Blumira

DATA SHEET

Faster Detection & Response

Time to security is more critical than ever to quickly detect and contain threats. Blumira's platform enables you to respond to threats faster to prevent ransomware and data breaches.

Simplify & Automate Threat Protection

With Blumira’s SIEM & XDR platform, you can get up and running in minutes — using your existing team and infrastructure. Get complete security coverage in hours to rapidly detect and stop attacks.

Detection

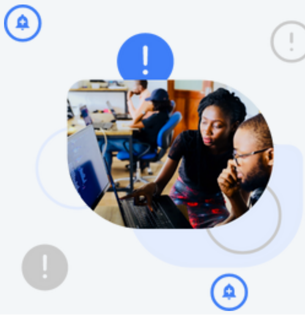
Monitor and detect real threats

- Get meaningful findings on real threats to reduce alert fatigue
- Easy-to-understand threat analyses
- Gain wide coverage across on-premises and cloud; track trends with security reports

Response

Enable your team to quickly respond

- Block threats with automated response
- Easily remediate with playbooks for every finding
- 24/7 Blumira SecOps support for further assistance



Expertise

Gain access to security expertise

- Security advice from Blumira’s responsive security team
- Help with onboarding, deployment, integrations and rule management
- Advanced support for incident response, triage and investigation

Benefits of Blumira:

- **Faster time to security** - deploy in minutes, 5x faster than industry average
- **Replace your legacy SIEM** (security incident event management) - automate manual triage and response
- **Lower TCO** (total cost of ownership) - all-in-one platform priced per user (not data or endpoints)
- **Custom and scheduled reporting** - On-demand access to all data for reporting and investigation purposes

Best Support WINTER 2025

Easiest Admin Mid-Market WINTER 2025

Easy for SMBs

> *"SIEMs have been unreachable for small or medium-sized companies for far too long, and we are glad to say that with Blumira, that's not the case anymore."*
>
> -- David S. CISO, SMB

Blumira

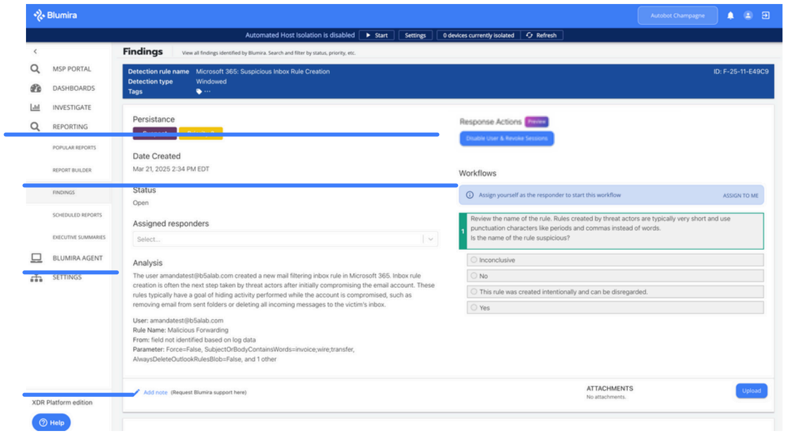
DATA SHEET

Comprehensive Coverage of Real Threats

Blumira leverages threat intelligence and behavioral analytics to detect patterns of attack, alerting you to high priority threats such as:

- **Cloud infrastructure threats** - Common misconfigurations, modified security groups, malware indicating a compromised cloud instance, attempts to connect with C2 (attacker-controlled) servers
- **Identity-based attacks** - Attempts to log in to your systems, including geo-impossible logins and fraudulent login attempts that could indicate the theft of usernames and passwords
- **Email & document risks** - Anomalous access attempts, external document sharing, email forwarding and new inbox rules created by attackers
- **Endpoint security threats** - Malware, unknown or blocklisted applications, malicious executables, and compromised processes running on devices within your network
- **Ransomware-related risk** - Blumira detects indicators of a ransomware attack through any of the threats listed above, then enables you to respond faster to prevent infection and a data breach

Actionable Findings, Automated Response & Access to Experts



Threat Response: Disable User

Playbooks For Response

Threat Analysis

Direct Message a Security Expert

Findings — View all findings identified by Blumira. Search and filter by status, priority, etc.

Detection rule name: Microsoft 365: Suspicious Inbox Rule Creation
Detection type: Windowed
Tags
ID: F-25-11-E49C9

Persistance

Date Created
Mar 21, 2025 2:34 PM EDT

Status
Open

Assigned responders
Select...

Analysis

The user amandatest@b5alab.com created a new mail filtering inbox rule in Microsoft 365. Inbox rule creation is often the next step taken by threat actors after initially compromising the email account. These rules typically have a goal of hiding activity performed while the account is compromised, such as removing email from sent folders or deleting all incoming messages to the victim's inbox.

User: amandatest@b5alab.com
Rule Name: Malicious Forwarding
From: field not identified based on log data
Parameter: Force=False, SubjectOrBodyContainsWords=invoice;wire;transfer, AlwaysDeleteOutlookRulesBlob=False, and 1 other

Workflows

Assign yourself as the responder to start this workflow

1 Review the name of the rule. Rules created by threat actors are typically very short and use punctuation characters like periods and commas instead of words.
Is the name of the rule suspicious?

○ Inconclusive
○ No
○ This rule was created intentionally and can be disregarded.
○ Yes

Add note (Request Blumira support here)

ATTACHMENTS
No attachments.

Blumira's XDR Edition

Benefits include:

- 1 year log retention for unlimited data
- 24/7 Security Operations Support for Critical Issues
- Detection rule management, allowlisting, customization
- Over 550+ managed detection rules
- Automated blocking of threats with Dynamic Blocklists
- Automated Host Isolation to immediately contain device threats
- Microsoft 365 Threat Response to disable users & revoke sessions
- Honeypots
- Endpoint detection and response with Blumira Agent
- Custom and scheduled reporting
- Over 130 integrations included at no additional cost

Simple Security For IT Admins

"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

ACI ATLANTIC CONSTRUCTORS