Blumira

Microsoft 365 Threat Response

Stay ahead of cyberattacks and contain threats faster by responding to M365, Azure, and Entra threats directly within Blumira for immediate remediation.

CHALLENGE

More than 2 million companies worldwide use Microsoft 365 (Statistica), making it a major target of threat actors and cyberattacks. Identity-related attacks are common, including compromised credentials, privilege escalation, phishing emails, brute-force attacks and more. Meanwhile, IT and security teams struggle to detect and respond to M365 threats efficiently, as they must juggle several different applications as they context-switch on a daily basis.

SOLUTION

There's a simple way to respond to Microsoft 365 threats through Blumira. Strengthen your security posture with threat response capabilities for M365, Azure, and Entra.

- Detect critical M365 events and receive instant alerts
- Lock out compromised users to contain threats quickly
- Respond to threats within one platform to save time and improve response speed

These actions address identity management, isolation, and remediation, protecting your environment from compromised users until further investigation is complete.

M365 Threat Detected → Review Finding → Disable User

HOW IT WORKS

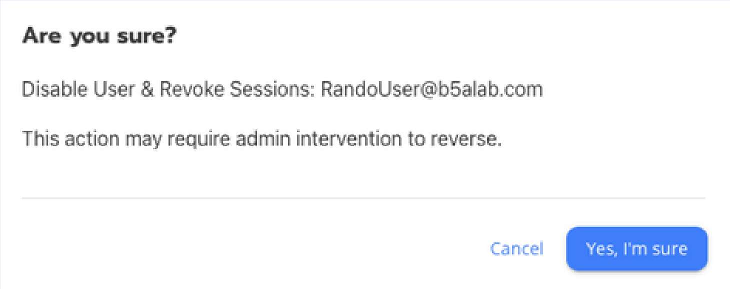
- Connect your Microsoft 365 application with Blumira through a Cloud Connector, an easy API-based integration that collects logs for detection & response
- Set up a response connector for Microsoft 365
- Test response actions by triggering a test finding, then use the available response actions
- To respond to a finding in Blumira, go to **Reporting** > **Findings**, open the Microsoft 365 finding, and click Disable User & Revoke Sessions on the detail page.

BENEFITS

✓ **Faster Threat Containment**
Take immediate action by locking out users directly within Blumira to prevent further malicious activity in your environment.

✓ **Simplified Response**
Reduce manual effort by streamlining security actions within one platform, no need to switch applications.

Blumira



Are you sure?

Disable User & Revoke Sessions: RandoUser@b5alab.com

This action may require admin intervention to reverse.

M365 FINDINGS

Blumira analyzes data from your M365, Azure & Entra environments, detecting suspicious activity and threats, and notifying you within minutes. To expedite remediation, we've built threat response into our platform for over 90+ detections, including:

Microsoft 365

- Impossible Travel Activity
- Activity From Infrequent Country
- Mass Deletion of M365 Objects
- Mass Download
- Suspicious Email Sending Patterns Detected
- Email Sending Limit Exceeded
- Elevation of Exchange Admin Privilege
- File Shared With Personal Email Addresses
- Multiple Failed User Log On Attempts to an App
- New MFA Device Added
- Malicious URL Click Alert
- And more!

Azure/Entra

- New User Created
- Non-Privileged Role Assignment
- Anomalous Agent Sign-In Activity
- Failed SSH Brute Force Attack Security Alert
- Failed Single Factor PowerShell Authentication Attempt
- Potential Token Theft via Entra Device Code Flow
- Add Unverified Domain
- Conditional Access Policy Added/Modified/Deleted
- And more!

AUTOMATED RESPONSE

Enable your team to do more, around the clock, without hiring additional security staff. Blumira automatically detects threats, sends you playbooks on how to respond, and takes automated action to contain threats by:

Isolating Endpoints

Detect endpoint-related threats, then immediately cut off an endpoint's access to your network to stop attacks in progress. Requires Blumira Agent.

Blocking Malicious Traffic

Detect known malicious sources of traffic, then immediately block their access to your environment. Requires on-prem sensor and firewall integration.

Disable Users

Detect suspicious users, then take action by disabling users and revoking sessions. Requires Microsoft 365 Cloud Connector and threat response configuration.

> ***When a user is compromised, every second counts.** It brings peace of mind to us and to our clients that **Blumira's M365 Response can lock bad actors out in seconds**, stopping them quicker than ever before!*
>
> *-- Matt Timm, Network Operations Center Team Lead, TR Computer Sales*

TRY SIEM + XDR

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

Sign up for a free 30-day trial of Blumira's SIEM + XDR platform.

BLUMIRA.COM/FREE