Blumira

SIEM + SOC Management

AUTOMATED CLOUD SIEM PLATFORM WITH SOC MANAGEMENT

Blumira provides an automated SIEM platform with teams of security experts to manage it, making security easy and accessible to small and mid-sized organizations.

SOLUTIONS

- Integrates log and security data across applications and network security tools both on-prem and in the cloud, including but not limited to:
    - Windows
    - Linux
    - macOS
    - Microsoft 365
    - Azure
    - AWS
    - Primary & secondary authentication providers
    - Firewalls
    - Network devices
    - Endpoint security
    - Cloud applications

- Parses log data into a cloud data lake
- Correlates log data with continuously updated threat intelligence feeds

- Incident Detection Engineering team:
    - Threat hunting
    - Creates rules
    - Provides detailed analysis
    - Provides remediation workflows

- Host isolation tools (automated & manual)
- Dynamic blocklists
- Threat response
- Honeypots

PROACTIVE SERVICES

- Using data collected, Blumira proactively detects attackers based on tactics, tools and behaviors earlier in the process, decreasing time-to-detect and time-to-respond

- The platform surfaces findings based on behavioral activity, resulting in higher efficacy and less noise than signature-based detections.

- Pretuned rules come with detailed analysis and step-by-step workflows to assist in remediation

- Dynamic blocklist can be configured to automatically block known-bad traffic when used with supported firewalls

- Automated host isolation can be configured to proactively isolate hosts from the network based on defined settings while still allowing for log collection and investigation

- Threat response can be configured to disable users & revoke sessions for M365

- Well-documented integrations streamline applications and systems' onboarding

- Blumira Solution Architect support is available to assist during onboarding to ensure proper deployment and improve best practice adherence

Blumira

SUPPORT AND MAINTENANCE

- Alert response and mitigation support in cooperation with the Security Operations Center
- Adding and removing licensing as employees and workstations / users are added or removed (fees adjusted accordingly per agreement)
- Cyber incidents, bulk data exports, and breach response due to user error may require additional time and materials fees for mitigation efforts
- Normal business hours response
- Critical after-hours response

ASSUMPTIONS & LIMITATIONS

- Two agents per billable user is included in plans that include the Blumira Agent
- Agent counts are based on total installed endpoints. If installation count exceeds user count additional fees may apply
- Includes 1 year of log data retention and unlimited data ingestion
- End users subject to Blumira terms located at blumira.help/ptt

> *"While not the traditional model, I absolutely think of Blumira as an outsourced SOC because you have a SecOps team available and we're able to reach out when alerts come in."*

– Chris Lewis, Information Security Manager
NetSource One

Users Love Us

VOTED BY USERS ON G2:

- MOMENTUM LEADER
- BEST ROI
- EASIEST TO USE
- LIKELY TO RECOMMEND

A SIEM BUILT FOR SMB

Blumira makes security easy and effective for SMBs, helping them detect and respond to cybersecurity threats faster to stop breaches and ransomware.

With Blumira's XDR platform you get:

- 1 Year of retention and unlimited ingestion
- 24/7 SecOps support
- Unlimited Integrations
- SIEM deployment in minutes
- Managed detection rules
- Endpoint visibility and response
- Automated response