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

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. 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...

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

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

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

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:


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

For this reason,
30% of respondents said they couldn’t investigate more than half.

Primary SIEM vendors for those using more than one provider (Top 10 Responses)

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

SIEM Vendors Currently in Use (Top 10 Responses)

Quality

Actionability

Advanced security analytics at scale

m4 Research

Market Intelligence

54% of respondents said they couldn’t investigate more than half.

64% of SIEM vendors give the quality of reporting alerts the highest importance...