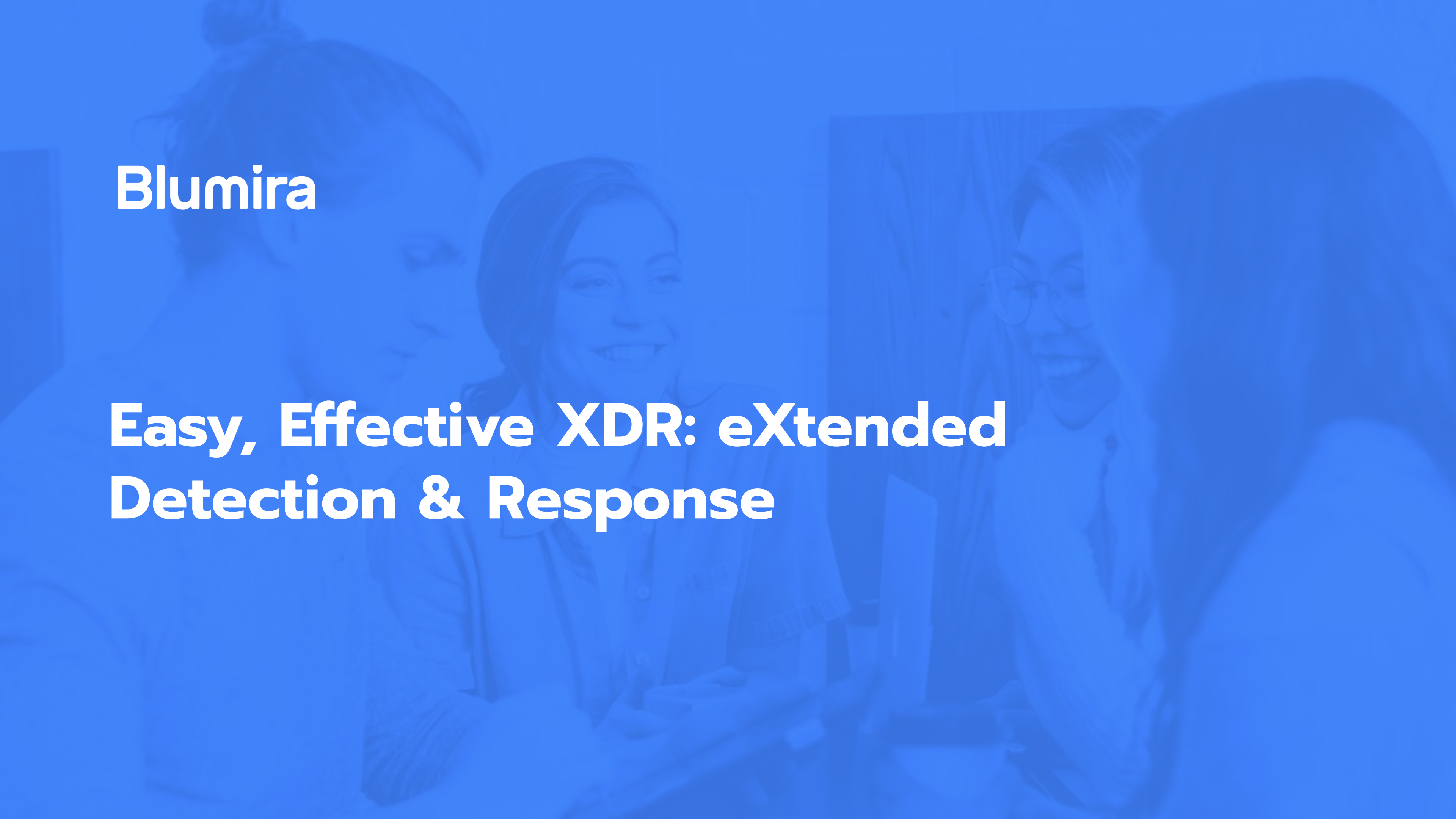


Blumira

Easy, Effective XDR: eXtended Detection & Response

Agenda

01

What is XDR?

A brief overview of security market trends.

02

Blumira XDR Value

How Blumira solves customer challenges.

03

How Blumira Works

Easy, effective and efficient detection and response.

01

What is XDR?

Blumira

WHAT IS XDR?

XDR = eXtended Detection & Response

*XDR unifies multiple security technologies into **a single platform**, providing greater visibility and control over threats. – Gartner*

1. Strong security tools integrated together
2. Centralized logs in one place
3. Insightful detections from correlated data
4. Automated response across endpoints & security tools

Why XDR?

XDR is born out of dissatisfaction with older tech, like standalone EDRs and SIEMs.

- **EDR** = only provides coverage for endpoints
- **SIEM** = traditional ones only collect logs, providing little detection & response functionality

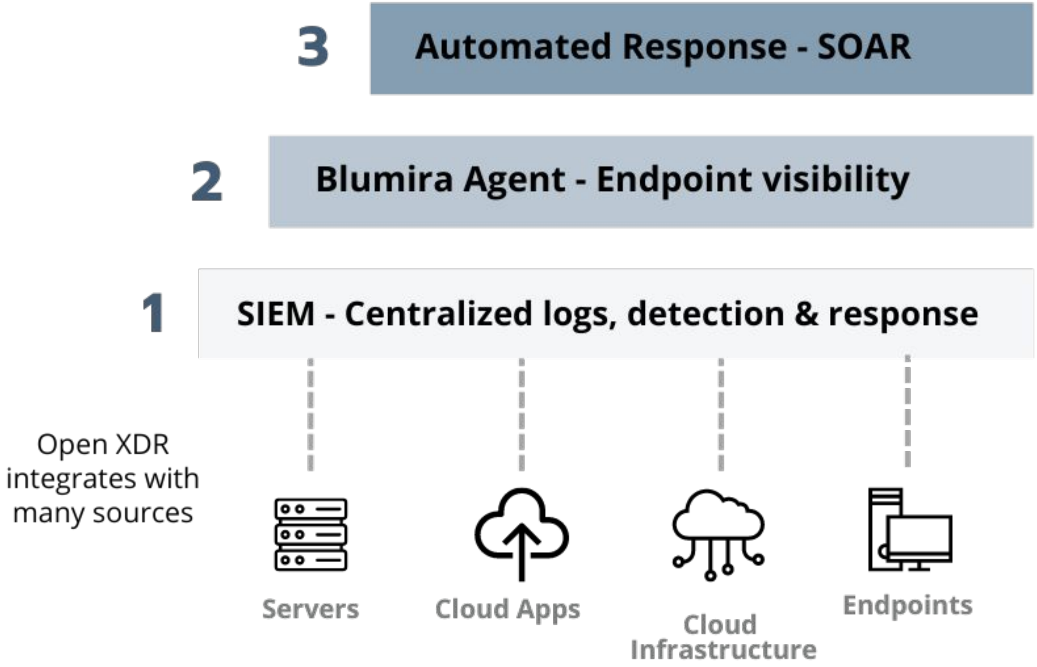
An open XDR platform combines the above & integrates broadly to give you insight into endpoints, emails, servers, the cloud, and networks.

It also includes automated response features to immediately contain or block threats.

WHAT IS BLUMIRA XDR?

Blumira's XDR Platform

- Reduce complexity by consolidating security tools into one platform
- Integrate broadly to provide insight across your entire environment
- Use automation to speed up detection and response


3
Automated Response - SOAR
2
Blumira Agent - Endpoint visibility
1
SIEM - Centralized logs, detection & response
Open XDR integrates with many sources
Servers
Cloud Apps
Cloud Infrastructure
Endpoints

Blumira

WHAT IS OPEN XDR?

Open XDR

Integrate with third-parties
Flexible as you grow
Coverage for modern hybrid IT
No vendor lock-in

Microsoft Security

cisco

vs. Native XDR

Must buy all 1 vendor’s solutions
Expensive, contract lock-in
Potential gaps in coverage
Built for the enterprise

02

Blumira XDR Value

Blumira

CHALLENGES

Small & medium-sized businesses struggle to protect their organization against ransomware and breaches

Time-Strapped

Managing security tools can require many manual tasks – threat hunting, managing rules, parsing data, developing integrations and more.

No 24/7 Team

Small IT teams can’t be fully staffed around the clock due to costly enterprise solutions, talent shortage and lack of security expertise.

Complexity

Too many disparate solutions results in redundancies and lack of visibility into remote endpoint risks.

*“**I don’t have the staff** dedicated to sit and read logs all day or with the **skillset to analyze our data**.”*
– Jim Paolicelli, IT Director, Atlantic Constructors

Blumira

BLUMIRA XDR VALUE

Blumira's open XDR platform simplifies advanced detection and response for small and medium-sized businesses

EASY

Free up time & refocus efforts

Reduce reliance on humans to complete manual security tasks to achieve faster time to security

EFFECTIVE

Faster time to security

Accelerate breach prevention and ransomware protection with automated response

EFFICIENT

Satisfy compliance & gain more visibility

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

"I feel comfortable now that we don't have unknown activity happening on our network -- we now have ***full visibility of our infrastructure****." – John Hwee, Director of IT, Duraflame*

Blumira

BLUMIRA XDR PLATFORM

Blumira delivers unique value to meet SMB needs:

✓ FLEXIBILITY OF AN OPEN XDR

Open platform supports multiple vendors for hybrid coverage of cloud, endpoint, identity, servers and more

✓ AUTOMATION ACCELERATES SECURITY

Deploy in minutes; stop threats immediately with automated response to isolate devices and block malicious traffic

✓ MANAGED PLATFORM SAVES TIME

Blumira's team manages the platform to do threat hunting, data parsing and analysis, correlation and detection at scale

✓ SATISFY MORE COMPLIANCE CONTROLS

Get more in one – SIEM w/1 year of data retention, endpoint, automated response & 24/7 SecOps support*

**For critical priority issues*

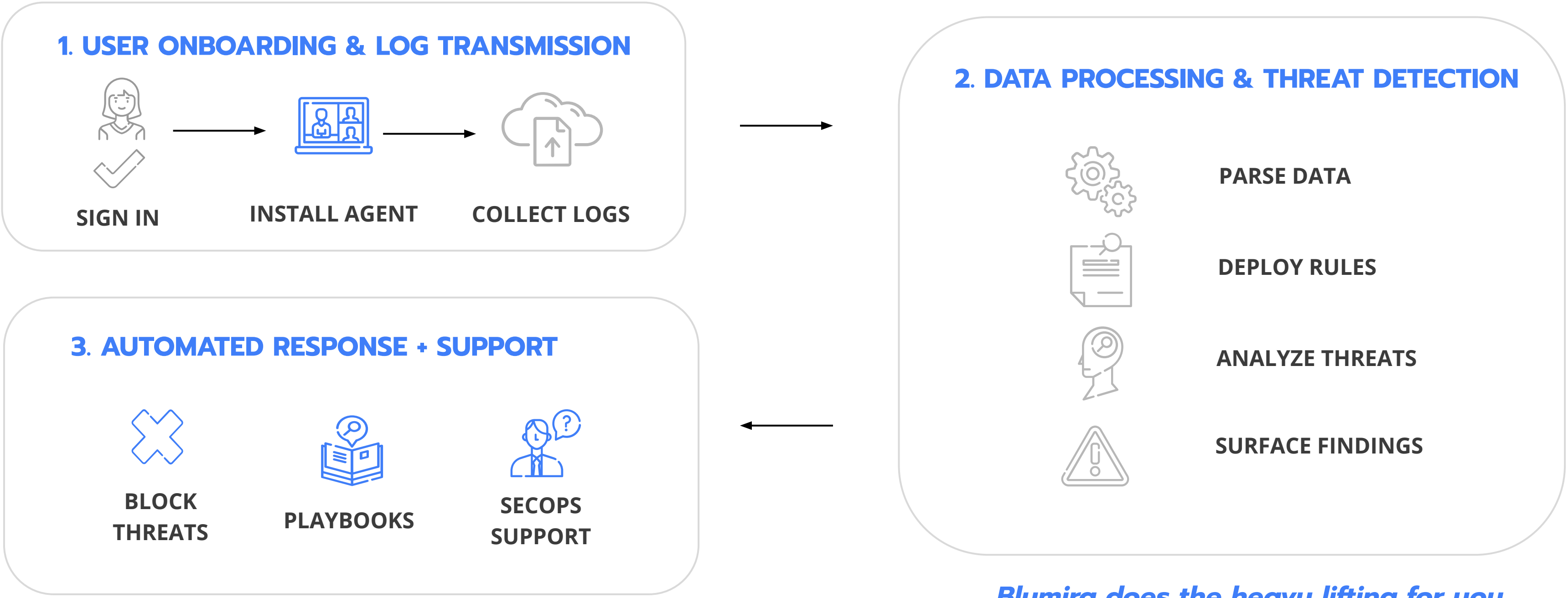
03

How Blumira Works

Blumira

HOW IT WORKS

Blumira analyzes threats with faster resolution to prevent a breach



1. USER ONBOARDING & LOG TRANSMISSION

SIGN IN → INSTALL AGENT → COLLECT LOGS

2. DATA PROCESSING & THREAT DETECTION

- PARSE DATA
- DEPLOY RULES
- ANALYZE THREATS
- SURFACE FINDINGS

3. AUTOMATED RESPONSE + SUPPORT

- BLOCK THREATS
- PLAYBOOKS
- SECOPS SUPPORT

Blumira does the heavy lifting for you.

ALL-IN-ONE XDR PLATFORM:
SIEM + ENDPOINT + AUTOMATED RESPONSE

BLUMIRA XDR PLATFORM

Fast, Easy & Automated

- Deployment is 5x faster than the industry avg.*
- Data is parsed, normalized, retained for 1 year
- Logs are automatically analyzed for threats

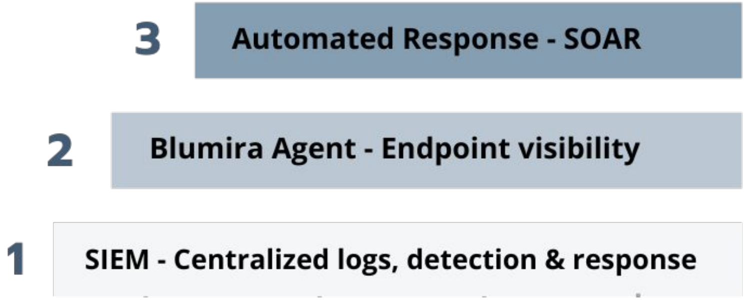
Reduce Alert Fatigue

- All findings are prioritized by level of criticality (P1-P3)
- All correlated data are consolidated under initial findings and tuned or adjusted to reduce fatigue
- Alerts sent within 50 seconds of initial detection for faster time to security

Fully Managed Detections

- Blumira engineers tune and develop new detections to automate threat hunting
- Platform updated regularly to protect against new threats
- Customers can filter alerts based on known safe activity to reduce noise

SIEM + MANAGED DETECTIONS →


3 Automated Response - SOAR
2 Blumira Agent - Endpoint visibility
1 SIEM - Centralized logs, detection & response

Blumira

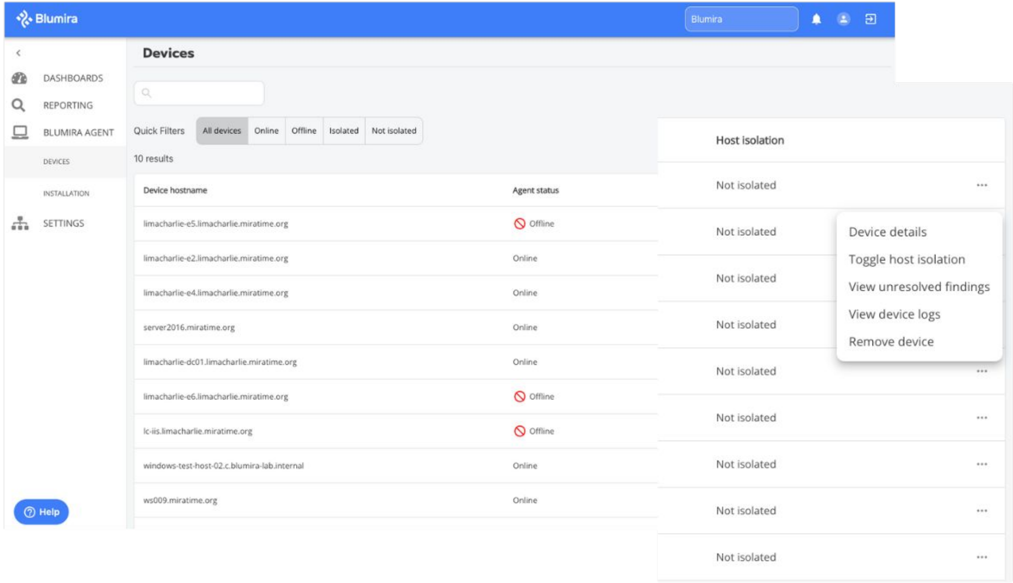
BLUMIRA XDR PLATFORM

Support Remote Work

- Blumira Agent extends coverage to Windows endpoints located anywhere
- Fast, easy to deploy in minutes – no infrastructure required
- Lightweight, minimal impact to your environment

Detect & Contain Threats Immediately

- Device/host isolation to automatically contain an identified threat
- Protect your network from a ransomware attack



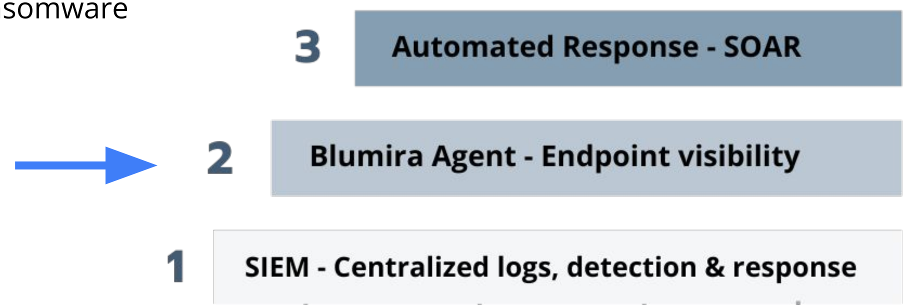
Devices

Quick Filters: All devices | Online | Offline | Isolated | Not isolated

10 results

Device hostname	Agent status	Host isolation
limacharlie-e5.limacharlie.miratime.org	Offline	Not isolated
limacharlie-e2.limacharlie.miratime.org	Online	Not isolated
limacharlie-e4.limacharlie.miratime.org	Online	Not isolated
server2016.miratime.org	Online	Not isolated
limacharlie-dc01.limacharlie.miratime.org	Online	Not isolated
limacharlie-e6.limacharlie.miratime.org	Offline	Not isolated
lc-iis.limacharlie.miratime.org	Offline	Not isolated
windows-test-host-02.c.blumira-lab.internal	Online	Not isolated
ws009.miratime.org	Online	Not isolated

ENDPOINT VISIBILITY WITH BLUMIRA AGENT



3 Automated Response - SOAR

2 Blumira Agent - Endpoint visibility

1 SIEM - Centralized logs, detection & response

BLUMIRA XDR PLATFORM

Automated Host Isolation

- Blumira Agent immediately isolates an endpoint from your network when a critical threat is identified

Automated Blocking

- Automatically block traffic from known malicious IP addresses
- Dynamic blocklists use updated threat feeds integrated with your firewall to identify threat sources

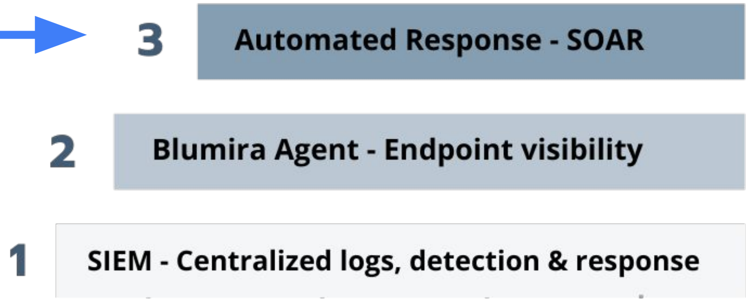
Response Playbooks

- Automatically sent with every finding
- Guide your IT team through easy remediation steps

24/7 SecOps Support

- Access to a responsive security team for critical priority issues
- Get security guidance, onboarding help and answer any questions about findings

AUTOMATED RESPONSE →


3
Automated Response - SOAR
2
Blumira Agent - Endpoint visibility
1
SIEM - Centralized logs, detection & response

Blumira's open XDR platform simplifies detection & response, accelerating ransomware and breach prevention.

EASY

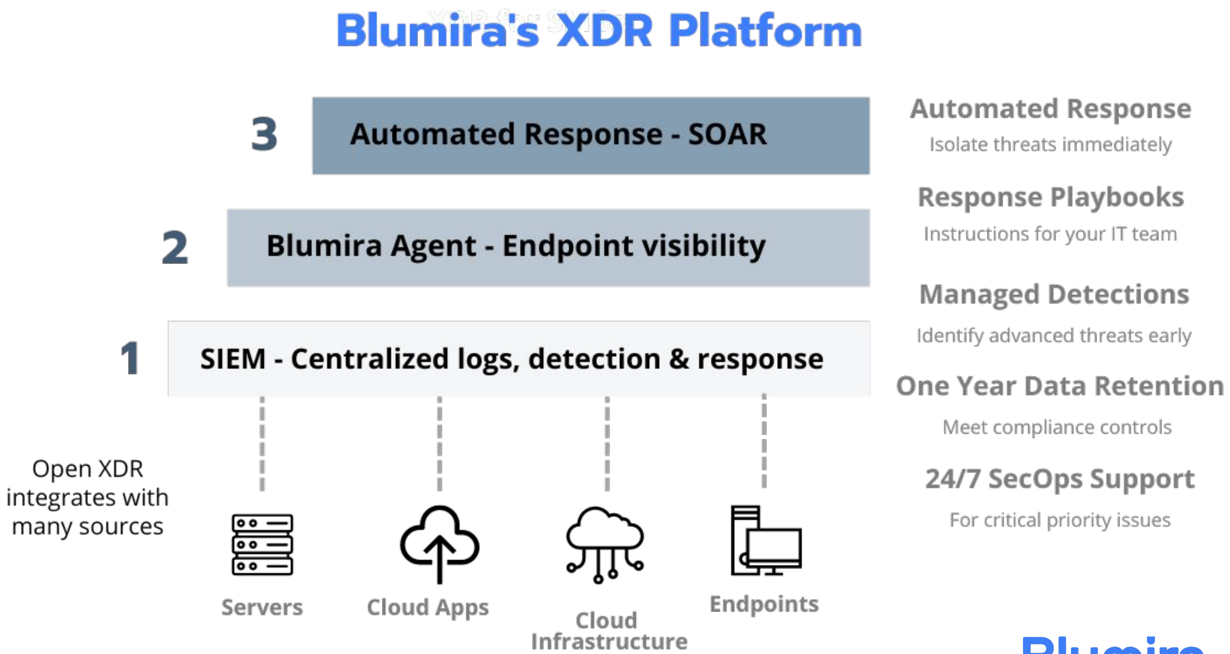
Free up time & refocus efforts

EFFECTIVE

Faster time to security

EFFICIENT

Satisfy compliance & gain more visibility



Blumira's XDR Platform

3 Automated Response - SOAR

2 Blumira Agent - Endpoint visibility

1 SIEM - Centralized logs, detection & response

Open XDR integrates with many sources

Automated Response
Isolate threats immediately

Response Playbooks
Instructions for your IT team

Managed Detections
Identify advanced threats early

One Year Data Retention
Meet compliance controls

24/7 SecOps Support
For critical priority issues

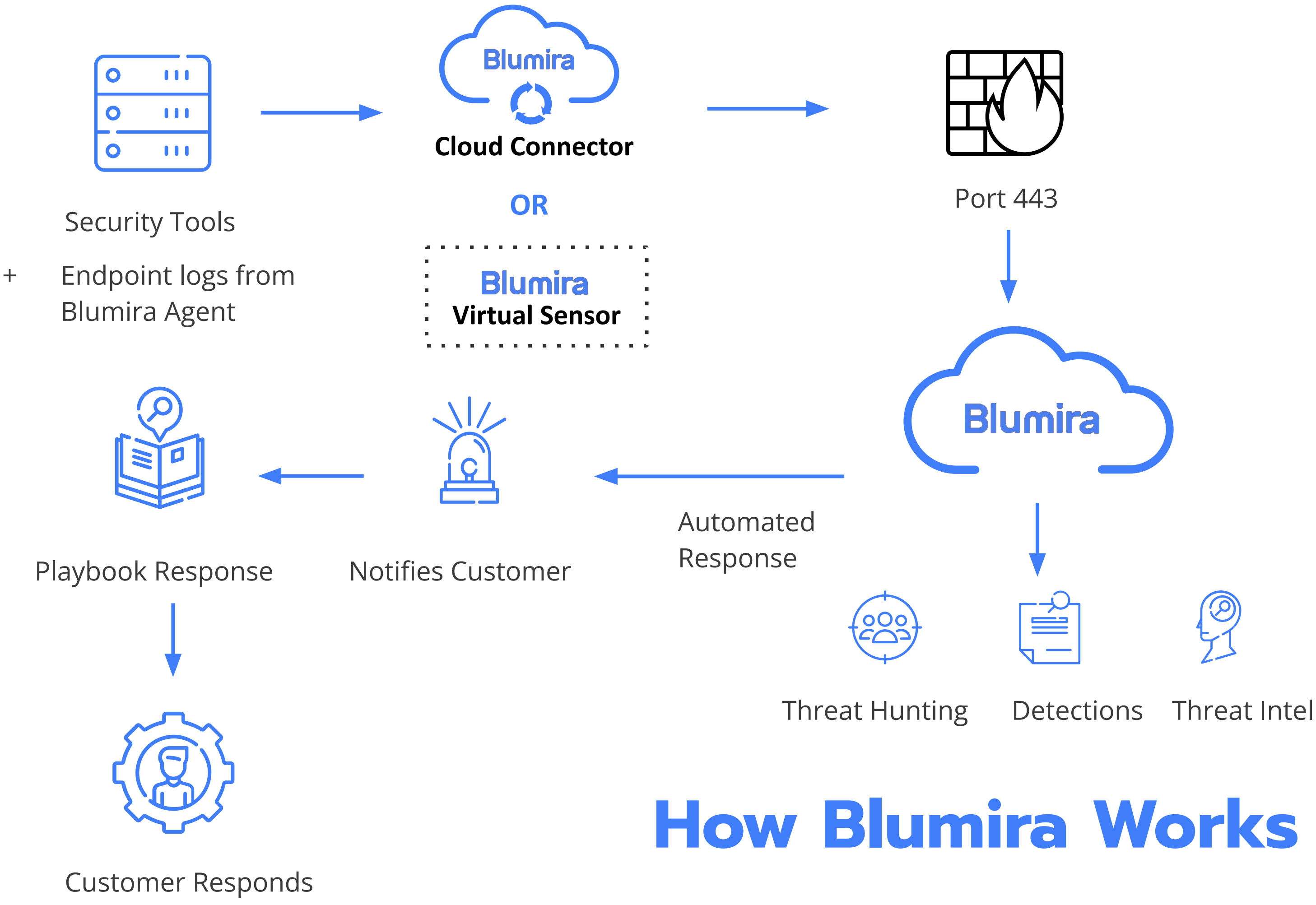
Blumira

Features	Free SIEM	SIEM Pro	SIEM + Endpoint Visibility	XDR Platform
Data retention	14 days	30 days	1 year	1 year +
Cloud integrations	Pick 3	✓ All	✓ All	✓ All
Sensor integrations		✓ All	✓ All	✓ All
Logging & analysis	✓	✓	✓	✓
Managed detections & playbooks	✓	✓	✓	✓
Filter detections for noise		✓	✓	✓
Blumira Agent / manual isolation			✓ 1/user +	✓ 1/user +
Automated host isolation / blocking				✓
Honeypots			✓	✓
Dashboards & reporting	Only basic	✓	✓	✓
24/7 support critical issues		✓	✓	✓

Additional Product Information

Blumira

How Blumira Works



Security Tools

+ Endpoint logs from Blumira Agent

Blumira

Cloud Connector

OR

Blumira

Virtual Sensor

Port 443

Blumira

Threat Hunting

Detections

Threat Intel

Automated Response

Notifies Customer

Playbook Response

Customer Responds

1. Collect
2. Parse
3. Correlate
4. Analyze
5. Detect
6. Automated Response
7. Notify
8. Playbooks
9. Respond

Blumira

Open XDR Integrates With Any Service

Cloud Infrastructure	Microsoft Azure Azure Active Directory okta DUO SECURITY aws
Endpoint	Carbon Black. SentinelOne CROWDSTRIKE SOPHOS Malwarebytes TREND MICRO eset Symantec BlackBerry CYLANCE
Productivity	Microsoft 365 G Suite proofpoint. cisco Cisco Umbrella
Host	Windows Server Windows Active Directory Linux
Firewall	paloalto NETWORKS FORTINET cisco Meraki Check Point SOFTWARE TECHNOLOGIES LTD. SOPHOS CITRIX WatchGuard

See complete list of integrations at blumira.com/integrations

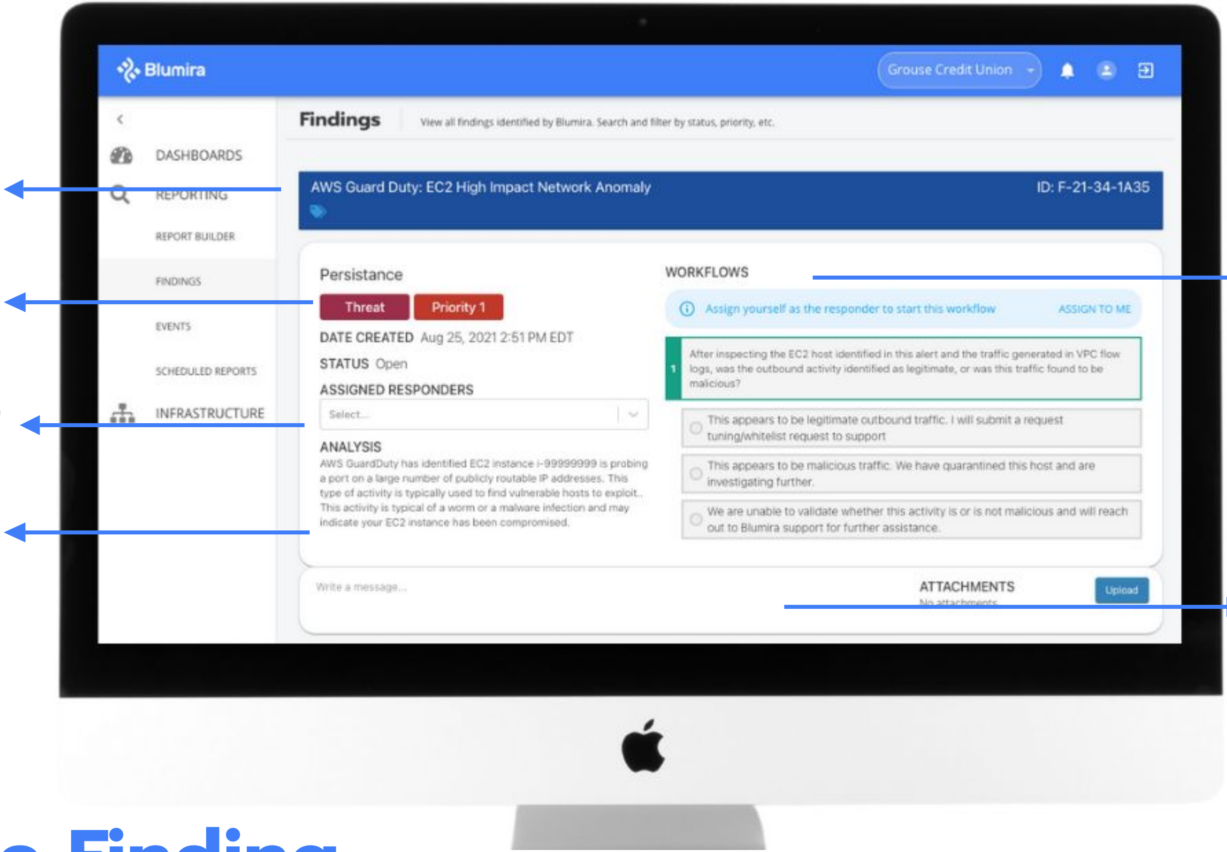
Blumira

Open XDR Integrates With Any Service

Additional Integrations	osquery APACHE NGINX
	Mac OS FORESCOUT PhishER
	mimecast vmware®
	logstash LastPass•••| Windows Defender

See complete list of integrations at blumira.com/docs

Blumira



Blumira

Grouse Credit Union

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

AWS Guard Duty: EC2 High Impact Network Anomaly — ID: F-21-34-1A35

Persistance

Threat | Priority 1

DATE CREATED Aug 25, 2021 2:51 PM EDT

STATUS Open

ASSIGNED RESPONDERS

Select...

ANALYSIS

AWS GuardDuty has identified EC2 instance i-99999999 is probing a port on a large number of publicly routable IP addresses. This type of activity is typically used to find vulnerable hosts to exploit.. This activity is typical of a worm or a malware infection and may indicate your EC2 instance has been compromised.

WORKFLOWS

Assign yourself as the responder to start this workflow — ASSIGN TO ME

1 After inspecting the EC2 host identified in this alert and the traffic generated in VPC flow logs, was the outbound activity identified as legitimate, or was this traffic found to be malicious?

○ This appears to be legitimate outbound traffic. I will submit a request tuning/whitelist request to support

○ This appears to be malicious traffic. We have quarantined this host and are investigating further.

○ We are unable to validate whether this activity is or is not malicious and will reach out to Blumira support for further assistance.

Write a message...

ATTACHMENTS

No attachments

Upload

Security Finding

Threat Level

Assign Responder

Threat Analysis

Response Playbooks

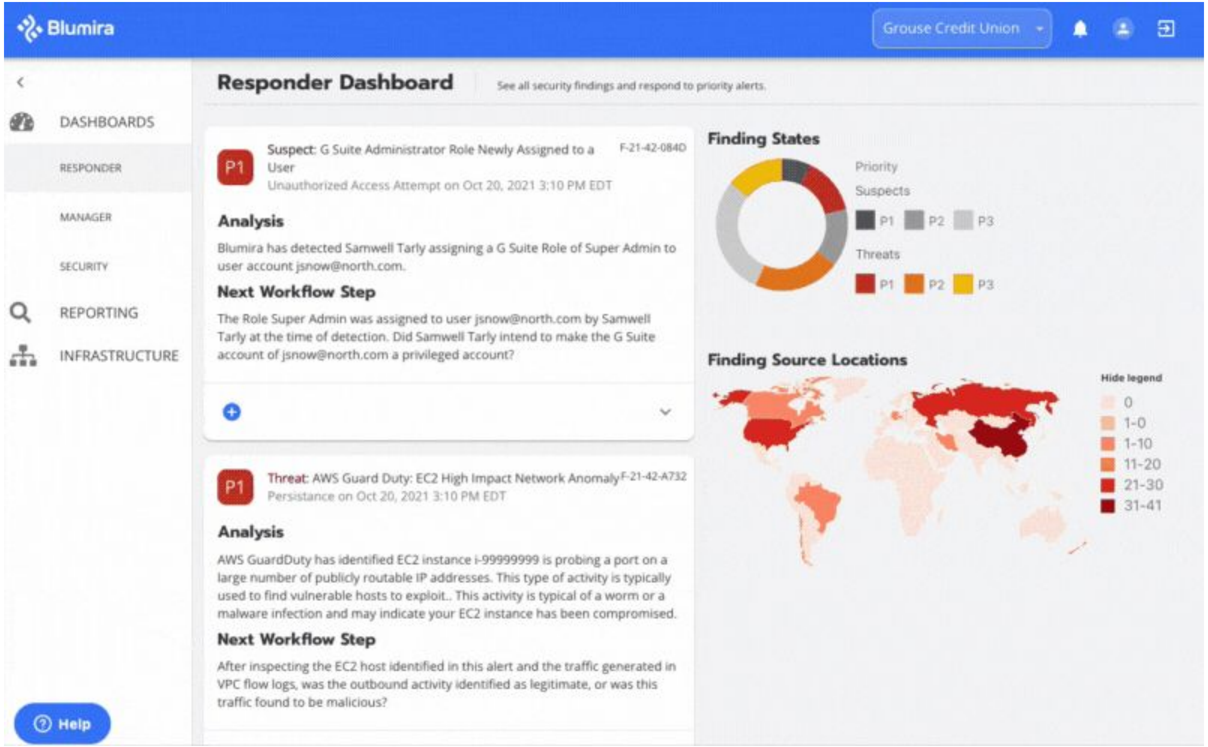
Ask an Expert

Example Finding

Blumira

See Blumira’s XDR Platform in Action

Automated extended threat detection & response



Responder Dashboard See all security findings and respond to priority alerts.

P1 Suspect: G Suite Administrator Role Newly Assigned to a User F-21-42-084D
Unauthorized Access Attempt on Oct 20, 2021 3:10 PM EDT

Analysis

Blumira has detected Samwell Tarly assigning a G Suite Role of Super Admin to user account jsnow@north.com.

Next Workflow Step

The Role Super Admin was assigned to user jsnow@north.com by Samwell Tarly at the time of detection. Did Samwell Tarly intend to make the G Suite account of jsnow@north.com a privileged account?

P1 Threat: AWS Guard Duty: EC2 High Impact Network Anomaly F-21-42-A732
Persistance on Oct 20, 2021 3:10 PM EDT

Analysis

AWS GuardDuty has identified EC2 instance i-99999999 is probing a port on a large number of publicly routable IP addresses. This type of activity is typically used to find vulnerable hosts to exploit.. This activity is typical of a worm or a malware infection and may indicate your EC2 instance has been compromised.

Next Workflow Step

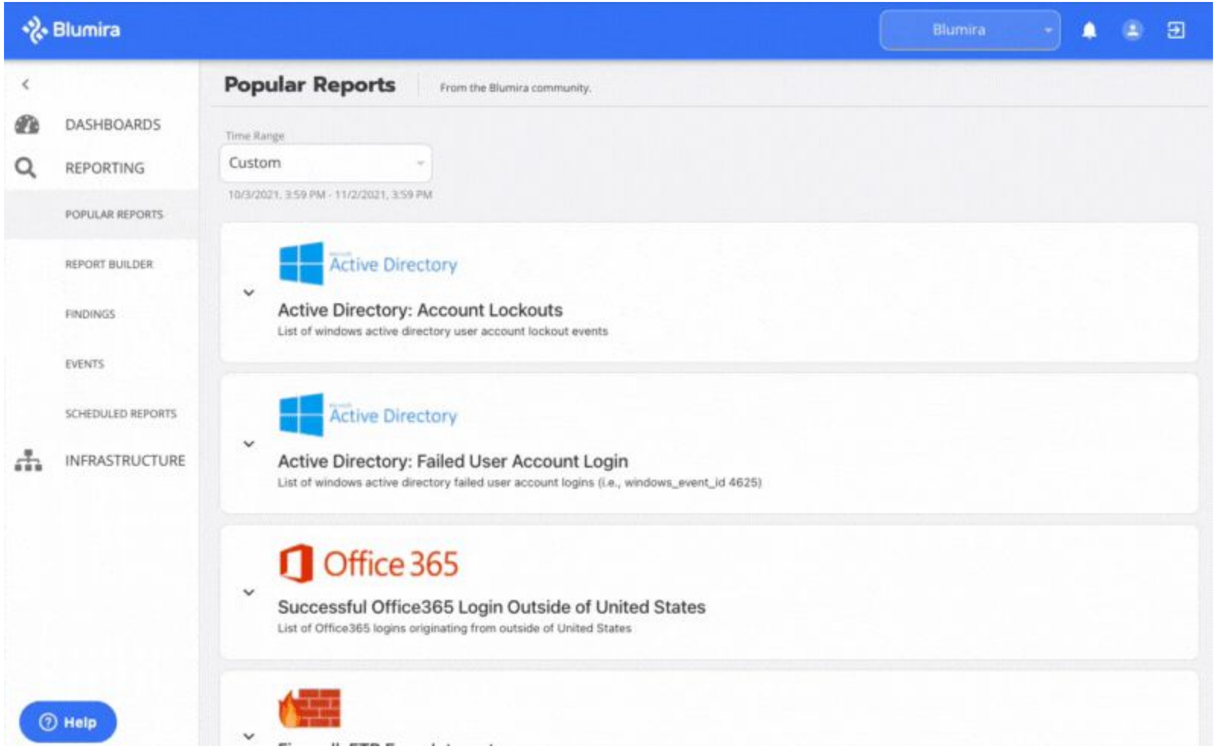
After inspecting the EC2 host identified in this alert and the traffic generated in VPC flow logs, was the outbound activity identified as legitimate, or was this traffic found to be malicious?

- Prioritized findings give you a full analysis of the threat
- Workflows for every finding tell you how to respond
- Correlated data sent with findings to help with investigation

Blumira

See Blumira's XDR Platform in Action

Easy-to-Use Security Reports With Click-Through Dashboards



Popular Reports From the Blumira community.

Time Range: Custom

10/3/2021, 3:59 PM - 11/2/2021, 3:59 PM

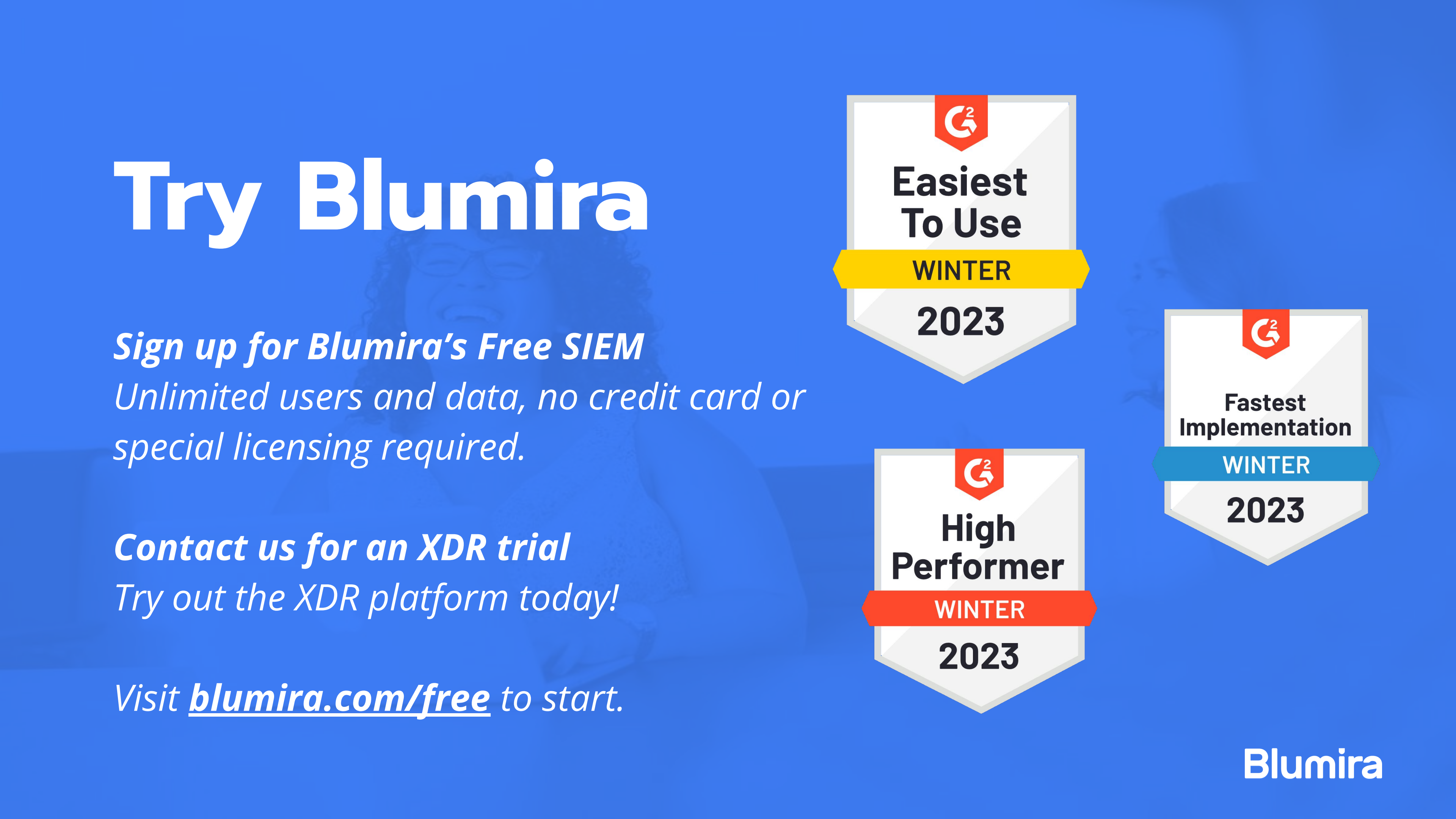
Active Directory: Account Lockouts
List of windows active directory user account lockout events

Active Directory: Failed User Account Login
List of windows active directory failed user account logins (i.e., windows_event_id 4625)

Successful Office365 Login Outside of United States
List of Office365 logins originating from outside of United States

- Scheduled security reporting is included
- Drill down into account lockouts, failed user logins and more
- Click-through dashboards provide customizable search through your data, filtered by data source

Blumira



Try Blumira

Sign up for Blumira's Free SIEM
Unlimited users and data, no credit card or special licensing required.

Contact us for an XDR trial
Try out the XDR platform today!

*Visit **blumira.com/free** to start.*

Easiest To Use
WINTER
2023

Fastest Implementation
WINTER
2023

High Performer
WINTER
2023

Blumira