451 Research
Pathfinder Paper

November 2024

Migrating legacy SIEMs to a cloud-native analytical platform

Commissioned by

paloalto NETWORKS | CORTEX

S&P Global
Market Intelligence

Executive summary

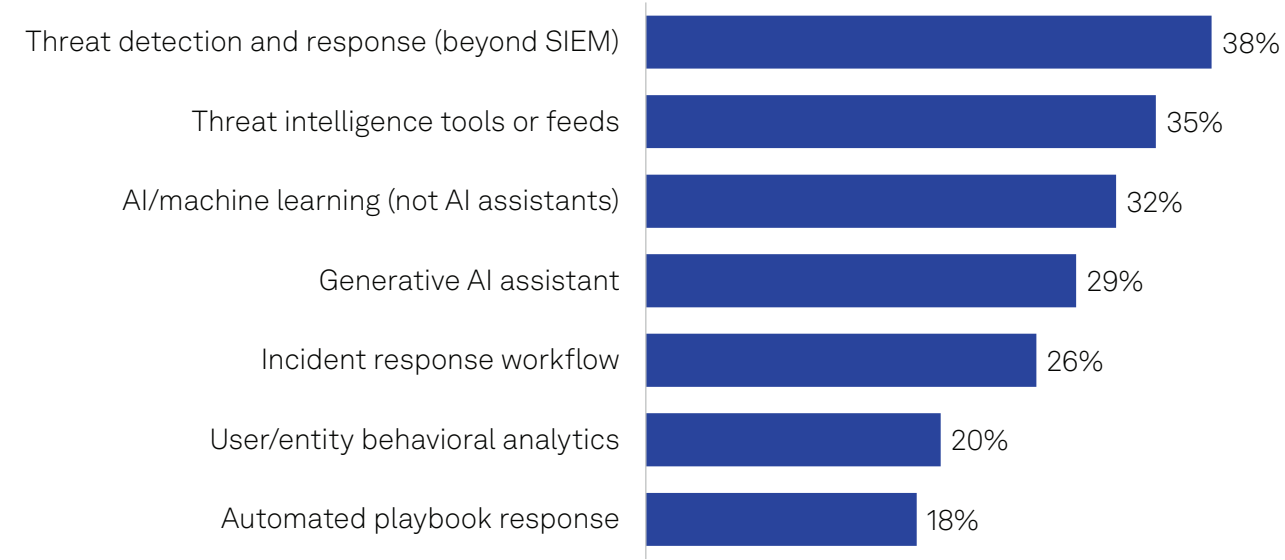
There is a sea change afoot in how organizations manage their cybersecurity, driven by the shift to cloud, accelerating adoption of AI workloads and rapid changes in the way enterprises develop and deploy critical applications. Meanwhile, most organizations have legacy on-premises applications and data that have not been or cannot be modernized. Examples include mainframes, operational technology devices and licensed applications that must be hosted in a traditional datacenter, or data and applications that must be hosted locally due to compliance or organizational policies and regulations. Hybrid cloud, which encompasses apps, data and microservices that may use multiple cloud service providers along with private cloud and on-premises architectures, presents additional challenges due to a wide variety of security platforms and technologies.

Unfortunately, many traditional analytics platforms — e.g., security information and event management systems (SIEMs) — designed in the early 2000s have not kept up with rapid cloud technological shifts that would require reengineering them to function as containerized cloud-native applications. Early solutions that attempted to backhaul cloud data to on-premises data stores were largely unsuccessful due to cost and latency factors. This resulted in a conundrum: continue running legacy SIEMs to support on-premises workloads in parallel with a cloud-native security solution for modernized applications or transform the security operations center (SOC) into a single cloud-based security platform that can support both worlds. With the increasing maturation, prevalence and affordability of cloud-native security platforms, the answer is increasingly the latter.

Key findings

- In a recent 451 Research end-user survey, 56% of organizations that are using or planning to use public cloud services say they will use multicloud and hybrid cloud together as their preferred cloud operating model. At the same time, respondents indicated that only about half (49%) of their third-party tools and services are designed to work with multicloud environments.
- More than four in five respondents (83%) say they are likely to leverage managed and professional services to support their cloud strategies.
- Nearly three-quarters (72%) of respondents say they have more than one SIEM, and 41% have more than two, with a survey-wide mean of 2.4. This is likely due to inheriting SIEMs via mergers and acquisitions or SIEMs that were bundled with other security technology licenses but are not used as the primary analytics platform.
- The top technology that organizations seek to layer on top of SIEM is threat detection and response (beyond SIEM), followed by threat intelligence feeds, AI/ML (excluding AI assistants), and GenAI assistants, indicating a continued desire to add advanced threat detection and AI into security analytics capabilities.
- The top information security pain points that respondents cite are cloud security (18%), AI/ML implementation (17%) and GenAI (14%), which indicates that organizations continue to struggle with securing cloud and AI environments.

Figure 1: Additional technologies often combined with SIEM/security analytics investments



Q. Security information and event management (SIEM) technology provides real-time analysis of security events or information gathered from logs generated by hardware and applications. Which of these additional technologies — if any — has your organization been able to combine with its security information and event management (SIEM)/security analytics investment? Please select all that apply.
Base: All respondents, abbreviated fielding (n=185).
Source: 451 Research's Voice of the Enterprise: Information Security, SecOps 2024.

The move to cloud-based cybersecurity platforms

> **"Specific to the workloads that I'm running, everything that we're doing is in the cloud … We were the first group to go to the cloud. But at the organization level, I see pretty much every team going to some cloud vendor of some sort … Probably like 70% of our infrastructure is in the cloud, maybe 30% of our applications are running on-prem now."**

IT/engineering manager/staff
Financial services, $10B+ revenue, 2,000-4,000 employees

Platform use over time

Early "platformization" attempts

IT operations and cybersecurity management platforms are hardly new: They date back to the 1990s when vendors bundled multiple capabilities into a "one size fits all" suite. However, they earned a negative reputation because the various components, some acquired from other companies, were often poorly integrated and required multiple user interfaces. They were generally not designed to integrate with third-party apps and data, engendering negative connotations due to perceived (or actual) attempts at vendor lock-in. Perhaps as a side effect, many security tools evolved either as stand-alone offerings with plenty of integration points, or as consolidators — think SIEM and security orchestration, automation and response (SOAR) — that succeeded based on their ability to integrate.

The move to cloud and rebirth of the platform

Fast-forward to the mid-2010s and early 2020s when cloud architectures began gaining market acceptance. So-called cloud-native environments, which began with the emergence of dominant cloud service providers (hyperscalers), are simpler to monitor and manage from the outset due to a set of well-designed APIs and integration points. This enabled cloud security vendors to capitalize on the opportunity, launching offerings that required little if any custom code and could leverage a wide variety of cost-effective storage options.

Today, the growth of cloud-native applications continues to accelerate, aided by newly developed business systems as well as modernization and digital transformation projects that endeavor to move formerly on-premises apps to the cloud. As a result, an increasing percentage of enterprise applications run in public and private clouds. By necessity, however, hybrid clouds will persist due to critical on-premises workloads that are not cloud-compatible.

Platformization has exhibited a significant resurgence, led by vendors providing a robust set of capabilities aided by a high degree of automation and integration. For example, security operations (SecOps) platforms for the detection, analysis and response side of cybersecurity, often referred to as cloud detection and response (CDR), enable organizations to centralize the collection, normalization, storage and correlation of security telemetry, using centralized data lakes, data fabrics or data platforms. This provides the ability to rapidly correlate data that may indicate threats, investigate and triage incidents, and initiate response and recovery processes. SIEM products have long been an anchor for these capabilities as they collect and store logs and other security data and perform anomaly and threat detection analyses. The need for these capabilities clearly still exists, whether the product is called SIEM or something else.

Additional developments in recent years include tools that can gather telemetry directly from sources such as endpoints — endpoint detection and response (EDR) — and networks — network detection and response (NDR) — that enable threat detection and response at the point of contact. These capabilities evolved into extended detection and response (XDR) platforms that incorporate security orchestration, automation and response capabilities. In some cases, these platforms disrupted incumbents such as SIEM providers, giving rise to new security market leaders. XDR and similar platforms such as secure access service edge (SASE) and cloud-native application protection platforms (CNAPP) also heralded an architectural shift from on-premises "racked and stacked" servers to hosted, cloud-native platforms. These combine the flexibility of cloud platforms with the ability to easily offer them as customer-managed (software as a service) or fully managed by managed security service providers.

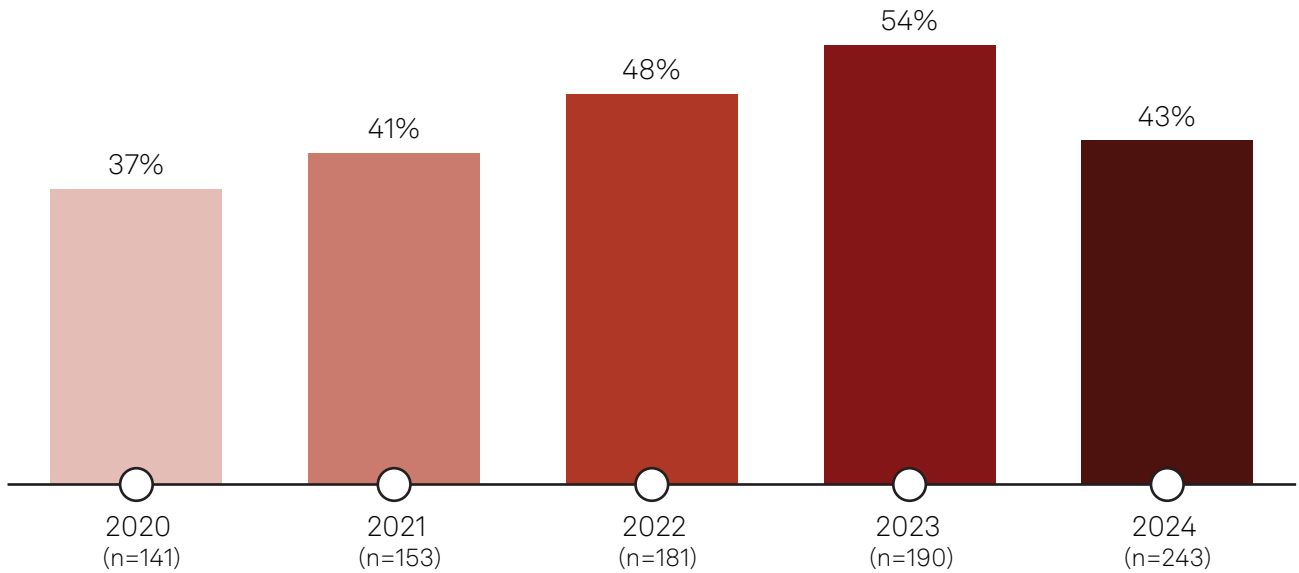
Key benefits of XDR, according to 451 Research respondents, include scaling SecOps capabilities (cited by 45%), providing higher-quality alerts (fewer false positives) and information for triage (44%), increased visibility (41%) and better response guidance for SecOps personnel (39%).

451 Research data also bears out the shift to platforms: 88% of respondents say they have a primary security vendor, and among those who do, an average of 36% of SecOps spending goes to the primary vendor (rising to 40% for organizations with more than 1,000 employees). We expect this trend to accelerate as the dominant platform vendors further develop of their offerings. Organizations often appear to seek an "anchor" technology as their core platform and then integrate existing third-party point solutions or replace them with tools from their primary vendor.

Another major development in cloud-native analytics platforms over the past few years is increasing emergence of AI, which is rapidly becoming a key competitive advantage. Most security analytics systems have used "classic" AI and machine learning (ML) for a decade or more for use cases such as user and entity behavioral analytics to establish typical behavior patterns and detect anomalous activities. More recently, generative AI (GenAI) has gained prominence in cybersecurity offerings, initially in the form of security "copilots" or "assistants" aimed at improving analyst productivity and up-leveling analyst skills. They are now showing promise in additional security use cases such as analyzing scripts and executables; detecting deep fakes; analyzing unstructured data such as video, audio and text, regardless of the source language; and hyperautomation.

451 Research Voice of the Enterprise data suggests positive results from the evolution of security operations technologies. Since 2020, we have asked survey respondents to indicate the percentage of security alerts they are unable to investigate in a typical day. In 2020, respondents on average indicated they were unable to address 37% of alerts, and that figure rose by an average of 6 percentage points per year to a peak of 54% in 2023. In 2024, the figure dropped 11 points to 43%, likely due in part to the influence of modernized SecOps platforms. We expect the figure to continue to gradually decrease as the advantages derived from investments in platformization and GenAI continue to pay dividends.

Figure 2: Percentage of alerts SecOps teams were unable to investigate in a typical day, 2020-2024



Q. What percentage of SIEM/security analytics alerts are you unable to investigate in a typical day?
Base: Respondents currently using SIEM security.
Source: 451 Research's Voice of the Enterprise: Information Security Vendor Evaluations 2020.
Base: Respondents currently using SIEM security, abbreviated fielding.
Source: 451 Research's Voice of the Enterprise: Information Security Vendor Evaluations 2021.
Base: Respondents who currently have SIEM/security analytics in use or pilot/proof of concept.
Source: 451 Research's Voice of the Enterprise: Information Security, Security Operations 2022.
Base: Respondents currently using SIEM/security analytics, abbreviated fielding.
Source: 451 Research's Voice of the Enterprise: Information Security, Security Analytics & SecOps 2023.
Base: Respondents currently using SIEM/security analytics, abbreviated fielding.
Source: 451 Research's Voice of the Enterprise: Information Security, SecOps 2024.

Factors to consider prior to cloud-native SOC transformation

Organizations evaluating SOC transformation from a classic on-premises or SaaS-based first-generation SIEM will need to consider several factors.

Vendor selection

Organizations will be well served to choose a vendor that is deeply invested in cloud-native security solutions with a portfolio of offerings that match the organization's current and expected use cases. Prospective vendors should offer a tightly integrated set of "born in the cloud" cloud detection and response capabilities backed by a data lake (and, optionally, a data fabric), EDR, NDR and SOAR capabilities, plus a fully integrated set of CNAPP capabilities. Organizations will likely want to look for vendors with heavy investments in AI-based detection and automations that have demonstrated positive results in terms of increased analyst productivity, decreased incident dwell time and faster response and remediation times. Availability of a wide range of purpose-built AI models and detection mechanisms is desirable, particularly for GenAI offerings. It is also important to evaluate the vendor's best practices for securing its AI systems.

Platform support

Given that most organizations are now multicloud and hybrid cloud, it is key that the vendor support the organization's architectures including telemetry sources (on-premises and cloud), major cloud service provider/hyperscaler platforms (e.g., AWS, Azure, Google Cloud and Oracle) plus private cloud and SaaS applications. It may also be beneficial to look for vendors that offer a robust marketplace with applications and code repositories supplied by the vendor and third parties, as well as vendor certification of marketplace offerings. Organizations should also consider migration capabilities from first-generation SIEMs: Does the vendor require extensive rewriting of rules and recreation of dashboards and reports, or is the platform capable of automating much of this process through a use case-based migration strategy?

Buying solutions, not acronyms

Organizations would be wise to resist "buying by acronym" — a strategic approach would be to document key security use cases and map those to vendor solutions, rather than assuming an "acronymized suite" will cover all necessary use cases. This is particularly critical for organizations looking to migrate an existing set of security capabilities.

While the general buying trend is toward security platforms, the hallmark of a good platform is one that not only works well with its own offerings but also integrates with third-party tools. Buyers may want to ask prospective vendors for a list of "out of the box" third-party integrations and speak with reference customers that have deployed them. Vendors should understand that buyers are typically not going to "rip and replace" the entire stack of security solutions, and their platform should be capable of supporting existing investments in third-party products. That said, while there may be a desire to preserve certain sunk costs, another advantage of SOC transformation is the ability to swap out older tangential technologies for newer ones. Technologies such as EDR, NDR, SOAR and attack surface management provided by the platform vendor or technology partners are designed to work with the main platform due to tight integration, and this can be particularly palatable if the vendor makes it cost-effective to migrate.

Planning and executing SOC transformation

Migrating from a legacy SIEM can be complex, particularly in larger organizations — even if the SIEM is cloud-based or running as a SaaS offering. Organizations may start by evaluating and documenting key security use cases (e.g., detections, dashboards, reports, compliance requirements and response playbooks), prioritizing those with the highest business value. The following steps provide an outline of project phases.

Assessment

The first phase of SOC transformation involves assessing the capabilities and scope of the existing SIEM and XDR deployment. This should also include a thorough gap analysis to identify weaknesses in the existing deployment, which can be translated into key use cases to be deployed during the planning and implementation phases. The organization should also document current workflows and use cases, and an inventory of current data sources and integration points will provide a sense of the project's scope.

Planning

After assessment, planning can begin. This includes defining transformation objectives, identifying stakeholders and the implementation team, and developing migration timelines. This is also the time to differentiate critical and non-critical use cases and data sources to be migrated to the new platform — distinctions that will mark key milestones during implementation. This phase may also include documenting key workflows, as well as orchestration playbooks if a SOAR platform is in use.

Preparation

With a plan in place (or in progress), vendor evaluation can begin. This step follows the organization's typical evaluation process, such as issuing requests for information/proposals, scheduling demonstrations and engaging with vendors to conduct proofs of concept and trial periods. Once a vendor is chosen, key personnel will need training on the new platform. The organization may enlist the help of the vendor's professional services or a certified partner to aid in the migration. Another key task is to map data sources and repositories from the legacy SIEM to the new platform. In some cases, it may be easier to retain data in the original platform for compliance and forensic reasons until data retention periods elapse rather than attempting to migrate petabytes of data to the cloud, which may be cost-prohibitive. Taking a use case-based approach may be easier than attempting to migrate hundreds or thousands of rules and searches, particularly since many modern platforms are not rule-based.

Implementation

Once a vendor is selected and the team prepared, implementation can begin. It is logical to start with the highest-priority, highest-value use cases and data sources. The legacy platform remains the system of record until cutover, so it will likely be necessary to send data to two platforms simultaneously during this period. Tools that provide data pipelining or a security data fabric may be helpful in these situations. In addition to initial platform deployment, it will be necessary to configure the environment, including provisioning of users and access levels. Organizations may want to use advanced authentication, role-based access and zero-trust methodologies where possible. This phase may also involve integrating existing security tools, automation workflows and response playbooks.

Data migration

Data migration can be difficult due to several factors including the complexity of transforming and moving existing data and the costs involved in doing so. Again, it may be more cost-effective to maintain the existing system for some time, moving only critical data to the new platform. Developing a data migration strategy will involve examining the existing data stores with an eye toward data quantities and locations, the formats of the legacy and target systems, and options for migrating. Data in a standard format, such as open cybersecurity schema framework, is easier to migrate than data in a proprietary format. Standardized data can also be more easily left in place and accessed with a federation technology such as a data fabric. Once critical data is identified, it is time to do a cost analysis, including assessment of data ingress costs imposed by the vendor or cloud service provider, impacts on bandwidth, the time and effort required for conversion, and the process required to validate data integrity after migration.

Testing and validation

This phase requires development and execution of all deployed components to ensure that use cases are being met, required data is being ingested and analyzed, and alerts and incident response processes are working. This will likely require running both the legacy and new systems in parallel, comparing them side-by-side and correcting any detected issues. This step will also identify gaps in implementation and data migration that must be corrected.

Optimization

Since most modern security platforms use AI and ML extensively, it is necessary to do some fine-tuning. In some cases, time on task fine-tunes the models because the longer they are allowed to run against data, the better they become. This is also the time to customize dashboards and reports to ensure that key stakeholder and compliance reporting requirements are met. Refining of automation rules and playbooks typically occurs at this stage as well.

Training and adoption

Even if the organization plans to use a managed service provider, it is important to fully train internal staff on the new platform. If the vendor offers certification, the organization may consider putting staff through this process. Because this is the final step prior before cutover, this is also the time to review use cases and standard operational processes that support the new platform, such as backup and recovery, disaster recovery and high availability options. It is also advisable to implement staff-feedback mechanisms so that issues are documented and quickly rectified.

Cutover

A phased cutover is conducted from the legacy SIEM to the new platform. The organization should create and test a detailed fallback plan prior to cutover, and it is critical to monitor system performance as the new system is brought online. This is also a good time to rehearse backup and recovery processes, testing to ensure that they work as planned.

Post-implementation review

After implementation, a thorough review of the new system allows for gathering metrics on improved efficiencies and capabilities. Key performance indicators may include the total number of incidents generated by the new system and the time required for analysts to investigate and implement a remediation plan. This step can also involve evaluating the new platform's supported capabilities and use cases with an eye toward expanding its footprint and potentially disintermediating redundant or inefficient systems that could be replaced by modernized equivalents.

Decommissioning

As mentioned previously, the legacy SIEM may need to run in parallel for some time after the new platform is implemented. After this period has elapsed, the last step is to decommission the old system. The organization must ensure that all critical data and use cases have been migrated, and work with SOC analysts to be certain that they no longer require the old system. If necessary, the organization may plan to archive data and then officially decommission the system.

Ongoing management

If done properly, ongoing "care and feeding" of the new system should be considerably less intensive than what was needed for the legacy SIEM, particularly since new platforms tend to be offered as a service, requiring little or no maintenance and code upgrades from the enterprise team. It is helpful to ensure that team members participate in continual training on new capabilities and look for new ways that the platform can benefit the business.

Looking ahead

AI shows great potential to provide substantial value to organizations dealing with increasingly sophisticated threats and cyber skills shortages. Combining classic AI/ML detection technologies with GenAI could reduce stress on security analysts by automating routine tasks and providing rapid access to data required to quickly analyze and respond to threats. We expect to see an increase in automated responses, starting with basic automations such as forcing password resets or isolating low-risk machines from the network when a potential issue occurs. As organizations become more comfortable with these automations, we expect them to start using more advanced, multi-step "hyperautomations." We do not expect a fully automated SOC will become a reality — at least not in the next five years. However, a short-term result may be happier security personnel who can focus on more interesting, proactive tasks — and make it home for dinner every evening.

About the author

Mark Ehr

Principal Research Analyst, Information Security

Mark Ehr is a principal research analyst on the 451 Research information security research team within S&P Global Market Intelligence. He focuses on cybersecurity with an emphasis on cloud security, security operations and AI/ML. Mark has more than 20 years of cybersecurity experience plus a decade in software development and many years in computer networking.

In his time at S&P Global, Mark has delivered go-to-market projects and contributed to 451 Research in areas such as SIEM, secure access service edge (SASE), network security, private key infrastructures (PKIs), AI, continuous security validation and threat modeling.

Before joining S&P Global in 2022, Mark spent 12.5 years at IBM, including three years in BigFix endpoint management product marketing, four years as a QRadar SIEM product manager, and six years leading security sales enablement across IBM's $1 billion threat management product family. He also spent four years as an industry analyst at Enterprise Management Associates.

Mark holds a bachelor's degree in computer science from Metropolitan State University of Denver with an emphasis on electronics engineering technology and is an ISC² Certified Information Systems Security Professional (CISSP). He also jokes that he holds an "MBA from the school of entrepreneurial hard knocks," gained in his five years as an equity partner in a Boulder, Colorado-based software firm.

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About S&P Global Market Intelligence

At S&P Global Market Intelligence, we understand the importance of accurate, deep and insightful information. Our team of experts delivers unrivaled insights and leading data and technology solutions, partnering with customers to expand their perspective, operate with confidence, and make decisions with conviction.

S&P Global Market Intelligence is a division of S&P Global (NYSE: SPGI). S&P Global is the world's foremost provider of credit ratings, benchmarks, analytics and workflow solutions in the global capital, commodity and automotive markets. With every one of our offerings, we help many of the world's leading organizations navigate the economic landscape so they can plan for tomorrow, today. For more information, visit www.spglobal.com/marketintelligence.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html