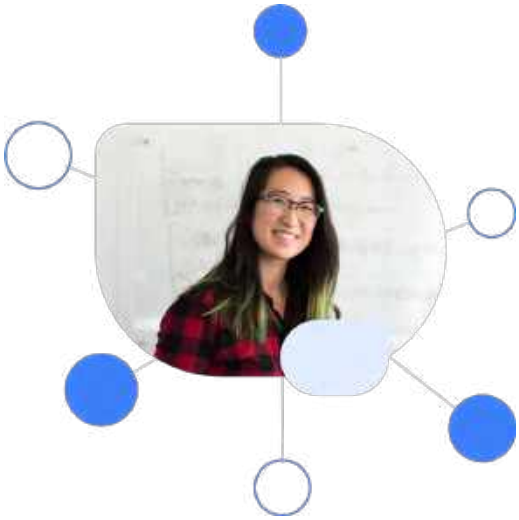
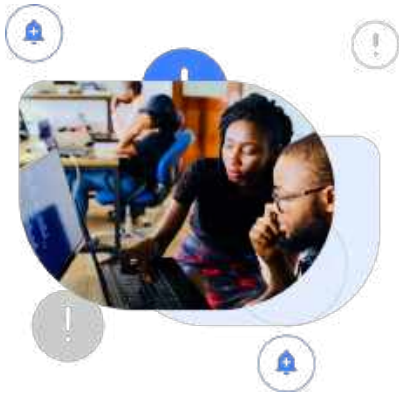




Threat Detection & Response Assessment

A checklist to measure your organization's current capabilities for logging, compliance, detection, response and much more.

Identify Your Organization's Security Gaps

These days, what many call the 'digital transformation' has accelerated rapidly in an era of remote work.

Companies are turning to cloud-based productivity and collaboration tools to enable remote employees to do their jobs efficiently. Many are using personal devices, as well as virtual private networks and remote access gateways to connect securely to networks and data.

All of these trends shift visibility and control out of the hands of already-lean IT and security teams, stretched to their limits. Many organizations aren't even sure what security gaps exist in their rapidly changing environment.

When deploying proof-of-concepts, Blumira has found that the average organization has only 10% coverage across all of the essential areas of threat detection and response.

To help you understand how to better secure this new world, Blumira has created a **threat detection and response gap assessment checklist** that you can use to determine where you need additional capabilities.

In this assessment, you'll learn:

- Best practices around **security log** repositories, configuration, parsing and correlation
- **Audit and compliance** must-haves, like generated or pre-built reports, and what to audit for compliance
- Critical incident **detections**, like lateral movement, common misconfigurations, indicators of data exfiltration and more.
- How automated incident **response** tools like playbooks can help small teams contain threats faster
- The importance of access to **security expertise** when you need it, and high **availability** and reliability of your security solution

SECTIONS

01 Identify Security Gaps
02 Why Should You Care?
03 Threat Detection & Response Assessment
04 Blumira's Automated Detection & Response

Why Should You Care?

Doing an assessment can highlight significant security gaps in the area of threat detection and response - but why should you care? Here's some potential consequences of failure in each essential area:

- **Logging** - Without proper logging and monitoring, you may miss key events essential for security, such as failed logins and misconfigurations that leave your network open to insecure connections.
- **Audits & Compliance** - Building, exporting and delivering security reports periodically for auditors and to meet compliance regulations can take away valuable time from your IT and security teams' daily duties.
- **Detection** - Without proper detections, you may miss key security incidents that can help you prevent or quickly mitigate and contain a compromise - such as indicators of lateral movement, data exfiltration and more.
- **Alerting** - Too many alerts results in responder fatigue and a lack of clarity around the most critical alerts your team needs to quickly address in order to keep your organization safe and secure.
- **Response** - Many solutions lack support for incident response, leaving a gap in your security operation workflow. Without response capabilities, organizations must hire costly SOC (security operations center) teams or layer expensive SOAR (security operations, automation and response) software on top of their logging and detection solution(s).
- **Security Expertise** - While automation can help small teams, sometimes you need to do deeper investigation for detection and response - without access to security expertise, organizations can be out of luck.
- **Monitoring & Availability** - If your security solution isn't designed for high availability and reliability, your organization could miss out on important security detections or delayed response times during any downtime.

Your Assessment Checklist

Logging

Logging and monitoring your IT and security environment are the critical first steps toward real-time insight into potential ongoing threats and attacks.

Capability	Existing	Blumira
Do you currently have a centralized security/audit log repository?		✓
Do you currently log security/audit log retention for 365 days?		✓
Are your logs automatically parsed and correlated?		✓
Have you configured your Windows hosts or GPO for verbose security logging?		✓
Does your solution monitor your on-premise applications for threats?		✓
Does your solution monitor your cloud applications for threats?		✓

Audits & Compliance

By automating report generation and delivery, you can expedite your compliance and audit needs to save your team time and resources.

Capability	Existing	Blumira
Do you currently have a way to easily generate audit reports?		✓
Do you have access to pre-built reports available for audit / compliance purposes?		✓
Do you currently have a way to schedule delivery of recurring audit/compliance reports?		✓
Do you have offsite retention of your security/audit logs?		✓
Do you currently audit new domain admin account creation?		✓
Does the solution allow logs to be exported in CSV or JSON?		✓
Does the solution guarantee that the logs can't be modified by administrators?		✓

Detection

Effective security programs provide visibility into threats in different areas broadly across your environment, including common misconfigurations, identity-based attacks and more.

Capability	Existing	Blumira
Do you have a solution that continually monitors for threats across your environment?		✓
Do you currently correlate third-party threat intelligence?		✓
Do you use third-party threat intelligence to detect threats?		✓
Do you have a solution in place that automates threat correlation?		✓
Are you able to detect lateral movement across your network with the use of a honeypot?		✓
Do you currently actively monitor for threats within your environment? If so, How?		✓
Are you able to detect common threats on firewall/border gateways?		✓
Are you able to detect common misconfigurations such as internet-accessible RDP or SMB?		✓
Are you able to detect any indicators of data exfiltration?		✓
Are you able to detect indicators of commonly used identity attacks such as password spraying and/or credential compromise?		✓
Does your solution natively with productivity suites such as G Suite & Office 365 to detect threats?		✓
Does your solution integrate with your cloud identity such as Okta, Duo Security and Azure AD to detect threats?		✓
Does your solution integrate with your cloud infrastructure such as Microsoft Azure to detect threats?		✓

Your Assessment Checklist, Cont.

Alerting

Reducing the noise is key to surfacing only the most important findings, while prioritizing the incidents by criticality in order to streamline security operations.

Capability	Y/N	Blumira
Does the solution in place stack evidence to help reduce the noise from too many alerts?		✓
Are only actionable threats identified while reducing or eliminating the noise of non-actionable information?		✓
Do you have escalations and notifications when high priority threats are identified?		✓
Are you able to notify a responder out of channel (phone call, SMS) in case email is compromised?		✓
Do your alerts provide a direct link back to the evidence and details of the threat identified?		✓

Response

With limited teams, you don't always have the resources to quickly and knowledgeably respond to security incidents in near real-time - automation can help.

Capability	Y/N	Blumira
Does your solution provide guided response playbooks that can be used to easily take action on to remediate the threats identified?		✓
Are you able to automatically block security threats on your gateway?		✓
Does the solution provide playbooks that can be used with basic IT helpdesk skills?		✓
Can you enable role-based admin for responders?*		✓

**To enable IT and/or third party providers to interact and respond with the security team*

Security Expertise

Even with automation, incident response sometimes requires a deeper level of human-powered security analysis and expertise that you may not have in-house.

Capability	Y/N	Blumira
Do you currently have access to a security analyst with deep security expertise?		✓
Do you have access to security expertise when you need to assess the risk of identified threats?		✓

Monitoring & Availability

High availability and reliability are essential components of the solid foundation of a critical security solution.

Capability	Y/N	Blumira
Does your detection solution have high availability?		✓
Does your detection solution have 24x7 automated detection?		✓
Does your solution queue logs in the event of an internet outage and resume once connectivity is re-established?		✓

Blumira: Automated Threat Detection & Response

Designed for easy deployment & use for organizations and IT teams of any size

Blumira's end-to-end platform offers both threat detection and response capabilities, automating the security operations workflow to enable organizations to defend against threats in near real-time. Its platform supports integrations with major tech and security systems for the broadest coverage. It provides greater security value than traditional SIEMs at an affordable cost and predictable pricing model for the mid-market.

Blumira's platform eases the burden of alert fatigue, the complexity of log management and lack of visibility across an IT environment. It brings an integrated platform to companies in many different industries struggling to defend against cybersecurity attacks with limited resources and staff.

Blumira allows you to:

Collect & Centralize Security Events

Easily integrate with applications and security tools across your environment, including cloud and on-prem. Blumira's cloud-delivered service collects and parses security events, logs and alerts for visibility through a single pane of glass.

Rapidly Detect Cybersecurity Threats

By correlating log data with continuously updated threat intelligence feeds, Blumira's platform detects known and suspected cybersecurity threats. It reduces the noise of false-positive alerts with automation and fine-tuning. With Blumira, you can deploy honeypots with the click of a button to detect lateral movement and unauthorized access across your environment.

Automate Remediation

When known cybersecurity threats are detected, Blumira's service allows you to easily implement blocking rules to quickly stop active threats without manual intervention.

Respond Quickly With Guided Playbooks

Blumira's guided and actionable remediation playbooks enable anyone in IT to easily respond to and stop cybersecurity threats – even without security expertise. Our security analysts give you step-by-step response workflows built into Blumira's platform.

Report on Security Findings & Activities

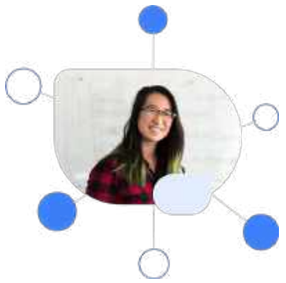
Blumira's pre-built searches and reporting help organizations investigate the security threats found within their environment while providing auditors with reports to help meet compliance.

> "Other tools are noisy; we don't have time to dig through layers & layers of data. Blumira does a good job summarizing detections and giving us advice on how to remediate."
>
> – **Steve Gatton,** VP of IT Network, Fechheimer

> "Blumira provides expertise in understanding alerts. With a limited staff, it's important that someone has my back – Blumira's team has a real commitment to its customers."
>
> – **Kevin Hayes,** CISO, Merit Network

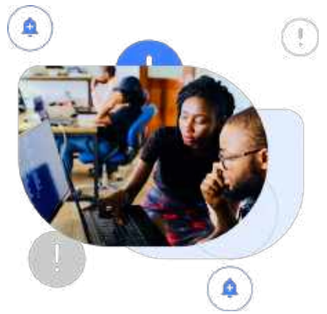
merit
NETWORK. SECURITY. COMMUNITY.

Streamline Your Security Operations



Deploy in Hours

Failed SIEM deployments can drag on for months and years. Blumira's cloud-delivered platform is designed for easy deployment in hours for small IT and security teams.



No More Alert Fatigue

Blumira's automated threat detection and response platform comes with pre-built rules and tuning, sending only prioritized alerts to your team.

Security Expertise

Staffing your own team isn't always an option. Blumira lets you run lean - while having access to our security team's expertise when you really need it.

Want to Learn More?

See how easy it is to protect your organization from cybersecurity threats with Blumira's automated threat detection & response solution.

Watch a Demo