Datasheet

Blockbit SIEM & SOAR

SECURITY INFORMATION AND EVENT MANAGEMENT & SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE

Intelligent Monitoring | **Security Automation** | **Orchestrated Threat Response**

Blockbit SIEM & SOAR is an integrated event management and incident response automation solution designed to deliver advanced detection, event correlation, and proactive mitigation.

By combining artificial intelligence, machine learning, and automation, the solution provides full cybersecurity visibility, accelerates incident response, and reduces the operational burden on SOC teams.

Native integration with Blockbit Cyber Threat Intelligence (CTI) and Blockbit Sandbox further strengthens detection and response capabilities, enabling dynamic analysis of suspicious files and real-time correlation with global intelligence. Additionally, advanced dashboards—such as the MITRE ATT&CK Framework, MITRE Radar, Attack Map, and customizable panels—offer strategic insights into adversary tactics and techniques, threat trends, and network behavior.

Blockbit SIEM & SOAR is compatible with over 150 market technologies, allowing comprehensive integration with network devices, firewalls, NDR, EDR, XDR, identity systems, and various other security solutions, ensuring unified visibility and coordinated response across the organization's security ecosystem.

Solution Differentiators:

Intelligent Threat Detection

Advanced event correlation and behavioral analysis to identify attacks in real time.

Advanced Dashboards

Strategic visibility with MITRE ATT&CK Framework, MITRE Radar, Attack Map, and customizable dashboards.

Response Automation and Orchestration

Automated playbooks reduce the need for manual intervention and accelerate mitigation.

Behavioral Analysis and UEBA

Identification of suspicious user and entity activities to detect lateral movement and insider threats.

Integration with Blockbit CTI

Global threat intelligence, enriching alerts and reducing false positives.

Unified Incident Management

Complete event traceability and detailed auditing.

Native Integration with Blockbit Sandbox

Dynamic and automated analysis of suspicious files, detecting unknown and evasive threats.

Monitoring and Compliance

Customizable reports to meet LGPD, GDPR, ISO 27001, PCI-DSS, and other regulatory requirements.

Integration with Blockbit XDR, NGFW & NDR

Event monitoring and correlation, automatic application of blocking rules, detection, and mitigation of advanced attacks.

Deployment Flexibility

Available for on-premises, public cloud, private cloud, or hybrid environments.

Key Features

Event Collection and Correlation (SIEM)

- **Continuous Monitoring:**
  Normalization and real-time log analysis from multiple sources, including endpoints, firewalls, and cloud services.
- **Advanced Correlation:**
  Intelligent algorithms connect isolated events to identify attack patterns.
- **Behavior-Based Detection:**
  Machine learning to identify anomalous activities and prevent attacks before they occur.

Orchestration and Automated Response (SOAR)

- **Intelligent Playbooks:**
  Automation of actions such as access blocking, device isolation, and automatic notifications.
- **Multi-Layer Automation:**
  Coordinated response across firewalls, NDR, EDR, XDR, identity systems, and other security tools.
- **Integrated Forensic Analysis:**
  Detailed incident investigation with attack timeline reconstruction.

Dynamic Threat Analysis with Blockbit Sandbox

Advanced Malware Detection	Behavioral Analysis of Suspicious Files	Remediation Automation
Identification of unknown malware, ransomware variants, and evasive attacks.	Secure execution of artifacts to identify malicious actions in real time.	Integration with SOAR for file quarantine, IOC blocking, and coordinated response.

Threat Intelligence with Blockbit CTI

Advanced Data Correlation

Use of global intelligence to validate threats and reduce false positives.

Continuous Updates on New Threats

Insights on malware, targeted attacks, and emerging vulnerabilities.

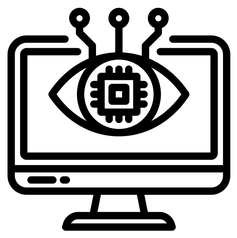
Predictive Detection

Identification of attack patterns before they impact the environment.

Automated Resolution

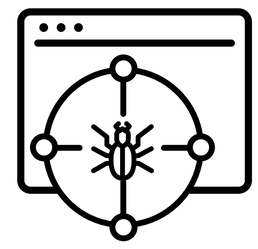
Application of responses based on contextualized intelligence for high-risk incidents.

Advanced Dashboards and Visual Intelligence



MITRE ATT&CK Framework

Mapping of tactics and techniques used by cyber adversaries.



Threat Hunting

Investigation to identify attack patterns and activities hidden from traditional defenses.

Attack Map

Real-time monitoring of active threats and correlation with geolocated data.

Custom Dashboards

Full customization of reports and charts, tailored to the SOC's needs.

Time Reduction and Operational Efficiency

With intelligent automation, Blockbit SIEM & SOAR drastically reduces the time required for an advanced 24×7 SOC to detect and mitigate threats.

Task	Manual Process (average time)	With Blockbit SIEM & SOAR
Artifact (IOC) Enrichment	1 hour	3 minutes
Event Triage	30 minutes	2 minutes
Suspicious File Analysis	2 hours	Automatically / Immediately
Compromised Device Isolation	15 minutes	Automatically / Immediately
Incident Documentation	90 minutes	Automatically / Immediately
Blocking of IOCs in Firewalls	45 minutes	Automatically / Immediately
Complete Incident Resolution	**6 hours**	**5 minutes**

Total: **Reduction from up to 6 hours to just 5 minutes!**

This information is for illustrative purposes only, based on estimates calculated by Blockbit. Each environment and team has unique characteristics that may result in significant variations in the times presented.

SOC Automation and Orchestration

The evolution of cyberattacks and the expansion of the digital perimeter in companies demand increasingly efficient SOCs. However, the high volume of alerts, lack of integration between tools, and absence of automation hinder the detection, investigation, and rapid response to threats.

Smart Triage and Alert Enrichment:
Reduction of false positives using CTI intelligence and advanced event correlation.

Full Orchestration and Automation
Automatic execution of playbooks for investigation, threat isolation, and immediate containment.

Integration with Over 150 Solutions
Unification of security tools, enabling a coordinated and efficient response.

Reduced Incident Resolution Time
From hours to minutes with intelligent automation and comprehensive operational dashboards.

Blockbit SIEM & SOAR transforms the traditional SOC into a highly efficient and automated environment, reducing operational workload and accelerating threat mitigation. With native integration to Blockbit CTI, behavioral analysis, and intelligent automation, it turns cybersecurity into a highly efficient and resilient environment.

- **Faster response time with intelligent automation**
- **Advanced threat detection and proactive mitigation**
- **Visibility and event correlation for a modern SOC**
- **Continuous compliance and auditing to meet regulatory standards**

About Blockbit

Blockbit is a leader in cybersecurity products, protecting thousands of companies and millions of users from digital threats and attacks.

+5M corporate clients

+2MM protected users