Blumira

Blumira Investigate

Quickly investigate security incidents by searching all logs in your environment

Blumira Investigate gives IT teams a holistic view of related security events to help speed up incident investigation and response.

Finding a needle in the haystack of your logs has never been easier.

Save Time

Surfacing related data in one easy-to-understand dashboard saves your lean IT team time digging deeper into security incidents like phishing, ransomware, malware, and more.

Faster Resolution

Blumira Investigate helps you better understand the scope of incidents to resolve issues faster and limit the impact of an incident on your organization.

Use Cases

Investigate security events like:

Phishing Attacks

A phishing email reported by an employee bypassed your security controls; you want to see if any other employees clicked on the phishing link.

Searching by the URL could return results from a DNS query log to help provide more information about the scope of the incident to your IT analyst.

Malicious Processes

A malicious process was observed running using a service account.

Searching by username allows your IT analyst to review authentication logs related to the compromised service account name to identify any potentially affected endpoints.

Unusual Network Traffic

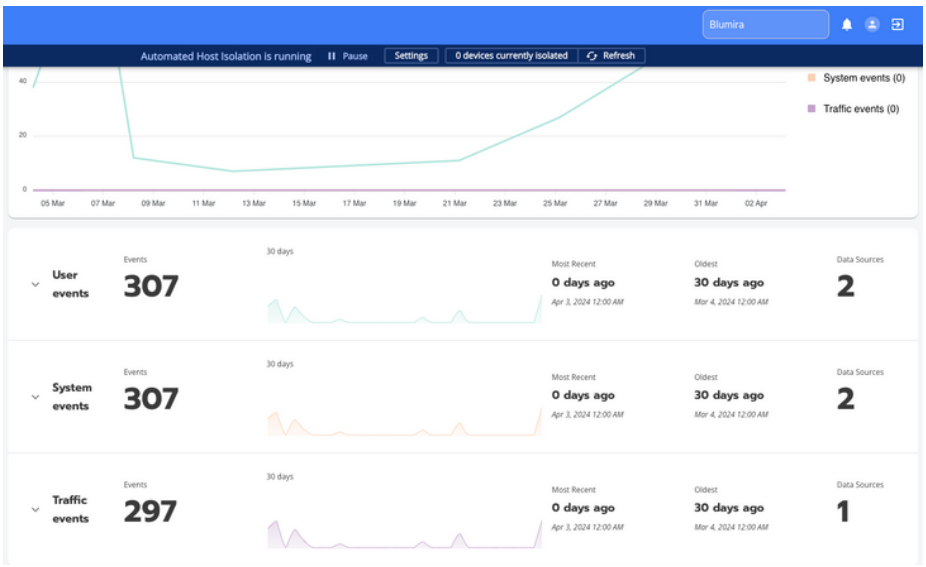
There was an unusual after-hours spike in network traffic to an external IP address over a certain port.

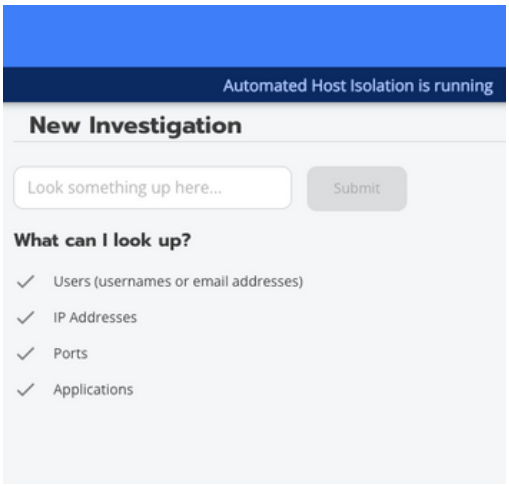
Searching by the port number allows your IT analyst to review and identify network traffic logs.

Blumira

How it Works

Take your first step toward discovering more about a security incident by searching your logs by an IP address (or user, endpoint, protocol, etc.) to see all related network traffic, users, devices and applications. Narrow down your search with quick filters to pinpoint only the data you need.





Blumira Investigate's dashboard provides visualizations of your data, including:

- All associated events over a period of time, and findings related to your search term
- **User events**: Data related to relevant users, user events, most recent events, data sources and more
- **Traffic events**: Data related to relevant network traffic, including network connections, most recent connections, data sources and more
- **System events**: Data related to relevant systems, including system events, most recent events, data sources and more

I had not wrapped my head around the actual benefits of a SIEM – it was almost more of a compliance checkbox. When we got it up and running, it hit me that **Blumira is providing us the visibility that we didn't have before**.

Craig Rhinehart
Chief Information Officer (CIO)

ROBINSON, GRIMES & COMPANY, P.C.
Certified Public Accountants Consultants
Committed to your success

SIEM + XDR TRIAL

Blumira's platform detects early signs of an attack and helps you respond faster to reduce its impact to your organization, preventing a data breach.

With our SIEM +XDR platform and 24/7 security operations team combined, you get 24/7 coverage – there's no need to hire full-time analysts to manage your security.

Visit blumira.com/trial