Blumira

Blumira For Compliance

SATISFY MORE REQUIREMENTS WITH ONE SOLUTION

Time-strapped IT teams can do more with one solution that combines SIEM, endpoint visibility and automated response. Meet compliance with one year of data retention.

Logging, Audit Trails, SIEM and Data Retention

All frameworks call for similar requirements for log collection, data retention and monitoring of system activity.

Blumira's platform includes:

- SIEM (Security Information and Event Management), with centralized logging and alerts
- Threat monitoring & ability to track user activity
- One year of log data retention available for investigation & reporting
- Search and reporting of audit logs, with pre-built, scheduled reports
- 24/7 SecOps support for critical Incidents

Blumira helps satisfy these requirements:

CYBER INSURANCE

Common cyber insurance application questions include:

- Do you use a security information and event management (SIEM) system?
- Do you actively monitor all admin access for unusual behavior patterns?
- Do you have centralized log collection and management that allows for review of all access and activity on the network?
  - For how long are logs maintained?

CMMC / NIST

Audit and Accountability (AU): AU.L2-3.3.2 - Ensure actions of users can be traced back to them to hold them accountable for actions.

AU.L2-3.3.1 – Create and retain system audit logs and records to enable monitoring, analysis, investigation, and reporting of unauthorized system activity.

AU.L2-3.3.3 requires you to review and update logged events, while AU.L2-3.3.4 calls for alerting in the event of an audit logging process failure.

CIS

8.0. Audit Log Management - Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack. CIS 8.0 subcontrols require you to collect detailed audit logs, including DNS query, URL request and command-line audit logs. It also calls for centralizing your audit logs, conducting audit log reviews and collecting service provider logs.

FTC SAFEGUARDS RULE

16 CFR 314.4(c)(8) - Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

HIPAA

The HIPAA Security Rule provision on Audit Controls (45 C.F.R. § 164.312(b)) requires Covered Entities and Business Associates to:

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information (ePHI).
- The majority of information systems provide some level of audit controls with a reporting method, such as audit reports.

PCI DSS

PCI DSS 10: Track and monitor all access to network resources and cardholder data.

10.1, 10.2, 10.5 and 10.5.1 require you to implement audit trails that link system access to individual users; implement logs to support detection of anomalies and suspicious activity, and forensic analysis of events; retain log history and make available for analysis; and retain log history for at least 12 months (with most recent three months immediately available for analysis).

Blumira

Threat Detection & Response

All frameworks call for similar requirements to monitor your network, detect suspicious activity or malware, implement an alerting solution, and establish incident response (IR) capabilities to help recover from a security incident.

Blumira's platform automates the review, analysis, detection and guided response for security incidents identified within your environment. Our expert, in-house Security Operations (SecOps) team provides 24/7 support for urgent priority issues to help with IR.

Blumira helps satisfy these requirements:

CYBER INSURANCE

Common cyber insurance application questions include:

- Do you use a network monitoring solution to alert your organization to suspicious activity or malicious behavior on your network?
- Provide details on whether you have a Security Operations Center (SOC) that is responsible for event monitoring and detection, and IR.
- Does the applicant use Endpoint Detection and Response (EDR) to secure all system endpoints?
- Does the applicant use a 24/7 staffed and managed Endpoint Detection and Response (EDR) for all endpoints?
- Do you use endpoint application isolation and containment technology on all endpoints?

CMMC / NIST

Incident Response (IR): IR.L2-3.6.1 – Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

IR.L2-3.6.2 – Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. IR.L2-3.6.3 calls for testing the organizational incident response capability.

CIS

13.0. Network Monitoring and Defense - Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

FTC SAFEGUARDS RULE

16 CFR 314.4(h) - Establish a written incident response (IR) plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control.

HIPAA

§ 164.308(a)(1) – Security Management Process: Implement policies and procedures to prevent, detect, contain and correct security violations.

PCI DSS

PCI DSS 5: Protect All Systems and Networks from Malicious Software
5.2 Malicious software (malware) is prevented, or detected and addressed.

THE BLUMIRA VALUE

Blumira's **open XDR platform** makes advanced detection and response easy and effective for SMBs, accelerating ransomware and breach prevention for hybrid environments.

Time-strapped IT teams can do more with one solution that combines SIEM, endpoint visibility and automated response.

THE BLUMIRA DIFFERENCE:

✓ **EASY**

Reduce reliance on humans to complete manual security tasks to save time and refocus efforts

✓ **EFFECTIVE**

Accelerate breach prevention and ransomware protection with security automation

✓ **EFFICIENT**

All-in-one open platform simplifies workflows with hybrid coverage, satisfying more compliance controls

> **We chose Blumira for its simplicity** – I needed a solution that would simplify, consolidate and show me what I really need to see.
>
> Jim Paolicelli, IT Director
> Atlantic Constructors

G2 Users Love Us

BLUMIRA IS FREE FOR MSP PARTNERS:

blumira.com/nfr