Market Forecast

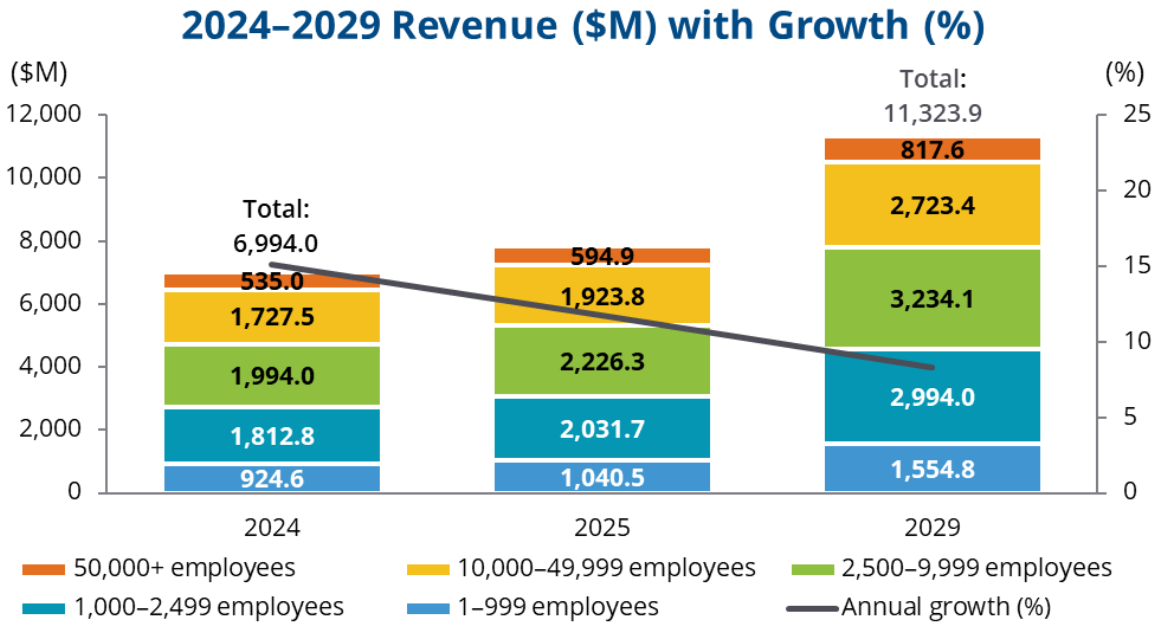
Worldwide Security Information and Event Management Forecast, 2025–2029: Continued Payment for One's SIEMs

Michelle Abraham

IDC MARKET FORECAST FIGURE

FIGURE 1

Worldwide Security Information and Event Management Revenue Snapshot



Selected Segment Growth Rate

- ▲ 1–999 employees CAGR 11.0%
- ▲ 1,000–2,499 employees CAGR 10.6%
- ▲ 2,500–9,999 employees CAGR 10.2%
- ▲ 10,000–49,999 employees CAGR 9.5%
- ▲ 50,000+ employees CAGR 8.9%

Total Market CAGR

10.1%

Note: Chart legend should be read from left to right, starting with the top row.

Source: IDC, January 2025

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from: “Worldwide Security Information and Event Management Forecast, 2025–2029: Continued Payment for One’s SIEMs” . (Doc #US51417524).

EXECUTIVE SUMMARY

The IDC Market Forecast for security information and event management (SIEM) from 2024 to 2029 highlights projected 10.1% CAGR growth, driven by increased demand in Asia/Pacific (AP) and EMEA regions. The NIS2 Directive in the European Union (EU), while not mandating SIEM, necessitates log analysis and system monitoring, indirectly boosting SIEM adoption.

The shift toward cloud-based SIEM solutions continues, with on-premises deployments expected to fall below 25% by 2029. Despite this, some customers will retain on-premises SIEMs due to their specific needs.

Key market drivers include increased automation and the integration of SOAR features, which aim to streamline alert triage and investigation processes. The growing volume of data ingested by SIEMs, priced on data ingest, also drives market growth. However, data pipeline management and the use of security data lakes are noted as inhibitors.

Dedicated SIEM staffing is the primary challenge for security teams using SIEM; therefore, vendors should provide customizable content to enhance usage. In addition, customers need help in automating processes to reduce alert fatigue. SIEM vendors are also advised to meet with customers regularly to help them understand new features and how they can be used to mature the customer’s SIEM workflows.

Significant vendor developments include the merger of Exabeam and LogRhythm, Palo Alto Networks’ acquisition of IBM QRadar SaaS, and SentinelOne’s launch of an AI SIEM. These changes underscore the dynamic nature of the SIEM market.

This IDC study provides a worldwide market forecast for the security information and event management market for the 2025-2029 period.

“Overall, the SIEM market is expected to grow more than previously forecast, driven by regulatory requirements and the need for comprehensive security monitoring and threat detection,” acknowledged Michelle Abraham, senior research director, Security and Trust at IDC. “Vendors should focus on enhancing the alert triage and investigation workflows of their SIEM platforms to capitalize on this growth.”

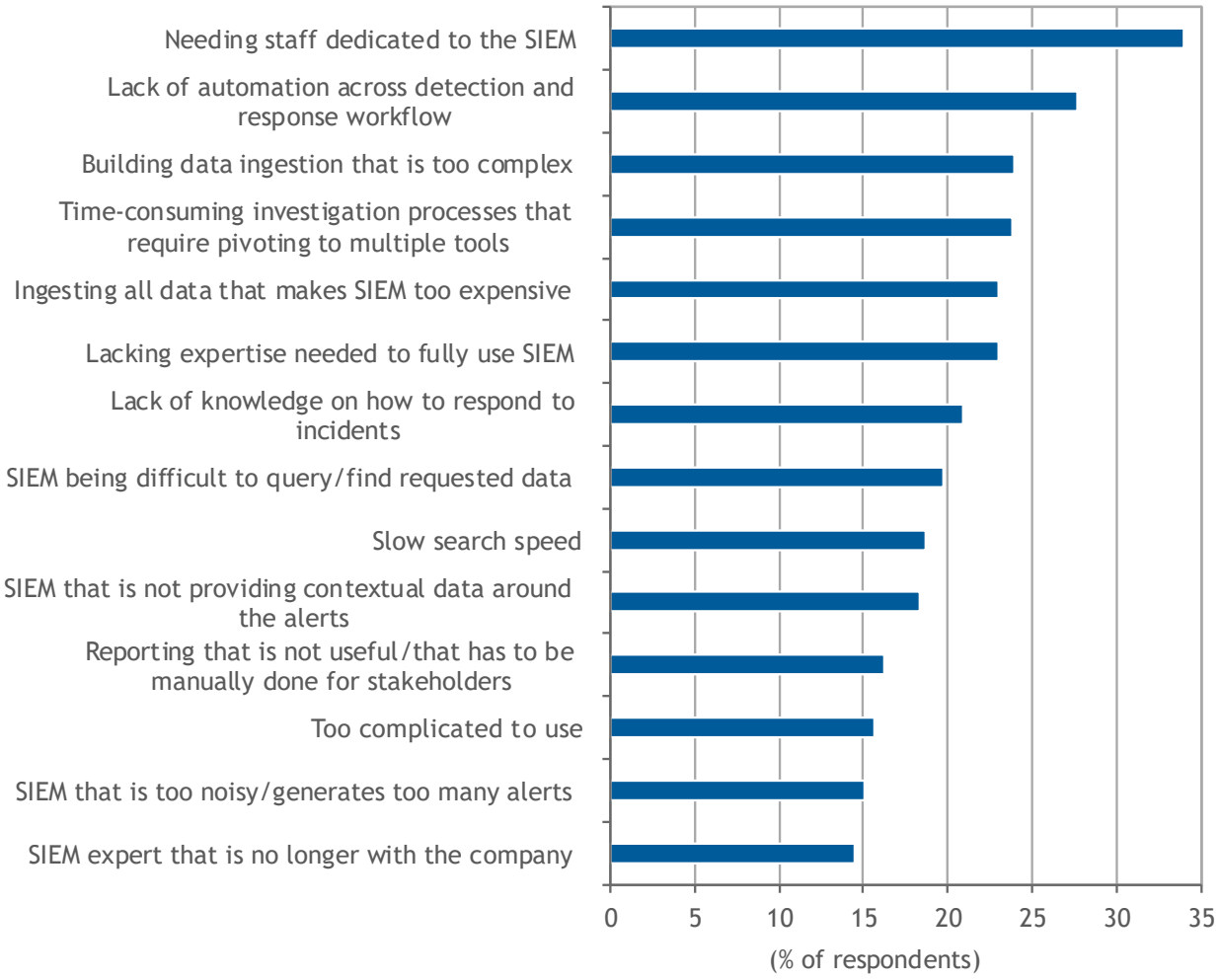
ADVICE FOR TECHNOLOGY SUPPLIERS

According to IDC's January 2024 *Worldwide Views on SIEM Survey,* the greatest challenge for security teams and their SIEM is the need for staff dedicated to the SIEM (see Figure 2).

FIGURE 2

Top Challenges in Security Information and Event Management

Q. What are the three greatest challenges to using the full capabilities of your SIEM platform?



n = 1,004

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

SIEM vendors should take note and ease their customers' path to using their SIEM to its fullest ability. In addition to helping customers get started, vendors need to help their customers mature in their use of the SIEM. This includes:

- **Providing content for customers: detections, connectors, threat hunts, playbooks, and so forth.** Customers cannot always use the content out of the box in their environment. But it often gets them part of the way there. It takes them less time to customize vendor-provided content than developing their own from scratch.
- **Holding regular sessions with customers to let them know of new features they may be able to use.** SIEMs are dynamic products; they must be to keep up with the ever-changing threat landscape.
- **Helping customers automate their processes and workflows with or without generative AI (GenAI) to reduce their alert fatigue and drudgery.**

MARKET FORECAST

IDC is forecasting SIEM revenue to grow by a 10.1% CAGR through 2029 on the expected growth in Asia/Pacific and EMEA markets. In the EU, the NIS2 Directive is being transposed into national legislation for the member states. For more, see *NIS 2 Comes into Force — What Is the State of Play in Europe?* (IDC #EUR151528024, December 2024). Although NIS2 does not require the use of a SIEM, organizations meeting NIS2 do need to analyze logs and monitor their systems, which is the work of the SIEM (see Table 1).

TABLE 1

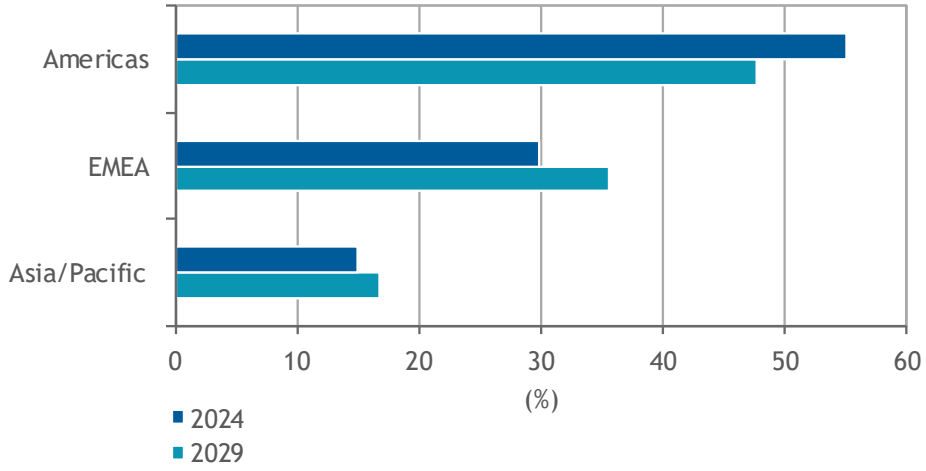
Worldwide Security Information and Event Management Revenue by Region, 2023–2029 ($M)

	2023	2025	2029	2024 Share (%)	2024–2029 CAGR (%)	2029 Share (%)
Americas	3,451.4	4,202.7	5,403.7	55.1	7.0	47.7
Asia/Pacific	925.4	1,175.3	1,891.4	15.0	12.5	16.7
EMEA	1,698.5	2,439.1	4,028.8	29.9	14.0	35.6
Total	6,075.3	7,817.2	11,323.9	100.0	10.1	100.0

The higher growth rate outside the Americas region is expected to result in a decline of the share of SIEM revenue from the Americas region and an increase in the share from other regions (see Figure 3).

FIGURE 3

Worldwide Security Information and Event Management Revenue Share by Region, 2024 and 2029



Source: IDC, January 2025

As we have seen for multiple prior years, the SIEM is moving to the cloud, which helps security teams move staff away from needing to manage SIEM infrastructure (see Table 2).

Table 2

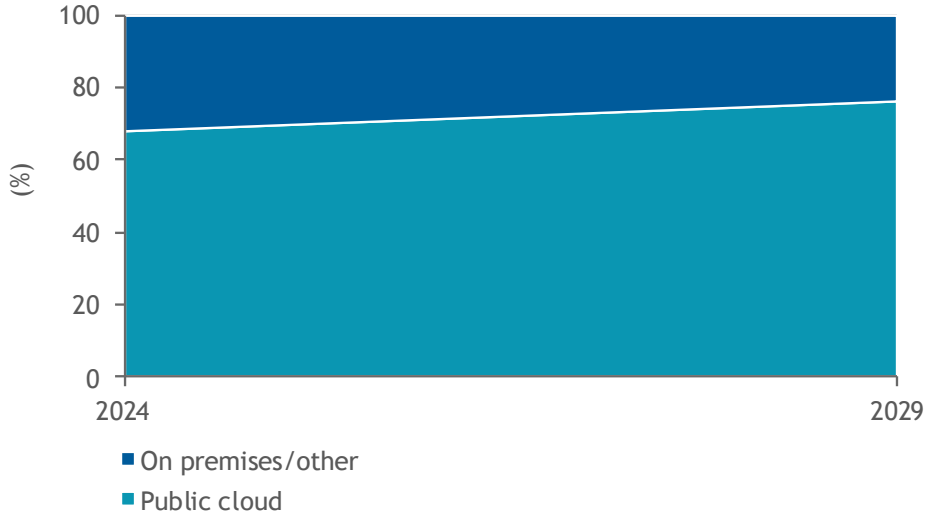
Worldwide Security Information and Event Management Revenue by Deployment Type, 2023–2029 ($M)

	2023	2025	2029	2024 Share (%)	2024–2029 CAGR (%)	2029 Share (%)
On premises/ other	2,251.3	2,265.4	2,731.9	31.9	4.1	24.1
Public cloud	3,823.9	5,551.8	8,592.0	68.1	12.5	75.9
Total	6,075.3	7,817.2	11,323.9	100.0	10.1	100.0

IDC believes while the share of on-premises SIEM will be below 25% in 2029, there will still be customers that keep their SIEM out of the public cloud (see Figure 4).

FIGURE 4

Worldwide Security Information and Event Management Revenue Share by Deployment Type, 2024 and 2029



Source: IDC, January 2025

Regions outside the United States have fewer very large enterprises with more than 10,000 employees. With expectations for higher growth in AP and EMEA, IDC anticipates that businesses with fewer than 10,000 employees will have higher CAGRs than those with more than 10,000 employees (see Table 3).

Table 3

Worldwide Security Information and Event Management Revenue by Size of Business, 2023–2029 ($M)

	2023	2025	2029	2024 Share (%)	2024–2029 CAGR (%)	2029 Share (%)
1–999 employees	802.7	1,040.5	1,554.8	13.2	11.0	13.7
1,000–2,499 employees	1,569.5	2,031.7	2,994.0	25.9	10.6	26.4
2,500–9,999 employees	1,731.8	2,226.3	3,234.1	28.5	10.2	28.6
10,000–49,999 employees	1,500.4	1,923.8	2,723.4	24.7	9.5	24.1
50,000+ employees	470.8	594.9	817.6	7.7	8.9	7.2
Total	6,075.3	7,817.2	11,323.9	100.0	10.1	100.0

MARKET CONTEXT

Drivers and Inhibitors

The drivers and inhibitors for SIEM have not changed much since our last forecast in 2023. The demand for security analytics solutions that sit on top of a third-party data lake did not have much impact on the SIEM market, yet some organizations do use data lakes for security data they do not want to ingest into their SIEM.

Drivers

More Automation

- **Assumption:** SOAR features are being combined into SIEM with more automation in the triage of an alert or investigation. SIEM vendors are also introducing generative AI assistants whose most common use cases are enabling natural language search, correlation of event data/logs, and summarizing information for reports.
- **Impact:** The goal is to help customers with 1 minute to detect and 10 minutes to investigate and the ability to respond within 1 hour. There is too much work for

the SOC team today, and the attack surface is growing. Automation is the only way through.

More Data to Ingest

- **Assumption:** There are more data sources being ingested and more data from those sources.
- **Impact:** SIEM is priced on ingest in many cases, so the more data brought in, the greater the amount spent on the SIEM.

Inhibitors

Data Pipeline Management

- **Assumption:** Most often, data pipelines are managed outside the SIEM. However, some SIEM vendors are incorporating the feature in their SIEM.
- **Impact:** To counteract the yearly increase in data and therefore the cost of the SIEM, greater use of data pipeline management makes it easier to send only the necessary data fields from logs to the SIEM, while others can be routed to less expensive storage.

Security Data Lakes

- **Assumption:** The use of the SIEM for log storage will potentially shift to data lakes. There are several vendors that offer security analytics on top of third-party data lakes today.
- **Impact:** Data lakes will be priced and sold separately, so SIEM pricing will no longer include data storage, reducing the amount a customer pays to its SIEM vendor.

Significant Market Developments

In mid-2024, several major changes occurred among the vendors that offer SIEM platforms. Exabeam and LogRhythm merged under the Exabeam name in July 2024. In September 2024, Palo Alto Networks finalized its acquisition of the IBM QRadar SaaS business. SentinelOne announced its AI SIEM in October 2024. Despite its maturity as a cybersecurity technology, the SIEM market remains dynamic with vendors exiting and new vendors entering.

Changes from Prior Forecast

Table 4 and Figure 5 provide a comparison of the prior-year forecast (see *Worldwide Security Information and Event Management Forecast, 2023–2027: In the Face of XDR, Many Organizations Are Still Living in SIEM,* IDC #US50271823, August 2023) with the current year's forecast for the SIEM software market.

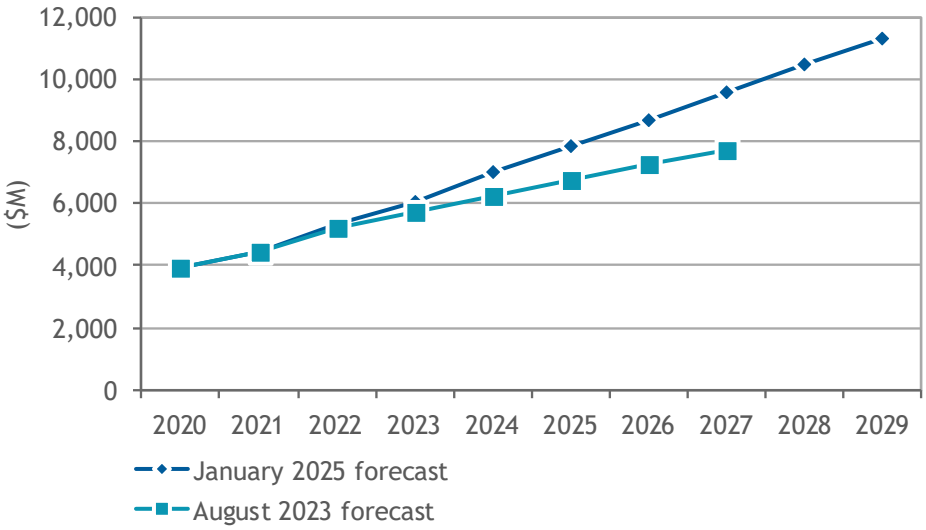
Table 4

Worldwide Security Information and Event Management Revenue, 2020–2029: Comparison of August 2023 and January 2025 Forecasts ($M)

	2020	2025	2029
January 2025 forecast	3,961.2	7,817.2	11,323.9
August 2023 forecast	3,953.0	6,771.2	NA

FIGURE 5

Worldwide Security Information and Event Management Revenue, 2020–2029: Comparison of August 2023 and January 2025 Forecasts



Note: 2024 data is estimated.

Source: IDC's Worldwide Semiannual Software Tracker, May 2023 and November 2024

Adjustments were made to several vendors' revenue for prior years changing the historical data. Higher growth rates in AP and EMEA have also improved the total revenue outlook.

MARKET DEFINITION

Security information and event management (SIEM) solutions are log-centric platforms used for policy and compliance assurance as well as to monitor the IT environment and initiate security investigations. SIEM solutions include products designed to aggregate data from multiple sources to identify patterns of events that might signify attacks, intrusions, misuse, or failure. Event correlation simplifies and speeds the monitoring of network events by consolidating alerts and error logs into a short, easy-to-understand package. Products can also consolidate and store the log data that was processed by the SIEM. This technology also includes products that collect and disseminate threat intelligence, provide early warning threat services, and provide information on countermeasures. The data from SIEM products may be provided to policy and compliance solutions for consistent reporting.

One of the criteria for a platform to be considered a SIEM is that it must drive like a SIEM. A SIEM must take in different logs and flows, offer dashboards specifically used for threat investigation, and be capable of compliance reporting. In this sense, SIEM is differentiated from security analytics products that are designed to allow users flexibility in specifying their particular security framework and running data against that framework to better analyze data. And SIEM is different from threat intelligence products that are designed to take in a variety of threat intelligence sources and provide a platform for organizations to analyze their own data against a variety of different threat intelligence feeds. Often, companies will use business intelligence (BI) platforms in combination with open source platforms to index data, but IDC does not count this as SIEM categorically. SIEM incorporates aspects of security and threat analytics, threat intelligence, business intelligence, and database management to provide search, storage, indexing and, most importantly, detections that facilitate incident detection and response.

METHODOLOGY

The SIEM forecast document contains revenue estimates that were derived in the same cycle as IDC's Worldwide Security Products Tracker.

In the tracker, IDC is tracking multiple markets. This means that the revenue generated for one SKU can only be realized once. (The revenue cannot be double counted in SIEM and policy and compliance, for instance.)

The IDC software market sizing and forecasts are presented in terms of commercial software revenue. IDC uses the term *commercial software* to distinguish commercially available software from custom software. Commercial software is programs or codesets of any type commercially available through sale, lease, rental, or as a service.

Commercial software revenue typically includes fees for initial and continued right-to-use commercial software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately. Upgrades may be included in the continuing right of use or may be priced separately. Commercial software must be available for competitive bidding. These use cases are counted by IDC as commercial software revenue.

Commercial software revenue excludes service revenue derived from training, consulting, and systems integration that is separate (or unbundled) from the right-to-use license but does include the implicit value of software included in a service that offers software functionality by a different pricing scheme. It is the total commercial software revenue that is further allocated to markets, geographic areas, and sometimes operating environments. For further details, see *IDC's Worldwide Security Products Taxonomy, 2024* (IDC #US51825024, February 2024).

As part of the cadence with this document and as intimated previously, IDC sent revenue estimates to companies in this study for review and a chance to comment. Under no circumstance will IDC disclose the degree of transparency a vendor provided for a specific revenue estimate. Many companies may offer a precise revenue estimate or guide an analyst to 10-K/10-Q or related statements. Other companies are privately held or do not comment; some still provide ballpark estimates. In addition, the security team works with the larger tracker group, and we reconcile revenue to add to a larger whole. Other tools at the disposal of the analyst are contracts won, press releases, and number of employees. Otherwise, it is unfair and unethical to compromise the confidentiality of the participating vendors.

The data presented in this study is IDC estimates only.

Note: All numbers in this document may not be exact due to rounding.

RELATED RESEARCH

- *Worldwide Security Information and Event Management Market Shares, 2023: The Leaders in SIEM City* (IDC #US52525024, September 2024)
- *IDC's Macroeconomic Forecast Assumptions, September 2024* (IDC #US52576624, September 2024)
- *Costs of Switching SIEM Platforms* (IDC #US52411524, July 2024)
- *Why Do Customers Keep or Replace Their SIEM?* (IDC #US52342924, June 2024)
- *Metamorphosis in the Multitude of SIEMs* (IDC #lcUS52283024, May 2024)
- *SIEM Users Rank Important Features* (IDC #US52074224, May 2024)

- *SIEM User Challenges in the Age of AI* (IDC #US50635424, April 2024)
- *Worldwide Security Information and Event Management Forecast, 2023–2027: In the Face of XDR, Many Organizations Are Still Living in SIEM* (IDC #US50271823, August 2023)

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com