

Sales/Marketing Demo Talking Points - XDR

1. Cloud Deployment

That's it! Setup is complete.

Cloud Connector Name	Current Status	Total Logs	Last Status Update	Created	Last Modified
Microsoft Cloud Connector 07-06-2022	Online	16M	Apr 3, 2023 9:12 AM EDT	Jul 6, 2022 8:00 PM EDT	Jul 6, 2022 8:00 PM EDT
Amazon Web Services Cloud Connector 10-27-2022	Online	49	Apr 3, 2023 9:14 AM EDT	Oct 27, 2022 11:20 AM EDT	Oct 27, 2022 11:21 AM EDT
ServiceNow Cloud Connector 09-20-2022	Online	349K	Apr 3, 2023 9:21 AM EDT	Nov 1, 2022 3:45 PM EDT	Jan 11, 2023 3:19 PM EDT
Duo Security Cloud Connector 09-20-2022	Online	64	Apr 3, 2023 9:19 AM EDT	Sep 20, 2022 1:57 PM EDT	Nov 1, 2022 4:06 PM EDT
Urbanscale Logon Keys Test - Smart Device	Online	820K	Apr 3, 2023 9:07 AM EDT	Nov 28, 2022 9:14 AM EDT	Jan 19, 2023 9:29 AM EDT
Microsoft 365 Cloud Connector 02-08-2023	Online	31K	Apr 3, 2023 9:22 AM EDT	Feb 8, 2023 7:08 PM EST	Feb 8, 2023 7:06 PM EST
S1 Account Level Viewer Account ID Default Site ID	Online	295K	Apr 3, 2023 9:18 AM EDT	Jan 19, 2023 8:50 AM EST	Jan 19, 2023 8:50 AM EST
S1 Account Level Viewer Account ID No Site ID	Online	296K	Apr 3, 2023 9:16 AM EDT	Jan 19, 2023 8:48 AM EST	Jan 19, 2023 8:48 AM EST

Easy SIEM deployment – Blumira is 5 times faster to deploy than the average SIEM provider (according to G2) – it only takes minutes to set up a cloud integration via API and start sending logs to Blumira for threat analysis, detection and response. Traditional SIEMs normally take weeks to months to set up.

Broad coverage for hybrid environments – We also provide additional integrations available to set up via sensors – see blumira.com/docs for full list of third-party integrations we support (including Windows, Microsoft Cloud, endpoint, firewall, identity providers, and more).

2. Detection Rules

That's it! Rule is disabled.

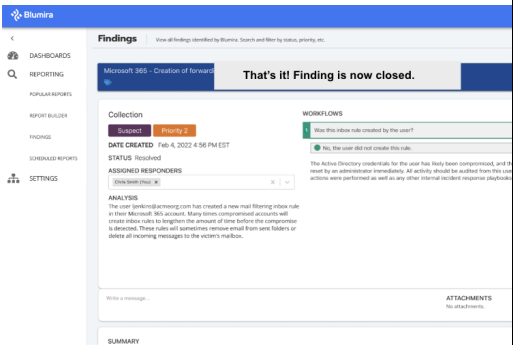
Rule name	Category	Priority	Data Type	Detection Type	Analysis summary	Filters
Microsoft User Cloud Questionable Link	Subject	P1	Microsoft TEF URL	Real Time	A user did a action against a URL categorized as malicious by Microsoft Trusted Threat Protection has been identified. Malware can gain initial access to an environment using phishing emails to lure users into navigating to malicious sites. These sites c...	0
Indicator: Microsoft 365 - Impassible Travel Activity	Subject	P1	Microsoft365 Compliance	Real Time	(Message) The user(s) should be contacted to verify their attempted/unsuccessful logins were made by them. It is possible they are authenticating over a VPN or cloud provider as opposed to their endpoint being compromised.	0
Azure AD Global Admin Role Assignment	Subject	P1	Microsoft365 Azure AD	Real Time	A Global Administrator Role has been assigned to the user or group (object) in your Azure Active Directory in the tenant (tenant ID). A Global Administrator has full permissions over the entire Azure tenant, similar to a Domain Administrator in on-premise.	0
Indicator: Microsoft 365 - ...	Subject	P2	Microsoft365 ...	Real Time	Microsoft has alerted on a malicious campaign targeting your Microsoft 365 ...	0

Detection Rules – See all rules enabled in your account and managed by Blumira’s security engineers.

- Our engineers do the work for you - researching, developing, tuning and automatically rolling out new rules to the platform on a regular basis to do threat hunting at scale for your team.
- Blumira’s engineers keep up to date with the latest vulnerabilities, threat research, understanding what’s critical, and tracking patterns of attacker behavior

Here, you can manage your own rules by toggling them on and off easily, or customize them using **Detection Filters** to allow known safe activity and further reduce the noise of alerts for your team.

3. Findings & Playbook



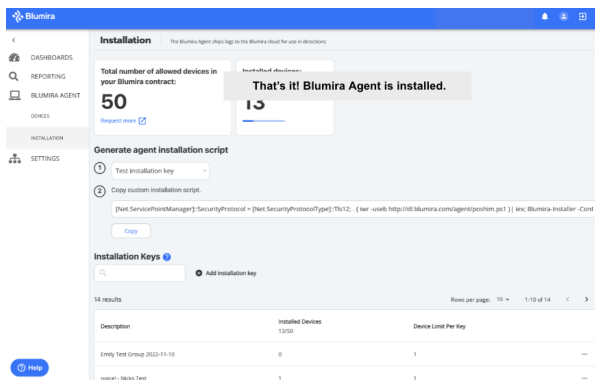
Time to Security: Findings are sent to you within 50 seconds of initial detection, prioritized by criticality so you know what's important to respond to right away.

- See all correlated data related to the finding, stacked below, saving you time on gathering information for investigation.
- From right within the app, you can assign a help desk tech the ticket for fast and easy triage.

Easy to Respond: Every finding comes with a pre-built playbook written by our security engineers to walk you through how to respond quickly.

Message Support: Need more help? Message our 24/7 SecOps team directly within the app (or call or email).

4. Endpoint Visibility

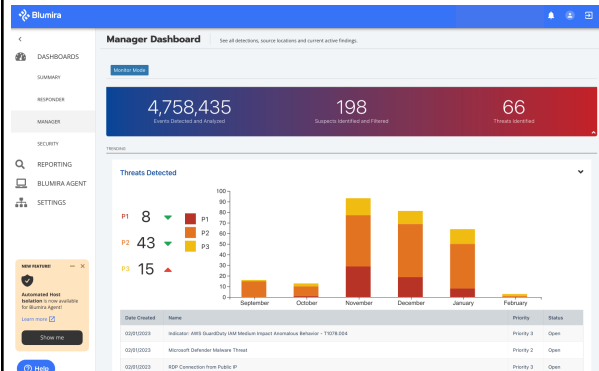


Endpoint visibility – Install a lightweight agent on Windows endpoints for detection and response. You can easily isolate an endpoint manually through our platform.

As part of our XDR platform, Blumira provides automated response for endpoints and malicious traffic:

- **Automated Host Isolation** – Set up auto-isolation for P1 and P2 threats to immediately contain compromised endpoints from your network to protect against spread of ransomware and attacker lateral movement. We cut off access from the endpoint to your network.
- **Automated blocking** – Block traffic from malicious sources (IP addresses) with Dynamic Blocklists – after integrating your firewall with Blumira, we can detect and automatically block malicious traffic (this requires sensor setup)

5. Dashboards & Reports



Visibility – See our at-a-glance dashboards:

- **Security** – Get a summary of your events, findings, users and endpoints
- **Manager** – See all detections prioritized by criticality, source locations, current active findings and more
- **Responder** – See all security findings and respond to priority alerts

Reporting

- **Report Builder** – Get access to your log data using Report Builder
- **Global Reports** – Use pre-built global reports to quickly populate and schedule to send reports of your log data.
- **Scheduled Reports** – See a list of your schedule reports, useful for investigation and compliance