Google Cloud
Security

White paper

The great SIEM migration: A guide to ditching dinosaurs

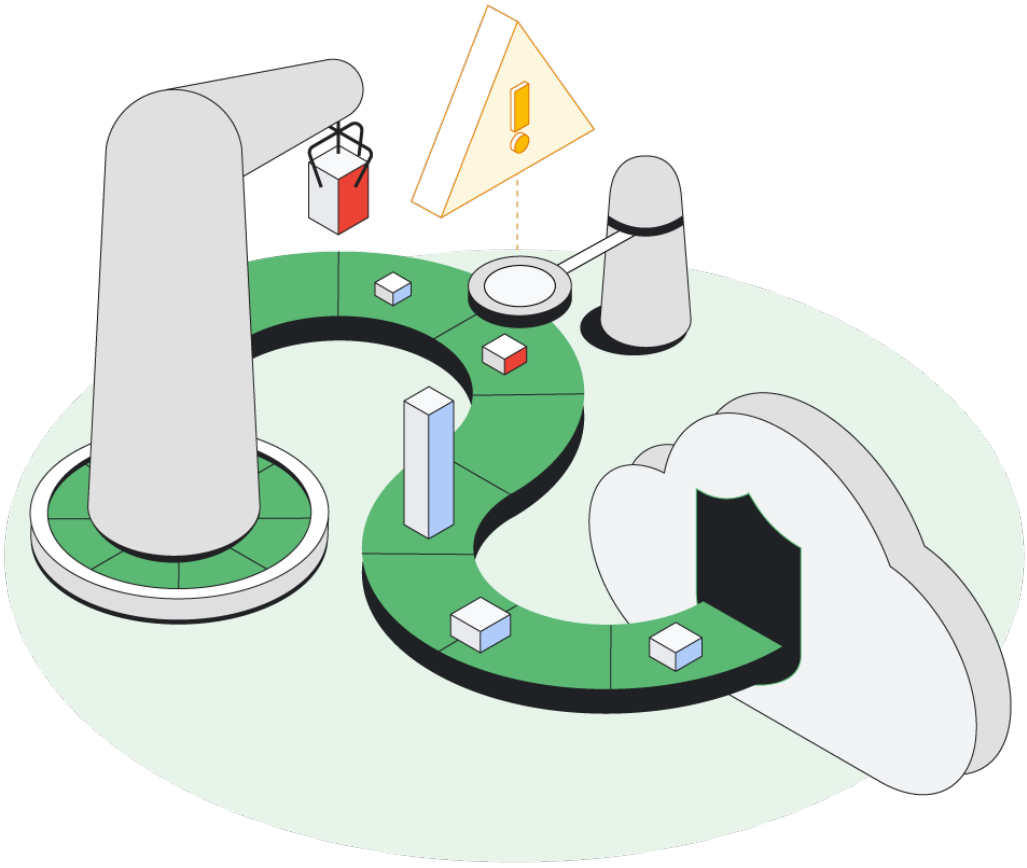


Table of Contents

SIEM is dead, long live SIEM!

If you are like us, you may be surprised that, in 2024, 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 15+ 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 of course AI, to name a few.

Legacy SIEMs 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 features and 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 may be poorly positioned to take advantage of the latest technological developments, such as artificial intelligence (AI).

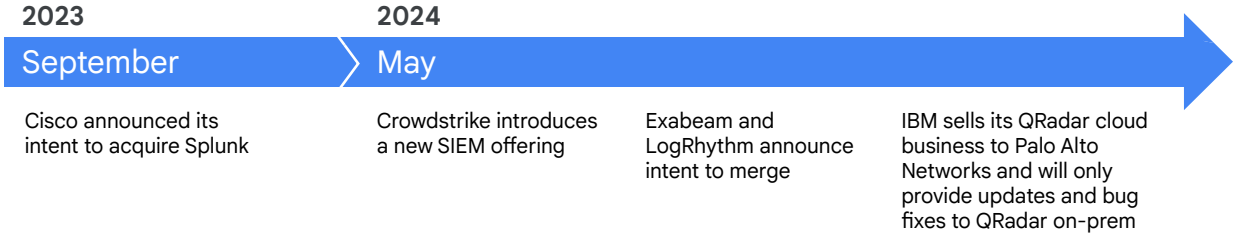
So while a SIEM by any other name may sound just as sweet, security operations teams will continue to rely on "security operations platforms" (or whatever name they go by) in the foreseeable future for threat detection, investigation and response.

The Great SIEM Migration has Begun

SIEM migration is not new. Organizations have fallen out of love with their existing SIEM and sought newer and better options for years. 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.

But recent months have introduced tectonic shifts in the SIEM space that cannot be under-stated. There is little doubt that the SIEM landscape will be completely transformed in a few short years from now — giving birth to new market leaders and seeing the decline and perhaps even the demise of "dinosaurs" who have ruled SIEM-land for decades (or "eons" in cybersecurity terms). 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.

Here is a summary of major moves in the last 9 months alone:



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. That's where this paper comes in. The authors have seen hundreds of SIEM migrations as practitioners, analysts, and vendors over multiple decades. So, let's take stock of the top SIEM migration tips for 2024. We'll divide this list into categories and sprinkle in lessons we've learned from the trenches.

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. For example:

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.

SIEM with 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 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.

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

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

Tip: 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 like 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.

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 to quickly identify and respond to security incidents.

SIEM with AI

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

The role of artificial intelligence in SIEM is still not fully understood (much less implemented) by any vendor. However, leading SIEMs already have tangible AI-driven features shipping today. These 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 threat detection and predictive adversary analysis to be some of the "holy grails" of AI-driven SIEM capabilities. No SIEM reliably offers these features today. As you choose a new SIEM in 2024, consider whether the vendor is investing the resources necessary to make meaningful progress on these transformational capabilities.

Google Security Operations (formerly Chronicle) 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 Google's Gemini AI technology 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 Security Operations 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 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 GCP service telemetry and also includes out of the box detection content for other major cloud providers like 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 to quickly detect and triage security incidents, and to 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 to quickly identify the root cause of an incident and to develop and implement effective response strategies.
- **Stay ahead of the threat landscape:** Threat intelligence can help organizations to 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 to quickly identify the root cause of an incident and to 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.

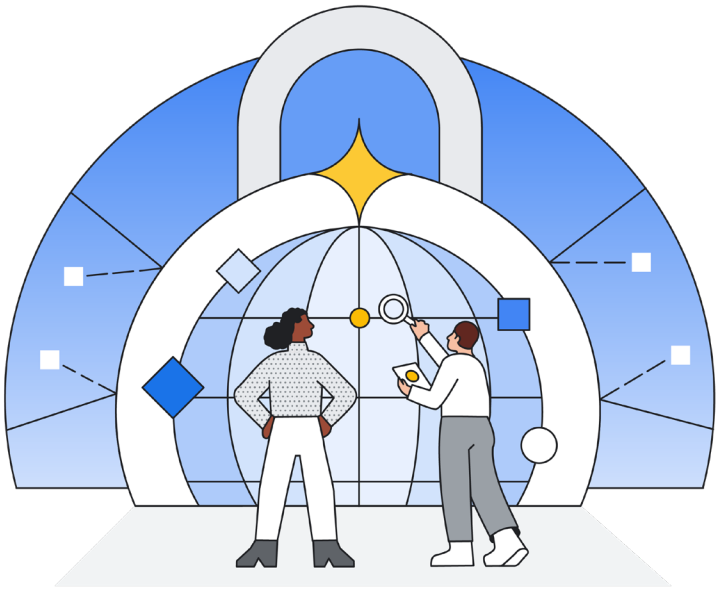
SIEM Migration

So you've decided to make the move. Your approach to migration is critical in ensuring 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."

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

- **Define your migration goals.** This sounds obvious, but your SIEM migration is a lengthy process, so defining your desired outcomes (e.g., faster threat detection, easier compliance reporting, improved visibility, reduced analyst toil, while also lowering cost) is strongly correlated with success.
- **Use the migration as an opportunity to clean house.** This is a good time to clean up your detection rules and log sources and only migrate the ones that you actually use. It's also a good time to review your alert triage and tuning processes and make sure they are up to date.
- **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.
- **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, to eliminate rules that could never fire due to lack of telemetry or faulty logic, or 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.
- **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, aligning sources with use cases, enables parallel migration efforts for optimal efficiency and results.
- **Detection content migration is a human-led process.** Prepare to rebuild detection content (rules, alerts, dashboards, models, etc.) (mostly) from scratch, using your old content as inspiration. Today, there is no fool-proof 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.
- **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 most rules, regardless of their provenance, need to be tuned for your organization’s specific environment.
- **Develop a realistic migration timeline.** This includes accounting for data transfer, testing, tuning, training and potential overlaps where you may need to run both systems in parallel. A well-defined migration plan will help you to identify and mitigate risks, and ensure that the migration is completed successfully. The plan should include a detailed timeline, a list of tasks, resources, and a budget. Recognize that major projects like a SIEM migration must be broken into phases.

- **Testing**. 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 testing like this.
- **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. Also, think twice about re-ingesting data from your old SIEM into the new. In some cases, you may have the ability to leave the previous SIEM running for extended periods to allow access to historical data.
- **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, training analysts on case management/investigation/triage, threat hunters on anomaly detection/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 training before those skills will be required.
- **Get help!** If you are lucky (or maybe unlucky?) as a practitioner or leader, you will have perhaps 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.



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 partners 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, or in your compliance environment, or in your region, or 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. 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 of each data type is flowing using gigabytes/day as the metric. Document the data pipeline for each data source (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.
- Make an inventory of integrations with external systems. Many SIEMs integrate with case management systems, relational databases, notification services (email, SMS, etc), and threat intelligence platforms.
- 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, what standard operating procedures rely on the SIEM. It's also important to ask broad questions such as what 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 config gathered in the Key Process: Document Current Configuration and Use Cases section.

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

1. **Discovery and inventory:** The first step is to discover and inventory all of the log sources that are currently being ingested by the old SIEM. This can be done using a variety of methods, such as reviewing the SIEM's configuration files or using APIs and related tooling.
2. **Prioritization:** Once the log sources have been discovered and inventoried, they need to be prioritized for migration. This can be done based on a number of factors, such as the analytics driven by the log source, the volume of data, the criticality of the data, compliance requirements, and the complexity of the migration process.
3. **Migration planning:** Once the log sources have been prioritized, a migration plan must be developed.
4. **Migration execution:** The migration process can then be executed according to the plan. This may involve a variety of tasks, such as configuring feeds in the new SIEM, installing agents, configuring APIs, etc.
5. **Testing and validation:** Once the migration is complete, it is important to test and validate the log data is being ingested properly. Use this as an opportunity to configure alerting for data sources which have gone quiet.
6. **Documentation:** Finally, it is important to document the new log source configuration.

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 are used to identify security incidents. Detection engineers who have deep knowledge of security threats actors and the tactics, techniques, and procedures (TTPs) common to them write them. 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 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 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).

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

Conclusion

Eventually, migration from a legacy SIEM to a modern solution is unavoidable. While the challenges may seem daunting, a well-planned and executed migration can lead to significant improvements in threat detection, response capabilities, and overall security posture.

By carefully considering the selection of a new SIEM, leveraging the strengths of cloud-native architecture, incorporating advanced threat intelligence, and utilizing AI-driven features, organizations can empower their security teams to proactively defend against ever-evolving threats. The successful migration process involves meticulous planning, comprehensive documentation, strategic log source and content migration, thorough testing, and comprehensive user training.

Partnering with experienced deployment specialists can be invaluable in 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 and bolster their security defenses for years to come.

Additional Reading

- "How Google SecOps Can Help Augment Your SIEM Stack" paper
- "Future of the SOC: Evolution or Optimization — Choose Your Path" 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)