The great SIEM migration: The AI era is here

White paper
April 2026

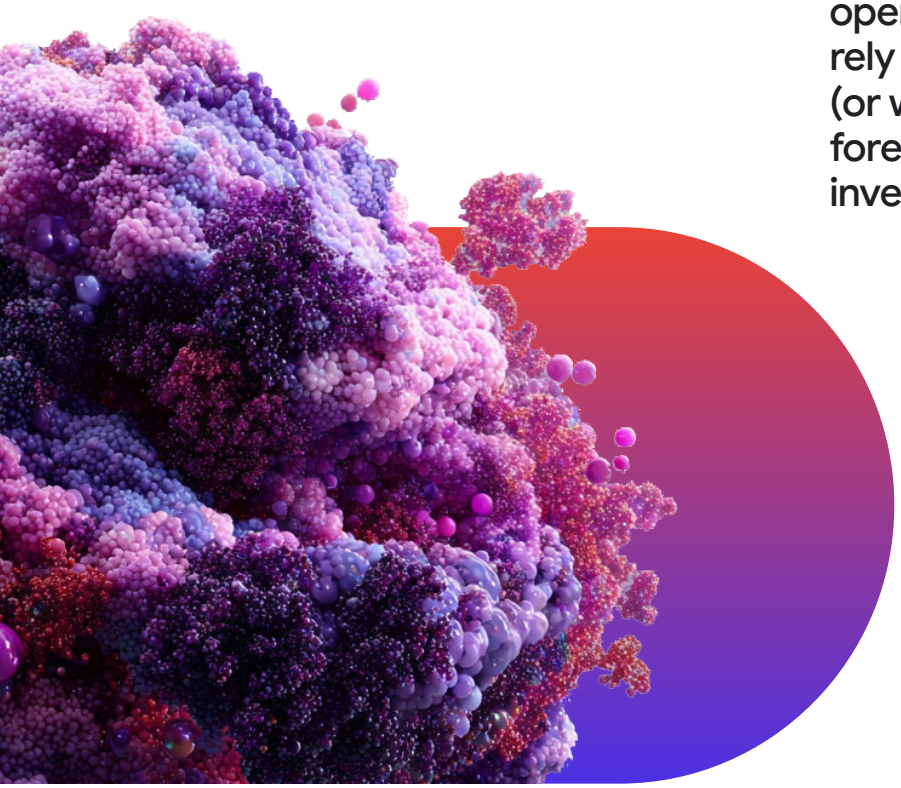
Table of contents

SIEM is dead, long live AI SIEM?

If you are like us, you may be surprised that, in 2026, security information and event management (SIEM) systems are still the backbone of most security operations centers (SOC). SIEMs have always been used for collecting and analyzing security data from across your organization to help you identify, investigate, and respond to threats quickly and effectively. But the reality is that today's modern SIEMs have little resemblance to those built 20+ years ago, before the rise of cloud-native architecture, user entity and behavior analysis (UEBA), security orchestration, automation and response (SOAR), attack surface management, and now generative artificial intelligence (AI) and AI agents.

SIEMs, conceived in the 1990s and 2000s, are often slow, cumbersome, and difficult to use. Their legacy architecture often prevents them from scaling to ingest high volume log sources, and they may be unable to keep up with the latest threats or support the latest analysis capabilities. They may not offer the flexibility to support your organization's specific requirements or be suited to the multi-cloud strategy that is the reality for most organizations today. Finally, they are not architected to take advantage of AI and AI agents.

So while a SIEM by any other name may sound just as sweet, security operations teams will continue to rely on 'security operations platforms' (or whatever name they go by) in the foreseeable future for threat detection, investigation, and response.



The great SIEM migration continues

SIEM migration is not new. Organizations have fallen out of love with their existing SIEM and sought newer and better options for years, and in fact decades. Perhaps more often, organizations have put up with their under-performing and/or overly expensive SIEM for longer than they would have liked, in part due to concerns over the complexity of having to deal with SIEM migration. The industry is full of stories about how a migration from one on-premises SIEM to a different one took 12–18 months in the past.

But recent months have introduced tectonic shifts in the SIEM space that cannot be understated. There is little doubt that the SIEM landscape is being transformed – giving birth to new market leaders and seeing the decline, and perhaps even the demise, of tools that ruled SIEM-land for decades. These developments will undoubtedly accelerate migration from legacy SIEM platforms to modern ones, with many organizations now facing a reality of *when* they should migrate instead of *if* they should migrate.

Identifying shortcomings in your current SIEM is much easier than selecting the best replacement and executing a successful migration. It's also important to note that SIEM deployment failures can also stem from processes (and occasionally people) and not just technology. We have seen hundreds of SIEM migrations as practitioners, analysts, and vendors over multiple decades.

Often, this ‘SIEM change’ forces leaders to choose one of three distinct paradigms:

01.

Just SIEM replacement

The occasionally ineffective attempt to seamlessly port all existing log sources, rules, and playbooks. This approach often fails because it ensures that years of operational inefficiencies and technical debt are inadvertently copied into the new, modern environment. It also does not account for new product advantages and capabilities and forces a superior modern product into a hole left by a broken legacy tool.

02.

‘Migration and transformation’

Replacing the technology while incrementally trying to modernize. This middle ground is often hampered by the desire to maintain backward compatibility, preventing the SOC from fully leveraging the new platform's cloud-native capabilities. This involves hard work, but delivers benefits in improved detection and response for years to come.

03.

‘Start anew’
(The scorched earth paradigm)

The most radical approach, which dictates throwing out all stale content and rebuilding detection logic and processes from a blank sheet. This philosophy is now viable because generative AI rules can act as a migration co-pilot, automating 70–80% of the manual rule-translation and recreation toil and neutralizing the primary historical argument against starting afresh.

Identifying the shortcomings in your current SIEM is easy; executing a successful structural transformation is the challenge.

This paper is designed to serve as a definitive guide for this journey, dissecting the execution phase and delineating the modern imperatives – from leveraging Telemetry Pipelines to adopting AI agents and Detection-as-Code – required to re-platform your SOC for the AI era.

Selecting a new SIEM

Start by asking yourself and your team some key questions to help uncover each offering's strengths and weaknesses. We recommend quickly identifying each SIEM's 'superpowers' and planning how your organization can take advantage of them.

Cloud-native SIEM

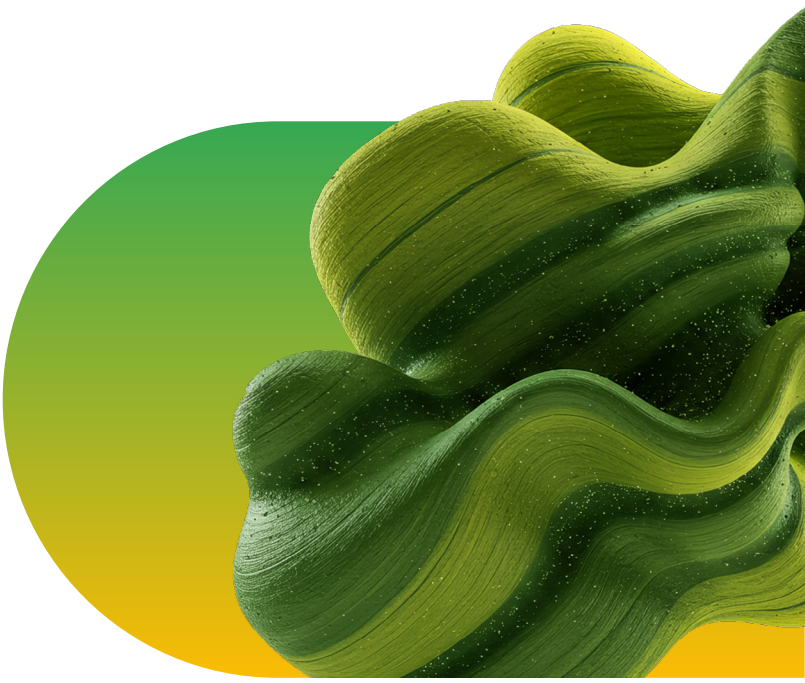
Is the SIEM offered by a primary cloud service provider (CSP) that can provide world-scale infrastructure at wholesale prices?

Our experience shows that SIEM providers who operate in clouds that they don't own have difficulty overcoming the inescapable 'margin stacking' that comes with such models. This question is inextricably linked to cost.

A cloud-native SIEM deployment model also allows the SIEM to scale up and down in response to new threats and also manage the dynamic nature of an organization's cloud workloads. Cloud infrastructure and applications can grow dramatically in minutes. A cloud-native SIEM architecture allows the security teams' critical tooling to scale at the same rate along with the needs of the larger organization.

Cloud-native SIEMs are also well-positioned to secure cloud workloads. They provide low-latency data ingestion from cloud services and ship with detection content to help identify attacks common in the cloud.

Beyond basic cloud scaling, modern architectures are increasingly moving toward decoupled telemetry pipelines. By utilizing vendor-agnostic platforms such as Cribl or Bindplane, organizations can aggressively filter, enrich, and route data before it reaches the high-cost analytics engine. This architectural shift prevents vendor lock-in and uncontrollable volume-based costs by pushing the heavy computational lifting of enrichment and parsing to the pipeline edge, ensuring only high-value telemetry is indexed for real-time correlation.



Telemetry platform support

Is the SIEM architected to function seamlessly with telemetry pipelines (for example, utilizing vendor-agnostic platforms such as Bindplane)?

Treating SIEM migration – including data inputs – as a pure 'lift and shift' is limiting because it often perpetuates technical debt. A decoupled pipeline aggressively filters, enriches, and routes data before it hits the high-cost analytics engine, which is a 2026 imperative to prevent vendor lock-in and uncontrollable volume-based costs.

A modern, necessary architectural countermeasure to being 'stuck with old data sources' is the deployment of a telemetry pipeline – which is quickly becoming the foundational cornerstone of any competent SIEM migration strategy. This pipeline sits strategically between all data sources and the ultimate analytics engines, providing a vendor-agnostic layer that aggressively filters out noise, enriches data in transit with threat intelligence, and routes different data streams based on their analytical value.

This pushes the heavy computational lifting of enrichment and parsing to the pipeline edge, ensuring only high-value, fully parsed, and enriched telemetry is indexed for real-time correlation. Massive volumes of low-value, raw logs can simultaneously be routed to drastically cheaper, specialized backend storage systems, such as cloud data lakes, instead of burdening the high-cost SIEM index.

SIEM with its own intelligence

Does the SIEM vendor have a continuous stream of frontline threat intelligence to drive out-of-the-box detection of new and emerging threats?

These golden sources typically arise from top-tier incident response (IR) practices, the operation of massive consumer IaaS or SaaS cloud offerings, or global installation bases of security software products or operating systems.

Threat intelligence is critical for organizations to effectively detect, triage, investigate, and respond to security incidents.

Frontline threat intelligence, in particular, is valuable because it provides real-time information about the latest threats and vulnerabilities. This information can be used to quickly identify and prioritize security incidents, and to develop and implement effective response strategies.

SIEM that is made with its own native (not merely increased) intel has powerful advantages:

- → **Seamless operational efficiency and efficacy:** Eliminates 'swivel chair, copy-paste' methods and brittle integrations, improving analyst experience.
- → **Superior detection fidelity and real-time context:** Native integration drives real-time detection rules, enriches alerts with context, and automatically adjusts alert confidence.
- → **Unparalleled golden source coverage:** The intelligence comes from 'golden sources' (top-tier IR, massive cloud offerings) providing a continuous, frontline stream of information that third-party TIPs cannot match.

To improve real-time threat detection and response capabilities, security organizations are seeking seamless integration of threat intelligence and associated data feeds into their security operations workflows and tooling. Swivel chair, copy-paste, and brittle integrations between SIEM and threat intel sources are productivity drains and they have a negative impact on the team's efficacy and on analyst experience.

SIEM with curated content that works

Does the SIEM offer an extensive library of supported parsers and detection rules, and response actions?

Some SIEM vendors rely almost exclusively on their user community or technical alliance partners to create parsers for popular data feeds. While a thriving user community is essential, over-reliance on it to provide fundamental capabilities, such as parsing, is a problem. Parsers for common data sources should be created, maintained, and supported directly by the SIEM vendor. Take the same approach when looking at detection rule content. Community rules are essential, but you should expect your vendor to create and maintain a solid library of core detections that are tested, supported, and improved regularly.

Trust and auditability
Transparent logic allows security engineers to audit, debug, and fully trust the detection content against their unique environment and 'red team' simulations. Opaque 'black box' rules prevent effective scrutiny, forcing analysts to treat the system as an untrustworthy source of truth.

Precision tuning and efficacy
User modifiability is essential for high-fidelity detection. All generic, out-of-the-box rules require tuning for an organization's specific baseline, network structure, and risk profile to prevent alert fatigue. Without this capability, teams are forced to write duplicative custom rules externally, creating detection debt.

Vendor-backed reliability
Curated and supported content ensures continuous maintenance and reliability. Relying solely on community-provided content is risky because community rules and parsers often lack performance guarantees and break when data sources update. The SIEM vendor must be responsible for core content to ensure it 'just works' and shifts the maintenance burden away from the customer.

High-quality, curated threat detection is critical for organizations to effectively manage their security posture. Google SecOps provides out-of-the-box detection of new and emerging threats, which can help organizations quickly identify and respond to security incidents.

SIEM with its own AI

Does the SIEM incorporate AI, and is it positioned to continue innovating?

The role of artificial intelligence in SIEM is still not entirely understood (and much less implemented) by many vendors. However, leading SIEMs already have tangible AI-driven features shipping today.

These features now include **fully agentic AI for select alert triage**, which autonomously investigates security alerts, provides a disposition (true positive or false positive) with a confidence score (a must when the system is not sure), and suggests next steps.

This agentic capability directly addresses pain points like alert fatigue and slow response times (MTTR). Other shipping features include natural language processing for expressing searches and rules, automated case summarization, and recommended response actions.

Most customers and industry observers consider features like deep threat detection and turning intelligence into robust detections to be some of the 'holy grails' of AI-driven SIEM capabilities. No SIEM reliably offers these holy grail features today. As you choose a new SIEM, consider whether the vendor is investing the resources necessary to make meaningful progress on these transformational capabilities.

Google Security Operations is a cloud-based SIEM solution offered by Google Cloud.

It is designed to help organizations centrally collect logs and other security telemetry, then detect, investigate, and respond to security threats in real time.

Detect and prioritize security threats
Google SecOps' out-of-the-box detection rules identify and prioritize security threats in real time. This helps organizations quickly and effectively respond to the most critical threats.

Investigate security incidents
Google SecOps provides a centralized platform for investigating security incidents. This helps organizations quickly and efficiently gather evidence and determine the scope of the incident.

Respond to security incidents
Google SecOps provides a variety of tools to help organizations respond to security incidents, such as automated remediation. Threat hunters find the platform's speed, search capabilities, and applied threat intelligence invaluable in tracking down attackers who may have slipped through the cracks. This helps organizations to quickly and effectively contain and mitigate the impact of security incidents.

Google SecOps has a number of advantages over traditional SIEM solutions, including:

Artificial intelligence
Google SecOps uses Gemini capabilities to enable defenders to search vast amounts of data in seconds using natural language and make faster decisions by answering questions, summarizing events, hunting for threats, creating rules, and delivering recommended actions based on the context of investigations. Security teams can also use Gemini in Google SecOps to easily build response playbooks, customize configurations, and incorporate best practices – helping simplify time-consuming tasks that require deep expertise.

Applied threat intelligence
Google SecOps natively integrates with Google Threat Intelligence (GTI) which encompasses combined intelligence from VirusTotal, Mandiant Threat Intelligence, and internal Google Threat Intelligence sources, to help customers detect more threats with less effort.

Scalability
Google SecOps is a cloud-based solution, so it can leverage hyperscale cloud infrastructure provided by Google Cloud to meet the capacity and performance needs of any organization, regardless of its size.

Integration with Google Cloud
Google SecOps is tightly integrated with other Google Cloud products and services, such as Google Cloud Security Command Center Enterprise (SCCE). This integration makes it easy for organizations to manage their security operations in a single, unified platform. Google SecOps is the best SIEM for Google Cloud service telemetry and also includes out-of-the-box detection content for other major cloud providers, such as AWS and Azure.

Applied threat intelligence
in Google SecOps

Google SecOps allows security teams to manage and analyze security data which is automatically correlated and enriched with threat data. By integrating threat intelligence directly into your SIEM, organizations can:

Improve detection and triage
Threat data can be used directly to create rules that can help identify malicious activity in real time. This data is also used to add context to other alerts and automatically adjust confidence in the alert. This helps organizations quickly detect and triage security incidents, and lets them focus their resources on the most critical threats.

Enhance investigation and response
Threat intelligence can be used to provide context and insights during security investigations. This can help analysts quickly identify the root cause of an incident and develop and implement effective response strategies.

Stay ahead of the threat landscape
Threat intelligence can help organizations stay ahead of the threat landscape by providing information about the latest threats and vulnerabilities. This information can be used to develop and implement proactive security measures, such as threat hunting and security awareness training.

Threat detection
in Google SecOps

Google SecOps' threat detection is based on a continuous stream of frontline threat intelligence from Google's security teams. This intelligence is used to create rules and alerts that can identify malicious activity in real time. Google SecOps also uses behavior analytics and risk scoring to identify suspicious patterns in security data. This allows Google SecOps to detect threats that can't be detected by traditional detection rules.

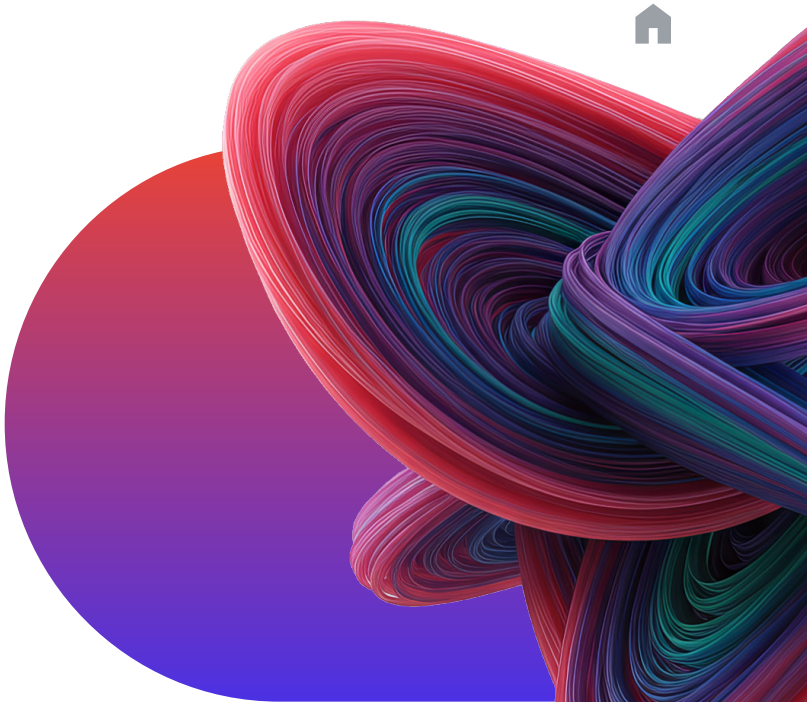
The value of high-quality, curated threat detection is clear. Organizations that use Google SecOps can benefit from:

Improved detection and triage
Google SecOps can help organizations quickly identify and triage security incidents. This allows organizations to focus their resources on the most critical threats.

Enhanced investigation and response
Google SecOps can provide context and insights during security investigations. This can help analysts quickly identify the root cause of an incident and develop and implement effective response strategies.

Stay ahead of the threat landscape
Google SecOps can help organizations stay ahead of the threat landscape by providing information about the latest threats and vulnerabilities. This information can be used to develop and implement proactive security measures, such as threat hunting and security awareness training.

SIEM migration



So you've decided to make the move. Your approach to migration is critical to ensuring that you maintain required capabilities and start extracting value from the new platform as soon as possible. It comes down to prioritization. A typical trade off is recognizing that while a SIEM migration represents an opportunity to modernize your entire approach to investigation, detection, and response, many SIEM migrations fail because organizations try to 'boil the ocean.'

Here are our best tips for planning and executing your successful SIEM migration:

01.

Define your migration goals

This sounds obvious, but your SIEM migration is often a lengthy process, so defining your desired outcomes (for example, faster threat detection, easier compliance reporting, improved visibility, and reduced analyst toil while also lowering cost) is strongly correlated with success.

02.

Develop a realistic migration timeline

This includes accounting for data transfer, testing, tuning, and training, as well as potential overlaps where you may need to run both systems in parallel. A well-defined migration plan will help you identify and mitigate risks and ensure that the migration is completed successfully. The plan should include a detailed timeline as well as a list of tasks, resources, and a budget. Recognize that major projects like a SIEM migration must be broken into phases.

03.

Assess AI readiness

Your migration is likely a structural re-platforming, rather than a tool swap. Factor in how the new platform will support agentic AI workflows. Define success not just by cost reduction, but by outcome-driven metrics like reduced analyst toil and improved 'time to context' – how quickly an analyst receives a complete, correlated narrative of an attack.

04.

Use the migration as an opportunity to clean house

This is a good time to clean up your detection rules and log sources so that you only migrate the ones that you actually use. It's also a good time to review your alert triage and tuning processes to ensure that they are up to date.

05.

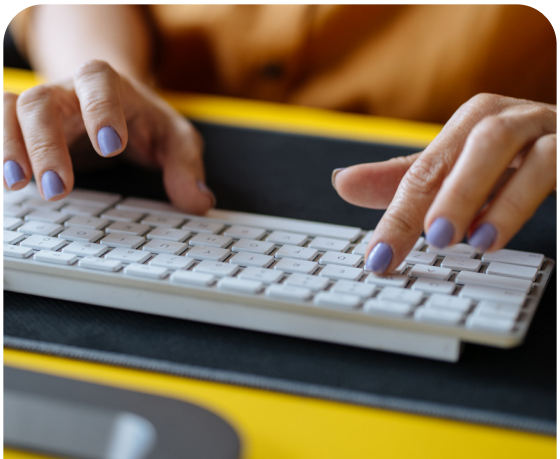
Don't migrate every log source

Moving to a new SIEM is a great opportunity to decide what logs you need, be it for compliance or security reasons. Many organizations accumulate a vast amount of log data over time and not all of it is necessarily valuable or relevant. By taking the time to evaluate your log sources before you migrate them, you can streamline your SIEM and focus on the data that is most important to your security and compliance needs.

06.

Implement telemetry pipelines

Replace monolithic SIEM collectors with a vendor-neutral data pipeline (for example, Bindplane) as your architectural cornerstone. Use this layer to aggressively filter, enrich, and route only high-value telemetry, preventing vendor lock-in and uncontrollable volume-based costs before data hits the analytics engine.



07.

Inventory integrations and context data sources

Conduct a thorough inventory of all external systems (for example, EDR, IAM, TIP, or ITSM) and their dependencies on the old SIEM. Actively test API and connector compatibility with the new SIEM and leverage the migration to formalize these connections, eliminating 'swivel-chair' toil.

08.

Leverage AI as the migration partner

The process is no longer purely 'human-led.' Use generative AI rule converters – LLMs trained on security Domain Specific Languages (DSLs) – to automate the translation of legacy logic (for example, SPL or KQL) into the new SIEM's format (for example, YARA-L). This converts months of manual toil into a rapid, editorial review process.

09.

Don't migrate all content

Migrating all of your existing detection content, rules, alerts, dashboards, visualizations, and playbooks to a new SIEM is not always necessary. Take the time to evaluate your current detection coverage and prioritize migration of the rules you need. You will find opportunities to consolidate rules, eliminate rules that could never fire due to lack of telemetry or faulty logic, or identify rules that are handled better by out-of-the-box content. Question any vendor or deployment partner who advocates for one-to-one rule migration.

10.

Evolve to Detection-as-Code (DaC) with CI/CD

Treat all detection logic, rules, and playbooks as software code. Store this code in version control, enforce peer-review, and integrate automated testing via Continuous Integration/Continuous Deployment (CI/CD) pipelines to ensure rules are validated against simulated attacks before reaching production. This does not mean you must program, but it does mean a lot more rigor and predictability in content development.

11.

Prioritize early content migration

Initiate detection content migration immediately upon availability of the log sources and enrichments required for each specific use case. This data-driven approach, that aligns sources with use cases, enables parallel migration efforts for optimal efficiency and results.

12.

Refine SOAR and agentic workflow integration

Do not treat SOAR as an afterthought to SIEM. Alerts that SIEM creates will need to be handled, processed, and escalated, etc. Embed automated workflows and response capabilities immediately for high-priority use cases. This includes integrating AI to autonomously perform alert triage and provide case summaries, ensuring human oversight for high-risk actions.

13.

Detection content migration is a human-led process

Prepare to rebuild detection content (for example, rules, alerts, dashboards, models, etc.) (mostly) from scratch, using your old content as inspiration. Today, there is no foolproof method to automatically convert rules from one SIEM platform to another. While some vendors offer syntax translators, they generally result in a good jumping off point rather than a perfectly translated rule, search, or dashboard. You should take maximum advantage of these tools, but recognize they are not a panacea.

14.

Detection content comes from many sources

Analyze your detection coverage needs, then adopt or create your detection use cases as needed. Your SIEM vendor will provide some out-of-the-box content which you should always leverage if you can. Also consider community rule repositories and third-party detection content providers. When necessary, write your own rules and remember that most rules, regardless of their provenance, need to be tuned for your organization's specific environment.

15.

Testing and validation

We recommend the practice of testing your SIEM and detection content by regularly injecting data that will trigger your detections, checking parsing, and validating data flow from detection to case to response playbook. A SIEM migration is the perfect time to adopt a rigorous detection engineering program that includes this sort of testing.

16.

Prepare for a transition period during which you'll run both old and new tools

Avoid a disruptive 'rip and replace' approach. A phased migration, where you migrate log sources and use cases gradually, helps control the process and reduces risk. Additionally, think twice about re-ingesting data from your old SIEM into the new one. In some cases, you may have the ability to leave the previous SIEM running for extended periods to allow access to historical data.

17.

Enable your teams

Your SIEM migration will fail if your analysts can't use the new system. A good migration plan will include deep enablement for your teams. Think about training: engineers on data onboarding and parsing; analysts on case management, investigation, and triage; threat hunters on anomaly detection and search; and detection engineers on rule-writing. Timing is critical for enablement. It's best to train staff as they embark on specific phases of migration, rather than delivering training before those skills will be required.

18.

Get help

If you are lucky (or maybe unlucky?) as a practitioner or leader, you may have gone through one or two SIEM migrations in your career. Why not seek help from specialists who have done it dozens or hundreds of times? Professional services teams from the vendor and/or consulting teams from qualified services partners are a great choice – SIEM migrations are largely human-centered efforts.

Mandiant helps organizations with their SIEM migrations and recommends the following:

→ Develop a target operating model (TOM) that defines your organization's ideal future state, detailing how your people, processes, and technology will work together to achieve business objectives.

→ Develop a threat profile specific to your organization to ensure you focus on the most relevant risks.

→ Evaluate your deployment via visibility and detection health checks and testing.

→ Set up an incident response retainer for fast access to experts in the event of a cyber incident.

Key process:

Choose a deployment partner

No decision will have a greater impact on the ultimate success of a SIEM migration than choice of a deployment partner. SIEM platforms are large-scale, complex, enterprise systems. Don't try to go it alone – stick with a deployment partner who has been through many migrations.

The deployment partner might simply be the professional services arm of the new SIEM vendor. However, it's more common to choose a third-party partner to run the migration. Remember, SIEM migration is a human-led endeavor. Choosing a partner with certifications in the new SIEM and plenty of referenceable customers is best. It also helps if they have expertise in the SIEM you are migrating from. Beyond references, a clever way to determine the level of experience of a partner with your new SIEM is to check out community forums to see whether the team has been an active contributor. In the opinion of the authors, highly engaged partner staff correlates with successful SIEM migrations.

Beyond the technical bits and bytes of the SIEM migration, you can also choose partners who have specific experience in your industry vertical, in your compliance environment, or in your region – or in all three. You can look for language skills and resources in advantageous time zones. You can also look for partners who operate your SIEM for you, or who deliver similar outcomes as a managed security service provider who can partially or fully outsource your organization's SIEM.

Key process:

Document current configuration and use cases

SIEM deployments are usually expansive, growing steadily in scope and complexity over years of use. Prepare for little or no documentation, and expect that personnel who performed initial configuration and customization of the SIEM are often long gone.

Thoroughly documenting the configuration and capabilities early in the migration process can mean the difference between success and failure.

- → **Document the identity and access management used by the SIEM:** You will certainly need to preserve some role-based access to data and features. On the other hand, migration is an opportunity to analyze and address access sprawl which occurs naturally in most organizations. You may also look at the migration process as an opportunity to modernize authentication/authorization methods – including federating identity with corporate standards and implementing multi-factor authentication.

- → **Capture the names of the data types being collected:** Note that some SIEMs call these names "sourcetype" or "logtype." Capture how much data from each data type is flowing using gigabytes/day as the metric. Document the data pipeline for each data source (for example, agent-based, API query, web hook, cloud bucket ingestion, ingestion API, HTTP listener, etc.) and capture the SIEM's parser configuration along with any customizations.

- → **Gather saved searches, dashboard definitions, and detection rules:** Many SIEMs also have persistent data storage mechanisms such as lookup tables. Be sure to understand and document how these are populated and used.

- → **Leverage AI:** Use generative AI to understand what the long-gone creators of the legacy queries, searches, and alerts intended. "Explain this SPL query" is a very useful trick at this stage. Later, use AI to automatically map obscure legacy log fields to a modern Unified Data Model (UDM), which solves the 'sourcetype' documentation nightmare.

- → **Make an inventory of integrations with external systems:** Many SIEMs integrate with case management systems, external storage, ticketing systems, notification services (for example, email, SMS, etc.), and threat intelligence platforms. A SOAR component of your SIEM may have even more linkages to external systems, such as for automated remediation purposes.

- → **Document response content:** Capture response content such as playbooks, case management templates, and any active integrations that have not already been documented.

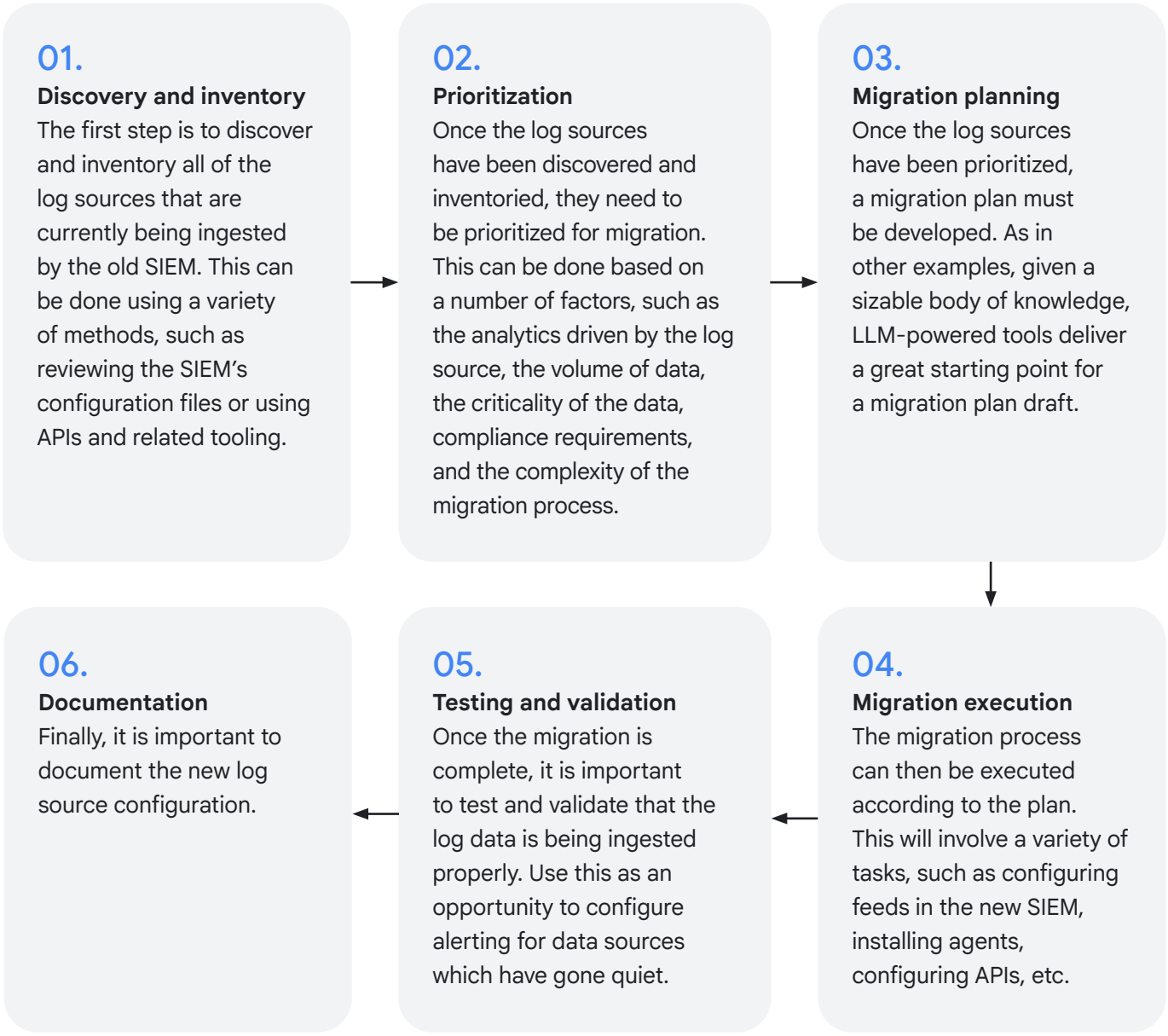
Beyond gathering these important technical details, it's critical to take time to interview users of the existing SIEM to understand their workflows. Ask how they use the SIEM and what standard operating procedures rely on the SIEM. It's also important to ask broad questions such as which teams outside of security might use the SIEM. For example, it's not uncommon for compliance teams or IT operations staff to rely on the SIEM. Failing to capture these use cases can cause missed expectations later in the migration process.

Key process:

Log source migration

Log source migration involves moving the data sources from the old SIEM to the new SIEM. This process depends on the documentation of the current configuration gathered in the Key process: Document current configuration and use cases section.

The following steps are typically involved in the log source migration process:



Key process:

Migrate detection and response content

SIEM detection and response content consists of rules, searches, playbooks, dashboards, and other configurations that define what your SIEM alerts on and how it helps analysts handle those alerts. Without properly configured content, the SIEM is just a fancy way to search. It's "expensive grep" – a term a colleague of the authors coined a number of years ago. SIEM content plays a key role in defining your organization's discovery coverage.

- **Detection rules:** The rules are used to identify security incidents and are written by detection engineers who have deep knowledge of security-threat actors and their tactics, techniques, and procedures (TTPs). Detection rules look for patterns that represent these TTPs in the log data. Detection rules often correlate different log sources together and make use of threat intelligence data.

- **Response playbooks:** These are used to automate the response to security alerts. They can include tasks such as sending notifications, isolating compromised hosts, enriching alerts with contextual data/threat intelligence, and running remediation scripts.

- **Dashboards:** These are used to visualize security data and track the status of security incidents. They can be used to monitor the overall security posture of the organization and to identify trends and patterns.

The development of new detection and response content is an iterative process. It is important to continuously monitor the SIEM and make adjustments to the content as needed. SIEM migration is an excellent time to improve your processes using approaches like detection as code (DaC).

In 2026, treat Detection-as-Code (DaC) not as an option, but as a mandatory architectural imperative. Stress that writing rules in a Graphical User Interface (GUI) is an anti-pattern and that modern detections must be treated strictly as software code, stored in version control, and continuously tested using CI/CD pipelines.

Key process:

Training and enablement

An often-overlooked process during SIEM migration is user training. The SIEM is perhaps the most important single tool that a security operations team uses. Their ability to use it effectively and productively will play a big role in the success of the migration and their ability to protect your organization. Rely on your SIEM provider and deployment partner to provide training content and delivery. Here is a brief list of topics on which your teams should be enabled:

- Log feed ingestion and parsing
- Search/investigation
- Case management
- Rule authoring
- Dashboard development
- Playbook/ automation
- AI trust and validation (queries, reports, rules, playbooks)
- Evolution of roles due to increased use of AI for alert triage

Conclusion

The migration from a legacy SIEM to a modern solution is now an unavoidable structural transformation. While the challenges may seem daunting, a well-planned migration can lead to significant improvements in threat detection and overall security posture.

A fundamental architectural imperative for 2026 is the adoption of telemetry pipelines. Security leaders must move away from monolithic SIEM ingestion collectors and establish vendor-agnostic platforms to aggressively filter, enrich, and route data before it hits the analytics engine. This foundational shift is necessary to prevent vendor lock-in and uncontrollable volume-based costs. Furthermore, while the traditional 'lift and shift' approach risks copying technical debt into the new environment, organizations must instead seize this opportunity to modernize detection logic and processes.

By leveraging cloud-native architecture, advanced threat intelligence, and utilizing AI-driven features, organizations can empower their security teams. To accurately measure success in the AI era, security leaders must shift their focus from traditional metrics like mean time to respond (MTTR) – which loses diagnostic value when agentic AI performs triage – to measuring 'time to context.' This new metric assesses how quickly an analyst receives a complete, correlated, human-readable narrative of an attack.

The successful migration process involves meticulous planning, comprehensive documentation, strategic content modernization, thorough testing, and comprehensive user training. Partnering with experienced deployment specialists is invaluable to navigating the complexities and ensuring a smooth transition. With a commitment to continuous improvement and a focus on detection engineering, organizations can harness the full potential of their new SIEM.

Additional reading

"Future of the SOC: Transform the How" paper

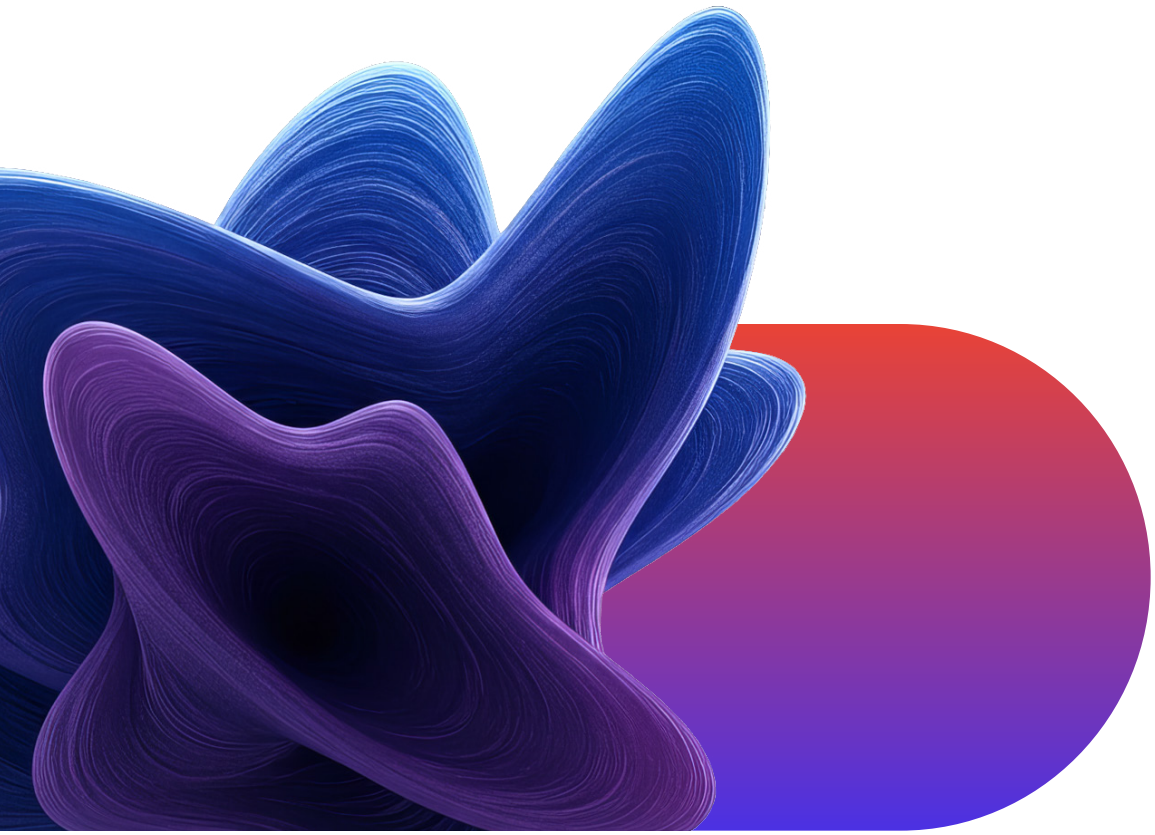
Google Cloud Security Community Blog

Detection Engineering Weekly Newsletter

detect.fyi – practitioner-centric tips on detection engineering

Getting Started with Detection-as-Code and Google Security Operations — David French (Part one, part two)

Implementing a Modern Detection Engineering Workflow — Dan Lussier (Part one, part two, part three)



Google Cloud