DATA SHEET

Blumira

All-in-One SIEM + Detection & Response

2022 State of Detection & Response

Blumira's platform detects and helps organizations respond to indicators of attacks in progress -- we analyzed 33,911 total findings from a sample of 230 organizations in 2021. Here's what we found:

Time to Security: Impact on Bottom Line

Breaches that take longer than 200 days to resolve can result in **35% higher cost**, from $3.6 million to $4.9 million on average (IBM/Ponemon's *2021 Cost of a Data Breach* report).

287 days

Average breach lifecycle to detect & respond

Time to Detect

99.4% faster

212 days

Average time to detect a breach

32 min

Blumira's average time to detect a finding

Time to Respond

99.4% faster

75 days

Average time to respond to a threat

6 hours

Average time to respond (customer closed a finding)

(Source: 2021 Cost of a Data Breach)

(Source: Blumira's 2021 dataset)

*"With our old provider, it was a **big time sink** trying to filter through false-positives & close out events.*

*[With Blumira], **we're able to respond to important activities sooner**, since we're not wading through unimportant things."*

- Bryan Allen
Sr. Systems Analyst

Lawrence Technological University

Blumira

DATA SHEET

Top Overall Findings

1. **Honeypot HTTP Authentication Attempt**
2. **Okta Log Failure**
3. **Service Execution With Lateral Movement Tools**
4. **Admin-Level Account Added**
5. **50 GB+ Inbound Connection via Generic Network Protocol**

Top Microsoft Findings

1. **Creation of Office 365 Security Group**
2. **10 Windows Password Resets in 1 Hour**
3. **PS-Exec Use on Network**
4. **Modification of Microsoft 365 Group**
5. **Clearing of Windows Event Logs**

Our Summary of Trends

Identity-Based Attacks

Cloud environments are particularly vulnerable to identity-based attacks and unauthorized access attempts, including the use of phishing, password spraying and more.

Living off the Land

This refers to attackers using legitimate, built-in tools to evade detection by typical security products, such as Microsoft's PsExec & PowerShell.

Targeting Microsoft 365

Our findings revealed patterns of Microsoft-related activity, including activity associated with password spraying, lateral movement, and business email compromise.

Download the full report:
blumira.com/2022-report

The Blumira Value

Meet compliance controls, save time on security tasks, focus on real threats and protect against a breach faster than ever -- with Blumira.

✓ Automate tasks for you

We do all the heavy lifting for your team to save them time, including parsing, creating native third-party integrations, and testing and tuning detection rules to reduce noisy alerts.

✓ Faster time to security

Our unique approach to detections notifies you of threats other security tools may miss, sending you real-time alerts in under a minute of initial detection to help you respond to threats faster than ever.

✓ Easily meet compliance

With a year of data retention and deployment that takes minutes to hours, we help you meet cyber insurance and compliance easily and quickly with the team you have today.

Detect & respond to Microsoft 365 threats with Blumira's free edition.

Sign Up Free!
blumira.com/free