Time to Redeem the SIEM?

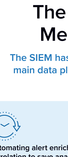
Security information and event management platforms have made significant strides since their debut about 20 years ago.

Michelle Abraham
Research Director,
Security and Trust, IDC

SIEM Challenges

Due to its complexity, the security information and event management (SIEM) is not an easy solution; it requires care and feeding.

34% of IDC survey respondents said their greatest SIEM challenge is the need for staff dedicated to the platform.



28% are challenged by the lack of automation.

According to IDC surveys, the median amount of data ingested into the SIEM grew from

1.7 TB in 2021

to **3.7 TB** in 2024.

Source: IDC's *Worldwide Views on SIEM Survey*, January 2024

The SIEM Evolution to Meet Today's Needs

The SIEM has advanced its capabilities to become the main data platform of the security operations center.

Key SIEM Advancements:

- Automating alert enrichment and correlation to save analysts' time
- Increasing connections to new data sources as companies report connecting a median of 85 data sources to the SIEM
- Shifting to SaaS so organizations no longer need to manage their SIEM infrastructure
- Ingesting only necessary data while routing other security telemetry to lower-cost storage

Source: IDC's *Worldwide Views on SIEM Survey*, January 2024

Generative AI Adds to The SIEM Capabilities

Generative AI (GenAI) enhances security analysts' knowledge and frees them for higher-value work by automating mundane tasks such as:

- Summarizing threat intelligence, alerts, and vulnerabilities
- Writing the after-action report
- Generating better queries to extract the desired information
- Providing guidance on the next steps

Hesitations About SIEM Migration

Leaving the old SIEM behind and moving to a new one isn't always an easy choice.

52% of IDC survey respondents report formally **reviewing the SIEM market annually** to evaluate their options.

76% **stayed with the same SIEM vendor after review** because they found upgrading their SIEM with the same vendor was the best option and/or their current vendor offered a good deal at renewal.

52 days is the mean time **between turning a new SIEM on and shutting down the old one** (therefore running them in parallel), but it can take much longer.

The median cost of professional services when switching SIEMs ranged from:

$93,750 **for smaller organizations** (fewer than 1,000 employees)

$1.175 million **for larger ones** (10,000+ employees)

in addition to the cost of running two platforms.

Source: IDC's *Worldwide Views on SIEM Survey*, January 2024

Guidance for Evaluating a Change of SIEM

Consider the following points before making the choice to migrate.

- **Think about the organization's needs for today and tomorrow.** Data sources and ingestion only seem to grow, so managing data is an ongoing process.
- **Evaluate the need for data retention and compliance reporting.**
- **Assess the potential of a GenAI assistant** to assist inexperienced analysts while ensuring compliance with the organization's AI governance policies.
- **Determine how a new SIEM will enable previous processes and workflows to change.** Do not carry over old ways of operating just because that is the way it has always been done.

Produced by: IDC Custom Solutions
IDC #US53577125
IDC Custom Solutions produced this publication. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC.com
idc
@idc

Message from the Sponsor

Google Cloud

The great SIEM migration has begun.

The SIEM market is undergoing tectonic shifts causing many security operations leaders to rethink their existing SecOps platforms. It's now a question of "when" and not "if" you should embark on a SIEM migration project.

Make Google part of your SecOps team