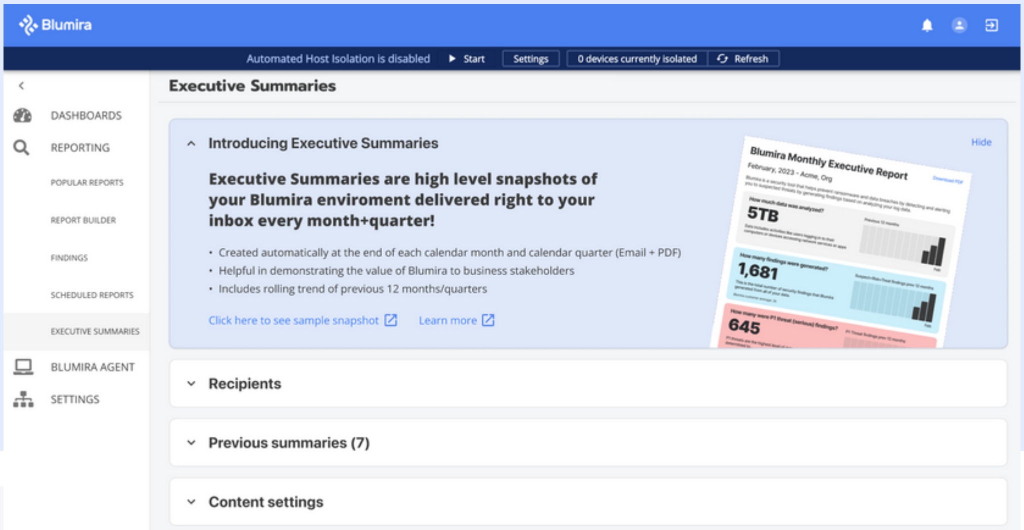
Blumira

Executive Summaries

Snapshots of your Blumira environment sent monthly or quarterly to your stakeholders

Immediately show security value to your C-level, key stakeholders, financial decision-makers and others.

The easy-to-understand, colorful reports give you a high-level overview of your Blumira environment:



Executive Summaries

Introducing Executive Summaries

Executive Summaries are high level snapshots of your Blumira enviroment delivered right to your inbox every month+quarter!

- Created automatically at the end of each calendar month and calendar quarter (Email + PDF)
- Helpful in demonstrating the value of Blumira to business stakeholders
- Includes rolling trend of previous 12 months/quarters

Click here to see sample snapshot   Learn more

Recipients

Previous summaries (7)

Content settings

Cost-Savings

How much money you're saving with Blumira's unlimited data & log storage (vs. thousands of dollars every month you would spend with other SIEM vendors with pay-as-you-go models)

Level of Risk

The level of risk in your environment, with a view of how many & what kinds of threats Blumira has identified in your environment by analyzing your log data

Typical SIEM pricing ($4k/month per 1024GB/1TB of logs) causes unpredictable costs and limited visibility. Blumira gives you affordable pricing with unlimited data for full coverage without tradeoffs.

Blumira's detection team creates detections, so you don't have to hire a team of security analysts to do that for you!

Security Trends

Trends over time, with a look back at your previous 12 months of data

Response Rates

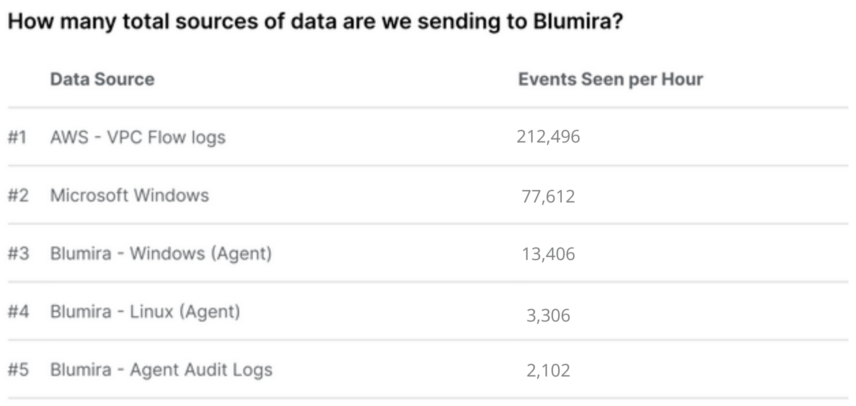
How many suspected threats were resolved, with the option to toggle it on and off for each report

Data Sources

Get an overview of the total sources of data you're sending to Blumira's platform for detection and response, with the number of events seen per hour. Adding more sources increases visibility into threats across your entire environment.

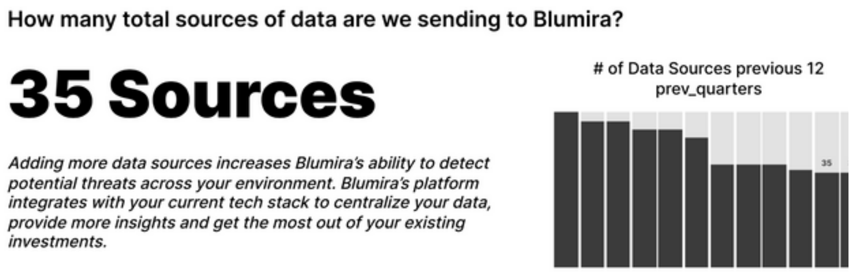
Business Impact

- *Gain holistic visibility*
- *Correlate data to detect threats earlier and faster*



How many total sources of data are we sending to Blumira?

	Data Source	Events Seen per Hour
#1	AWS - VPC Flow logs	212,496
#2	Microsoft Windows	77,612
#3	Blumira - Windows (Agent)	13,406
#4	Blumira - Linux (Agent)	3,306
#5	Blumira - Agent Audit Logs	2,102



How many total sources of data are we sending to Blumira?

35 Sources

Adding more data sources increases Blumira's ability to detect potential threats across your environment. Blumira's platform integrates with your current tech stack to centralize your data, provide more insights and get the most out of your existing investments.

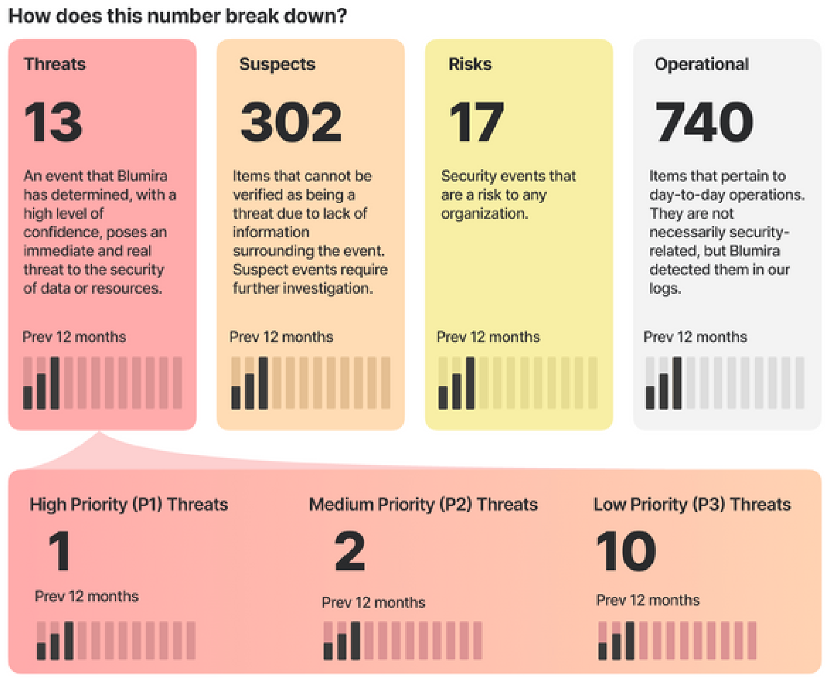
Prioritized Findings

See a breakdown of the types & priority of findings in your environment. Blumira's incident detection engineers build priority into your alerts so you know what's critical to respond to right away, saving your team time on triaging findings.

Business Impact

- *Save your team's time*
- *No need to hire additional security FTE*

By automatically prioritizing your threats, Blumira's security expertise saves time on triaging by focusing your attention on actual threats.



How does this number break down?

Threats

13

An event that Blumira has determined, with a high level of confidence, poses an immediate and real threat to the security of data or resources.

Prev 12 months

Suspects

302

Items that cannot be verified as being a threat due to lack of information surrounding the event. Suspect events require further investigation.

Prev 12 months

Risks

17

Security events that are a risk to any organization.

Prev 12 months

Operational

740

Items that pertain to day-to-day operations. They are not necessarily security-related, but Blumira detected them in our logs.

Prev 12 months

High Priority (P1) Threats

1

Prev 12 months

Medium Priority (P2) Threats

2

Prev 12 months

Low Priority (P3) Threats

10

Prev 12 months

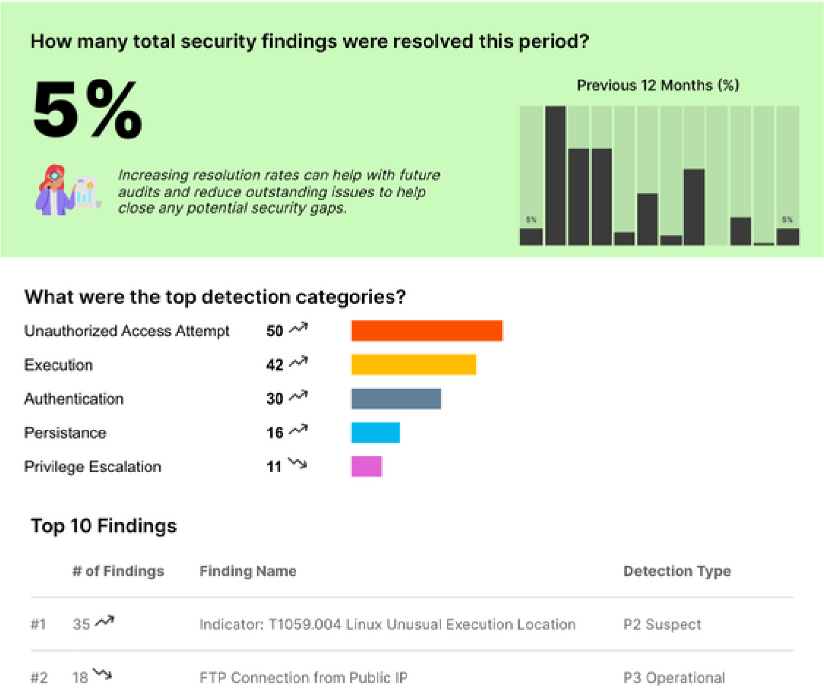
Blumira

Detection Trends

See what your top detection categories are and how they break down across your findings, including top suspected threats based on the number of findings generated.

Business Impact

- *Improve time to respond to close gaps*
- *Understand where you need to focus your security efforts*



How many total security findings were resolved this period?

5%

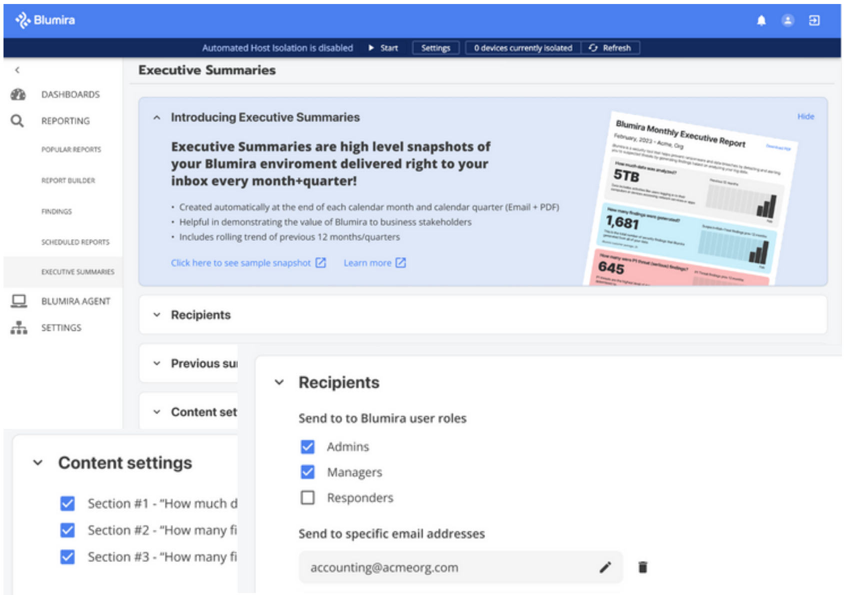
Increasing resolution rates can help with future audits and reduce outstanding issues to help close any potential security gaps.

What were the top detection categories?

Unauthorized Access Attempt	50 ↗	🟥
Execution	42 ↗	🟨
Authentication	30 ↗	▨
Persistance	16 ↗	🟦
Privilege Escalation	11 ↘	🟪

Top 10 Findings

	# of Findings	Finding Name	Detection Type
#1	35 ↗	Indicator: T1059.004 Linux Unusual Execution Location	P2 Suspect
#2	18 ↘	FTP Connection from Public IP	P3 Operational



Executive Summaries

Introducing Executive Summaries

Executive Summaries are high level snapshots of your Blumira enviroment delivered right to your inbox every month+quarter!

- Created automatically at the end of each calendar month and calendar quarter (Email + PDF)
- Helpful in demonstrating the value of Blumira to business stakeholders
- Includes rolling trend of previous 12 months/quarters

Click here to see sample snapshot   Learn more

Recipients

Previous su

Content set

Content settings

☑ Section #1 - "How much d

☑ Section #2 - "How many fi

☑ Section #3 - "How many fi

Recipients

Send to to Blumira user roles

☑ Admins

☑ Managers

☐ Responders

Send to specific email addresses

accounting@acmeorg.com

Auto-Generated

Access reports in the app under **Reporting** > **Executive Summaries.** From here, you can customize recipients, content, and see previous summaries. Summaries are automatically generated monthly and quarterly.

Business Impact

- *Saves time & effort to create reports*
- *Shows value to your stakeholders*

> 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)

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

SIEM + XDR TRIAL

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

Contact us to try Blumira's SIEM + XDR platform:

- SIEM deployment in minutes
- Managed detection rules
- Endpoint visibility and response
- Automated response

Visit blumira.com/trial