451 Research

S&P Global
Market Intelligence

What SIEM/Security Analytics Attributes Are Most Important to Enterprises?

Insight must lead to action

Security information and event management (SIEM) is often regarded as a foundational technology for security operations. But it has to be more than a platform for gathering and correlating a variety of security-relevant inputs.

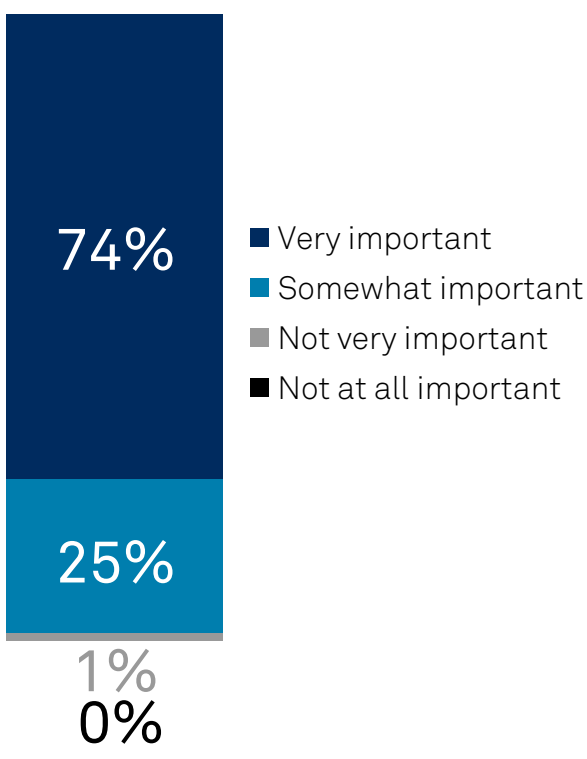
SIEM has to make this information **actionable** for security teams, prioritizing what's most significant and facilitating more effective response.

For this reason,

74%
of enterprises using SIEM give the quality of reporting and alerts **the highest importance** when selecting SIEM vendors.

100%
of those planning to deploy SIEM in the next **2 years** rate quality of reporting/alerts as very/somewhat important

Importance of Quality of Reports/Alerting When Selecting SIEM Vendor



Why is quality so important?

Security teams must cope with a **volume of events and alerts that can be overwhelming** – yet they can't afford to lose sight of the evidence that matters most.

Number of SIEM/security analytics alerts SecOps teams investigate on a typical day

▪ = 10 SIEM/security analytics alerts

▪▪ Nearly half (49%) investigate **20 or more alerts**

One-fourth (26%) investigate **100 or more alerts**

As many as 12.5% investigate **500 or more alerts**

That's the number of alerts SIEM-using organizations actually examine.

When asked what percentage of alerts they are unable to address on a typical day...

30%
of respondents said **they couldn't investigate more than half.**

38%
of all SIEM-using organizations have **no idea** how many alerts they investigate per day

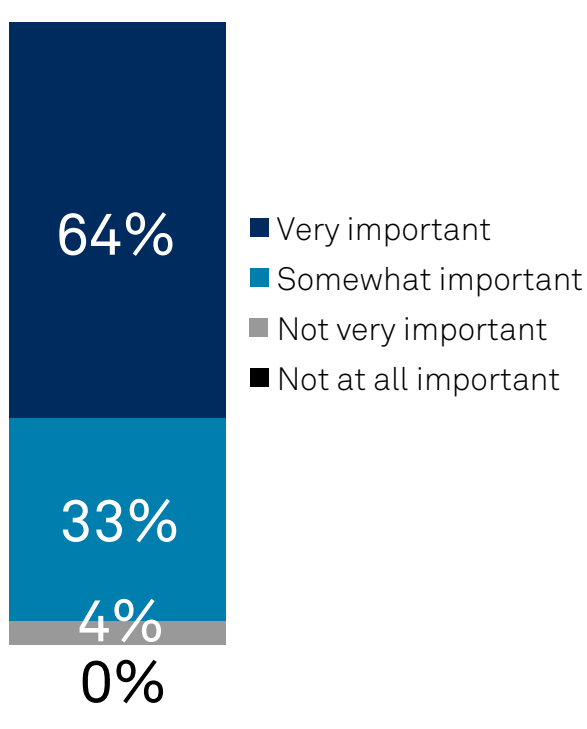
Triage and prioritization are vital – and threat intelligence is a key enabler

Threat intelligence is also highly rated among survey respondents.

The correlation of monitoring and event data to threats and adversarial behavior seen 'in the wild' helps security teams prioritize issues and escalate response when warranted:

64%
rate **integration and correlation of threat intelligence as very important** when selecting SIEM vendors

Importance of Integration and Correlation of Threat Intelligence When Selecting SIEM Vendor



When asked which SIEM/security analytics vendors they currently use, enterprises reported the following:

SIEM Vendors Currently in Use

(Top 10 Responses)

Primary SIEM Vendors for Those Using More Than One Provider

(Top 10 Responses)

Quality

Actionability

Making the most of available resources to make security operations more effective

These are among the characteristics of SIEM that yield high value in realizing the benefits of security analytics and information management

Sources: 451 Research's Voice of the Enterprise, Information Security: Vendor Evaluations 2021

splunk>

Advanced security analytics at scale

The content of this artifact is for educational purposes only. S&P Global Market Intelligence does not endorse any companies, technologies, products, services, or solutions. Permission to reprint or distribute any content from this artifact requires the prior written approval of S&P Global Market Intelligence.

©2021 S&P Global Market Intelligence | **WWW.451RESEARCH.COM**