare	Li ue	
t data.sca.check.rationale	🛗 timestamp	Mar 18, 2025 @ 18:17:55.295	

Logs confirming the attack.

4. Automated Responses and Mitigation Actions

Blockbit XDR allows marking a complete group of events or isolated events as a threat and initiating response and mitigation actions.

4.1 Machine Isolation on the Network

If Blockbit XDR detects an ongoing ransomware attack:

- Stops processes related to the attack.
- Isolates the endpoint to prevent malware spread.
- Isolates the suspicious file.
- Restores deleted or encrypted files to their pre-attack state.
- Finally, reverts data events to a secure state.

Blockbit		
Security Events		
t_index		timestamp per 30 minutes
t agent.id	Time 🚽	_source
t agent.ip	> Mar 18, 2025 @ 18:20:10.845	agent.name: XDR_POC_WINDOWS rule.groups: ransomware, ransomware_rollback cluster.node: blockbit-xdr-manager-worker-0
t agent.name		cluster.name: blockbit-xdr input.type: log agent.ip: 192.168.66.103 agent.id: 406 manager.name: blockbit-xdr-manager-worker-0
t cluster.name		data.rollback_status: File restore completed for DESKTOP-3FAA43M at 03/14/2025 09:26:48 rule.firedtimes: 1 rule.mail: false
t cluster.node		rule.level: 5 rule.description: BBXDR_Ransomware_Protection: Files restored successfully. rule.id: 100800 location: active-
t data.command		response\active-responses.log decoder.name: BBXDR_Ransomware id: 1742332810.833241546 full_log: BBXDR_Ransomware_Protection: File
t data.extra_data	> Mar 18, 2025 @ 18:18:11.443	agent.name: XDR_POC_WINDOWS rule.groups: malware, ransomware, ransomware_pre_detection cluster.node: blockbit-xdr-manager-worker-
t data.id		0 cluster.name: blockbit-xdr syscheck.mode: realtime syscheck.path: c:\users\xdr-poc\desktop\antitamper_new\bkp\how to restore
t data.origin.module		your files.txt syscheck.shal_after: abee599dc58c21a7cacf4bc6a727fee782df8b23 syscheck.uname_after: xdr-poc
t data.origin.name		syscheck.mtime_after: Mar 14, 2025 @ 09:20:27.000 syscheck.attrs_after: ARCHIVE syscheck.size_after: 1,475 syscheck.uid_after: S-
t data.parameters.alert.agent.id		1-5-21-1579519592-3895728182-791390580-1002 syscheck.win_perm_after: { "allowed": ["DELETE", "READ_CONTROL", "WRITE_DAC",
t data.parameters.alert.agent.ip) Mar 18, 2025 @ 18:17:5€⊕ ⊖	full_log: {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-
t data.parameters.alert.agent. name		06f5698ffbd9}","eventID":"1","version":"5","level":"4","task":"1","opcode":"0","keywords":"0x80000000000000","systemTime":"2025-
t data.parameters.alert.cluster.		<pre>Sysmon/Operational","computer":"DESKTOP-3FAA43M","severityValue":"INFORMATION","message":"\"Process Create:\r\nRuleName:</pre>
t data.parameters.alert.cluster.		technique_id=T1059,technique_name=Command-Line Interface\r\nUtcTime: 2025-03-18 20:38:40.193\r\nProcessGuid: {b6270aa7-d9d0-67d9-
node	Mar 18, 2025 @ 18:17:55,295	anant asmay VDD DOC WINDOWS guila groups, cancemare detection glupter ander blackbit-ydr-mananer-warker-0
(b) data.parameters.alert.data.win. eventdata.commandLine	,	cluster.name: blockbit-xdr input.type: log agent.jp: 192.168.66.103 agent.id: 406 manager.name: blockbit-xdr-manager-worker-0
data.parameters.alert.data.win. eventdata.company		data.win.eventdata.originalFileName: VSSADMIN.EXE data.win.eventdata.image: C:\\Windows\\System32\\vssadmin.exe
data.parameters.alert.data.win. eventdata.currentDirectory		uata.win.eventoata.product: wircosoft" Windows" Uperating System uata.win.eventoata.parentProcessGuid: {b6278aa7-lfla-67d4-l6la- 000000001100} data.win.eventdata.description: Command Line Interface for Microsoft® Volume Shadow Copy Service
(ata.parameters.alert.data.win. eventdata.description	> Mar 18, 2025 @ 18:13:34.355	agent.name: XDR_POC_WINDOWS rule.groups: malware, ransomware, ransomware_pre_detection cluster.node: blockbit-xdr-manager-worker-
(1) data.parameters.alert.data.win.		0 cluster.name: blockbit-xdr input.type: log agent.ip: 192.168.66.103 agent.id: 406 manager.name: blockbit-xdr-manager-worker-0
data parameters alert data win		data.win.eventdata.originalFileName: VSSADMIN.EXE data.win.eventdata.image: C:\\Windows\\System32\\vssadmin.exe
eventdata.hashes		data.win.eventdata.product: Microsoft® Windows® Operating System data.win.eventdata.parentProcessGuid: {b6270aa7-lefb-67d4-ff19-
@ data.parameters.alert.data.win. eventdata.image		000000001100} data.win.eventdata.description: Command Line Interface for Microsoft® Volume Shadow Copy Service

Log of endpoint isolation action.

4.2 Reverting System Changes

Blockbit XDR can undo any changes made by an attack, restoring system configurations, registry edits, and file permissions.

4.3 File and Data Recovery

For Windows systems, **Blockbit XDR** can recover destructive events, restoring deleted or encrypted files from ransomware automatically or via the administration console.

To confirm, check if the rollback was activated in the event (data.rollback_status).

Verify the successful restoration through logs in the event panel.

Blockbit													
Security Events													a
🗑 🗸 Search							DQL	*	Last 24 hours			Show dates	C Refresh
agent.name: XDR_POC_WINDOWS ×	rule.group	s: ransomware $ imes$	+ Add filter										
blockbit-xdr-alerts-* \lor							5 h	its					
Search field names					Mar 17, 202	5 @ 18:24:27	.860 - Mar 18, 3	2025@1	8:24:27.860	iuto 🔍			
 Filter by type 	5												
Selected fields	4												
() _source	3 ount												
Available fields	0 2												
Popular	,												
t rule.groups			21:00	00:00		03:00	06:0	0	09:00		12:00	15:00	18:00
t_index							timestamp	per 30 m	nutes				
t agent.id	1	ïme 🗸		_source									
t agent.ip		lar 18, 2025 @	18:20:10.845	agent.name:	XDR POC WIND	NOWS rule.gr	ouns: ransom	vare, rai	somware rollb	ack cluster.n	ode: blockb	it-xdr-manager-worker-	θ
t agent.name				cluster.nam	e: blockbit-x	dr input.ty	pe: log agen	t.ip: 19	2.168.66.103	agent.id: 406	manager.na	me: blockbit-xdr-manag	er-worker-0
t cluster.name				data.rollba	ck_status: Fi	ile restore o	completed for	DESKTOP	-3FAA43M at 03	8/14/2025 09:2	6:48 rule.f	iredtimes: 1 rule.mai	l: false
t cluster.node				rule.level:	5 rule.desc	ription: BB)	(DR_Ransomware	_Protect	ion: Files re	stored success	sfully. rule	e.id: 100800 location:	active-
t data.command				response\ac	tive-responses	s.log decode	er.name: BBXD	R_Ransom	ware id: 1742	332810.8332415	546 full_log	g: BBXDR_Ransomware_Pr	otection: File

Example of a restored file action log protected by Blockbit XDR.

5. Playbooks for Incident Resolution

Blockbit XDR enables automated event correlation and efficient threat response. This chapter provides detailed procedures for dealing with ransomware attacks, meeting the requirements of the security policy.

5.1 Playbook – Automatic Detection and Containment

Blockbit XDR automatically correlates alerts related to the same attack (Item 14), allowing rapid containment and mitigation of threats.

Steps:

Automatic Event Filtering:

- Use rule.group=ransomware to identify suspicious activities.
- The system automatically correlates events related to the same attack, grouping them for easier analysis.

Automatic Log Analysis and Response Activation:

- Blockbit XDR applies custom rules to trigger detections automatically.
- When a threat is detected, automatic actions can be configured for immediate response.

Automatic Endpoint Isolation:

- XDR can mark a complete group of events or isolated events as a threat and initiate response and mitigation actions.
- If malicious behavior is detected, the infected machine can automatically be removed from the network via Active Response.
- A customized Playbook can also be applied using rule.groups or rule.id via the API, enhancing the incident response and enabling automated, customized actions as per the environment's needs.

Additional Firewall Blocks:

Based on correlated events, XDR can apply firewall rules to block malware communication with external servers.

Automatic Escalation to Security Team:

If an attack is detected and automated measures are insufficient, alerts can be sent to the SOC team for additional actions.

5.2 Playbook – Recovery and Remediation

If ransomware has caused impacts, Blockbit XDR offers automated recovery and remediation mechanisms.

Steps:

Confirming Automatic Rollback:

- The system automatically checks the integrity of the entire system, including files, system configurations, registry, and file permissions (data. rollback status).
- If the system has been compromised or files encrypted, **Blockbit XDR** triggers recovery, restoring files, system configurations, registry edits, and file permissions—essentially restoring the entire system.

Running Malware Scan and System Fix:

- · After containment, XDR can automatically initiate an advanced scan on endpoints to remove malicious files.
- System configurations can be automatically restored to secure standards.

Reactivating the Endpoint and Returning to the Network:

After complete mitigation, Blockbit XDR automatically removes the machine's restrictions and reintegrates it back into the network.

Marking Events and Incident Reporting:

• The administrator can mark a group of events as a completed threat and generate reports for auditing and future security improvements.

6. Conclusion

These features ensure that **Blockbit XDR** not only detects but also responds and mitigates threats automatically, reducing response time and minimizing operational impact.

With this guide, the administrator can operate the solution efficiently, ensuring advanced protection against ransomware and other emerging threats.

XDR - Custom Dashboards

Blockbit XDR allows you to create custom visualizations and dashboards according to your network needs.

Clicking on Custom Dashboard will take you to the list of created dashboards.

Custom Dasht	poards		① Cr	eate Dashboard
🔍 Search				
Title	Туре	Description	Last updated	Actions
JG	Dashboard		Oct 11, 2024 @ 16:46:55.056	Ø
JG Copy	Dashboard	aaaa	Oct 11, 2024 @ 16:47:11.653	Ø
jg dash 3	Dashboard		Oct 14, 2024 @ 17:25:31.819	Ø
Rows per page: 20 🗸				$\langle \underline{1} \rangle$

Use the Search bar to find a specific dashboard.

To create a dashboard, click on Create Dashboard.

Dashboards are classified by:

- Title: Title of the dashboard
 Type: Type of the dashboard
 Description: Description of the dashboard
 Last updated: Time of the last dashboard edit

The Actions button (

XDR - Custom Dashboards - Create Dashboard

By clicking on Create Dashboard, you will be directed to this page.

Search	DQL	m ~	Last 24 hours	Show dates	ි Refresh
😇 — + Add filter					
Add an existing or new object to this dashboard					
Constanting of the					
+ Create new					

Search

The bar allows you to search for specific events. For more information, refer to the Search System.

Here, you can add a visualization to the dashboard by clicking Add an existing or new object to this dashboard.

A modal will open with a list of already created visualizations:

Add panels			×
🔍 Search	Sort ∨	Types 4 V	① Create new
lucas			
如 MAPS			
å8 ok			
🗠 savejv			
m Teste1			
teste121 teste121			
lᡜ testejv			

To select a visualization, click on it to add it to the dashboard. To find a specific visualization, use the Search bar.

In Sort, you can arrange the visualizations in ascending or descending order.

In **Types**, you can filter visualizations by type.

Sort ∨	Types 4 🗸	① ① Create new
Visuali	zation	•
VisBui	der	
Maps		
Saved	search	-

To create a new visualization, click on **Create new** (^{① <u>Create new</u>})

A modal with the available visualizations will open:

New Visualization Select a visualization type 🔍 Filter Start creating your visualization by selecting Е a type for that visualization. ≌ 0 == \simeq Controls Coordinate Map Data Table Area 3 63 Document Table Enhanced Table Gantt Chart Gauge **°** R ര N Goal Heat Map Horizontal Bar Line $\{\hat{\mathbf{T}}\}$ Q æ 8

XDR - Custom Dashboards - How to - Create visualization

In this how-to, you will learn how to create a Gauge visualization for the data rule.frequency.

After clicking on Dashboards > Create new, select Gauge in the modal.

Select a data source. Here, blockbit-xdr-alerts- has been selected.

New Gauge / Choose a source			
Q Search	Sort \checkmark	Types 2	\sim
. <u>blockbit-xdr-alerts-*</u>			
blockbit-xdr-mor blockbit-xdr-alerts-* (Index pattern)			
blockbit-xdr-states-vulnerabilities-*			
blockbit-xdr-statistics-*			

You will go to this screen:



The chart in question counts all the data from the source.

Click on Metric count.

A submenu will open.

In Aggregation, select Average.

Metrics

∨ Metric	
Aggregation	Average help 🕑
Average	~
Metric Aggregations	-
✓ Average	
Count	
Max	
Median	
Min	
Sum	-

In Field, rule.frequency has been selected.

Click on Update.

The screen will display the average of the rule.frequency data in the blockbit-xdr-alerts- data source in relation to the total data.



XDR - Custom Dashboards - Visualizations

In Blockbit XDR, the following visualizations are available:



Area

This type of visualization allows you to track changes over time.

Controls

This option allows you to build dynamic visualizations.

Coordinate Map

This visualization allows you to track data on a world map based on geographic coordinates.

Data Table

This visualization allows you to create tables comparing numerical values.

Document Table

Similar functionality to Data Table but comparing document content.

Enhanced Table

Similar functionality to Data Table with additional features.

Gantt Chart

Charts that show the start, end, and duration of events.

Gauge

Charts that show how much of a resource has been used.

Goal

Charts that show how much is left to reach a goal.

Heat Map

A chart that shows the frequency of an event over time.

Horizontal Bar

A chart that represents the variation of a categorical data over time horizontally.

Line

A chart that summarizes changes in a variable over time.



Maps

A tool that allows the creation of maps with various information.

Markdown

A tool that allows the creation of objects using Markup language.

Metric

A tool that allows the comparison of different numerical values.

Pie

A chart that represents the percentage of each component within a whole.

Region Map

A tool that allows you to track events classified by location.

TVSB

The time-series visual builder is a tool that allows the creation of time-based visualizations.

Tag Cloud

Word cloud. Allows visualization of word usage frequency.

Timeline

A timeline. Allows visualization of data over time.

Vega

A visualization grammar that allows the creation, sharing, and saving of interactive visualization data. For more information, visit https://vega.github.io/.

Vertical Bar

A chart that represents the variation of a categorical data over time vertically.

VisBuilder

Drag and drop tool for creating visualizations.

For an example of creating a visualization, visit the How To.

XDR - Reports

On this page, you can access the reports generated by the Analyzer. All reports produced by Blockbit XDR are stored here.

🍳 Search				C Refresh
File	Size	Created ψ	Actions	
blockbit-xdr-module-overview-pm- 1723138691.pdf	57.98KB	Aug 8, 2024 @ 14:38:13.269	ம் பீ	
Rows per page: 10 🗸				$\langle \underline{1} \rangle$

In Search, you can look for specific reports.

Clicking on Refresh will update the list of reports.

The list of reports is sorted by:

- File: name of the report file.
- Size: size of the report file.
- Created: date and time the report file was created.

In Actions, you can:

- Download the report file in Download report.
 Delete the report file in Delete report.

The report will be generated in PDF.

blockbit-xdr-module-agents-020-general-1742283313.pdf	1 / 9 - 100% + 🗄 🕎		* 0
Brook com	Blockbit	contato@blockbit.com https://www.blockbit.com	
	Threat hunting report		
1	ID Name IP address Version Manager	Operating Registration date Last keep alive system	
Bleashit	020 thyterroom issues both blockbit-xdr- manager- worker-0	Microsoft Dec 26, 2024 @ Mar 18, 2025 @ Windows 10 Pro 16:44:37,000 04:35:05.000 10.0.19043.2130	
	Groups: default, PD, TI		
	Browse through your security alerts, identifying issues	and threats in your environment.	
	© 2025-03-17T04·34·16 to 2025-03-18T04·34	16	
2			
Bitechit sector	Alert groups evolution		
з	26- 1.1.1 (10) (10) (10) (10) (10) (10) (10) (10	210 8/4 630	
	Top 5 rule groups		

XDR - Endpoint Control Center

The **Blockbit XDR Endpoint Control Center** allows the creation and application of security policies for endpoints, by endpoint, groups, and subgroups, located across multiple sites, locations, departments, and geographically separated environments. The configurations include firewall rules, USB port control, and Bluetooth control. With this functionality, administrators can remotely manage security policies, ensuring protection and compliance on a large scale.

Blockbit XDR agents are capable of receiving schedules directly from the administration console, enabling the application of policies either individually or in bulk. This facilitates centralized and efficient management, reducing the time required to configure and distribute security rules across multiple devices.

Key Features

Creation and Application of Firewall Policies

Allows the definition of traffic filtering rules, controlling network communications on endpoints to ensure the security and integrity of the environment.

USB and Bluetooth Port Management

Enables the creation of rules to block, restrict, or allow the use of USB devices and Bluetooth connections, preventing data leakage and attacks via removable media.

Policy Distribution and Automation

Agents receive security policies directly from the console and can apply them automatically, ensuring fast and efficient deployment across multiple devices simultaneously.

The created policies are listed on the main page.

Firewall Policies (2) Search		C'Refresh
Policy name	Operating system	Actions
Webinar	iii windows	▷ ℓ む
Novo teste jv	iii windows	▷ 🖉 宦
Rows per page: 10 V		< 1 >

- To search for a specific policy, use the search bar.
- To refresh the list, click Refresh.
- To create a policy, click Create Policy (
- To select visible fields in the list, click the gear icon (

List Fields:

- **ID:** Unique identifier of the policy.
- Policy Name: Name of the policy.
- Operating System: The OS where the policy will be applied.
- Actions: Available actions:

	-
	~

Deploy Commands (): Apply the policy. Clicking this button will require multi-factor authentication. For more details, visit Multi-Factor Authentication. The requirement for MFA (Multi-Factor Authentication) when applying policies reinforces security, preventing unauthorized modifications and ensuring that only properly authenticated administrators can implement critical changes in the

environment.

Û

): Delete the policy.

• Delete (

	▲ Warning!	
Policy name	To ensure security, Multi-Factor Authentication (MFA) confirmation is required to proceed with this action.	Actions
	Info You are about to confirm the deployment of the configuration: Ballians Windows Sustam. This action will	
	apply the specified settings. Please review the details carefully before proceeding.	
	MFA Code	
	Cancel Confirm	
	windows	

60

XDR - Endpoint Control Center - Create policy

Creating a Policy in Blockbit XDR

To create a policy, click the **Create Policy** (• Create Policie) button.

Endpoints

In the Endpoints tab, you define which endpoints the policy will apply to.

Endpoints General Advanced	
Basic Settings	
Policy Name	
um dois	
Select Operating System	
Windows	
Agents / Groups	
Select Agents	
Select agents	
Select Group	
Select agent groups	

- Policy Name: Set the policy name.
- Select Operating System: Choose the operating system.
- Select Agents: Select the agents to apply the policy to.
- Select Group: Select the group to apply the policy to.

General

In the General tab, you create policies.

Endpoints Gene	Advanced					
Bluetooth Policie	S					
C Enable All						
Device Name		Device Type		Action		Actions
Device Name		Device Type	No ite	Action ems found		Actions

Bluetooth Policies

Here, you define policies for Bluetooth connections.

- The Enable All (Enable All) switch allows all peripherals except the listed ones (default setting).
 Switching to Disable All blocks all peripherals except the listed ones.

To create a policy, click Add	Policy (Add Policy) and	d configure:		
Device Name	Device Type	Action		Actions
Enter device name	External	Seny Deny	۹.	Ē
 Device Name: Enter Device Type: Select 	er the peripheral's name. ct Internal (built-in) or Externa	I (removable).		

Action: Choose Allow (permit) or Deny (block).

	Ē	
To delete a policy, click the trash icon ().

USB Policies

Enable All			
Serial Number	Device Type	Action	Actions
	Enter device type	Read-Only Access	Ê
	Enter device type	Read-Only Access	Ê
Enter serial number	SanDisk Cruzer Blade USB Devic	Allow All Devices	Ê
Enter serial number	General USB Flash Disk USB Devic	e Full Block 🔍	Ê

Here, you define policies for USB-connected peripherals.

- The Enable All (Enable All) switch allows all peripherals except the listed ones (default setting).
 Switching to Disable All blocks all peripherals except the listed ones.

To create a policy, click Add USB Policy (Add USB Policy) and configure:

- Serial Number: Enter the device's serial number.
- Device Type: Enter the type of device.
- Action: Choose from Allow All Devices, Read-Only Access, or Full Block.

	Ê
To delete a policy, click the trash icon ().

Firewall Rules

Domain	Source IP	Destination IP	Port	Protocol		Direction	Action	Action
Public Doma 🔍				TCP	۹	Inbound 🔍	Allow 🔍	Ê
Public Doma 🔍				TCP	۹	Outbound 🍳	Allow 🔍	Û
Public Doma 🔍				TCP	۹	Inbound 🔍	Block 🔍	Û
Domain 🔍				ТСР	۹	Outbound 🔍	Allow 🔍	Û

Here, you can create firewall rules.

To create a rule, click Add Firewall Rule (

Add Firewall Rule
) and configure:

- Domain: Select Public Domain, Private Domain, or Domain.
- Source IP: Enter the source IP.
- Destination IP: Enter the destination IP.
- Port: Enter the port(s), separating multiple ports with commas (e.g., 1000, 2000 or 5000-5500).
- **Protocol:** Select the protocol.
- Direction: Choose Inbound (incoming) or Outbound (outgoing).
- Action: Choose Allow (permit) or Deny (block).

To delete a policy, click the trash icon ($\ensuremath{\textcircled{\sc b}}$).

Note: Firewall rules set by Blockbit XDR always take precedence over locally configured firewall rules on the endpoint, ensuring centralized and effective network security management.

Advanced Settings

In Advanced Settings, you can enter direct commands.

Advanced Settings

Warning! Be careful when entering commands! Any executed configuration is your sole responsibility.	
Script Commands	
	Î

• To cancel, click Cancel (





XDR - Endpoints Summary

On this page, you can view available endpoints.

The first screen is a list of available agents.

Agents (46)						G	Refresh 쇼 Export forma	tted 💿
Search							DQL	C Refresh
Name	IP address	Group(s)	Operating system	Cluster node	Version	Last keep alive 🛆	Status	Actions
kali-linux-bob	192.168.0.5	default	A Kali GNU/Linux 2024.3	blockbit-xdr-manager-worker-0	v1.0.0	Sep 5, 2024 @ 13:38:00.000	• active ⑦	<u>ه</u> کې
qaubt	172.31.250.92	default	(Å) Ubuntu 22.04.4 LTS	blockbit-xdr-manager-worker-0	v1.0.0	Sep 5, 2024 @ 13:37:57.000	active	۵ کې
xdr-win11-vm	172.23.53.200	default	Microsoft Windows 11 Pro 10.0.22000.2652	blockbit-xdr-manager-worker-0	v1.0.0	Sep 3, 2024 @ 16:19:00.000	disconnected ③	۵ کې
Ipereira-win10	172.25.0.11	default	Microsoft Windows 10 Pro 10.0.19045.4529	blockbit-xdr-manager-worker-0	v1.0.0	Sep 4, 2024 @ 10:33:52.000	disconnected ③	۵ ٩,
jcarvalhal-note	172.16.12.173	default	Microsoft Windows 11 Pro 10.0.22000.2538	blockbit-xdr-manager-worker-0	v1.0.0	Sep 5, 2024 @ 13:38:00.000	• active ⑦	۵ کې
eliezer-linux	192.168.0.107	default	👌 Ubuntu 24.04.1 LTS	blockbit-xdr-manager-worker-0	v1.0.0	Sep 5, 2024 @ 13:37:55.000	• active ①	@ &s
gschristofano	172.16.12.163	default	Microsoft Windows 10 Pro 10.0.19045.3803	blockbit-xdr-manager-worker-0	v1.0.0	Sep 5, 2024 @ 13:38:02.000	• active ⑦	<u>ه</u> کې
tleite	192.168.10.104	default	Microsoft Windows 10 Pro 10.0.19044.3086	blockbit-xdr-manager-worker-0	v1.0.0	Sep 5, 2024 @ 13:25:51.000	disconnected ③	۵ کې
bb-xdr-proxy-geo	192.168.2.10	default	(Å) CentOS Linux 7.9	blockbit-xdr-manager-worker-0	v1.0.0	Sep 5, 2024 @ 13:37:56.000	• active ⑦	۵ کې
Ipereira-VM	172.16.12.21	default	Microsoft Windows 10 Pro 10.0.19042.631	blockbit-xdr-manager-worker-0	v1.0.0	Sep 5, 2024 @ 13:38:00.000	• active ⑦	۵ ٩
Rows per page: 10 $$ $$ $$							< 1 2	3 4 5 >

To search for a specific agent, use the search bar (Search), where you can construct a query to look for agents.

In Refresh, you can reload the list.

In Export formatted, you can export a .csv file with the list of agents.

For each agent, the following characteristics are available:

- Name: the name of the agent.
- IP address: the agent's IP address.
- Group: the group to which the agent belongs. Clicking on the group will display only the agents in that group.
- Operating system: the agent's operating system.
- Cluster node: the agent's location in the network.
- Version: the version of the agent.
- Last keep alive: the last connection check.
- Status: the agent's status, which can be either active or disconnected.

Each agent has two actions:

- Open summary panel for this agent (): Opens the agent's details.
- Open configuration for this agent (): Opens the agent's settings.

XDR - Endpoints Summary - Configurations

Blockbit XDR agents can be configured directly through the interface. Settings that are not supported by the agent's operating system will appear as disabled.

Main Settings

To access the settings, click the **eye icon ()**. To export the settings as a PDF, click **Export PDF ()**.

Global Configuration

These settings are for internal logs:

- Write internal logs in plain text: Enables logging in plain text format.
- · Write internal logs in JSON format: Enables logging in JSON format.

Communication

Settings related to agent communication with the manager:

- · Method used to encrypt communications: Defines the encryption method.
- Remote configuration is enabled: Enables or disables remote configuration.
- Auto-restart the agent when receiving a valid configuration from the manager: Restarts the agent automatically after receiving a valid configuration.
- Time (in seconds) between agent check-ins to the manager: Sets the interval between agent check-ins.
- Time (in seconds) before attempting to reconnect: Defines the wait time before reconnection attempts.

Configuration Profiles – Server Settings

Lists available managers for connection:

- Address: Manager's URL.
- Port: Manager's port.
- Protocol: Manager's protocol.
- Maximum retries to connect: Max connection attempts.
- · Retry interval to connect: Time (in seconds) between connection attempts.

Anti-Flooding Settings

Parameters to prevent event flooding:

- Buffer status: Displays the amount of pending data.
- Queue size: Sets the max number of pending requests.
- Events per second: Defines the max number of events per second.

Auditing and Policy Monitoring

Policy Monitoring

Settings related to policy monitoring:

- Policy monitoring service status: Enables policy monitoring.
- Scan the entire system: Enables full system scanning.
- Frequency (in seconds) to run the scan: Sets scan frequency.
- Check /dev path: Scans connected devices.
- Check files: Scans files.
- Check network interfaces: Scans network interfaces.
- Check process IDs: Scans processes.
- · Check network ports: Scans network ports.
- Check anomalous system objects: Detects anomalous objects in the system.
- Check trojans: Scans for trojans.
- Check UNIX audit: Checks UNIX audit logs.
- Skip scan on CIFS/NFS mounts: Skips scanning CIFS/NFS files.

Rootkit Database Paths

- Rootkit files database path: Specifies the directory for rootkit files.
- Rootkit trojans database path: Specifies the directory for rootkit trojans.

Security Configuration Assessment (SCA)

- Security configuration assessment status: Enables or disables SCA.
- Interval: Sets the interval between scans.
- Scan on start: Enables scanning at system startup.
- Skip NFS: Skips scanning NFS files.
- · Policies: Lists security policies by name.

CIS-CAT Scanner & SCAP Check

- CIS-CAT integration status: Enables or disables CIS-CAT integration.
- Timeout (in seconds) for scan executions: Defines max scan duration.
- Path to Java executable directory: Sets the Java directory.
- Path to CIS-CAT executable directory: Sets the CIS-CAT directory.
- Interval between scan executions: Sets the interval between scans.
- Scan on start: Enables scanning at system startup.

System Threats & Incident Response

Osquery

Settings for Osquery, a system query tool:

- Osquery integration status: Shows Osquery status (enabled/disabled).
- Auto-run the Osquery daemon: Runs Osquery automatically.
- Path to the Osquery executable: Defines the Osquery executable path.
- Path to the Osquery results log file: Defines the log file path.
- Path to the Osquery configuration file: Defines the config file path.
- Use defined labels as decorators: Allows labels to modify Osquery behavior.

Inventory Data

Main Settings

- Syscollector integration status: Shows Syscollector status (enabled/disabled).
- Interval between system scans: Sets the interval between scans.
- Scan on start: Enables scanning at system startup.

Scan Settings

Defines what is scanned:

- Scan hardware info
- Scan current processes
- Scan operating system info
- Scan installed packages
- Scan network interfaces
- Scan listening network ports
- Scan all network ports

Active Response

Configures real-time response actions:

• Active response status: Shows whether Active Response is enabled/disabled.

Commands

Configures commands for Active Response:

- Command status: Shows the status of a command.
- Command name: Name of the command.
- Command to execute: File to be executed.
- Interval between executions: Time between executions.
- Run on start: Runs the command at system startup.
- Ignore command output: Ignores command results.
- Ignore checksum verification: Skips checksum verification.

Log Collection

Log Files

Displays log file settings:

- Log format: Defines log format.
- Log location: Sets the log directory.
- Only receive logs that occurred after start: Accepts logs only after startup.
- Filter logs using this XPATH query: Filters logs using an XPATH query.
- Redirect output to this socket: Redirects log output to a selected socket.
- If the expression matches, the log will be ignored: Defines patterns for logs to ignore.
- The log will only be processed if the expression matches: Defines required patterns for log processing.

Windows Event Logs

Configures Windows log processing:

- Log format: Defines log format.
- Channel: Defines log channel.
- Query: Allows query input.
- · Only future events: Logs only future events.
- Reconnect time: Sets reconnection interval.

Integrity Monitoring

Monitors system integrity for changes in files, attributes, and ownership.

General Settings

- Integrity monitoring status: Shows whether integrity monitoring is enabled/disabled.
- Interval (in seconds) to run the integrity scan: Sets scan frequency.
- Time of day to run integrity scans: Defines scan time.
- Day of the week to run integrity scans: Defines scan day.
- Scan on start: Enables scanning at system startup.
- · Skip scan on CIFS/NFS mounts: Skips scanning CIFS/NFS files.
- Skip scan of /dev, /sys, and /proc directories: Skips scanning system directories.
- Remove old local snapshots: Deletes old snapshots.
- Interval (in seconds) to check directories' SACLs: Sets directory check frequency.
- Command to prevent prelinking: Defines a command to prevent prelinking.
- Maximum event reporting throughput: Sets the max event reporting rate.
- Process priority: Sets process priority.
- Database type: Defines database type.

Monitored Directories

Lists directories being monitored.

- Enable real-time monitoring
- Enable auditing (who-data)
- Report file changes
- Perform all checksums
- · Check files owner, groups, permissions, size, modification time, and inodes
- Recursion level
- Follow symbolic links

Monitored Registry Entries

Lists monitored registry entries by Entry Name and Architecture (Arch).

Ignored Entries

Lists ignored registry entries:

- Path: Directory of ignored entries.
- Sregex: Regex patterns to ignore.

Synchronization

Configures database synchronization settings:

- Synchronization status: Shows sync status.
- Maximum interval (in seconds) between syncs
- Interval (in seconds) between syncs
 Response timeout (in seconds)
- Queue size of manager responses
- Maximum message throughput
- Number of threads

Files & Registry Limits

- File limit status: Enables or disables file monitoring limits.
- Maximum number of files to monitor: Defines the max number of monitored files/registries.

XDR - Endpoints Summary - Summary Panel

The Blockbit XDR integrates **Sysmon** on Windows and **auditd** on Linux, enabling detailed monitoring of system activities. The solution logs critical events, such as process execution, file modifications, and registry changes, providing a comprehensive and forensic view of operations on the endpoint.

To facilitate threat analysis, Blockbit XDR visually presents a process tree, allowing security analysts to view the relationship between legitimate and suspicious processes, identify malicious execution chains, and understand the impact of events on the system.

This feature enables proactive threat detection, detailed investigation, and automated incident response, ensuring greater control over the security of the environment.

On the page, you can check all the information and access all the functionalities of the XDR for the Agent.



ID: Agent identifier;

Status: Agent status: There are two statuses: active and disconnected;

IP address: Agent's IP address;

Version: Agent version;

Groups: Agent groups;

Operating system: Agent's operating system;

Registration date: Date and time the agent was registered;

Last keep alive: Last connection check of the agent;

Cores: Number of processors;

Memory: Machine's memory;

Arch: Processor architecture version;

Operating system: Machine's operating system;

CPU: Processor model;

Host name: Server name;

Board serial: Machine's serial number;

Last scan: Last scan on the agent.

Events count evolution: Number of events per 30 minutes;

General Stats: Event statistics involving the agent. They are classified by Location, Events, and Size (Bytes). You can change the measurement interval at the top right.

FIM: Recent eve	nts					Ľ		SCA: Lastest scans								ß		
Time \downarrow	Path	Action	Rule descriptio	1	Rule Le	Rule Id		System audit for Unix based systems	U	inix_audit								
Sep 5, 2024 @ 10:56:59.121	/etc/apt/trusted.gpg.d/microsoft	Integrity check	sum changed.	7	550		Policy		End scan		Passed	Failed	Not applic	Score				
Sep 5, 2024 @ 10:56:59.121	/etc/apt/trusted.gpg.d/google-ch	sum changed.	7	550		System audit for Unix based systems		Sep 5, 202 10:56:44.00	4 @ 00	3	13	7	18%					
															< 1	>		
MITRE ATT&CK			ß	PCI-DISS						GDPR								
Top Tactics		Top 5 PCI-DISS						5 PCI-DISS Top 5 GDPR										
Defense Evasion		2	6.1 IV_35.7.d											240				
Impact		2										2						
	10.2.6						4											
				11.5				2										
NIST-800-53			HIPAAA					GPG13			TSC							
Top 5 NIST-800-53			Top 5 HIPAAA					Top 5 GPG13			Top 5 TS	SC						
AU.6		102	164.312.b			102		10.1		86	CC7.2					104		
AU.14		101	164.312.c.1			2		4.10		16	CC7.3					104		
AU.5		4	164.312.c.2			2		4.11		2	CC6.8					103		
SI.7		2									CC8.1					16		

FIM: Recent events: File integrity monitoring for the agent;

SCA: Latest scans: Configuration assessment for the agent;

MITRE ATT&CK: Specific MITRE ATT&CK statistics for the agent;

PCI DSS: Specific PCI DSS statistics for the agent;

GDPR: Specific GDPR statistics for the agent;

NIST-800-53: Specific NIST-800-53 statistics for the agent;

HIPAA: Specific HIPAA statistics for the agent;

GPG13: Specific GPG13 statistics for the agent;

TSC: Specific TSC statistics for the agent;

FIM: Recent eve	nts				Ľ	SCA: Lastest scans							Ø	
Time \downarrow	Path	Action	Rule description		Rule Le	Rule Id	System audit for Unix based systems	unix_audit						
Sep 5, 2024 @ 10:56:59.121	/etc/apt/trusted.gpg.d/microsoft	I Integrity checks	sum changed.	7	550	Policy	End scar		Passed	Failed	Not applic	Score		
Sep 5, 2024 @ 10:56:59.121	/etc/apt/trusted.gpg.d/google-ch	I Integrity checks	sum changed.	7	550	System audit for Unix based systems	Sep 5, 2 10:56:44	024 @ .000	3	13	7	18%		
													< <u>1</u>)	>
MITRE ATT&CK			C	PCI-DISS				GDPR						
Top Tactics	Top 5 PCI-DISS						Top 5 GDPR							
Defense Evasion			2	10.6.1			240	240 IV_35.7.d						240
Impact			2	10.2.7			97 II_5.1.f							2
10.2.6						4								
11.5							2							
NIST-800-53			HIPAAA				GPG13		TS	SC				
Top 5 NIST-800-53			Top 5 HIPAAA				Top 5 GPG13		Top 5	5 TSC				
AU.6		102	164.312.b			102	10.1	86	CC7.2	2				104
AU.14		101	164.312.c.1			2	4.10	16	CC7.3	3				104
AU.5		4	164.312.c.2			2	4.11	2	CC6.8	В				103
SI.7		2							CC8.1	1				16

Network interfaces: Network interfaces. Their characteristics are:

- Name: Name;
- MAC: Network interface address (MAC address);
- State: State. It can be up (functioning) or down (not functioning);

- MTU: Maximum packet size;
- Type: Network type.

Network settings: Network configurations. Their characteristics are:

- Interface: Network interface;
- Address: Network address. It can be standard IPv4 or IPv6;
- Netmask: Network mask;
- Protocol: Network protocol. It can be standard IPv4 or IPv6;
- Broadcast: Broadcast domain.

Ports: Network ports. Their characteristics are:

- Local port: Local port;
- Local IP address: Local IP address;
- Process: Executed service;
- PID: Service consumption;
- State: State. It can be up (functioning) or down (not functioning);
 Protocol: Used protocol.
- Processes (245) C Refresh DOL Search PID Parent PID VM size Priority NLWP Command Name 1 Aggrega C:\Windows\System32\Aggreg torHost. 4300 6807552 8 2 7724 atorHost.exe exe AnyDes C:\Program Files 4176 5 1008 43143168 13 k.exe (x86)\AnyDesk\AnyDesk.exe C:\Program Files\Common AppVSh Files\microsoft Notify.ex 20416 1772 2514944 8 1 shared\ClickToRun\AppVShNo е tify.exe Applicati C:\Windows\System32\Applica onFram 2 7068 1100 35880960 8 eHost.e tionFrameHost.exe xe **DDVColl** C:\Program 2 ectorSv 9800 1008 4325376 8 Files\Dell\DellDataVault\DDVC cApi.exe ollectorSvcApi.exe DDVDat C:\Program aCollect 3620 1008 127381504 8 23 Files\Dell\DellDataVault\DDVD or.exe ataCollector.exe DDVRul C:\Program 6 esProce 4824 1008 22777856 8 Files\Dell\DellDataVault\DDVR ulesProcessor.exe ssor.exe

Processes: Their characteristics are:
- Name (Process Name): Displays the name of the process running on the system.
- PID (Process ID): A unique identifier for the process, allowing tracking and management of its execution.
- Parent PID (Parent Process ID): Indicates the process that initiated the execution of the current process. From this identifier, it is possible to view the process hierarchy, making it easier to analyze suspicious behaviors, such as code injection and malware execution.
- VM Size (Virtual Memory Size): Represents the total amount of virtual memory allocated by the process, serving as an important indicator for detecting anomalous resource consumption.
- Priority: Defines the execution priority of the process within the operating system, influencing its CPU allocation and resources. Processes with high priority may indicate critical tasks or suspicious activities.
- NLWP (Number of Threads): Displays the number of threads used by the process, a relevant factor for identifying anomalous behaviors, such as malware creating multiple threads to evade detection.

Packages (229)			ී Refresh 👍 Export formatted
Search			DQL
Name 1	Architecture	Version	Vendor
7-Zip 21.07 (x64)	x86_64	21.07	Igor Pavlov
AnyDesk	i686	ad 7.0.15	AnyDesk Software GmbH
Blockbit Client	i686	1.2.4	Blockbit
Blockbit VPN Client	x86_64	4.39.9772	Projeto VPN Blockbit
Blockbit XDR Agent	i686	1.0.0	Blockbit XDR.
CleanUp!	i686		
Clima	x86_64	4.54.63007.0	Microsoft Corporation
Cortana	x86_64	4.2308.1005.0	Microsoft Corporation
Câmera	x86_64	2025.2501.1.0	Microsoft Corporation
DBeaver 24.3.3	x86_64	24.3.3	DBeaver Corp
Rows per page: 10 $ \smallsetminus$			< 1 2 3 4 5 23 >

Packages: Their characteristics are:

This section displays the complete list of applications and packages installed on the monitored endpoint. The view facilitates software auditing, detection of unauthorized applications, and compliance control.

Fields and their definitions:

Name: Name of the installed package or application.

Architecture: System architecture compatible with the package (e.g., x86_64 or i686).

Version: Current version of the installed application or component.

Vendor: Vendor or developer responsible for the application.

Additionally, the interface allows:

- · Filtering packages by name, version, or vendor using the search field.
- Updating the list by clicking "Refresh."
- Exporting data in a structured format by clicking "Export formatted."
- Viewing across multiple pages with adjustable pagination.

This functionality is essential for maintaining full visibility over the software environment, ensuring control, traceability, and prevention against potentially unwanted applications.

XDR - Endpoint Groups & Sub-groups

Group Management and Custom Policies in Blockbit XDR

Blockbit XDR allows implementation based on the organizational structure, ensuring that administrators can manage multiple sites, locations, departments, and geographically separated environments within a single console, without restrictions. Through segmentation by groups of endpoints and users, custom policies and specific rules can be applied to each organizational unit.

Organizational Structure

The solution allows the creation of Custom Groups and Subgroups:

- Administrators can organize endpoints into distinct groups, reflecting the organization's structure, such as departments, business units, branches, or geographic regions.
- Each group can have its own individual security and monitoring configurations, ensuring appropriate protection for different usage profiles.

Centralized Management and Flexible Segmentation:

- The console allows monitoring, applying policies, and taking corrective actions individually or in bulk across any group of endpoints.
- Groups can be dynamic or static, providing greater flexibility to adapt to the organization's infrastructure.

Policy Application with Inheritance at Any Level:

- Blockbit XDR supports policy inheritance, allowing rules defined at a higher level to be automatically applied to subgroups and associated endpoints.
- · Administrators can define global configurations for the company and allow individual units to adjust specific parameters as needed.

Group-Based Policies for Security and Monitoring:

- Isolation of compromised endpoints, ensuring threat containment.
- Blocking malicious processes and automated incident response.
- Automatic correction of configurations altered by malware or attacks.
- Definition of rules for preventing new threats and mitigating risks.

Custom Exceptions and Exclusions by Group and Subgroups:

- · Enabling or disabling specific protection engines for certain groups.
- Exclusions by file type (MIME-Type), hash, or specific directories. Exclusions for trusted programs, digital certificates, and applications.
- Defining exceptions for suspicious behavior, allowing granular control over threat response.

Groups & Sub-groups (2) From here you can list and check your groups and sub-groups, its agents and files.			ී Refresh	실 Export formatted
Search				DQL
Name 1	Agents	Actions		
default	24			
default_subgroup	0	● / † F B		
Rows per page: 10 \lor				$\langle 1 \rangle$

To create a group, click on Add new group.

Create a name for the group and click on Save new group.



To see the new groups created, click on Refresh.

By clicking on Export formatted, a .csv file with information about the groups will be created.

For each group, there are 5 actions:

View details (⁽⁽⁾): Displays details of the agents and files within the group. For more information, go to View details.

Edit group configuration (): Opens an editor with the group's information, allowing customization of settings, rules, and exceptions for the endpoints belonging to that Group or Sub-group, to enable automatic detections.

Blockbi	Blockbit					
Endp	Net Groups	0				
< agent	conf of default group	D Save				
2 3 4 + 5 6 7 7 8 9 10 - 11 2 + 13 14 15 16 16 17 18 + 20 - 21 22 22 22	<pre>il= mers para Betecolo de Criptopartia Superia</pre>					
24 25 27 28 * 38 31 32 33 34 34 35 36 * 37 37	<pre>idescription>Gassible ransomware activity: high file modification rate//description> (/rules c/group) (rule file) group name='ransommare, shadow_copy_deletion'> (rule file) (rule file) (decoded_ass_sysmon/decoded_ass cdfetd_name='verwer_data.CommandIne'>.+(vssadmin.exe_delete shadowsjwmic_shadowcopy_delete).+ cdfetd_name='verwer_data.CommandIne'>.+(vssadmin.exe_delete shadowsjwmic_shadowcopy_delete).+ cdfetd_name='verwer_data.CommandIne'>.+(vssadmin.exe_delete shadowsjwmic_shadowcopy_delete).+ cdfetd_name='verwer_data.CommandIne'>.+(vssadmin.exe_delete shadowsjwmic_shadowcopy_delete).+ cdfetd_name='verwer_data.CommandIne'>.+(vssadmin.exe_delete shadowsjwmic_shadowcopy_delete).+ cdfetd_name='verwer_data.CommandIne'>.+(vssadmin.exe_delete_shadowsjwmic_shadowcopy_delete).+ cdfetd_name='verwer_data.CommandIne'>.+(vssadmin.exe_delete_shadowsjwmic_shadowcopy_delete).+ cdfetd_name='verwer_data.CommandIne'>.+(vssadmin.exe_delete_shadowsjwmic_shadowcopy_delete).+ cdfetd_name='verwer_data.CommandIne'>.+(vssadmin.exe_delete_shadowsjwmic_shadowcopy_delete).+ cdfetd_name='verwer_data.CommandIne'>.+(vssadmin.exe_delete_shadowsjwmic_shadowcopy_delete).+</pre>					
309 40 42 43 44 45 46	<pre>cepecture.command closetion.local/location <levelij2< pre=""></levelij2<></pre>					

Delete (1): Deletes the group or subgroup.

Add Sub-groups (): Creates a subgroup within a main group, allowing for customizations, while always inheriting the configurations of the parent group, ensuring standardized security.



Clone group (): Duplicates an existing group, copying all configurations and endpoints, ensuring standardization and efficiency in creating new groups.

In the Search bar, you can create a query to search for groups.

Q	Search	run the search query
@)	name	filter by name
6 0	count	filter by count
@ D	configSum	filter by configuration checksum
11	(open group

In **name**, you can filter by name.

In **count**, you can filter by quantity.

In **configsum**, you can filter by checksum.

XDR - Endpoint Groups - Inheritance

Blockbit XDR allows the granular application and segmentation of security policies, ensuring configuration inheritance at any organizational **level.** The solution provides flexibility to define centralized rules and policies, while also enabling specific adjustments by site, location, department, or group of endpoints.

Based on a scalable organizational structure, the Blockbit XDR administration console allows administrators to manage multiple units without restrictions on the number of distinct sites or locations. In this way, security policies can be applied hierarchically, ensuring that essential configurations are inherited by sublevels, while custom adjustments can be implemented to meet the specific needs of each environment.

Additionally, the Blockbit XDR rule system enables intelligent event correlation, generating security alerts and allowing for the automatic execution of Active Response actions. The applied policies determine which events should be analyzed, when to escalate the severity of an alert, and which automated responses should be activated to mitigate threats in real-time.

Below, we explain how this "hierarchy" of rules works and how they can chain or overlap:

1. Rule Overlap and Chaining

Generic Rules vs. Specific Rules

A "generic rule" can detect a broad condition (for example, "Login failure"). Then, another "more specific rule" can "catch" that same event to check for something additional (for example, "Login failure of the user Administrator"). This chaining happens through directives like <if_sid> (which checks if a previous rule with a given rule ID triggered) or <if_level> (which evaluates if the previous rule had a certain severity level).

Replacement (replace) and Continuation (continue)

- <replace>true</replace>: The last rule to trigger can completely replace the previous rule's settings. This can raise the severity level, change the description, and even redefine the alert.
- <continue>yes</continue>: Indicates that after triggering a rule, the analysis engine continues searching for other subsequent rules that may also apply to the same event.

Practical Effect: Hierarchy

By using <if_sid>, <replace>, and <continue>, we can create a "chain" of rules where events pass through multiple layers of verification. A "more specific" rule inherits the event from a generic rule and adjusts the severity or description, creating a more precise final alert.

<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=filestime.reprime in the second <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"> <ir/>
iter roots/concerned the interface of the inte </rule> <rule id="100627" level="7" timeframe="30" frequency="10" ignore="300"> <if_matched_sid>559</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> <proup name="ransomware,ransomware_detection" <if_sid>100626,100627,100615,100616,100617,100618,100619</if_sid> <description>Ransomware activity detected.</description> </rule> </group>

2. File Load Order (Alphabetical) and Enumeration

Another way to understand the "hierarchy" is in the order in which the rules are read by the system. Blockbit XDR loads rule files in alphabetical order:

Therefore, native rule files are numbered (for example, 0010-, 0020-, 0100-...) to ensure a logical sequence of loading.

When creating custom files, you can name them something like 9999-custom_rules.xml so that it is loaded after the official ones, allowing your definitions (or overrides) to take precedence in case of conflicts.

The loading order does not override the rule chaining during analysis time; however, it defines which one "wins" if there is duplication of rule IDs or if two rules have the same <rule id="..."> tag.

Example configuration snippet in ossec.conf (or bbxdr.conf):

```
<ruleset>

<!-- Default rules -->

<rule_dir>ruleset/rules</rule_dir>

<!-- Custom user rules -->

<rule_dir>etc/rules</rule_dir>

</ruleset>
```

In this case, the content of ruleset/rules is read first, and then the content of etc/rules. Within each folder, the reading follows the order of file names in alphanumeric order.

sh-5,2# ls						
0010-rules_config.xml 0830-sysmon id 11.xml	0110-ms_dhcp_rules.xml	0215-policy_rules.xml	0320-clam_av_rules.xml	0420-freeipa_rules.xml	0530-mysql_audit_rules.xml	0625-cisco-asa_rules.xml
0015-ossec_rules.xml	0115-arpwatch_rules.xml xml	0220-msauth_rules.xml	0325-opensmtpd_rules.xml	0425-cisco-estreamer_rules.xml	0535-mariadb_rules.xml	0625-mcafee_epo_rules.xml
0016-bbxdr_rules.xml	0120-symantec-av_rules.xml	0225-mcafee_av_rules.xml	0330-sysmon_rules.xml	0430-ms_wdefender_rules.xml	0540-pfsense_rules.xml	0630-nextcloud_rules.xml
0017-bbxdr-api_rules.xml	0125-symantec-ws_rules.xml	0230-ms-se_rules.xml	0335-unbound_rules.xml	0435-ms_logs_rules.xml	0545-osquery_rules.xml	0635-owlh-zeek_rules.xml
0020-syslog_rules.xml	0130-trend-osce_rules.xml	0235-vmware_rules.xml	0340-puppet_rules.xml	0440-ms_sqlserver_rules.xml	0550-kaspersky_rules.xml	0640-junos_rules.xml
0025-sendmail_rules.xml	0135-hordeimp_rules.xml	0240-ids_rules.xml	0345-netscaler_rules.xml	0445-identity_guard_rules.xml	0555-azure_rules.xml	0675-panda-paps_rules.xml
0030-postfix_rules.xml	0140-roundcube_rules.xml	0245-web_rules.xml	0350-amazon_rules.xml	0450-mongodb_rules.xml 0455-docker_rules.xml	0560-docker_integration_rules.xml	0680-checkpoint-smart1_rules.xml 0905-cisco-ftd_rules.xml
0910-ms-exchange-proxy	logon rules xml	0250-apache_rates rate	usou-serv-d_racoursine	ouss-docker_rates.ant	0505-ms_cpace_rd tearning	obo-gcp_rates.tait
0040-imapd_rules.xml 0915-win-novershell rul	0150-cimserver_rules.xml	0255-zeus_rules.xml	0365-auditd_rules.xml	0460-jenkins_rules.xml	0570-sca_rules.xml	0695-f5_bigip_rules.xml
0045-mailscanner_rules.xml	0155-dovecot_rules.xml	0260-nginx_rules.xml	0375-usb_rules.xml	0470-vshell_rules.xml	0575-win-base_rules.xml	0700-paloalto_rules.xml
0050-ms-exchange_rules.xml	0160-vmpop3d_rules.xml vml	0265-php_rules.xml	0380-redis_rules.xml	0475-bbhips_rules.xml	0580-win-security_rules.xml	0705-sophos_fw_rules.xml
0055-courier_rules.xml 0935-cloudflare-waf_rul	0165-vpopmail_rules.xml es.xml	0270-web_appsec_rules.xml	0385-oscap_rules.xml	0480-qualysguard_rules.xml	0585-win-application_rules.xml	0715-freepbx_rules.xml
0065-pix_rules.xml 0945-sysmon id 10 xml	0170-ftpd_rules.xml	0275-squid_rules.xml	0390-fortiddos_rules.xml	0485-cylance_rules.xml	0590-win-system_rules.xml	0750-github_rules.xml
0070-netscreenfw_rules.xml 0950-sysmon_id_20.xml	0175-proftpd_rules.xml	0280-attack_rules.xml	0391-fortigate_rules.xml	0490-virustotal_rules.xml	0595-win-sysmon_rules.xml	0755-office365_rules.xml
0075-cisco-ios_rules.xml 0960-macos_rules.xml	0180-pure-ftpd_rules.xml	0285-systemd_rules.xml	0392-fortimail_rules.xml	0495-proxmox-ve_rules.xml	0600-win-wdefender_rules.xml	0770-gitlab_rules.xml
0080-sonicwall_rules.xml 0990-amazon-security-1	0185-vsftpd_rules.xml ake rules.xml	0290-firewalld_rules.xml	0393-fortiauth_rules.xml	0500-owncloud_rules.xml	0601-win-vipre_rules.xml	0775-arbor_rules.xml
0085-pam_rules.xml 0995-microsoft-graph ru	0190-ms_ftpd_rules.xml les.xml	0295-mysql_rules.xml	0395-hp_rules.xml	0505-vuls_rules.xml	0602-win-wfirewall_rules.xml	0780-fireeye_rules.xml
0090-telnetd_rules.xml 0997-maltiverse_rules.x	0195-named_rules.xml ml	0300-postgresql_rules.xml	0400-openvpn_rules.xml	0510-ciscat_rules.xml	0605-win-mcafee_rules.xml	0785-huawei-usg_rules.xml
0095-sshd_rules.xml	0200-smbd_rules.xml	0305-dropbear_rules.xml	0405-rsa-auth-manager_rules.xml	0515-exim_rules.xml	0610-win-ms_logs_rules.xml	0800-sysmon_id_1.xml
0100-solaris_bsm_rules.xml 0105-asterisk_rules.xml	0205-racoon_rules.xml 0210-vpn_concentrator_rules.xml	0310-openbsd_rules.xml 0315-apparmor_rules.xml	0410-imperva_rules.xml 0415-sophos_rules.xml	0520-vulnerability-detector_rules.xml 0525-openvas_rules.xml	0615-win-ms-se_rules.xml 0620-win-generic_rules.xml	0810-sysmon_id_3.xml 0820-sysmon_id_7.xml
sh-5.2#						
sh-5.2#						

3. How It Works in Practice

Creating Rule Files

```
Each .xml file contains <group> blocks with <rule>.
You can define <match>, <field name="...">, <if_sid>, and other conditions to detect and correlate events.
```

Simplified Example:

First, rule 100000 recognizes "Login failed" and generates a level 5 alert. Then, if the same event contains "administrator," rule 100001 triggers (chained to 100000) and replaces (<replace>true</replace>) the previous rule, raising the level to 10 and changing the description.

Why Enumerate Files

If you had a file 0010-windows_rules.xml with generic Windows rules and a 9999-custom_rules.xml with specific rules, the file 9999-custom_rules.xml would be loaded last.

In the case of rule ID overrides or additional definitions, your custom file takes precedence in the final configuration of the manager.

XDR - Endpoint Groups - View details

On this page, details of the agent and file group are shown.

There are two tabs: Agents and Files.

Agents

ld ↑	Name	IP address	Operating system	Version	Status	Actions
003	xdr-windows-Ipereira	172.28.0.25	E Microsoft Windows 10 Pro 10.0.19045.4529	v1.0.0	• active 💿	◎ 菅
004	xdr-windows-AD-246	172.16.13.246	Kicrosoft Windows Server 2019 Standard 10.0.17763.6054	v1.0.0	• active 💿	◎ 菅
005	xdr-windows-vmLucas	172.16.12.21	II Microsoft Windows 10 Pro 10.0.19042.631	v1.0.0	• active ⑦	◎ む

For each agent, the following characteristics are displayed:

- ID: The identifier number of the agent.
- **Name**: The name of the agent.
- **IP address**: The IP address of the agent.
- Operating system: The operating system of the agent.
- Version: The version of the agent.
- Status: The status of the agent. There are two statuses: active and disconnected.

Actions: Actions for the agent:

• Go to the agent: Opens the agent's information in the Endpoint Summary.

Files

File 🛧	Checksum	Actions
agent.conf	ab73af41699f13fdd81903b5f23d8d00	© 🖉
ar.conf	16f479864e611bf4a7af48d2b59e5d37	0
merged.mg	bbd91c1aed8140ca72bb7982e9ed3584	0

For each file, the following characteristics are displayed:

- Name: The name of the file.
- Checksum: The checksum of the file.

There are two actions per file:

- See file content: Opens the content of the file.
- Edit: Opens an editor for the file's content.

XDR - Endpoints Groups - Active Response

Blockbit XDR Active Response is an automated incident response mechanism designed to mitigate threats in real-time by applying containment and remediation actions quickly and efficiently. This feature is part of the SOAR (Security Orchestration, Automation, and Response) approach, enabling intelligent orchestration of responses to security events. Remediation actions can be applied simultaneously across multiple systems and events, reducing response times and minimizing operational impacts.

Through the use of Playbooks, Active Response executes predefined automation workflows, ensuring that when a threat is detected, the system can block, isolate, or neutralize malicious activities automatically. These Playbooks can be customized to meet the specific needs of the organization, enabling everything from endpoint isolation to the revocation of compromised credentials.

With Active Response, Blockbit XDR transforms threat data into automated actions, ensuring a safer and more resilient environment against cyberattacks.

Below are some examples provided by Blockbit XDR:

Active response/EXE	Associated rules (rules_id)	Function
<pre>notification_remove-threat (uses notification.exe + r emove-threat.exe)</pre>	87105	Displays a notification (notification.exe), then removes (or quarantines) the malicious file from the endpoint (remove-threat.exe).
remove-threat	87105	Removes or quarantines the malicious file from the endpoint.
(remove-threat.exe)		
firewall-drop	2502, 5710	Blocks or "drops" connections (by IP or host) on the system's firewall. In
<pre>(usually uses firewall_manag er.exe Of network_block. exe)</pre>		Windows, it may use netsin. exe in the background.
rollback_windows	100628	Reverts previously made changes (e.g., firewall rules, file removal), restoring the
(calls rollback.bat or rollb ack.psl)		
notification_network_block	100628, 100616, 100200, 100904, 100063, 100238	Displays a notification to the user/administrator while simultaneously executing a network block on the endpoint (by IP host etc.)
(uses notification.exe + n etwork_block.exe)	100194, 100915	
network_block	100628, 100616, 100200,	Blocks network traffic (by IP, URL) locally on the endpoint. In some installations,
(network_block.exe)	100194, 100915	
notification_win_security	501, 503, 62152	Displays an alert/warning and applies security adjustments or reinforcements on Windows (e.g., enabling policies or checking system integrity)
(USES notification.exe + w indows_security.exe)		white wa (e.g., chabing policies of checking system integrity).
windows_security	501, 503, 62152	Performs specific security actions on Windows (e.g., enforcing GPOs, activating defenses, etc.)
(windows_security.exe)		
yara_windows	100303, 100304	Runs a local YARA scan on Windows to identify malware patterns or IOCs (Indicators of Compromise)
(normally calls yara.bat)		
yara_linux	100300, 100301	YARA scan version for Linux systems.
(equivalent in Linux)		
notification	100508	Simply generates a pop-up notification or local log alerting about the triggered alert (without taking additional actions)
(notification.exe)		
ensure_policies	111000, 111001	Generally calls "endpoint_control" binaries or specific managers (e.g., bluetoot h_manager.exe, usb_manager.exe) to check/apply hardware or security policies.
bluetooth_manager.exe (inside endpoint_control)	N/A (varies)	Manages/disables Bluetooth connections according to security or defined policies.
firewall_manager.exe (inside en dpoint_control)	N/A (varies)	Manages firewall rules on the endpoint; can be triggered by the ARs "firewall- drop" or "network_block."

usb_manager.exe (inside endpo int_control)	N/A (varies)	Manages/disables USB devices (storage, USB Bluetooth dongles, etc.) according to defined policies.
endpoint_control.exe	N/A (varies)	Generic application to execute endpoint control functions; can be triggered to check various policies (network, USB, Bluetooth).
logger.exe	N/A	Internal tool for logging additional information related to Active Responses or binary executions.
netsh.exe (native Windows)	N/A	Windows standard tool for manipulating network and firewall settings; may be used "behind" the binaries that perform blocking.
notify_screen.exe	N/A	Similar to notification.exe, but generates a pop-up interface on the user's screen displaying alert messages.
restart-bbxdr.exe	N/A	Restarts the Blockbit XDR service/client on the endpoint (useful when forcing a reload of configurations).
windows_defender.exe	N/A	Invokes Microsoft Defender (on Windows machines) to perform scans, updates, or removal actions.
route-null.exe	N/A	Possible internal tool for inserting null routes (routing block) in the system, an advanced IP/traffic blocking function.

SOAR (Security Orchestration, Automation, and Response) and Active Response in Blockbit XDR are continuously evolving to ensure maximum endpoint security, keeping pace with changes in the cyber threat landscape.

In addition to native automated responses, custom Playbooks can be created, tailoring mitigation and remediation actions to meet the specific needs of each environment. This flexibility allows custom responses for different sites, organizational units, endpoint groups, and individual devices, ensuring intelligent and efficient orchestration of security.

With this approach, Blockbit XDR ensures that incidents are handled in an automated and contextualized manner, reducing response times and operational impacts.

XDR - Security

The Blockbit XDR allows you to define who will access what. In Security, you can create users, define roles, and grant or revoke permissions.

To create and manage roles, go to Roles;

To create and manage users, go to Users;

To create and manage permissions, go to Permissions;

To manage multi-factor authentication, go to Multi-Factor Authentication;

XDR - Security - Roles

To determine what a user accesses, you can create roles in Roles. These roles are defined by the given permissions.

Blockbit XDR supports authentication via **LDAP** and **SAML** (version 2.0 or higher), enabling integration with corporate directories and single sign-on (S60) authentication. The solution allows for synchronization of users, groups, organizational units, domains, and forests, ensuring centralized, secure, and efficient management, simplifying administration and access control within the organization.

- LDAP: Enables centralized authentication through servers like Active Directory.
- SAML: Offers single sign-on (SSO), allowing users to access multiple systems without needing to re-enter credentials.

Integrations are done via the XDR API. To integrate, please contact the Blockbit team.

Blockbit	ıs				(
Security Roles	Roles				
Users Permissions Multi Factor Authentication	Roles (25) Roles are the core way of controlling acc document- and field-level security. Then	ess to your cluster. Roles contain any combination of cluster you map users to these roles so that users gain those permi	-wide permission, index-specific pern ssions. Learn more 🕑	nissions, Actions V	Create role
	🔍 Search		Cluster permissions \vee In	dex permissions \checkmark Users \checkmark	Backend roles \checkmark
	Role	Cluster permissions	Index permi	ssions Internal users	Backend roles
	kibana_user	cluster_composite_ops	.kibana .kibana-6 .kibana_* 	blockbit_xdr_user blockbit_xdr_admin	kibanauser
	own_index	cluster_composite_ops	\${user_na	me} *	-
	alerting_full_access	cluster_monitor cluster:admin/opendistro/alerting/*	*	_	-

Roles are classified by:

- Role: name of the role;
- · Cluster permissions: permissions to access cluster resources;
- Index permissions: permissions to access index resources;
- Internal users: users with access to clusters and indexes;
- Backend role: default group of permissions for a user.

You can search for a specific rule in Search. You can refine the search by selecting permissions, users, and roles.

In the Actions button, the following options are presented:

	Actions ~	
nissio	Edit	в
	Duplicate	
Inte	Delete	в

- Edit: edit rule. This option is enabled when a rule is selected.
- Duplicate: duplicate rule. This option is enabled when a rule is selected.

• Delete: delete rule. You can delete more than one rule.

To create a rule, click on Create role.

XDR - Security - Create role

To create a role, first give it a name.

₿B	lockbit			
≡	Security	Roles	Create Role	a
Cr	eate Role			
Role: tenar	are the core way of ts. Once you've crea	controlling access ated the role, you o	to your cluster. Roles contain any combination of cluster-wide permission, index-specific permissions, document- and field-level security, and an map users to the roles so that users gain those permissions. Learn more 🕜	
N	lame			
N SI	ame becify a descriptive a	nd unique role na	me. You cannot edit the name once the role is created.	
	abc			
T	ie role name must co	ontain from 2 to 50	characters.	
In	valid characters foun	d in role name. Va	ilid characters are A-Z, a-z, 0-9, _underscore, (-) hyphen and unicode characters.	
T	ne role name must co	ontain from 2 to 50	characters. Valid characters are A-Z, a-z, 0-9, (_)underscore, (-) hyphen and unicode characters.	

Next, determine what permissions this role will have when accessing the cluster.

Select the permissions and click on Create new permission group.

Cluster permissions Specify how users in this role can access the cluster. By default, no cluster permission is granted. Learn more 🕑				
	Cluster Permissions Specify permissions using either action groups or single permissions. An a create your own reusable permission groups.	ction group is a list of single permissions. You can often achieve your desired security posture using some combination of the default permission groups. You can also		
	Search for action group name or permission name	Create new permission group 🖸		
	Permission groups			
	cluster_manage_pipelines			
	manage_snapshots			
	cluster_manage_index_templates	3 specific indices. By default, no index permission is granted. Learn more 2		
	cluster_all	Permane		
	cluster_composite_ops_ro	Remove		
	cluster_composite_ops -			

Then, determine what permissions this role will have when accessing the indexes:

Select the indexes.

Index permissions Index permissions allow you to specify how users in this role can access the speci	cific indices. By default, no index permission is	granted. Learn more 🕑			
✓ Add index permission				Remove	
Index					
Search for index name or type in index pattern					
Specify index pattern using *					
Index permissions You can specify permissions using both action groups or single permissions. A permission group is a list of single permissions. You can often achieve your desired security posture using some combination of the default permission groups. You can also create your own reusable permission groups.					
Search for action group name or permission name	Create new permission group 🛛				

Next, specify permissions within them.

get X crud X manage_data_streams X	0 🔍	Create new permission group 🖸
Permission groups	A	
data_access	1	
delete		
manage_aliases		
search		
write		
indices_all	•	

You can also restrict access to certain documents in the index with Document Level Security.

To do this, you need to structure a query in DSL (Domain-specific Language).

Example:

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

In Field Level Security, you can restrict access to certain fields within documents.

Enter the field name and select Include to include it among the restricted fields, or Exclude to exclude it from the restricted fields.

In Anonymization, you can mask certain fields. Simply enter the name of the field to be anonymized.

Document level security - optional You can restrict a role to a subset of documents in an index. Learn more C	
<pre>{ "bool": { "must": { "match": { "genres": "Comedy" } Field level security - optional</pre>	
Exclude	
Anonymization - optional Masks any sensitive fields with a random value to protect your data security. Type in field name	

In Tenant Permission, you define which tenants (groups of users who share access privileges) have access to certain roles.

In Tenant, select the tenant.

Next to it, you can define the tenant's privileges:

- Read and write: can read and edit information.
- Read only: can only read information.

XDR - Security - Users

Those who access and manage the XDR are users, or people who are authenticated and have permission to access the platform.

Blockbit XDR supports authentication via **LDAP** and **SAML** (version 2.0 or higher), enabling integration with corporate directories and single sign-on (S60) authentication. The solution allows for synchronization of users, groups, organizational units, domains, and forests, ensuring centralized, secure, and efficient management, simplifying administration and access control within the organization.

- LDAP: Enables centralized authentication through servers like Active Directory.
- SAML: Offers single sign-on (SSO), allowing users to access multiple systems without needing to re-enter credentials.

Integrations are done via the XDR API. To integrate, please contact the Blockbit team.

By clicking on User, you will go to the user list.

Blockbit					
Security Users			a		
Security L	Jsers				
Users Permissions Multi Factor Authentication	Users (10) The Security plugin includes an user database. Use this database in place of, or in addition to, an external authentication system such as LDAP server or Active Directory. You can map an user to a role from Roles. First, click into the detail page of the role. Then, under "Mapped users", click "Manage mapping" Learn more C				
	Username	Backend roles	Attributes		
	odilon_teste	admin	-		
	blockbit-xdr-admin	admin	-		
	snapshotrestore	snapshotrestore	_		
	gfaraujo	admin	_		

Users are classified by:

- Username: name of the user;
- Backend role: default group of permissions for a user;
- Attributes: characteristics of the user.

You can select more than one user by clicking on the checkboxes.

You can search for a specific user in Search users.

In the Actions button, the following options are presented:

Actions ~
Edit
Duplicate
Export JSON
Delete

- Edit: edit user. This option is enabled when a user is selected.
 Duplicate: duplicate user. This option is enabled when a user is selected.
 Export JSON: export JSON with user data. This option is enabled when a user is selected.
 Delete: delete user. You can delete more than one user.

To create a user, click on Create user.

XDR - Security - Create User

To edit a user, follow these steps.

To create a user, first create a **username** and a **password**:

Blockbit		
E Security	Users	Create internal user
Create int	ernal user	JSET database. Use this database in place of, or in addition to, an external authentication system such as LDAP or Active Directory. Learn more 🕑
Credentials		
Username Specify a descriptive an	d unique user nar	me. You cannot edit the name once the user is created.
The user name must co	ntain from 2 to 50	characters. Valid characters are A-Z, a-z, 0-9,underscore, (-) hyphen and unicode characters.
Password		
ê		
Password should be at	east 8 characters	long and contain at least one uppercase letter, one lowercase letter, one digit, and one special character.
Re-enter password		
۵		
The password must be	identical to what y	ou entered above.

Next, define the roles:

Backend roles - optional Backend roles are used to map users from external authentication systems, such as LDAP or SAML to OpenSearch security roles. Learn more 🕐			
Backend role			
Type in backend role	Remove		
Add another backend role			

Finally, define the attributes:

Attributes - optional Attributes can be used to further describe the user, and, more importantly they can be used as variables in the Document Level Security query in the index permission of a role. This makes it possible to write dynamic DLS queries based on a user's attributes. Learn more (2)			
Variable name Type in variable name	Value Type in value	Remove	
Add another attribute			

To create the user, click on Create.

XDR - Security - Permissions

Permissions are specific actions that a specific user is authorized to take.

Blockbit					
≣ Security Perr	nissions				a
Security Roles	Permissions				
Users <u>Permissions</u> Mutti Factor Authentication	Permissions (293) Permissions are individual actions, such as cluster.ac reusable collections of permissions, such as MANAG can often meet your security needs using the default Learn more action group name or permission	dmin/snapshot/restore, which lets you restore sn E_SNAPSHOTS, which lets you view, take, dele action groups, but you might find it convenient to on name	apshots. Action groups are tle, and restore snapshots. You o create your own.	Actions V Create a	action group ∨ Il permissions ∨
	Name	Туре 🛧	Cluster permission	Index permission	
	data_access	Action group		\checkmark	\sim
	delete	Action group		\checkmark	~
	cluster_manage_pipelines	Action group	~		~
	manage_aliases	Action group		\checkmark	~

Permissions are classified by:

- Name: name of the permission;
- **Type**: type of the permission;
- Cluster permissions: permissions to access cluster resources;
- Index permissions: permissions to access index resources.

You can search for a specific permission in **Search**. You can refine the search by selecting between single permissions and action groups, and cluster and index permissions.

In the Actions button, the following options are presented:



- Edit: edit permission. This option is enabled when a permission is selected.
- Duplicate: duplicate permission. This option is enabled when a permission is selected.
- **Delete**: delete permission. You can delete more than one permission.

To create an action group, click on Create action group.



- Create from blank: create an action group and select permissions manually;
 Create from selection: create an action group from pre-selected permissions.

Create new action group	×					
Name Enter a unique name to describe the purpose of this group. You cannot change the name after creation.						
The name must contain from 2 to 50 characters. Valid characters are A-Z, a Permissions	-z, 0-9, (_)underscore, (-) hyphen and unicode characters.					
data_access						
delete	Cancel Create					
cluster_manage_pipelines						
manage_allases						
crud						
manage_snapshots						
kibana_all_read v						

To create an action group, give it a name and select the permissions.

XDR - Security - Multi Factor Authentication

Multi-factor authentication is a way to enhance access security by requiring more than one factor to verify a user's identity.

Blockbit				
E Security Multi	Factor Authentication			a
Security Roles	🔍 Search user		Delete Users Generate Tol	ken
Users Permissions	Username	Token	Actions	
Multi Factor Authentication	Dereira	KRMFWKSRD5UBQWBP		
	gfaraujo	DECWKSC7I4SUOTDM		
	odilon_teste	CB7RGMTKA5SE2ECH		
	admin	PRXFCNJOPECTCEJE		

In Blockbit XDR, a random token is generated for the user.

Users are listed with their respective tokens.

To generate a token, click on Generate Token.

Generate MFA Token	
ielect the user	
Search user	•

Select a user and click on Submit. You can select more than one user.

The token will appear in the list.

To delete one or more tokens, select the users and click on Delete Users.

XDR - Indices

In Blockbit XDR, Indices are ways to structure documents in a database to facilitate access.

By clicking on Indices, you can access:

- State Management PoliciesIndices

XDR - Indices - Indices

Indices in Blockbit XDR

Indices are data tables that store and organize documents.

Documents are the basic units of data, represented in JSON format and identified by a unique ID within an index.

These documents are stored in **shards**, which are hosted on a **data node**. When you search for data in Blockbit XDR, the request interacts with multiple shards, which can be either primary or replicated.

In Blockbit XDR, you can manage indices in the Indices tab.

Indices (52)					C R	lefresh	Actions \sim	Creat	te Index
Q Search							O×	Show data str	eam indices
□ Index ↓	Health	Managed b	Status	Total size	Size of pri	Total docu	Deleted do	Primaries	Replicas
	• Yellow	No	Open	389.3mb	389.3mb	18132	0	1	1
	• Yellow	No	Open	2mb	2mb	1173	0	1	1
	• Yellow	No	Open	1.7mb	1.7mb	1015	0	1	1
	• Yellow	No	Open	954kb	954kb	485	0	1	1
	• Yellow	No	Open	988.7kb	988.7kb	469	0	1	1
	• Yellow	No	Open	829.8kb	829.8kb	386	0	1	1
	• Yellow	No	Open	880kb	880kb	492	0	1	1
	• Yellow	No	Open	937kb	937kb	542	0	1	1

Searching for an Index

- To find a specific index, use the **Search** bar.
- To display data stream indices (which handle continuous data), click on Show data stream indices.

Index Classification

Indices are classified by:

- Index: Name of the index
- Health: Index health status Green (good), Yellow (moderate), or Red (bad)
- Status: Index state Open or Closed
- Total size: Total size of the index
- Size of primaries: Size of the primary shards
- Total documents: Total number of documents
- Deleted documents: Number of deleted documents
- Primaries: Primary shards
- Replicas: Replicated shards

By clicking on an index, you can also configure it.

Actions \sim

Index Actions

• Refresh (

)button: Updates the indices

Actions (

)button: Provides the following options:

- Apply policy: Apply a policy to selected indices
- Close: Close selected indices
- **Open**: Open selected indices
- Reindex: Reindex selected indices
- Shrink: Compress selected indices

- Split: Split selected indices
 Force merge: Merge selected indices
 Download: Download selected indices
 Clear cache: Clear cache
 Flush: Permanently remove data
 Refresh: Refresh data
 Delete: Delete indices

Creating an Index

To create an index, click on Create index (



XDR - Indices - Indices - Create index

To create an index, follow these steps:

1. Define the Index Name

- In Index name, enter the name of the index.
- In Index alias, you can set an alias or define a group of indices.

Define index	
Index name	
Specify a name for the new index.	
Must be in lowercase letters. Cannot begin with underscores or hyphens. Spaces, commas, and characters :, ", *, +, /, , , ?, #, > are not allowed.	
Index alias – optional	
Allow this index to be referenced by existing aliases or specify a new alias.	
Select aliases or specify new aliases.	\sim

2. Configure Index Settings

In Index Settings, define:

- Number of primary shards: Set the number of primary shards.
- Number of replicas: Specify the number of replicas.
- Refresh interval: Define how often the index refreshes.

Index settings

Number of primary shards

Specify the number of primary shards for the index. Default is 1. The number of primary shards cannot be changed after the index is created.

1

Number of replicas

Specify the number of replicas each primary shard should have. Default is 1.

1

Refresh interval

Specify how often the index should refresh, which publishes the most recent changes and make them available for search. Default is 1 second.

1s

> Advanced settings

In Advanced settings, you can modify advanced configurations using JSON.

Advanced settings

Specify advanced index settings

Specify a comma-delimited list of settings. View index settings. All the settings will be handled in flat structure. Learn more \mathcal{O} .

```
1 * {
2 "index.number_of_shards": 1,
3 "index.number_of_replicas": 1,
4 "index.refresh_interval": "1s"
5 }
```

3. Configure Index Mapping

To define how a document is stored in an index, go to **Index mapping**:



4. Create the Index

Click Create (Create) to finalize the process.

XDR - Indices - Settings

Blockbit XDR allows you to export audit logs in JSON format.

Ex	port Settings				Save	Export
Type S	Server Opensearch	0 ٩	Host 167.234.224.223		Index security-auditlog-2025.01.27	
User adn	in			Password		۲

1. Configure the Logging Server

- Type Server: Logging servers supported:
 - **Opensearch** (XDR to XDR)
 - SysLog (XDR to SysLog)
- Host: Enter the IP of the exported host.
- Index: Choose the index to export.
 - Any listed index can be exported.
 - To export a category of indices, use an asterisk (*) to select everything before it.
 - Example:
 - auditlog-2025* exports all indices from 2025.
 - auditlog-2025.01* exports all indices from January 2025.

2. Authentication for Opensearch

If the server type is **Opensearch**, the system will request admin credentials:

- User: The user exporting the log.
- Password: The password for the exporting user.

3. Network Configuration for SysLog

If the server type is **SysLog**, the system will request network protocol settings:

- **Protocol**: Supported options:
 - UDP (port 514)
 TCP (port 601)
- **Port**: Specify the port number.

4. Exporting Logs



XDR - Indices - State Management Policies

In State Management Policies, you can create policies to manage indices.

State management policies Indices	State manager	ment policies	Delete Edit	Create policy
	🔍 Search			
	Policy ψ	Description	Last updated time	
		There are no existing policies. Create a polic	cy to apply to your indices.	
		Create policy		

Upon accessing this section, you will see a list of policies classified by:

- Policy: Name of the policy.
- Description: Policy description.
 Last updated time: The last time the policy was updated.

To search for a specific policy, use the **Search** bar.

- To edit a policy, click Edit.
- To create a new policy, click Create policy.

Configuration method	×
Choose how you would like to define your p JSON.	policy, either using a visual editor or writing
• Visual editor	◯ JSON editor
Use the visual editor to create your policy using pre-defined options.	Use the JSON editor to create or import your policy using JSON.
	Cancel Continue

There are two ways to create a policy:

- 1. Visual editor: Use the Blockbit XDR built-in editor.
- 2. JSON editor: Create or import a JSON file with the policy configuration.

XDR - Indices - State Management Policies - JSON editor

When selecting the JSON editor, you will be directed to this page:

Create policy		
Name policy		
Policies let you automatically perform administrative operations on indices Policy ID example_policy		
Specify a unique ID that is easy to recognize and remember.		
Define policy	🖺 Сору	E Auto indent
You can think of policies as state machines. "Actions" are the operations IS	M performs when an index is in a certain state. "Transitions" define when to move from one state to another. Learn more 🖄	
<pre>2 * "policy": { 3 "description": "A simple default polic 4 "default_state": "example_hot_state", 5 * "states": [6 * {</pre>	y that changes the replica count between hot and cold states.",	

Enter a name in Policy ID.

In **Define policy**, create or paste a JSON file with the policy definitions.

Available Actions

- Click Copy to copy the JSON.Click Auto indent to automatically format the JSON.

XDR - Indices - State Management Policies - Visual editor

When selecting the Visual editor, you will be directed to this page:

Create policy Policies let you automatically perform administrative operations on	ndices. Learn more 🖉
Policy info	
Policy ID Specify a unique and descriptive ID that is easy to recognize and remember hot_cold_workflow	
Description Describe the policy.	
A sample description of the policy	

Enter a name in Policy ID.

(Optional) Add a description in Description.

Error notification – optional You can set up an error notification for when a policy execution fails. Learn more 🕑	
Channel ID	
C C Manage channels	

In Error notification, you can configure error alerts.

Enter the channel where notifications will be sent in Channel ID.

In Manage Channels, you can create new notification channels.

ISM templates – optional Specify ISM template patterns that match the index to apply the policy. Learn more ⊘
No ISM templates
Your policy currently has no ISM templates defined. Add ISM templates to automatically apply the policy to indices created in the future.
Add template

ISM (Index State Management) templates help automate operations, such as changing a policy state after a specific time.

- To add a template, click Add template.
- Enter the Index pattern (index reference ID) and set its priority.
- Click Add template to confirm or Remove to delete it.

States (0)

You can think of policies as state machines. "Actions" are the operations ISM performs when an index is in a certain state. "Transitions" define when to move from one state to another. Learn more 🖄	
Initial state	
No states	
Your policy currently has no states defined. Add states to manage your index lifecycle.	
Add state	

In States, you define the different states an index will go through, with specific actions performed in each state.

In **Initial state**, you can search for an initial state. To create a new state, click **Add state**.

Create state: aaa	
State name	
aaa	
Order	
Add after	۹
• Enter the State name .	
In Order , set its priority among other states.	
Click Add action to include an action.	
Actions	
Actions are the operations ISM performs when an index is in a certain state.	
No actions have been added.	
+ Add action	

Define the Action type for the state.

Click Add transition to define conditions for state changes.

Transitions

Transitions define the conditions that need to be met for a state to change. After all actions in the current state are completed, the policy starts checking the conditions for transitions.

No transitions have been added.

+ Add Transition

Specify the Previous state and set the Conditions for transitioning.

Add transition

Transitions define the conditions that need to be met for a state to change. After all actions in the current state are completed, the policy starts checking the conditions for transitions. Learn more 🕐

Destination state

If entering a state that does not exist yet then you must create it before creating the policy.

Condition

Specify the condition needed to be met to transition to the destination state.

No Condition

XDR - Audit

Blockbit XDR allows you to generate audit logs, which track access to the cluster.

By clicking on Audit, you can access:

- OverviewSettings

XDR - Audit - Overview

The graph displays the number of audit logs per day.

- Hover over the bars for more details.
- Use the **search bar** to find specific logs.
- Set a time range using the calendar. More details in the search system.
- To download a CSV file with audit logs, click the download button (

Below the graph, a list of generated logs is displayed.

ia <u>Columns</u>	Density	Full screen								
Timestamp \sim	Audit cat $ \smallsetminus $	Audit clu $ \smallsetminus $	Audit for $ \smallsetminus $	Audit no $$	Audit no $$	Audit no $$	Audit req \vee	Audit req \lor	Audit req \lor	Audit req \vee
2025-01-23T		blockbit-xdr	4					admin	TRANSPORT	REST
2025-01-23T		blockbit-xdr	4							REST
2025-01-23T		blockbit-xdr	4							REST
2025-01-23T		blockbit-xdr	4							REST
2025-01-23T		blockbit-xdr	4						TRANSPORT	REST
2025-01-23T		blockbit-xdr	4						TRANSPORT	REST
2025-01-23T		blockbit-xdr	4							REST
2025-01-23T		blockbit-xdr	4							REST
2025-01-23T		blockbit-xdr	4							REST
2025-01-23T		blockbit-xdr	4	_				ch aumi,		REST
Rows per page	:10 ~							<	<u>1</u> 2 3 4	5 15 >

ځ

The Columns button allows you to select which categories to display.

Search

@timestamp	=
audit_category	=
audit_cluster_name	=
audit_format_version	=
audit_node_host_address	=
audit_node_host_name	=
audit_node_id	=
audit_request_body	=
audit_request_effective_user	=
audit_request_layer	=
audit_request_origin	=
audit_request_privilege	=
audit_request_remote_address	=
audit_trace_resolved_indices	=
audit_trace_task_id	=
audit_transport_headers	=

Show all

Hide all

Log Categories

- @timestamp: Date and time of the log.
- audit_category: Log category. Possible values:
 - FAILED_LOGIN
 - MISSING_PRIVILEGES
 - BAD_HEADERS
 - SSL EXCEPTION
 - OPENSEARCH_SECURITY_INDEX_ATTEMPT
 - AUTHENTICATED
 - GRANTED_PRIVILEGES
- audit_cluster_name: Name of the audited cluster.
- audit_format_version: Version of the log message format.
- audit_node_host_address: Node host address where the event occurred.
- audit_node_host_name: Node host name where the event occurred.
- audit_node_host_id: Node host ID where the event occurred.
- audit_request_body: HTTP request body.
- audit_request_effective_user: User whose authentication failed.
- audit_request_layer: Layer that generated the request (TRANSPORT or REST).
- audit_request_origin: Origin layer of the request (TRANSPORT or REST).
- audit_request_privilege: Privilege required for the request.
- audit_request_remote_address: IP address that initiated the request.
- audit_trace_resolved_indices: Names of resolved indices affected by the request.
- audit_trace_task_id: Request identification.
- audit_transport_headers: Request headers.
- audit_transport_request_type: Type of request.

Additional Display Options

- Density button: Adjusts the density of the log list.
- Full screen button: Expands the log list to full screen.
XDR - Audit - Settings

In **Settings**, you can configure audit log options.

Audit logging	
Storage location	
	Configure the output location and storage types in
	opensearch.yml . The default storage location is
	internal_opensearch, which stores the logs in an
	index on this cluster. Learn more 🗹
For the second telescole second	
Enable audit logging	Enabled

Configure

)

To determine where audit logs are stored, visit the designated site.

Enable audit logging in Enable audit logging.

At General Settings, you can modify settings. To do so, click Configure (

General settings			<u>Configure</u>
Layer settings			
REST layer Enabled	REST disabled categories AUTHENTICATED, GRANTED_PRIVILEGES	Transport layer Enabled	
Transport disabled categories AUTHENTICATED, GRANTED_PRIVILEGES			
Attribute settings			
Bulk requests Disabled	Request body Enabled	Resolve indices Enabled	
Sensitive headers Enabled			
Ignore settings			
Ignored users kibanaserver	Ignored requests —		

Available General Settings:

- **REST layer**: Enable auditing of events in the REST layer.
- **REST disabled categories**: Specify categories to be ignored in the REST layer.
- Transport layer: Enable auditing of events in the Transport layer.
- Transport disabled categories: Specify categories to be ignored in the Transport layer.
- Bulk requests: Audit bulk requests.
- Request body: Include request body in audit logs.
- Resolve indices: Resolve indices in audit logs.

- Sensitive headers: Exclude sensitive headers from audit logs.
- Ignored users: Define users to be ignored in audit logs.
- Ignored requests: Define request patterns to be ignored in audit logs.

Compliance Settings



• To modify compliance settings, click Configure (

Available Compliance Settings:

- Compliance logging: Enable compliance logging.
- Internal config logging: Enable logging of internal security index events.
- External config logging: Enable logging of external configurations.

Read Events

(Read events occur when a request does not modify a document.)

- Read metadata: Enable logging of document metadata only (no document fields will be logged).
- Ignored users: Define users to be ignored in audit logs.
- Watched fields: List indices and fields to monitor during read events.
 When adding an index, one log entry per document will be generated.

Write Events

(Write events occur when a request modifies a document.)

- Read metadata: Enable logging of document metadata only (no document fields will be logged).
- Log diffs: Include only differences between write events.
- Ignored users: Define users to be ignored in audit logs.
- Watched indices: List indices to monitor during write events.
 When adding an index, one log entry per document will be generated.

XDR - Quarantine

Suspicious files are quarantined by Blockbit XDR to prevent system damage. In the Quarantine section, you can check the suspicious files and decide whether to allow execution, delete them, or restore them.

Dashboard				((ọ)) (7)	Ŧ
Search						DVF	:
Detection ID	Process Name		Status		Actions		
	41}		Quarantined		© C	~	Ē
	CA}	exe	Quarantined		© C	~	Ê
	3}	exe	Quarantined		@ C	~	Ē
	C}	.exe	Quarantined		© C	~	Ê

To view the list of quarantined files, first select the agent.

In the search bar, you can look for a specific file. To the right of the bar, you can select the query language.



Below, quarantined processes are listed.

Processes are classified as follows:

Detection ID: the identifier assigned to the file by Blockbit XDR; **Process name**: the file name;

Status: the file status, which can be Quarantined, Removed, Allowed (permitted in quarantine), or Restored (returned to its original location).

For each file, four actions are available:

View threat details (^(IIII)): opens a modal with file details, where you can manage the file.

Quarantine Details

{	
"AMProductVersion": "4.18.24090.11",	
"ActionSuccess": true,	
"AdditionalActionsBitMask": 0,	
"CimClass": {	
"CimClassMethods": [],	
"CimClassProperties": [
"ActionSuccess = False",	
"AdditionalActionsBitMask",	
"AMProductVersion = $\"\"$,	
"CleaningActionID",	
"CurrentThreatExecutionStatusID",	
"DetectionID",	
"DetectionSourceTypeID",	
"DomainUser",	
"InitialDetectionTime",	
"LastThreatStatusChangeTime",	
"ProcessName",	
"DemodiationTime"	
C Restore 🗸 Allow 🗊 Remove	
Restore (C): returns the file to its original location.	
\checkmark	
Allow (): permits the file to execute within quarantine.	
ही ह	
Remove (): deletes the file.	

 \times

XDR - Configuration Assessment

The Configuration Assessment searches for vulnerabilities in the configurations selected by the agents on the network.

CIS MICROSOFT WINDOWS 10 ENTERPRISE BE							
 Passed (113) 	CIS Micros	oft Windows 10 Enter	prise Benchmark	v1.12.0 💿			
Failed (278)Not applicable (3)	Pass 11	ed Fi 3 2	ailed 78	Not applicable	Score 28%	End sca Aug 14, 20 08:10:18	an)24 @ 6.000
	Checks (39	4)			C Refresh	🕁 Export fo	ormatted
Policy	Search ID ↑	Title		Target		Result	
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0	15500	Ensure 'Enforce password	history' is set to '24 or	Command: net.exe accounts		• Failed	~
Rows per page: 15 \checkmark \langle 1 \rangle	15501	Ensure 'Maximum passwor	rd age' is set to '365 o	Command: net.exe accounts		Failed	\sim
	15502	Ensure 'Minimum passwor	d age' is set to '1 or m	Command: net.exe accounts		• Failed	\sim
	15503	Ensure 'Minimum passwor	d length' is set to '14	Command: net.exe accounts		• Failed	~
	15505	Ensure 'Relax minimum pa	ssword length limits' i	Registry: HKEY_LOCAL_MACHINE\Sys Set\Control\SAM	tem\CurrentControl	• Failed	~
	15506	Ensure 'Account lockout du	ration' is set to '15 or	Command: net.exe accounts		Failed	~

At the top of the screen, the results of the check are listed:

- Passed: Configurations considered satisfactory.
- Failed: Configurations considered unsatisfactory.
- Not applicable: Configurations that were not considered in the scan.
- **Score**: Percentage of configurations considered satisfactory.
- End scan: The time when the scan ended.

You can check the description and checksum of the agent by clicking on the informational icon.

s document provides pres r Microsoft Windows 10 Er	criptive guidance for establishing a secure nterprise.
80/016520005401931/06	eua3daeca68a8013c01/c1264/3126910189351
8d7b	f652bcd054cf9317ce

- ID: Check identifier.
- **Title**: Title of the check.
- Target: Target of the check.
 Result: Result of the check

Result: Result of the check. Clicking on the result provides more information about the test.

 15500
 Ensure 'Enforce password history' is set to '24 or...
 Command: net.exe accounts
 • Failed

 Rationale

 The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords until they can reuse their original password.

Remediation

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history

By clicking on Inventory, you can view the list of agents that were tested.

Policy	Description	End scan	Passed	Failed	Not applicable	Score
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0	This document provides prescriptive guidance f	Aug 14, 2024 @ 08:10:18.000	113	278	3	28%
Rows per page: 15 🗸						$\langle \underline{1} \rangle$

- Policy: Name of the agent.
 Description: Description of the agent.
 End scan: The time when the scan ended.
 Passed: Configurations considered satisfactory.
 Failed: Configurations considered unsatisfactory.
 Not applicable: Configurations that were not considered in the scan.
 Score: Percentage of configurations considered satisfactory.

XDR - Malware Detection

Blockbit XDR employs a robust set of advanced techniques for the detection and mitigation of malware, ensuring continuous protection against known and unknown threats (Zero Day), fileless attacks, ransomware, miners, APTs (Advanced Persistent Threats), and lateral movement.

The solution operates independently, allowing detection and response to threats even without a connection to the network or the administration console.

The main approaches used include:

Continuous Endpoint and Server Monitoring:

- Identification of suspicious behaviors and anomalous activities in real-time, ensuring protection against zero-day attacks.
- Autonomous threat detection, even when the endpoint is offline, without the need for a connection to the cloud or administration console.

File and Process Analysis:

- Use of advanced detection rules to identify malicious activities, including signatureless malware and real-time exploits.
- Behavioral monitoring and analysis to identify fileless malware and RAM-based threats, which evade traditional detection methods.
- Before sending an alert to the administration console, the agent examines process information locally, evaluating behavior, signatures, and executable characteristics.

Protection Against Zero-Day Attacks and Advanced Exploits:

- Behavioral analysis to detect and block threats without relying on traditional signatures.
- Active monitoring of zero-day exploits, ransomware, cryptocurrency miners, and advanced attack techniques, mitigating risks before they cause damage.

Integration with Threat Intelligence and Indicators of Compromise (IoCs):

- Automatic event correlation with global threat databases, eliminating the need for external queries for immediate responses.
- In-depth analysis of IPs, domains, file hashes, and attack patterns to predict and block emerging threats.

File Integrity Monitoring (FIM):

- · Continuous monitoring of modifications to critical system files, detecting suspicious changes, deletion attempts, and tampering with system logs.
- Detection of ransomware and rootkit-like behaviors, ensuring the integrity of the protected environment.

Advanced Malware Detection with YARA and Heuristic Analysis:

- · Identification of unknown malware patterns through behavioral rules and custom signatures.
- Advanced heuristic evaluation, allowing detection of emerging threats without the need for pre-existing signatures.

Multi-Engine Analysis with VirusTotal and Threat Intelligence:

- Scanning files and URLs using multiple threat detection engines.
- Correlation of threat intelligence to identify malicious behavior patterns and proactively mitigate risks.
- Rapid incident response, automatically blocking suspicious files and processes before they can compromise the environment.

Operational Independence of the Agent:

- The Blockbit XDR agent does not rely on the administration console or the cloud to detect and respond to sophisticated threats, ensuring autonomous and continuous protection.
- Even in isolated environments, the agent can identify and block zero-day attacks, fileless malware, ransomware, miners, and lateral movement techniques, ensuring total protection.

On this page, you can view alerts for anomalies that may be malware over a selected interval.

Malware Detection							. a
Dashboard					१९१ Explore	agent 🗈	Generate report
🗈 🗸 Search				DQL 🔲 🗸 Last 24 hours		Show dates	ී Refresh
cluster.name: blockbit.xdr nule.groups: rootcheck + Add filter							
Activity	~	Alerte					2
6	rule.groups : "rootch	ė.					i i
		Time	r agent.name 🗸 ru	le.description	- rule.level	rule.id 🗸 🗸	Count ~
5-		11:30	blockbit-xdr-manager-master-0 He	ost-based anomaly detection event (rootcheck).	7	510	2
		11:30	Eliezer-Silva Ho	ost-based anomaly detection event (rootcheck).	7	510	4
4		15:30	blockbit-xdr-manager-worker-0 He	ost-based anomaly detection event (rootcheck).	7	510	2
Ŧ		18:00	Eliezer-Silva He	ost-based anomaly detection event (rootcheck).	7	510	2
8 3-		21:30	AD-246 He	ost-based anomaly detection event (rootcheck).	7	510	1
		23:30	blockbit-xdr-manager-master-0 He	ost-based anomaly detection event (rootcheck).	7	510	2
2		03:30	blockbit-xdr-manager-worker-0 He	ost-based anomaly detection event (rootcheck).	7	510	2
		09:30	AD-246 H	ost-based anomaly detection event (rootcheck).	7	510	1
		10:00	Eliezer-Silva He	ost-based anomaly detection event (rootcheck).	7	510	2
12:00 15:00 16:00 21:00 00:00 05:00 05:00 05:00 15:00 16:00 05:00 15:00 16:00 05:00 15:00 16:00 05:00 15:00 16:00 05:00 05:000							< 1 >

Search

The bar allows you to search for specific events. For more information, see the Search System.

Click on Explore agent to select the agent. For more information, see Agents.

To create a report, click on Generate report. The reports are stored in Reports.

Charts



Activity: A graph of anomalies detected in 30-minute intervals. Hovering over a point on the graph shows the number of events at the selected time.

Alerts: List of alerts. They can be classified according to:

- **Time**: Time of detection.
- **agent.name**: Name of the agent that generated the alert.
- rule.description: Description of the rule that generated the alert.
- rule.level: Level of the rule that generated the alert.
- rule.id: Identifier of the rule that generated the alert.
- count: Shows how many times the same rule and agent generated the alert.

XDR - File Integrity Monitoring

Blockbit XDR's File Integrity Monitoring (FIM) provides continuous monitoring of files, directories, and registry keys across all volumes, local disks, removable devices, and volatile storage, detecting in real-time any attempts to create, modify, or delete. This ensures full visibility over suspicious changes, enabling automatic responses such as blocking malicious processes, restoring compromised files, and isolating the endpoint, thereby ensuring data integrity and operational continuity.

File Integrity Monitoring supports:

- · Continuous monitoring of critical files and registries.
- Identification of suspicious changes.
- Real-time alert generation for quick action.



Search

The bar allows you to search for specific events. For more information, see Search System.

Click on Explore agent to select the agent. For more information, see Agents.

To create a report, click on Generate report. The reports are stored in Reports.

In Dashboard, you can view the main information of the selected agent.

Most active users: The most active individual users. Action: The most used actions.

- Add: Add a file.
- · Modify: Modify a file.
- Delete: Delete a file.

Events: Number of events counted every 30 minutes.

Files added: Names of the last files added. Files modified: Names of the last files modified. Files deleted: Names of the last files deleted.

In Inventory, you have a list of the files on the agent's endpoint.

Files (5005)					C Refresh	신 Export formatted
Search						
File 🔨	Last Modified 🛆	User	User ID	Group	Group ID	Size
/bin	Dec 22, 2023 @ 15:26:20.000	root	0	root	0	7
/boot/System.map-6.5.0-44-generic	Jun 18, 2024 @ 10:18:59.000	root	0	root	0	8269177
/boot/System.map-6.8.0-40-generic	Jul 30, 2024 @ 11:33:58.000	root	0	root	0	8654773
/boot/config-6.5.0-44-generic	Jun 18, 2024 @ 10:18:59.000	root	0	root	0	280697
/boot/config-6.8.0-40-generic	Jul 30, 2024 @ 11:33:58.000	root	0	root	0	287007

The following information is shown for each file:

- File: Name of the file.
- Last modified: Last modification.
- User: File user.
- User ID: User identifier.
- Group: File group.
- Group ID: Group identifier.
- Size: File size.

Clicking on a file opens a modal with additional information and events involving the file.

/bo	ot/config-6.8.0-40-generic					×
\sim	Details					
(Last analysis Aug 21, 2024 @ 10:15:43.000	٩	Last modified Jul 30, 2024 @ 11:33:58.000	2	User root	
2	User ID 0	٩	Group root	٩	Group ID 0	
[]	Size 280.28 KB	Õ	Inode 3932176	~	MD5 89883d4a45aebed99039de31c1a21d75	
~	SHA1 d9ceac07bda18106938b15a8d11e297b619e631b	~	SHA256 182b423e6e9ff47614232b5b66733b69d6ae986697	6b31b	f0a7d855f07222c8c	
•	Permissions rw-rr					
\sim	Recent events 🕜				0 h	nits
Sea	rch	DQL			Show dates C Refresh	
+ A	dd filter					

Besides the details shown in the general list, the page also displays:

- Inode: Information about the file's location on the network.
- MD5: File checksum.
- SHA1: File's 160-bit security algorithm.
- SHA256: File's 256-bit security algorithm.
- Permissions: File permissions.

Below are the most recent events involving the file. Clicking on an event shows the data. For more information, visit Collected Data.

XDR - Secure Internet Gateway

The Secure Internet Gateway is a DNS black hole that protects your network from unwanted content. It works by comparing DNS queries against a dynamic list of malicious domains. When a query points to a domain on the list, the Secure Internet Gateway responds with a non-routable IP address.

To access the Secure Internet Gateway, you need a specific password. To avoid entering the password every time, click "Remember Me."



The Secure Internet Gateway dashboard is divided into several sections.

Total Queries



Shows the total number of network queries and the currently active clients. Clicking on it takes you to the client list.

Queries Blocked



Displays the number of blocked queries, with a clickable link to the blocked query list.

Percentage Blocked



Indicates the percentage of blocked queries, leading to the most recent blocked queries when clicked.

Domains on Adlists



Represents the number of domains in the Adlist, which blocks unwanted domains, and links to the full domain list.

Total Queries Over Last 24 Hours



Visualizes queries over the past day in 10-minute intervals.





Tracks client activity over the past day in 10-minute intervals. **Query Types**



Categorizes queries by type, with hover-over percentages for each.

Upstream Servers



Displays the most frequently used upload servers, also with percentage details on hover.

Top Permitted Domains

Lists the most accessed allowed domains, categorized by domain URL, number of hits, and frequency of access.

Top Permitted Domains

Domain	Hits	Frequency
www.google.com	2790	
gateway.fe2.apple-dns.net	1995	
teams.events.data.microsoft.com	1675	
lbdns-sdudp.0.20.16.172.in-addr.arpa	1450	
teams.microsoft.com	1369	
mmx-ds.cdn.whatsapp.net	1278	
lbdns-sdudp.relax.blockbit.com	1271	
outlook.office365.com	1219	
gateway.icloud.com	1204	

Top Blocked Domains

Lists the most frequently blocked domains categorized by domain URL, number of hits, and frequency of access.

Top Blocked Domains

Domain	Hits	Frequency
graph.facebook.com	1288	
mobile.pipe.aria.microsoft.com	1268	
horizon-track.globo.com	484	
web.facebook.com	351	
app-measurement.com	339	
7ba3f64df98de730df38846b54ecfbdf7f61f80f.cws.conviva.com	277	
mqtt-mini.facebook.com	261	
www.facebook.com	236	

Top Clients (Total)

Top Clients (total)

Client	Requests	Frequency
10-244-2-12.ama-metrics-operator-targets.kube- system.svc.cluster	117468	
10-244-1-35.ingress-nginx-pi-hole-tcp-controller.pi- hole.svc.clu	9861	_
localhost	143	

Lists the clients with the most requests, showing client ID, number of requests, and request frequency.

Top Clients (Blocked Only)

Top Clients (blocked only)					
Client	Requests	Frequency			
10-244-2-12.ama-metrics-operator-targets.kube- system.svc.cluster	6389				
10-244-1-35.ingress-nginx-pi-hole-tcp-controller.pi- hole.svc.clu	1759				

Lists clients with the highest number of blocked requests, also categorized by client ID, request count, and request frequency.

XDR - Secure Internet Gateway - Groups

The Secure Internet Gateway allows the creation of client or domain groups.

With these groups, you can enable or disable DNS blocking simultaneously for all elements in the group.



Below, there is a list of groups.

List	of groups					
Show	10 v entries				Search:	
					Previou	s Next
	Name	↓† Status	ļţ	Description		↓↑
	Default	Enabled		The default group		
	group	Enabled		New group		Û
	group,	Enabled				0
	nouvelle	Enabled				
Show	ring 1 to 4 of 4 entries				Previou	s Next
Groups are created with DNS blocking enabled by default. Click Enabled (Enabled) to disable it.						
To edit th	e name and description, click on the Name or Des	scription fields.				
To delete	a group, click the trash icon (
You can	delete multiple groups simultaneously by selecting	them and clicking	Delete All ().		



) when no group is selected or the + (

Ð

) when at least one group is selected.

To select all groups, click the dark green box (

XDR - Secure Internet Gateway - Groups - Adlists

An Adlist is a list of domains known for delivering advertisements. By blocking DNS queries to these domains, the advertising content on a page does not load.

On this page, you can add Adlists and organize them into groups.

After updating an Adlist, refresh Gravity (the blocked domains list).	
Add a new adlist	
Address:	Comment:
URL or space-separated URLs	Adlist description (optional)
Hints: 1. Please run blockbithole -g or update your gravity list online after modifying you 2. Multiple adlists can be added by separating each <i>unique</i> URL with a space 3. Click on the icon in the first column to get additional information about your lists. T	our adlists. he icons correspond to the health of the list. A
Fo add an Adlist, enter the URL in Address , provide a description in Comr Fo enter multiple URLs, separate them with spaces.	nent, and click Add ().
n List of Adlists, you will find a list of Adlists.	
Inder Address, the URLs of the Adlists are listed.	
Clicking the () and () icons provides additional information abo	but the Adlist.
Adlists are enabled by default. In Status, click Enabled (to disable it.
o enable it, click Disabled (
o edit the description, click on the Comment field.	
n Group Assignment, you can assign the Adlist to a group.	
Click the button with the group name (e.g., Default) and select the group for	or the Adlist.
Apply	

To delete an Adlist, click the trash icon (

Û

earch:

Default

group, nouvelle groupe

Default 🔺

-



Ð

You can delete multiple Adlists simultaneously by selecting them and clicking Delete All (



To select all Adlists, click the dark green box (

) when no Adlist is selected or the + (

when at least one Adlist is selected.

XDR - Secure Internet Gateway - Groups - Clients

Known clients:	Comment:
Select client	Client description (optional)
	onfirming your entry with 🖻 .
	bnets (CIDR notation, like 192.168.2.0/24), their MAC addresses (like / are connected to (prefaced with a colon, like :eth0).
	address, host name or interface recognition as the two latter will only be available after some ing hop away from your blockbit-sgi.
	Add

Add

) or press Enter.

A client can be identified by its IPv4 or IPv6 address, IP Subnet, MAC Address, hostname, or the interface it is connected to.

In List of Configured Clients, you can assign the client to a group.

Click the button with the group name (e.g., Default) and select the group for the client.

To add a client to the group, select it from the list of known clients and click Add (

Li Sł	st of configured clients ow 10 ✔ entries 2 ๗				Apply All None Default 🖍 group,	Previous	Next
	Client	11	Comment	11	groupe		.↓↑
	a				Default 🔺		
						Previous	Next
Sł	owing 1 to 1 of 1 entries						
To ec	it the description, click or lete a client, click the tra :	n the Comment field	d.				
				_			
You o	an delete multiple clients	simultaneously by	selecting them and clicking De	elete All (
To se	ect all clients, click the d	ark green box () when no client is select	ted or the + () w	vhen at least one client i	s selected.	

XDR - Secure Internet Gateway - Groups - Domains

The Secure Internet Gateway has two domain lists:

Whitelist: A list of acceptable domains. Blacklist: A list of unacceptable domains.

You can add a domain or a regular expression (Regular Expression or RegEx) to either list.

Domain	RegEx filter				
Domain:			Comment:		
Domain t	o be added		Description (optional)		
Add dom Check this b	ia in as wildcard box if you want to involve all subdomains. The entered domain will be conv	erted	to a RegEx filter while adding.		
Note: The domain o Other groups	or regex filter will be automatically assigned to the Default Group. can optionally be assigned in the list below (using Group assignment).				
				Add to Blacklist	Add to Whitelist

To add a domain, enter the URL in the Domain field and a description in Comment.

You can add the domain as a Wildcard, which will match queries to non-existent domains.

Domain RegEx filter	
Regular Expression:	Comment:
RegEx to be added	Description (optional)
Hint: Need help to write a proper RegEx rule? Have a look at our online regular expressions tutorial.	

To add a RegEx, enter the expression in the Regular Expression field and a description in Comment.

	Add to Blacklist	
To add to the Blacklist, click Add to Blacklist ().
To add to the Whitelist click Add to Whitelist (Add to Whitelist	

In List of Domains, you will find a list of domains or RegEx entries and their groups.

List of domains		✓ Exact whitelist	✓Regex whitelist	✓Exact blacklist	ex blacklist
Show 10 v entries				Search:	
				Previous	Next
Domain/RegEx	↓↑ Туре	↓† Status ↓† Comme	ent	↓↑ Group assignment	11
	Exact blacklist 🐱	Enabled		Default -	
	Exact blacklist 🐱	Enabled Adde	ed from Query Log	Default -	
	Exact whitelist 🐱	Enabled Adde	ed from Query Log	Default -	D
	Regex blacklist 🗸	Enabled		Default -	
	Regex whitelist 🗸	Enabled		Default -	
				Previous	Next
Showing 1 to 5 of 5 entries					
Under Type , you can change	e the domain record type:				

Exact Whitelist: Adds the exact domain to the Whitelist. RegEx Whitelist: Applies the defined RegEx rule to the Whitelist. Exact Blacklist: Adds the exact domain to the Blacklist. RegEx Blacklist: Applies the defined RegEx rule to the Blacklist.

You can filter records by type in the upper right corner.

Exact whitelist	Regex whitelist	✓Exact blacklist	Regex blacklist
Domains are added with DNS b	locking enabled by default. In	Status, click Enabled (abled) to disable it.
To enable it, click Disabled (Disabled).		
To edit the description, click on	the Comment field.		
In Group Assignment, you can	assign the domain or RegExt	to a group.	
Click the button with the group r	name (e.g., Default) and selec	t the group for the domain or	RegEx.
Apply			

Ŵ



To delete a domain or RegEx, click the trash icon (

You can delete multiple domains or RegExes simultaneously by selecting them and clicking Delete All (



lick the dark green box () when no domain or RegEx is selected or the + () when at least one domain

To select all domains or RegExes, click the **dark green box** () when no domain or RegEx is selected or the + or RegEx is selected.

XDR - Secure Internet Gateway - Local DNS

In this section, you can list local DNS servers. These servers resolve domains within the local network instead of using external servers.

You can add servers using domain/IP pairs or CNAME records.

DNS Records

This option lists domain/IP pairs.

Domain:		IP Address:
Domain or comma-separated list of domains		Associated IP address
Note: The order of locally defined DNS records is: 1. The device's host name and pi.hole 2. Configured in a config file in /etc/dnsmasq.d/ 3. Read from /etc/hosts 4. Read from the "Local (custom) DNS" list (stored in /etc/pihole/custom Only the first record will trigger an address-to-name association.	.list)	Add
o add a pair, enter the domain in Domain and the associated IP a	ddress in I	in IP Address, then click Add ().
List of local DNS domains		
Show 10 v entries		Search:
Domain 4	IP	11 Action
www.domain.com	2.2.2.2	2 🔟
www.site.org	1.1.1.1	1 🔟
Showing 1 to 2 of 2 entries		Previous Next

In List of Local DNS Domains, you will find a list of domain/IP pairs.

- Domain: The domain name.
- IP: The IP address associated with the domain.

Û

To delete a pair, click the trash icon (

CNAME Records

This option lists alias domain and canonical domain pairs.

Example: **blog.site.com** is an alias domain, and **www.site.com** is the canonical domain.

Add a new CNAME record	
Domain:	Target Domain:
Domain or comma-separated list of domains	Associated Target Domain
Note: The target of a CNAME must be a domain that the blockbit-sg	gi already has in its cache or is authoritative for. This is a universal limitation of CNAME records.
The reason for this is that blockbit-sgi will not send additional q to the client may be incomplete. blockbit-sgi just returns the inf <i>activ</i> e DHCP leases work as targets - mere DHCP <i>leases</i> aren't su	queries upstream when serving CNAME replies. As consequence, if you set a target that isn't already known, the repl formation it knows at the time of the query. This results in certain limitations for CNAME targets, for instance, only ufficient as they aren't (yet) valid DNS records.
Additionally, you can't CNAME external domains (bing.com serve content for the requested domain.	to google.com) successfully as this could result in invalid SSL certificate errors when the target server does not
	Add
er the alias domain in Domain and the canonical d	domain in Target Domain .
Add	
add, click Add (

- Domain: The alias domain. Target: The canonical domain.



XDR - Secure Internet Gateway - Query Log

The page lists the most recent queries.

To search for a specific query, use the search bar.

You can choose how many queries are displayed per page. To show all, click Show All.



- Time: Date and time of the query.
- Type: Type of query. Each type retrieves different data.
- Domain: The domain the query is expecting a response from.
- Client: The client making the query.
- Status: The state of the query, which can be Blocked (query blocked) or OK (query answered).
- **Reply**: The response time and type.
- Action: Possible actions.



XDR - Secure Internet Gateway - Query Log - Long Term Data

On these pages, you can track data over a specific time range.

To display data, select the time range in Select Date and Time Range. For a custom range, choose Custom Range.

Graphics

This page displays the number of queries over time in a graphical format.



Query Log

This page lists queries within the selected time range.

Total Queries



The total number of queries on the network.

Queries Blocked



The number of blocked queries.

Queries Blocked (Wildcard)



The number of queries blocked and redirected to a default domain.

Percentage Blocked



The percentage of blocked queries.

The query list contains the following data:

- Time: Date and time of the query.
 Type: Type of query. Each type retrieves different data.
- **Domain**: The domain the query is expecting a response from.
- Client: The client making the query.
 Status: The state of the query, which can be Blocked (query blocked) or OK (query answered).
- Reply: The response time and type.
- Action: Possible actions.

⊗ Blacklist If a query has been answered, it can be blocked and moved to the Blacklist (✓ Whitelist

If a query has been blocked, it can be allowed and moved to the Whitelist (

Top Domains

Top Domains

Domain	Hits	Frequency
www.google.com	8193	
gateway.fe2.apple-dns.net	2703	
outlook.office365.com	2410	
mmx-ds.cdn.whatsapp.net	2371	
chat.cdn.whatsapp.net	2367	
in.appcenter.ms	2160	
i.instagram.com	1809	
www.msftconnecttest.com	1761	
teams.microsoft.com	1692	
teams.events.data.microsoft.com	1482	

This list shows the most accessed allowed domains. It is divided into:

- Domain: The domain URL.
- Hits: The number of accesses.
- Frequency: The access frequency.

Top Blocked Domains

Top Blocked Domains

Domain	Hits	Frequency
graph.facebook.com	1288	
mobile.pipe.aria.microsoft.com	1268	
horizon-track.globo.com	484	
web.facebook.com	351	
app-measurement.com	339	
7ba3f64df98de730df38846b54ecfbdf7f61f80f.cws.conviva.com	277	
mqtt-mini.facebook.com	261	
www.facebook.com	236	

This list shows the most accessed blocked domains. It is divided into:

- Domain: The domain URL. Hits: The number of accesses.
- Frequency: The number of access attempts.

Top Clients (Total)

Top Clients (total) Client Requests Frequency 117468 9861 143

This list shows the clients with the most requests. It is divided into:

- Client: The client ID.
- Requests: The number of requests.
 Frequency: The request frequency.

40

XDR - Threat Hunting

Threat Hunting in Blockbit XDR is an active search process for threats, allowing security analysts to investigate early-stage cyberattacks, suspicious activities, and behavioral anomalies even before alerts are triggered.

Blockbit XDR offers complete workflows for threat research and investigation, combining automation, artificial intelligence, and manual analysis. Through an interactive timeline, you can conduct deep forensic analyses, visualizing the entire sequence of events and processes related to the threat, from its origin to its final impact. This approach allows for identifying the attack's behavior, entry vectors, and compromised assets, ensuring a swift and accurate response.

With Blockbit XDR, you can:

- Analyze unusual behaviors and anomalies in endpoints, network, and applications.
- · Automatically correlate events and indicators of compromise (IoCs).
- Access and filter detailed logs to identify attack patterns and lateral movement.
- Create and automate custom search and detection rules.
- Map threats to the MITRE ATT&CK framework, enabling a strategic and effective response.

With this structured workflow, Blockbit XDR enables analysts to identify and neutralize advanced threats such as APTs (Advanced Persistent Threats), fileless malware, zero-day exploits, and data exfiltration attempts, reducing risks and strengthening the organization's security.

In this page, you can check ongoing threats.

Dashboard				ଏଡ଼) qaubt (002) 📮 📄 Generate report
E V Search	DQL	iiii ∽ Last 24 hours	Show dates C Refresh		
cluster.name: blockbil-xdr agent.ld: 002 + Add filter					
Top 5 rule groups	Top 5 alerts	2	Тор	10 Alerts by Level	c ⁿ
60 Count	±			Ł.	
50	Description V Count	~	Le	vel ~ Count	~
	Apparmor DENIED 40		7	45	
40 - 14 -	Listened ports status (netstat) changed (new 16		3	43	
8 30-	Dpkg (Debian Package) half configured. 12				
20 -	New dpkg (Debian Package) installed. 7				
10 -	Integrity checksum changed. 6				
	Host-based anomaly detection event (rootche 4				
syste oses change	PAM: Login session opened. 3				
ant <u>e</u>					
rule.groups: Descending	< 1	>			< 1 >

Search

The bar allows you to search for specific events. For more information, see Search System.

Click on Explore agent to select the agent. For more information, see Agents.

To create a report, click on Generate report. The reports are stored in Reports.

The page presents the following charts:

Top 5 rule groups: Rule groups that generated the most alerts.

Top 5 alerts: Most common alerts.

Top 10 alerts by level: Rule levels with the most alerts.

Top 10 alerts group evolution: Number of alerts per 30-minute period, separated by group.

Alerts: Number of alerts per 30 minutes.

Below is the list of alerts.

Secu	Security Alerts								
	Time	Technique(s)	Tactic(s)	Description	Level 个	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: Time of the alert.
 Technique(s): Techniques detected in the alert.
 Tactic(s): Tactics detected in the alert.
 Description: Description of the alert.
 Level: Level of the violated rule.

- Rule ID: Identification of the violated rule.

Clicking on each event will show the involved data. For more information, see Collected Data.

XDR - Threat Monitor - CTI

Blockbit XDR offers the Threat Monitor - CTI, a space where you can store, organize, and visualize your threat intelligence and observations database.

XDR - Threat Monitor - CTI - Dashboard

The first page you encounter is the Dashboard. Here, you will find key information about what is happening in your organization.

To locate any element in the platform, use the search bar.





In Bulk Search (

you can search for batches of elements by entering keywords.

In the upper right corner, there are four available actions. For more information, visit Actions.



Key Metrics

- · Intrusion sets: Number of intrusion sets (consistent malicious activities);
- Malware: Number of malware instances;
- Reports: Number of reports;
- Indicators: Number of indicators.

Charts

- Most active threats (last 3 months): List of the most prevalent threats in the last 3 months;
- Most targeted victims (last 3 months): List of the most intensely targeted victims in the last 3 months;
- Relationships created: Number of relationships created in the last 12 months, separated by month;
- Most active malware (last 3 months): Most active malware in the last 3 months;
- Most active vulnerabilities (last 3 months): Vulnerabilities with the most relationships in the last 3 months;
- Targeted countries (last 3 months): Countries most intensely attacked in the last 3 months.

Latest Reports

The Latest Reports section contains a list of the most recent reports. These reports are categorized by:

- Type: Clicking the label redirects you to a page with information about the type of threat;
- Value: The recorded value;
- Author: The author of the threat report;
- Date: The date of the threat report;
- Labels: Tags assigned to the threat, used for classification;
- Markings: Status markings assigned to the threat, used for classification;
- Platform creation date: The date the threat was cataloged on the platform.

Next to this section, there is an additional chart:

• Most active labels (last 3 months): The most frequently assigned labels in the last 3 months.

XDR - Threat Monitor - CTI - Dashboard - Actions

In the upper right corner, there are four available actions:



Here, you can check system notifications.

Notifications are classified by:

	OPERATION	MESSAGE	ORIGINAL CREATI	•	TRIGGER
 Operation Message Original 	on: The operation e: The notificatio creation date:	n that generated the notification; n message; The date of the notification;			

Trigger: The trigger responsible for the notification.



Triggers (

Here, you can check the triggers that generate notifications.

Triggers are classified by:

TYPE	NAME	•	NOTIFICATION	TRIGGERING ON	DETAILS

- **Type**: The type of trigger;
- Name: The name of the trigger;
- Notification: The notification generated by the trigger;
- **Triggering on**: The event that activated the trigger;
- Details: Additional details about the trigger.



Here, you can manage the user profile.

Profile

Profile
Name
Emeil address
Organizations
Firstname
Lastname
Description

Modify user details such as name, email, organization, and description.

Feedback

Write P	Preview]	НB	I S	o ,,	«Þ 🖪	:= 1	≣∛≣					
Confidence	level											
100						<u>1-C</u>	onfirmed b	y other sour	ces			_
												•
Rating												
\odot	900											
Entities												Ô
Associated file	1											
SELECT	YOUR FILE	No file	e selected.									
1-												
Labels											+	<u> </u>
										CANCEL	CREA	TE

Provide feedback about the platform.

Specify:

- Description: A description of your feedback;
 Confidence level: Enter the confidence level and the probability of being correct;
 Rating: Select a rating for your experience. One face means dissatisfied, five faces mean satisfied;
 Entities: Enter the involved entities;
 Associated file: Upload an associated file;
 Labels: Add relevant tags.

Logout

Log out of CTI.
XDR - Threat Monitor - CTI - Analyses

On this page, threat analyses are grouped together.

To search for a result, use the search bar. You can filter searches in Add filter.

When selecting an element, the action bar appears. The following actions are available:



Reports

Here, you will find Report objects, which are collections of threat descriptions focused on specific topics.

٩	Search these results Add filter	▼ X					4 1-25/1	9K 🕨 🚉
	NAME	ТҮРЕ	AUTHOR	CREATORS	LABELS	DATE 👻	STATUS	MARKING
	DNS Early Detection - Fast		AlienVault	admin	information stealer fa	ke Feb 28, 2025	NEW	TLP:CLEAR
	Long Live The Vo1d Botnet: New		AlienVault	admin	botnet vold pro	xy Feb 28, 2025	NEW	TLP:CLEAR
	akira has published a new		Ransomware.Live	admin	No label	Feb 28, 2025	NEW	TLP:CLEAR

These objects are categorized by:

- Name: Object name;
- Type: Object type. Clicking the label redirects you to a page with information about the threat;
- Author: Threat author;
- Creators: Object creator;
- Labels: Tags assigned to the threat, used for classification;
- Date: Threat date;
- Status: Object status;
- Markings: Status markings assigned to the threat.

Groupings

Here, you will find Grouping objects, which are ongoing threat investigations.

	IAME	CONTEXT	AUTHOR	CREATORS	LABELS	ORIGINAL CRE	STATUS	MARKING
N	IAT	SUSPICIOUS	MongoDB	admin	No label	Jul 31, 2024	DISABL	TLP:AMB)

These objects are categorized by:

- Name: Object name;
- Context: Object context;
- Author: Threat author;
- Creators: Object creator;
- Labels: Tags assigned to the threat, used for classification;
- Original creation: Threat creation date;
- Status: Object status;
- Markings: Status markings assigned to the threat.

Malware Analyses

Here, you will find Malware analyses.

RESULT NAME	PRODUCT	OPERATING SYSTEM	AUTHOR	CREATORS	LABELS	SUBMISSION DATE	MARKING

These analyses are categorized by:

- Result name: Name of the analysis;
- Product: Analysis result;
- Operating system: Operating system;
- Author: Analysis author;
- Creators: Analysis creator;
- Labels: Tags assigned to the threat, used for classification;
- Submission date: Date of analysis submission;
- Markings: Status markings assigned to the threat.

Notes

Notes are annotations made by CTI users.

ABSTRACT	ТҮРЕ	AUTHOR	CREATORS	LABELS	ORIGINAL CRE	STATUS	MARKING

They are categorized by:

- Abstract: Summary of the note;
- Type: Note type;
- Author: Note author;
- Creators: Note creator;
- Labels: Tags assigned to the note, used for classification;
- Original creation date: Note creation date;
- Status: Note status;
- Markings: Status markings assigned to the note.

External References

External references are knowledge bases outside the CTI.

SOURCE NAME	EXTERNAL ID	URL	CREATORS	ORIGINAL CREATION DAT
cve@mitre.org		http://marc.info/?l=bugtraq&m=107696235424865&w=2	admin	Jul 22, 2024
cve@mitre.org		http://www.securityfocus.com/archive/1/262074	admin	Jul 22, 2024

They are categorized by:

- Source name: Reference name;
- External ID: Reference identifier;
- URL: Reference URL;
- Creators: Reference creator;
- Original creation date: Reference creation date.

XDR - Threat Monitor - CTI - Cases

Here are grouped cases that need attention.

To search for a result, use the search bar. You can filter searches in Add filter.

When selecting an element, the action bar appears. The following actions are available:



Incident Responses

Here, incident responses are grouped together.

NAME	PRIORITY	SEVERITY	ASSIGNEES	CREATORS	LABELS	ORIGINAL CRE	STATUS	MARKING
CVE-2024-6387				admin	No label	Jul 31, 2024	DISABL	NONE >

- Name: Case name;
- Priority: Case priority;
- Severity: Case severity;
- Assignees: Individuals responsible for the case;
- Labels: Tags assigned to the case, used for classification;
- Original creation: Case creation date;
- Status: Case status;
- Markings: Status markings assigned to the case.

Requests for Information

Here, requests for information are grouped together.

NAME	PRIORITY	SEVERITY	ASSIGNEES	CREATORS	LABELS	ORIGINAL CI	STATUS	MARKING
 Name: Request name; Priority: Request priority; Severity: Request severi Assignees: Individuals re Labels: Tags assigned to Original creation: Request status; Markings: Status marking 	; ity; esponsible fo o the request, est creation d	r the request; used for class ate;	sification;					

Requests for Takedown

Here, takedown requests are grouped together.

NAME	PRIORITY	SEVERITY	ASSIGNEES	CREATORS	LABELS	ORIGINAL CI	STATUS	MARKING

- Name: Request name;
- Priority: Request priority;

- Severity: Request severity;
- Assignees: Individuals responsible for the request;
- Labels: Tags assigned to the request, used for classification;
- Original creation: Request creation date;
- Status: Request status;
- Markings: Status markings assigned to the request.

Tasks

Here, assigned tasks are grouped together.

NAME	DUE DATE	ASSIGNEES	LABELS	STATUS
Name: Task name; Due date: Task deadline;				

- Assignees: Individuals responsible for the task;
- Labels: Tags assigned to the task, used for classification;
- Original creation: Task creation date;
 Status: Task status.

Feedbacks

Here, case evaluations are grouped together.

NAME 🔺	RATING	AUTHOR	CREATORS	LABELS	ORIGINAL CRE	STATUS	MARKING

- Name: Evaluation name;
- Rating: Evaluation score;
- Author: Evaluation author;
- Creators: Evaluation creators;
- Labels: Tags assigned to the evaluation, used for classification;
- Original creation: Evaluation creation date;
- Status: Evaluation status;
- Markings: Status markings assigned to the evaluation.

XDR - Threat Monitor - CTI - Observations

Here are grouped elements that needs to be observed.

To search for a result, use the search bar. You can filter searches in Add filter.

When selecting an element, the action bar appears. The following actions are available:



Observables

Here, observable objects or immutable elements are listed.

ТҮРЕ	REPRESENTATION	AUTHOR	CREATORS	LABELS	PLATFORM CRI	MARKING
• Type: Object	type;					

- Representation: Object
- Author: Object creator;
 Creators: Individuals who obsorp
- Creators: Individuals who observed the object;
- Labels: Tags assigned to the object, used for classification;
- Platform creation date: Date the observable was created;
- Markings: Status markings assigned to the object.

Artifacts

Here, artifacts are listed, which are specific observables.



- Value: Artifact value;
- File name: File name;
- MIME/Type: Artifact type;
- File size: File size;
- Author: Artifact creator;
- Creators: Individuals who observed the artifact;
- Labels: Tags assigned to the artifact, used for classification;
- Platform creation date: Date the artifact was created;
- Markings: Status markings assigned to the artifact.

Indicators

Here, indicators or detection objects are listed.

	PATTERN TYPE	NAME	AUTHOR	CREATORS	LABELS	ORIGINAL CREATION DAT	MARKING
--	--------------	------	--------	----------	--------	-----------------------	---------

- Pattern type: Search pattern type. This pattern helps identify potential threats;
- Name: Object name;
- Author: Object creator;
- Creators: Individuals who created the object;
- Labels: Tags assigned to the object, used for classification;

- Platform creation date: Date the object was created;
- ٠ Markings: Status markings assigned to the object.

Infrastructures

Here, infrastructures are listed, which are resources used by a threat in its activities.

NAME	TYPE	AUTHOR	CREATORS	LABELS	ORIGINAL CRE	MARKING

- Name: Object name;
 Type: Object type;
 Author: Object creator;
 Creators: Individuals who created the object;
 Labels: Tags assigned to the object, used for classification;
 Original creation date: Date the object was created;
 Markings: Status markings assigned to the object.

XDR - Threat Monitor - CTI - Threats

This tab is part of the CTI library. Here, threat entries are listed.

Threats are divided into:

- Threat actors (groups): Groups known for attacks.
- Threat actors (individuals): Individuals known for attacks.
- Intrusion sets: Consistent malicious activities, including technical and non-technical elements that define when, how, and why a threat acts.
- Campaigns: Series of attacks occurring over a period or targeting consistent victims.

To search for a result, use the search bar. You can filter searches in Add filter.

o abyss January 25, 2	025
KNOWN AS	USED MALWARE
TARGETED	TARGETED SECTORS
-	
ransomware	

In addition to the name, date, and labels, each entry has a card with the following information:

- Known as: Alias of the threat;
- Used malware: Malware used;
- Targeted countries: Affected countries;
- Targeted sectors: Affected sectors.

Clicking on a label will show all CTI information related to the entry.

XDR - Threat Monitor - CTI - Arsenal

This tab is part of the CTI library. Here, elements for an attack are listed.

To search for a result, use the search bar. You can filter searches in Add filter.

Malware

Malware refers to any piece of code designed to cause harm or gain unauthorized access to a system.

Here, malwares are listed by entry.

#HSTR:HackT July 22, 2024	ool:Win32/Mimikatz 🛧
KNOWN AS	CORRELATED INTRUSION SETS -
TARGETED COUNTRIES -	TARGETED SECTORS
No label	

In addition to the name, date, and labels, each entry has a card with the following information:

- Known as: Alias of the threat;
- Correlated intrusion sets: Related intrusion sets;
- Targeted countries: Affected countries;
- Targeted sectors: Affected sectors.

Clicking on a label will show all CTI information related to the entry.

Channels

Here, channels used by threat actors to disseminate information are listed.

	TYPES	LABELS	ORIGINAL CREATION DAT	MODIFICATION DATE
 Name: Channel to Type: Channel to Labels: Tags as: Original creation Modification data 	name; /pe; signed to the channel, used for classificatior n date : Channel creation date; te : Channel modification date.	ı;		

Tools

Here, legitimate tools that can be used in attacks are listed.

NAME 🔺	TYPES	LABELS	ORIGINAL CREATION DAT	MODIFICATION DATE
Name: Tool name;				

152

• Type: Tool type;

- Labels: Tags assigned to the tool, used for classification;
- Original creation date: Tool creation date;
 Modification date: Tool modification date.

Vulnerabilities

Here, known vulnerabilities that can be exploited in an attack are listed.

NAME A	CVSS3 - SEVERITY	LABELS	ORIGINAL CREATION DAT	MODIFICATION DATE	CREATORS

- Name: Vulnerability name;
 CVSS3 Severity: Vulnerability severity rating;
 Labels: Tags assigned to the vulnerability, used for classification;
 Original creation date: Vulnerability creation date;
 Modification date: Vulnerability modification date;
 Orginal creation date: Vulnerability modification date;

- Creators: Individuals who created the vulnerability entry.

XDR - Threat Monitor - CTI - Techniques

This tab is part of the CTI library. Here, attack techniques are listed.

To search for a result, use the search bar. You can filter searches in Add filter.

Attack Patterns

Here, attack patterns used by a threat are listed. These patterns are based on MITRE ATT&CK.

	KILL CHAIN PHASE	ID		LABELS	ORIGINAL CREATION DAT	MODIFICATION DATE			
Addit	 Kill chain phase: MITRE ATT&CK phase; ID: Identifier; Name: Pattern name; Labels: Tags assigned to classify the pattern; Original creation date: Pattern creation date; Modification date: Pattern modification date. Additionally, the following are listed:								
Thes	 Narratives: Attack narratives used by threat actors; Course of action: Actions taken to prevent or respond to an attack; Data components: Values from a data source that can be detected; Data sources: Data sources that can be collected. 								
		-							
	NAME A			LABELS	ORIGINAL CREATION DAT	MODIFICATION DATE			

- Name: Element name;
- Labels: Tags assigned to classify the element;
- Original creation date: Element creation date;
 Modification date: Element modification date.

XDR - Threat Monitor - CTI - Entities

This tab is part of the CTI library. Here, entities that may be involved in an attack are listed.

To search for a result, use the search bar. You can filter searches in Add filter.

Sectors

Here, sectors that may be targeted in an attack are listed.

▦	Academic Institutions	This sector does not have any description.
	Accounting	This sector does not have any description.

They are categorized by Type and a Description.

Events

Here, real-world events are listed.

NAME 🔻	TYPES	START DATE	END DATE	ORIGINAL CREATION DATE
 Name: Event name; Type: Event type; Start date: Event start date: 				

- date
- End date: Event end date;
- Original creation date: Event creation date.

Organizations

Here, real-world organizations are listed.

NAME 🔻	LABELS	ORIGINAL CREATION DATE	MODIFICATION DATE
• Name: Organization name;			
 Labels: Tags assigned to classify the o 	rganization;		
 Original creation date: Organization cl 	reation date;		
 Manifelia esta an alasta : Ourora la stica ana alti 	and an allow		

Modification date: Organization modification date.

Systems

Here, systems and technologies are listed.

NAME 👻	LABELS	ORIGINAL CREATION DATE	MODIFICATION DATE
Name: System name;			
 Labels: Tags assigned to classify the system; 			
 Original creation date: System creation date; 			
 Modification date: System modification date. 			

Individuals

Here, individuals are listed.

NAME 🔻	LABELS	ORIGINAL CREATION DATE	MODIFICATION DATE

- Name: Individual's name;
 Labels: Tags assigned to classify the individual;
 Original creation date: Individual creation date;
 Modification date: Individual modification date.

XDR - Threat Monitor - CTI - Locations

This tab is part of the CTI library. Here, real-world locations are listed.

To search for a result, use the search bar. You can filter searches in Add filter.

NAME - ORIGINAL CREATION DATE MODIFICATION DATE

- Name: Location name;
- Original creation date: Location creation date;
- Modification date: Location modification date.

Locations are categorized as:

- Regions: Large areas, such as continents;
- Countries: Countries of the world;
- Areas: Extensive regions, such as subnational units;
- Cities: Cities of the world;
- **Positions**: Precise locations on the globe.

XDR - Threat Monitor - CTI - Events

All the events are grouped in this page.

To search for a result, use the search bar. You can filter searches in Add filter.

When selecting an element, the action bar appears. The following actions are available:



Incidents

Here, incidents are listed, which are negative events occurring in the system.

INCIDENT	SEVERITY	ASSIGNEES	CREATORS	LABELS	ORIGINAL CRE	STATUS	MARKING

- Name: Incident name;
- Incident type: Type of incident;
- Severity: Severity of the incident;
- Assignees: People responsible for the incident;
- Creators: Creators of the incident report;
- Labels: Labels assigned to the incident. Labels help classify the incident;
- Original creation date: Incident creation date;
- Status: Incident status;
- Markings: Markings received by the incident. Markings help classify the incident's status.

Sightings

Here, sightings are listed, which are observable events occurring in the system. Each sighting is treated as an entity.

QUALIFICATION	N	NAME	ENTITY TYPE	ENTITY	FIRST OBS.	LAST OBS. 🔻	CONFIDENCE	STATUS

- Qualification: Entity qualification. It can be false positive or true positive;
- Nb.: Filtered entities;
- Name: Entity name;
- Entity type: Type of entity;
- Entity: The observed entity;
- First obs.: Date of first appearance;
- Last obs.: Date of last appearance;
- Confidence: Reliability of the information;
- Status: Sighting status.

Observed data

Here, log extracts containing observable data are listed.

NAME	NB.	FIRST OBS.	LAST OBS. 🔻	AUTHOR	LABELS	MARKING
						1

- Name: Name of the observed data;
- Nb.: Filtered data;

- First obs.: Date of first appearance;
 Last obs.: Date of last appearance;
 Author: Author of the observation;
 Labels: Labels assigned to the observation. Labels help classify the observation;
 Markings: Markings received by the observation. Markings help classify the observation's status.

XDR - Threat Monitor - CTI - Data

In this tab, you can consult behavior, relationships, and data ingestion.

Entities

Here, you can consult entities.

ТҮРЕ	NAME	AUTHOR	CREATORS	LABELS	PLATFORM CREATION DAT	MARKING
• Type	e. Entity type:					
• Nam	e: Entity name:					
Auth	or: Entity author;					
Creation	tors: Entity creator;					
 Labe 	els: Labels assigned to the entity	. Labels help classify the entit	ty;			
 Plat 	orm creation date: Creation date	te;	-			
 Marl 	kings: Markings received by the	entity. Markings help classify	the entity's status	6.		

Relationships

Here, relationships created between various data are listed.

		FROM TYPE	FROM NAME	TYPE	TO TYPE	TO NAME	AUTHOF	CREATO	PLATFORM CREATI	MARKING
--	--	-----------	-----------	------	---------	---------	--------	--------	-----------------	---------

Relationships are classified by:

- From type: Source type;
- From name: Source name;
- Type: Relationship type;
- To type: Destination type;
- To name: Destination name;
- Author: Relationship author;
- Creators: Relationship creator;
- Platform creation date: Creation date;
- Markings: Markings received by the relationship. Markings help classify the relationship's status.

Ingestion

In this tab, you can check data ingestion flows (streams and feeds).

Workers statistics					
3	0	0/s	257.4/s	0.2/s	241.091
CONNECTED WORKERS	QUEUED BUNDLES	# BUNDLES PROCESSED	READ OPERATIONS	WRITE OPERATIONS	TOTAL NUMBER OF DOCUMENTS
Registered connectors					
# NAME -	ТҮРЕ	AUTOMATIC TRIGGER	MESSAGES STATUS	MODIFIED	

Workers statistics:

Here are statistics for the connected flows:

- Connected workers: Connected flows;
- · Queued bundles: Bundles in the queue;
- Bundles processed: Processed bundles;
- Read operations: Number of read operations per second;
- Write operations: Number of write operations per second;
- Total number of documents: Total number of documents.

Registered connectors are listed by:

- Name: Connector name;
- Type: Connector type;
- Automatic trigger;
- Messages: Number of messages received;
- Status: Connector status;
- Modified: Connector modification date.

Data ingestion sources:

- OpenCTI Streams: OpenCTI streams;
- TAXII feeds: Feeds created using the TAXII (Trusted Automated eXchange of Intelligence Information) protocol;
- TAXII streams: Streams created using the TAXII protocol;
- RSS feeds: Feeds created using the RSS (Rich Site Summary) format;
- CSV feeds: Feeds created using the CSV (Comma-Separated Value) format.

Import

Here, you can import files.



Files are classified by:

- Name: Object name;
- Creators: Object creator;
- Labels: Labels assigned to the file. Labels help classify the file;
- Modification date: File modification date.

Processing

Here, you can check tasks.

- IN PROGRESS TASKS	
	No task
COMPLETED TASKS	
	No task

• In-progress tasks: Ongoing tasks;

Completed tasks: Completed tasks.

Data sharing

Here, RSS and TAXII streams and feeds are listed.





- Name: Stream name;
- Description: Stream description;
 Stream ID: Stream ID;
- Public: Indicates whether the stream is public or not;
- Status: Stream status;
 Filters: Filters applied to the stream.

TAXII



- Name: Stream or feed name;
- Description: Stream or feed description;
 Collection: Type (can be stream or feed);
- **Filters**: Filters applied to the stream.

40

XDR - Threat Monitor - CTI - Trash

Here are the discarded elements.

ТҮРЕ	REPRESENTATION	DELETED BY	DELETION DATE	MARKING

- Type: Element type;
 Representation: Element ID;
 Deleted by: Who deleted the element;
- Deletion date: When the element was deleted;
 Marking: Markings received by the element. Markings help classify the element's status.

XDR - Threat Monitor - CTI - Settings

Here are the listed labels and markings.

To search for a result, use the search bar.

Security

Here are the entity labels.

ТҮРЕ	DEFINITION -	- COLOR	ORDER	ORIGINAL CREATION
 Type: Label type; Definition: Label definition; Color: Label color; Order: Label order; Original creation: Label creation 	ation date.			
To create a new label, click the + in th	ne bottom right corner (+		
Туре				
Definition				
Color				e
Order				
			CANCEL	CREATE
Determine:				

- Type: Label type;Definition: Label definition;
- Color: Label color;
- Order: Label order.



Taxonomies

Here are the taxonomy labels.

COLOR	PLATFORM CREATION DATE

- · Value: Label value; • Color: Label color;
- Platform creation date: Label creation date.



To create a new label, click the + in the bottom right corner (

Value			
Color			Ŷ
		CANCEL	CREATE

Determine:

- Value: Label value;Color: Label color.

To create, click create (CREATE).
To cancel, click cancel	CANCEL).

Kill chain phases

Here are the attack phase labels.

	KILL CHAIN NAME	PHASE NAME	ORDER 🔺	ORIGINAL CREATIO
• • •	Kill chain name: MITRE ATT&CK phase name; Phase name: Phase type; Order: Label order; Original creation: Label creation date.			
To crea	te a new label, click the + in the bottom right corner	(+).		
Kill	chain name			
Pha	se name			
Ord	er			
			CANCEL	CREATE

Determine:

- Kill chain name: MITRE ATT&CK phase name;
- Phase name: Phase type;
 Order: Label order.



Vocabularies

Here are listed the vocabularies.

NAME 👻	USED IN	DESCRIPTION
 Name: Vocabulary name; Used in: Where it is used; Description: Vocabulary description 	scription.	
Clicking any category will take you to	a list of entries.	

		USED IN	ALIASES	DESCRIPTION	USAGES ORDER
NameUsed	e : Entry name; I in : Where it is used	;			

- Aliases: Other known names;
- Description: Entry description;
 Usages: Number of times the entry is used;
- Order: Entry order.

Status templates

Here are the status labels.

NAME A	COLOR	USAGES
 Name: Status label name; Color: Status label color; Usages: Number of times the status label is used. 		
To create a new label, click the + in the bottom right corner (+	
Name		
Color		*
	CANC	CREATE

Determine:

- Name: Status label name;
- Color: Status label color.



Case templates

Here are the case labels.

NAME	•			DESCR	IPTION							TASKS
NamDescTask	e : Label name; cription: Label d ss: Tasks related	lescription I to the la	n; bel.									
To create a ne	To create a new label, click the + in the bottom right corner (
Name												
Description												
Write	Preview	н	B I	ĉ	ତ	"	< }		≡	Ш	Æ	
												<u>k</u>
Tasks												+ •
											CANCEL	CREATE

Determine:

- Name: Label name;
 Description: Label description;
 Tasks: Tasks related to the label.



To cancel, click cancel (



XDR - Vulnerability detection

On this page, you can check the vulnerabilities detected by the agents.



Search

The bar allows you to search for specific events. For more information, see Search System.

Click on Explore agent to select the agent. For more information, see Agents.

Hovering over an element will display this button: . Clicking it allows you to view data or requests. By clicking on Download CSV, you can download a CSV file with the data.

Vulnerabilities are classified by severity:

- Critical: Critical
- High: High
- Medium: Medium
- Low: Low

Vulnerabilities can be filtered by severity by clicking on each classification.

Below, relevant data about vulnerabilities are listed. The elements and the number of times they appear are shown. You can sort the data in ascending or descending order.

Top 5 vulnerabilities: The most frequently appearing vulnerabilities are shown.

Top 5 OS: The operating systems with the most vulnerabilities are shown.

Top 5 agents: The agents with the most vulnerabilities are shown.

Top 5 packages: The packages with the most vulnerabilities are shown.

There are also charts with data on vulnerabilities.

Most common vulnerability score: Shows the most common severity rating of detected vulnerabilities, ranging from 0 (low) to 10 (critical).

Most vulnerable OS families: Ranks operating system families by the number of detected vulnerabilities.

Vulnerabilities by year of publication: Shows the number of detected vulnerabilities by their year of publication and severity.

XDR - Vulnerability detection - Inventory

Here, the vulnerabilities found on the network are listed.

Se	Search DQL										
bb	bbxdr.cluster.name: blockbit-xdr + Add filter										
•	C Export Formated 18 47 columns hidden ☐ Density ♀ Sort fields □ Full screen										
	agent.name ~	package.name ~	package.version ~	vulnerability.description ~	vulnerability.severity ~	vulnerability.id 🗸					
١ <u>כ</u>	Ipereira-centos9	kernel-devel	5.14.0-503.el9	In the Linux kernel, the following vulne		CVE-2024-39502					
١ō,	Ipereira-centos9	kernel-devel	5.14.0-503.el9	In the Linux kernel, the following vulne	Medium	CVE-2023-52905					
lα	Ipereira-centos9	kernel-devel	5.14.0-503.el9	In the Linux kernel, the following vulne		CVE-2024-26698					
R	Ipereira-centos9	kernel-devel	5.14.0-503.el9	In the Linux kernel, the following vulne		CVE-2024-26700					
١ō,	Ipereira-centos9	kernel-devel	5.14.0-503.el9	In the Linux kernel, the following vulne		CVE-2024-27437					
Q	Ipereira-centos9	kernel-devel	5.14.0-503.el9	In the Linux kernel, the following vulne	Medium	CVE-2024-39473					
١ō,	Ipereira-centos9	kernel-devel	5.14.0-503.el9	A flaw was found in the Linux kernel's \ldots	Medium	CVE-2023-2019					
R	Ipereira-centos9	kernel-devel	5.14.0-503.el9	In the Linux kernel, the following vulne		CVE-2024-26704					
R	Ipereira-centos9	kernel-devel	5.14.0-503.el9	In the Linux kernel, the following vulne		CVE-2024-26708					
Q	Ipereira-centos9	kernel-devel	5.14.0-503.el9	An issue was discovered in drivers/tty/	Medium	CVE-2023-31082					
Q	Ipereira-centos9	kernel-devel	5.14.0-503.el9	In the Linux kernel, the following vulne		CVE-2024-26717					
Q	Ipereira-centos9	kernel-devel	5.14.0-503.el9	In the Linux kernel, the following vulne		CVE-2024-26740					
÷						0.15 0001 11000					

Search

The bar allows you to search for specific events. For more information, see Search System.

Click on Explore agent to select the agent. For more information, see Agents.

In Refresh, you can reload the list.

In the header, the number of vulnerabilities is displayed.

Export formatted: You can export a .csv file with the list of agents.

Columns hidden: You can add or remove columns. The columns are based on the collected data. For more information, visit Collected Data.

Density: You can select the density of the displayed information.

Sort fields: You can reorder the fields that appear.

Full screen: You can enable full-screen mode.

XDR - MITRE ATT&CK

You can search for and view Indicators of Compromise (IoCs) within the environment monitored by Blockbit XDR. Alerts are automatically classified according to MITRE ATT&CK tactics and techniques, allowing security analysts to understand the attack's progression and investigate its origin.

When an IoC is identified, Blockbit XDR enables you to create a detailed incident timeline, correlating events and showing the threat's trajectory within the network. This facilitates the detection of attack patterns, identification of intrusion vectors, and a rapid response to persistent threats.

On this page, you can view alerts according to the MITRE ATT&CK classification. For more information, visit the MITRE ATT&CK page.

Dashboard Intelligence Framework		(৩়) xdr-VM-lpereira (003) 🌹 📄 Generate report
Ĩs ✓ Search	DQL 🛗 ~ Last 24 hours	Show dates C Refresh
cluster.name: blockbit-xdr rule.mitre.id: exists agent.id: 003 + Add filter		

This section is divided into 3 tabs:

- Dashboard: Graphs of events classified by MITRE ATT&CK.
- Intelligence: A library with information on malicious agents, attacks, resources, techniques, and mitigations.
- Framework: Allows you to view and filter alerts by tactics and techniques.

Search

The bar allows you to search for specific events. For more information, see Search System.

Click on Explore agent to select the agent. For more information, see Agents.

To create a report, click on Generate report. The reports are stored in Reports.

XDR - MITRE ATT&CK - Dashboard

In the Dashboard, you can view charts related to each type of threat cataloged in MITRE ATT&CK.

Dashboard Intellig	ence Framew	rork												890 lpe	reira-BLKBT-N-	095 (007) 👎	🖻 Ge	enerate report
© √ Search DQL 🛱 √ Last24 hours													Show	dates	ී Refresh			
dustername: blockbih skr nele mitre ist exists agentist: 007 + Add filter																		
Top factice		Ľ	Top Techniques		2	A	lierte evolu	tion over time										2
4			4				1										Modify	Registry
Tactic	✓ Count	~	Technique	✓ Count	× 1		500 -									1	Stored	Data Manipula
Defense Evasion	849		Modify Registry	589			400 -										 Valid A Data D 	estruction
Impact	560		Stored Data Manipulation	509			1 200 -										🔵 File De	letion
Persistence	255		Valid Accounts	251		8	300 -											
Privilege Escalation	255		Data Destruction	50			200 -											
Initial Access	251		File Deletion	50			100 -											
			Disable or Modify Tools	9			_									in		
		< 1 >			$\langle 1 \rangle$	1		12:00	15:00	18:00	21:00 timest	imp per 30	oc.oo minutee	03:00	06.00	09.00		

- Top tactics: Lists the tactics that generated the most alerts.
 Top techniques: Lists the techniques that generated the most alerts.
 Alerts evolution over time: Shows alerts by type in 30-minute intervals.

XDR - MITRE ATT&CK - Framework

Blockbit XDR provides an advanced automatic alert correlation system, grouping related events from the same attack for more efficient analysis and a quick incident response. The solution allows administrators to customize settings by endpoint groups, ensuring that detection and response policies are applied according to the criticality of each monitored environment.

On this page, you can view alerts classified by tactics and techniques. Each technique groups the related tactics.

IMPACT		Ê	EXFILTRATION		Ê	COMMAND AND CONTROL			COLLECTION	
Stored Data Manipulation	6		Exfiltration Over Web Service	0		Socket Filters	0		Archive via Utility	
Disk Structure Wipe	0		Scheduled Transfer	0		Standard Encoding	0		Screen Capture	
Direct Network Flood	0		Exfiltration Over Other Network Me	0		Domain Generation Algorithms	0		Adversary-in-the-Middle	
Stored Data Manipulation	0		Exfiltration Over Bluetooth	0		DNS	0		Keylogging	
External Defacement	0		Automated Exfiltration	0		Domain Fronting	0		Data from Configuration Repository	
OS Exhaustion Flood	0		Exfiltration Over Symmetric Encrypt	0		Symmetric Cryptography	0		Sharepoint	
Application Exhaustion Flood	0		Traffic Duplication	0		Fast Flux DNS	0		Audio Capture	
Disk Wipe	0		Exfiltration to Code Repository	0		Application Layer Protocol	0		Archive via Custom Method	
Service Stop	0		Exfiltration Over Asymmetric Encry	0		Custom Cryptographic Protocol	0		Email Collection	
Application or System Exploitation	0		Exfiltration Over C2 Channel	0		Remote Access Software	0		Data from Removable Media	
Disk Structure Wipe	0		Exfiltration Over Alternative Protocol	0		Multilayer Encryption	0		Local Data Staging	
Runtime Data Manipulation	0		Exfiltration over USB	0		Traffic Signaling	0		Local Email Collection	
Reflection Amplification	0		Data Compressed	0		Standard Cryptographic Protocol	0		Automated Collection	
Service Exhaustion Flood	0		Exfiltration to Text Storage Sites	0		Protocol Tunneling	0		Clipboard Data	
Defacement	0		Exfiltration to Cloud Storage	0		Domain Generation Algorithms	0		Data from Cloud Storage	
Internal Defacement	0	-	Data Transfer Size Limits	0	~	Mail Protocols	0	-	Remote Data Staging	

Search

The bar allows you to search for specific events. For more information, see Search System.

By clicking on Hide techniques with no alerts, you can hide techniques without alerts.

When you hover over a technique, two buttons will appear:

- Show in dashboard (): Creates a specific dashboard for this technique.
- Inspect in security events (

Clicking on each technique will open a list of the most recent times events in the category were detected.

Technique details

ID

T1078.002

Tactics Persistence Privilege Escalation Defense Evasion Initial Access

Version

1.3

At the top, you will see the technique ID and the associated tactics.

Search DQL			Last 24 hours		Show dates C Refresh	
+ Add filter						
Time \downarrow	Technique(s)		Tactic(s)	Level	Rule ID	Description
Aug 15, 2024 @ 10:01:52. 675	T1021.001 T1078.002		Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	92653	User: BLOCKBIT\lpereira logged using Remote Desktop Connection (RDP) from ip:172.28.0.25.
Aug 15, 2024 @ 10:01:52. 586	T1021.001 T1078.002		Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	92653	User: BLOCKBIT\lpereira logged using Remote Desktop Connection (RDP) from ip:172.28.0.25.
Aug 15, 2024 @ 09:28:43. 656	T1021.001 T1078.002		Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	92653	User: BLOCKBIT\lpereira logged using Remote Desktop Connection (RDP) from ip:172.28.0.25.
Aug 15, 2024 @ 09:28:43. 449	T1021.001 T1078.002		Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	92653	User: BLOCKBIT\lpereira logged using Remote Desktop Connection (RDP) from ip:172.28.0.25.

Below are the most recent events where the technique was detected, classified by time, associated techniques, associated tactics, level, rule ID, and description.

XDR - MITRE ATT&CK - Intelligence

In Intelligence, you will find a library with information on malicious agents, attacks, resources, techniques, and mitigations.

GROUPS	MITIGATIONS	SOFTWARE	TACTICS
APT38 🖸	Password Filter DLL Mitigation 🖸	HDoor 🖸	Credential Access 🖸
Indrik Spider 🖸	Space after Filename Mitigation 🖄	TrickBot 🖸	Execution 🖸
NEODYMIUM 🔀	HISTCONTROL Mitigation 🖸	PowerDuke 🖄	Impact 🗷
Elderwood 🗠	Credentials in Files Mitigation 🖄	EKANS 🖄	Persistence 🖄
SideCopy 🖄	Exploitation for Credential Access Mitigation 🖄	BLINDINGCAN 🖄	Privilege Escalation 🖄
GALLIUM 🖸	Query Registry Mitigation 🖸	Wiarp 🖄	Lateral Movement 🖄
APT17 🖸	Login Item Mitigation 🖸	RCSession 🖸	Defense Evasion 🖸
АРТЗ 🖸	Setuid and Setgid Mitigation 🖸	Spark 🖸	Exfiltration 🖸
GCMAN 🖸	Compiled HTML File Mitigation 🖄	QuietSieve 🖄	Discovery 🖸
Kimsuky 🖸	Data Destruction Mitigation 🖄	SynAck 🖄	Collection 🖸
EXOTIC LILY 🖄	Windows Management Instrumentation Event Subscription Mitigation 🖄	Bumblebee 🖄	Resource Development 🖄
admin@338 🕜	File System Permissions Weakness Mitigation 🖄	MURKYTOP	Reconnaissance 🕜
Patchwork 🖸	AppInit DLLs Mitigation 🖸	GRIFFON 🖸	Command and Control 📝
APT41 🖸	Launch Agent Mitigation 🕜	Exaramel for Windows 🖸	Initial Access 🖸

The information is divided by topics:

- Groups: Groups that carry out malicious attacks.
- Mitigations: Techniques for mitigating attacks.
- Software: Software used in malicious attacks.
- Tactics: Objectives and strategies of malicious attacks.
- Techniques: Techniques used in malicious attacks.

To search for a specific entry, use the search bar (Search in all resources).

Clicking on an entry will provide more details. There is general information (ID, name, creation and modification times, and version) and a description of the element. Below, there is a list of articles where the element may appear (e.g., the technique "Malicious file" appears on the page of the software "BLINDINGCAN").

×

BLINDINGCAN

BLINDINGCAN is a remote access Trojan that has been used by the North Korean government since at least early 2020 in cyber operations against defense, engineering, and government organizations in Western Europe and the US.(Citation: US-CERT BLINDINGCAN Aug 2020)(Citation: NHS UK BLINDINGCAN Aug 2020)

```
Acess the original source
✓ Groups
Lazarus Group 2
✓ Techniques
Match Legitimate Name or Location 2
Obfuscated Files or Information 2
Web Protocols 2
Code Signing 2
Rundll32 2
Deobfuscate/Decode Files or Information 2
Standard Encoding 2
Malicious File 2
```

Clicking on Access the original source will open a new tab with the relevant documentation on the MITRE ATT&CK page.

XDR - Security Operations

This section presents dashboards with event alerts that violate guidelines from six regulations:

- LGPD (Lei Geral de Proteção de Dados): Brazilian law that controls the privacy and use/treatment of personal data.
- PCI DSS (Payment Card Industry Data Security Standard): Data security standard for the payment card industry.
- GDPR (General Data Protection Regulation): Data protection law of the European Union.
- HIPAA (Health Insurance Portability and Accountability Act): US law that regulates the collection, use, and protection of health information.
- NIST 800-53 (National Institute of Standards and Technology Special Publication 800-53): Information security standard for US federal agencies.
- TSC (Trust Service Criteria): Criteria for evaluating the adequacy of solutions to an organization's security standard.



Search

The bar allows you to search for specific events. For more information, see Search System.

Click on Explore agent to select the agent. For more information, see Agents.

To create a report, click on Generate report. The reports are stored in Reports.

Dashboard

Each regulation has a specific dashboard:

- LGPD
- GDPR
- HIPAA
- NIST 800-53
- PCI DSS
- TSC

Controls

On this page, you can view alerts separated by requirements.

Hide empty items $\bigcirc \times$ Requirements S Filter requirements 1.4 - Install personal firewall software or equivalent functio... 88 op configuration standards for all system comp. 1316 4.1 - Use strong cryptography and security protocols (for ex... 126 2.2 - Deve 1.3.4 - Do not allow unauthorized outbound traffic from the ... 2.2.4 - Configure system security parameters to prevent mis... 49 1.1.1 - A formal process for approving and testing all networ... 2.2.3 - Implement additional security features for any requir... 38 2.2.2 - Enable only necessary services, protocols, daemons, ... 3 6 8 5.2 - Ensure that all anti 15 6.5 - Address common coding vulnerabilities in softwar... 5093498 8.1.5 - Manage IDs used by third parties to access, support, ... 15 6.2 - Ensure that all system components and software are pr... 13 8.2.4 - Change user passwords/passphrases at least once ev... 14 5.1 - Deploy anti 8 6.5.8 - Improper access control (such an insecure direct obj... 4 8.1.8 - If a session has been idle for more than 15 minutes, r... 12 8.1.2 - Control addition, deletion, and modification of user I... 6 6.5.1 - Injection flaws, particularly SQL injection. Also consi... 0 6.5.2 - Buffer overflows 8.1.4 - Remove/disable inactive user accounts within 90 days. 0 6.5.5 - Improper error handling 0 8.1.6 - Limit repeated access attempts by locking out the us... 0 6.5.7 - Cross 0 8.5.1 - Additional requirement for service providers: Service... 6.5.10 - Broken authentication and session management. 0 8.7 - All access to any database containing cardholder data (... 0 6.6 - For public 0

To show only requirements with alerts, click on Hide requirements with no alerts.

Clicking on each requirement will show the subparagraphs. Clicking on each subparagraph will show the description and related alerts.

You can use the Filter requirements field to filter requirements.

Hovering over a requirement will show a brief description and two buttons:

1	2	
1.4 - Install personal firewall software or equivalent fu	2.2 - Develop configuration standards for all system comp 1314	4.1 - Use strong cryptography
1.3.4 - Do not allow unauthorized outbound traffic from the 1.4 - Install persona	I firewall software or equivalent functionality on any portable computing devices (ncluding company and/or employee
介		

- Show requirement in Dashboard (): Shows the specific requirement data in the Dashboard.
- Inspect requirement in Security Events (

Clicking on the requirement will open a modal with its description.

1.1.1

Goals

P

Build and Maintain a Secure Network

Requirement description

A formal process for approving and testing all network connections and changes to the firewall and router configurations

 \times

XDR - Security Operations - GDPR

The GDPR (General Data Protection Regulation) is the data protection law of the European Union.



The Dashboard shows the following charts:

- Last alerts: Latest alerts by article;
- GDPR Requirements: Number of alerts every 30 minutes;
- Top 10 agents by alerts number: Agents with the most related alerts;
- Requirements by agents: Alerts related to agents divided by articles.

XDR - Security Operations - HIPAA

HIPAA (Health Insurance Portability and Accountability Act) is the U.S. law that regulates the collection, use, and protection of health information.



The Dashboard shows the following data:

- Stats: Two statistics are shown:
 - ° Total alerts: Total number of HIPAA violation alerts;
 - Max rule level detected: Highest level of violated rule.
- Requirements distribution by agent: Violations distributed by agents;
- Top 10 requirements: Requirements with the most violations;
- Total HIPAA by Agent: Violations by agent over time.

XDR - Security Operations - LGPD

The LGPD (Lei Geral de Proteção de Dados) is the Brazilian law that regulates the privacy and use/processing of personal data.



The Dashboard shows the following data:

- Last alerts: Latest alerts by article;
- LGPD/GDPR Requirements: Number of alerts every 30 minutes;
- Top 10 agents by alerts number: Agents with the most related alerts;
- Requirements by agents: Alerts related to agents divided by articles.

XDR - Security Operations - NIST 800-53

The NIST 800-53 (National Institute of Standards and Technology Special Publication 800-53) is the information security standard for U.S. federal agencies.



The Dashboard shows the following data:

- Most active agents: Agents with the most alerts;
- Stats: Two statistics are displayed:
 - Total alerts: Total number of NIST 800-53 violation alerts;
 - ° Max rule level detected: Highest level of violated rule.
- Top 10 requirements: Requirements with the most violations;
- Requirements distribution by agent: Violations distributed by agents.
XDR - Security Operations - PCI DDS

The PCI DSS (Payment Card Industry Data Security Standard) is the data security standard for the payment card industry.



The Dashboard shows the following charts:

- PCI DSS Requirements: Last 24 Hours: Number of alerts every 30 minutes in the last 24 hours;
- Top 10 PCI DSS Last Alerts: Requirements with the most linked alerts;
- Top 10 agents by alerts number: Agents with the most linked alerts;
- Last Alerts: Most recent alerts.

XDR - Security Operations - TSC

TSC (Trust Service Criteria) are criteria from the American Institute of Certified Public Accountants (AICPA) for evaluating the adequacy of solutions to an organization's security standards.

Top 5 rule groups		Top 5 rules			iop 5 TSC requirements e^{2i}					
Ł			<u>å</u> .		50 -					
rule.groups: Descending	 ✓ Count 	~	rule.description: Descending V Count	~	40					
syslog	24		Listened ports status (netstat) changed (new 17		40					
ossec	23		Dpkg (Debian Package) half configured. 12		30 -					
config_changed	19		New dpkg (Debian Package) installed. 7		Count					
dpkg	19		Integrity checksum changed.		20 -					
syscheck	6		PAM: Login session opened. 3		10 -					
							-	-		
					0-	cces	CC7.2	cc73	CC8.1	cce.1
		< 1 >		$\langle \underline{1} \rangle$				rule.tsc: Descending		

The Dashboard shows the following data:

- Top 5 rule groups: Rule groups with the most violations.
- Top 5 rules: Rules with the most violations.
 Top 5 TSC requirements: Requirements with the most violations.

XDR - Cloud Security

Blockbit XDR can be used to monitor cloud instances.

By collecting metadata, XDR obtains information such as instance ID, region, machine type, tags, and network configurations via cloud provider APIs.

Using artificial intelligence to process this data, XDR can automatically apply policies, enabling Dynamic Adjustment and Active Response.

If the machine changes state (e.g., tag modification, region, or resources), XDR automatically readjusts its settings. This allows for quick reactions, such as blocking suspicious access or activating additional protections as needed.

Blockbit XDR enhances security on the following cloud platforms:

- Docker
- Amazon Web Services
- Google Cloud
- GitHub
- Azure/Microsoft 365

Integrations are performed via the XDR API. To integrate, contact the Blockbit team.

XDR - Cloud Security - Amazon Web Services

The agents use the AWS Instance Metadata Service (IMDS) to collect information such as instance ID, machine type, region, VPC, and associated tags. With this data, the solution automatically adjusts security policies according to the instance profile in the AWS cloud.

XDR - Cloud Security - Azure/Microsoft 365

The integration with the **Azure Instance Metadata Service (IMDS)** allows the agents to identify details such as VM ID, SKU, resource group, and virtual network. This way, security policies are applied according to the configuration of the **Azure environment**.

Panel

On this page, you can monitor cloud activities in more detail.

S	ubscription 0 V User Type 0 V	Result Status 0	\sim	⊞ ∨ Last 24 hours	Show dates C Refresh
=	cluster.name: blockbit-xdr rule.groups: office365 + Add filter				Advanced filters
•	Top users		-	Top client IP address	
	User	Count \downarrow		Client IP address	Count ↓
	No items found		No items found		
	Top rules		-	Top operations	
	Rule	Count ↓		Operation	Count ↓
	No items found			No items fou	Ind

The bar allows you to search for specific events. For more information, check the Search System.

By clicking Refresh, you can update the report list.

By clicking the Advanced filters switch, you gain access to 3 new filters:

- Subscription: allows filtering by subscription;
- User Type: allows filtering by user type. Clicking will display the profiles created under Users;
- Result Status: allows filtering by result status.

The 4 panels display lists of the most common events and their counts.

- Top Users: shows the most active users;
- Top Client IP Address: shows the client IPs that accessed the monitored services the most;
- Top Rules: shows the most triggered security rules;
- Top Operations: shows the most executed operations.

40 mini

XDR - Cloud Security - Docker

For Docker and Kubernetes-based environments, the **Blockbit XDR agents** access environment variables and orchestration infrastructure configurations, such as container ID, namespace, labels, volume mounts, and network configurations. This allows security to be applied based on the container context, protecting dynamic workloads without impacting performance.

XDR - Cloud Security - GitHub

For **CI/CD environments**, the agents extract metadata from **GitHub Actions runners**, such as runner ID, environment type (self-hosted or GitHub-hosted), repository, branch, and triggering events. Based on this, the solution applies security measures to ensure that automated executions are protected from unauthorized access or security failures.

Panel

On this page, you can monitor cloud activities in more detail.

	Actor 0 V Organization 0 V Repository	0 ~ Act	tion 0	\sim	₩ v Last 24 hours	Show dates	ි Refresh
7	cluster.name: blockbit-xdr rule groups: github + Add filter		\bigcirc ×	Advanced filters			
6	Actors Actor		Count ↓	C	Organizations		Count ↓
	No items found				No	tems found	
	Repositories			ŀ	Actions		
	Repository		Count ↓		Action		Count ↓
	No items found				No	tems found	

The bar allows you to search for specific events. For more information, check the Search System.

By clicking Refresh, you can update the report list.

By clicking the Advanced filters switch, you gain access to 3 new filters:

- Subscription: allows filtering by subscription;
- User Type: allows filtering by user type. Clicking will display the profiles created under Users;
- Result Status: allows filtering by result status.

The 4 panels display lists of the most common events and their counts.

- Actors: shows the most active users;
- Organizations: shows the organizations with the most activity;
- Repositories: shows the most accessed repositories;
- Actions: shows the most executed actions.

XDR - Cloud Security - Google Cloud

In GCP, the agents access the GCP Instance Metadata Server, obtaining information such as zone, project name, tags, and VM identity. This enables dynamic security configuration, adapting to the context of the Google Cloud infrastructure.

XDR - Download

- 1. Windows: (Link)
 - a. Windows Server 2008 (all versions), 2011, 2012, 2012 R2, 2016, 2019, 2022, 2025 and up;
 - b. Windows versão 7 (all versions), 8.1, 10, 11 and up;
- 2. macOS
 - a. Big Sur, Monterey, Ventura, Sonoma, Sequoia and up;
 b. ARM (Link)
 c. AMD/Intel (Link)
- 3. Linux
 - a. Ubuntu, Debian, Raspbian, Fedora, CentOS, Red Hat Enterprise Linux (RHEL), Rocky Linux, AlmaLinux, SUSE Linux Enterprise or OpenSUSE;
 - b. Public clouds, like AWS Linux, Oracle Linux, Azure Linux or Google Cloud Ubuntu Pro;
 - c. RPM (Link)
 - d. DEB (Link)