exabeam

WHITE PAPER

EIGHT STEPS TO MIGRATE YOUR SIEM

SUMMARY

ORGANIZATIONS USE A SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PLATFORM BECAUSE IT'S A CRITICAL, NECESSARY COMPONENT OF A MULTILAYERED SECURITY CONTROL INFRASTRUCTURE.

In a large enterprise, security and IT system logs and other inputs can easily reach hundreds of thousands or millions of events every day and having to store terabytes of logs daily. Event volume is surging especially as organizations embrace the cloud and global Internet of Things. It's impossible for humans to manually keep up with this deluge of data, so they use a SIEM do the work more efficiently. With the relentless wave of cyberattacks and data breaches, however, performance of legacy SIEMs is under scrutiny due to their inability to detect threats at scale and to help security teams investigate and respond to incidents efficiently. Organizations are also struggling to find qualified technical staff to effectively operate SIEMs.

For these reasons, many enterprises are re-evaluating their SIEM and migrating to new technology. Migrating a SIEM is no trivial task – especially being the lynchpin of security operations centers (SOCs).

This white paper provides eight strategic steps to guide migration and put your organization on a path to success. The paper also mentions specific benefits that result from migrating to Exabeam Security Management Platform (SMP) as organizations look to modernize their security operations and improve employee productivity. Our guidance is aimed toward business leaders, security leaders and other stakeholders to help ensure a successful enterprise collaboration.

WHY MIGRATE FROM A LEGACY SIEM?

The surge in cyberattacks, shortage of qualified security analysts, and sheer volume of events and number of devices pumping data into the enterprise SEIM is posing several operational issues. For example, SOC teams universally complain about time wasted by chasing false positive alerts. The culprit for issues like this is legacy technology in many SIEMs, which is approaching two decades since early solutions appeared in the market. Four legacy characteristics of many SIEMs include:

Excessive logging costs – Charging SIEM usage based on amount of data ingested and processed made sense prior to common use of Big Data. Modern requirements to use Big Data with SIEMs means organizations are subjected to unpredictable cost increases. This is a disincentive to collecting everything for analysis with Data Science. It also limits capabilities for threat detection and creates blind spots during incident investigations.

Can't catch unknown threats – The legacy SIEM model typically was based on correlation rules. At a minimum, the manual effort required to create, tune and update correlation rules is unproductive. Worse, as the variety of threats – especially by unknown actors – has risen, a reliance on rules has left legacy SIEMs unable to detect advanced threats.

Missing distributed attacks – When tracking is substandard, SOC analysts get an incomplete picture of users' activities. A common scenario is lateral movement, where an attack first breaches a network and then moves around inside an organization – often in ways that on the surface, appear to be unconnected patterns of different people. These events might occur in a variety of places such as the on-premise corporate network, on mobile devices or in the cloud. Consequently, the team misses threats or is sidelined by false negatives, and is unable to determine the full scope of attacks.

Manual investigation and remediation – When legacy SIEM technology limits automation, the organization is faced with increased risk and longer durations of exposure to threats. For example, every investigation requires construction of a timeline to evaluate events, understand their implication for security, and prepare relevant incident response. For legacy SIEMs, those steps are usually manual and time consuming. Supporting the manual processes is a drain on operational efficiency. It also creates a scenario of steadily growing needs for more skilled analysts.

Solving these legacy issues is a strong motivation for SIEM migration. Before initiating the process of migration, it's useful for stakeholders to get a big-picture sense of what these steps entail and how they may affect new workflows. We address these points in the balance of this white paper.

PROCESS FLOW FOR SIEM MIGRATION

Migrating a legacy SIEM to new technology is a complex process. Although the process described in this white paper is specific to SIEM migration, some elements draw from the experience of other largescale IT implementations. Exabeam's eight-step model for SIEM migration takes inspiration from interviews with security practitioners and How to Architect and Deploy a SIEM Solution, published by Gartner.[1]

Our model presents steps in context of preparing for the entire SIEM migration in typical scenarios: augmenting a legacy SIEM with behavioral analytics or replacing a legacy SIEM with a modern SIEM. These considerations also apply to more specific use cases such as SIEM consolidation due to M&A and standing up a new company as part of a corporate divestiture.

Exabeam's eight-step process flow for SIEM migration is as follows:

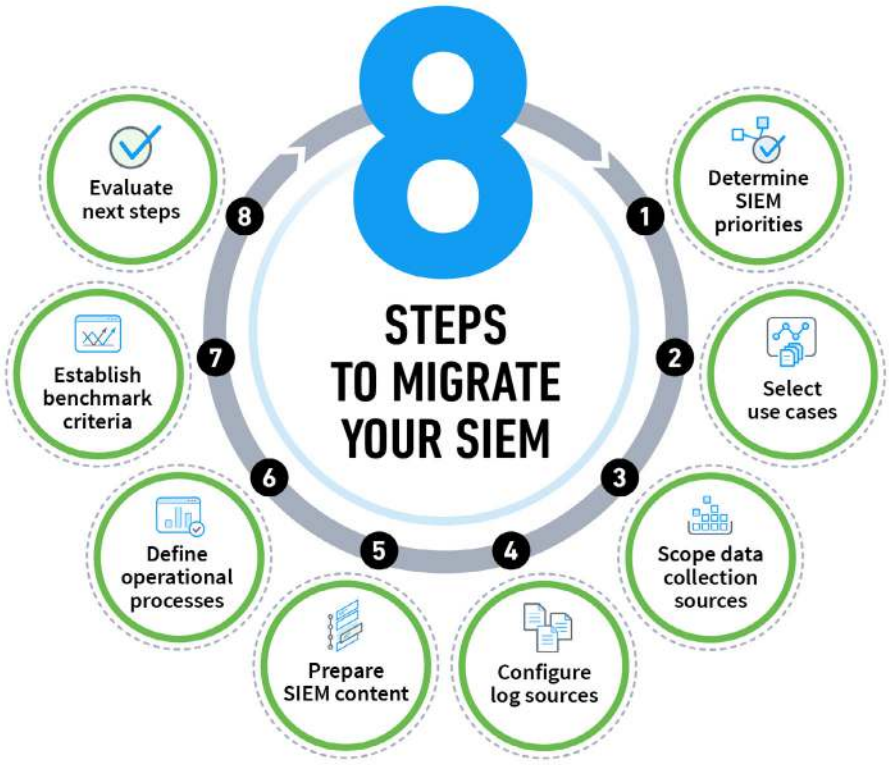


FIGURE 1: EIGHT STEPS TO MIGRATE YOUR SIEM

[1] Anton Chuvakin, Anna Belak, and Augusto Barros, "How to Architect and Deploy a SIEM Solution," 16 October 2018, ID: G00366351.

THE EIGHT STEPS OF SIEM MIGRATION

Structuring SIEM priorities is important because priorities will determine when the migration is "done" and if the migration was a success. SIEM migration is a strategic effort that will touch many areas of the enterprise. The migration team should check with all stakeholders to determine priorities for protecting specified data and systems. Examples may include intellectual property (IP), customer records, financial records, personnel records, systems running critical applications, networks, security devices, etc. These are the "crown jewels" whose compromise could result in considerable damage to the business.

The SIEM migration team must consider the organization's risk management framework in determining priorities for the SIEM, including compliance with relevant industry guidelines, regulations and statutes. Be sure to include relevant executives and senior managers in this initial process step to ensure that business priorities are included with migration. Including these stakeholders is important because they are increasingly tasked with responsibility to make IT drive business outcomes.

Also determine your organization's criteria for the migration. Will it be modular and done in phases over a period of time? Migration does not necessarily require a wholesale replacement. Some organizations will feel more comfortable by augmenting the legacy SIEM with a new SIEM's capabilities such as behavioral analytics or automated response capabilities; others may prefer a phased approach that temporarily runs the new SIEM in parallel with the legacy SIEM. A common driver is a pending legacy SIEM license renewal date; if so, how will that affect decommission and cutover?

If your organization is engaged in a large-scale cloud-first architecture initiative, consider where the SIEM migration destination will occur: on-premises, a public cloud, a hybrid cloud, or to Software-as-a-Service (SaaS). Modernizing your SIEM creates fresh options such as new use cases or automating methods of issue remediation. Exabeam supports migration to all of these options.

Timeline: It typically takes 2-4 weeks to identify all the stakeholders and get a consensus on your top business issues and priorities.

Selection of use cases for the SIEM migration should answer the question: what problems are we trying to solve with the new SIEM? Consider use cases in terms of business priority. How would an event impact the business? How often does the use case occur? Ignoring or minimizing the business aspect of use cases may seem like an obvious misstep, but it occurs frequently and will lead to disappointing results for the migration.

Examples of typical use cases include protecting against insider threats; identifying compromised credentials; detecting account creation and management; augmenting endpoint analytics; monitoring high-risk employees; and prioritizing security alerts. Exabeam highlights several in 10 SIEM Use Cases in a Modern Threat Landscape. Strategically, it is helpful to specify use cases within higher-level risk initiatives, such as threat management, process control, and asset control. This approach will help engage executives who are not familiar with the technical details. A valuable reference framework for potential use cases is MITRE ATT&CK, a globally-accessible knowledge base of 11 adversary tactics and 232 techniques based on real-world observations.[2]

[2] The MITRE ATT&CK framework is available at https://attack.mitre.org/.

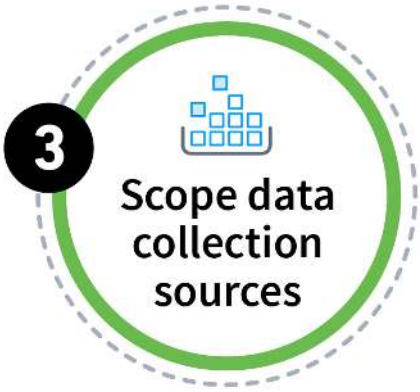
It's common for a legacy SIEM to have 50, 100 or even hundreds of use cases. A new SIEM provides technology that can manage these use cases more effectively such as by reducing the need to create and maintain correlation rules or increasing automation. Replicating all legacy use cases may be unnecessary as new technology can eliminate the need to manually manage some scenarios.

Technical stakeholders should avoid focusing on use cases for technically "interesting" scenarios that have minimal practical impact on protecting critical business operations and sensitive data. A good strategy for migration is to implement business-critical use cases first, and gradually phase in lesser-priority use cases as the migration team gains experience with the new SIEM.

Elements for each use case must address People (who will perform the tasks), Process (how the use case will be accomplished) and Technology (what aspects of the new SIEM and supporting IT infrastructure will provide related functionality). Also consider support for specific use cases that is included with the new SIEM.

Exabeam provides more than 400 use case models to help accelerate this phase of migration planning for your organization.

Timeline: It usually takes 2-4 weeks to select the use cases for your new SIEM. In most cases, it is a fairly straightforward task since security teams have usually outlined their use cases for their existing SIEM. However, this is the time to reevaluate whether changes need to be made to include new use cases that weren't covered by your existing SIEM.



The ultimate purpose of a SIEM is allow analysts to quickly detect security threats and remediate them. Having a SIEM that integrates data logs from a broad array of IT and security products is essential for effective remediation.

Each use case requires data from a list of related physical and virtual systems and applications such as servers, network devices, firewalls, endpoints, operating systems, applications, databases, Directory Services, Information Services, and other related infrastructure hosted in public, private or hybrid clouds. Also consider contextual data sources such as human resources or a configuration management database.

Exabeam provides integrations with over 200 data sources.[3]

This process includes aligning essential log data from security and IT devices and solutions with each use case. For example:

- **Insider threat** use case requires log integration from Data Loss Prevention, Email Management, Database Activity, Privileged Account Management, and Identity Access Management solutions;
- **Compromised credentials** use case needs logs from Authentication, Identity Access Management and Cloud Access Security Broker solutions;
- **Account creation and management** use case needs logs from Privileged Account Management and Identity Access Management solutions;
- **Endpoint anomalies** use case needs logs from Endpoint, Endpoint Monitoring, and Endpoint Detection and Response, and Mobile Device Management solutions;
- **Security alerts** use case needs logs from Network, Cloud Infrastructure and Applications, Firewall, Malware Scanning, Sandbox, Threat Intelligence, Geolocation, VPN Servers, and Physical Access solutions. Many of these sources will provide duplicative data, which the new SIEM must be able to factor in alert processing.

The migration team should ensure that the systems with the required log data exists to support each respective use case. If not, the team may need to re-prioritize the order of implementing use cases.

Determine if log files are available for each of the required assets. SOC analysts do not always own systems that generate data so some negotiation with owners may be required. To help encourage their engagement, be prepared to offer the owners the new intelligence that will be gleaned from the log data generated by the new SIEM. They may discover previous administration and remediation processes will become easier with the new SIEM.

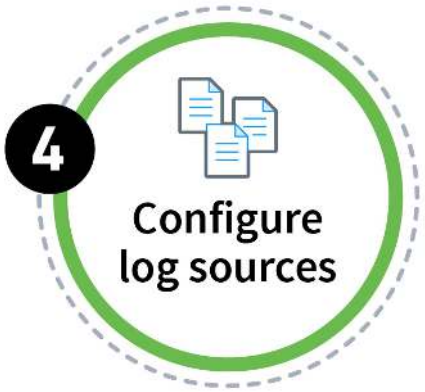
[3] For a list of data sources and other integrations, visit Exabeam.com to download the Exabeam Security Management Platform Integrations document

It's very important to determine how and where log data will be stored, and for how long. Storage is a huge limiting factor for legacy SIEMs that modern SIEMs are addressing with data lakes, sometimes with an option of being hosted in the cloud. A major benefit is that these architectures return quicker search results.

Finally, financial stakeholders will insist that the pricing model of your new SIEM can accommodate all the data you need to collect within budget.

Unlike legacy vendors who charge based on data volume, Exabeam provides a flat user-based pricing model for unlimited data collection and analytics by the SIEM.

Timeline: It usually takes 4-8 weeks to map the appropriate data sources to the use cases for your new SIEM. Timing depends a lot on whether use cases have been changed or added as you migrate to your new SIEM. Another big influence on timing is whether your security team is also changing other security tools in parallel with your SIEM migration as part of a bigger upgrade of security operations. Data sources are likely to change if your organization is undergoing a broader transformation of security operations.



Configuration of log sources is a non-trivial process. It entails far more than simply putting logs into configuration scripts. One option for success is to assemble a team with skills for configuration as this task may exceed capabilities of existing analysts. Your new SIEM provider can provide assistance if needed.

Configuration usually entails three steps; the first is enabling ingestion of log files, which may require building out infrastructure to ensure that log files can get into the SIEM and that each field of data is properly identified.

Next, you may need to create specific parsers to parse each field used in the log file for SIEM detection. Log files and naming conventions are not always clear, so creating parsers may entail some detective work. Some SIEM providers require you to do this work yourself, or will charge extra to do it for you.

Exabeam provides customers with more than 2,500 parsers for over 200 products to help them quickly make sense of logs. If a parser does not already exist for a particular data source, Exabeam customers can quickly get one at no extra charge, usually within days, by sending log samples to Exabeam. Customers can easily build their own parsers as well.

After clarifying parsers, move the legacy SIEM database of log files into the new SIEM. This will entail collaboration with storage, backup, IT operations, and compliance teams. Modern SIEMs are capable of ingesting and using vastly greater amounts of data, in the cloud if that is desired.

If your migration will entail temporarily running the legacy SIEM in parallel, the sources of log files will need to simultaneously feed data to the old and new systems in parallel or in sequence. Collaboration with respective log source owners and related IT infrastructure will be required to facilitate dual log feeds. Feed maintenance includes identifying systems that drop off, or new systems that are added but not feeding logs into the SIEM.

Timeline: Configuring log sources is one of the lengthiest steps in a SIEM migration. It can take 2-6 months. One of the key reasons this step can take so much time is that security operations teams are usually dependent on other members of the IT and security teams to set up the feeds.

Train SOC analysts in the approach of the new SIEM if you are moving from exclusive reliance on rules triggering alerts to models built using behavioral analytics based on machine learning. In most cases, behavioral analytics speeds detection, provides more accurate results, and enables rapid, precise response to critical incidents.

Your SOC analysts will need help understanding what capabilities the new SIEM provides. Using Exabeam SMP as an example, your new SIEM: (1) identifies the most important events requiring investigation; (2) provides a point-and-click dashboard to simplify and structure daily work; and (3) provides reporting for audit and compliance.

As part of content preparation, the migration team will need to ensure the new SIEM's dashboard, reports and alerting system meet requirements of use cases selected for migration. Modify reports if needed to match your new use case requirements.

Executives will be keen to ensure the new SIEM addresses requirements for compliance, which will vary by the company's industry. Your organization's Risk Manager can provide specific requirements.

Timeline: Preparing SIEM content takes 2-8 weeks. The time range is mainly due to the choice of use cases being implemented as some are more complex than others.

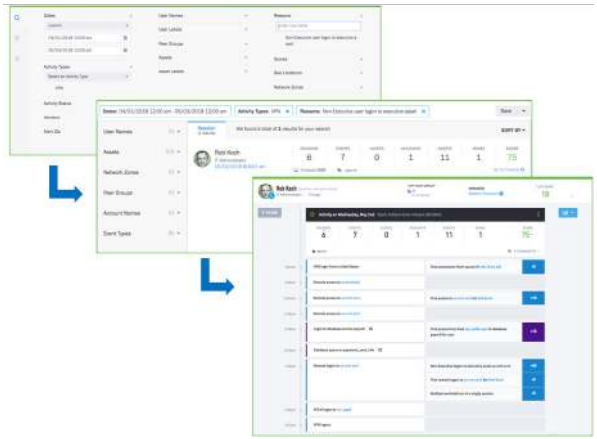
Getting good results from the new SIEM will require SOC analysts to adjust their daily operating processes. Analysts will especially want to know if they have to learn a new query language. A modern SIEM often has a point-and-click interface which alleviates the need for command line controls.

A critical point of understanding is how your new SIEM's alert-and-response system varies from the legacy SIEM. A new SIEM will exponentially reduce the number of false positives, "noisy" interruptions that could be ignored but demanded response actions.

Determine which SOC analysts are appropriate for new SIEM operations. A modern SIEM's ease of use allows Tier 1 analysts to do many things a more technically knowledgeable and experienced Tier 2 analyst was required to do with a legacy SIEM. Ironically, inaccurate results produced by legacy SIEMs often mired even the senior Tier 1 analysts in a reactive mode. Migration to a modern SIEM can improve everyone's productivity!

Speaking of productivity, another important realignment entails expectations of productivity for SOC analysts. A legacy SIEM query often requires hours to get search results, while a modern SIEM's results may appear in just a few minutes. This capability, coupled with instant response playbooks and machine-built timelines can immediately boost overall productivity for SOC analysts and allow them to focus on higher-priority issues.

THREAT HUNTING WITH PRE-BUILT TIMELINES



Legacy SIEMs typically require seasoned SOC analysts to handle threat hunting. Skills needed include deep security domain expertise, mastery of query languages, and the ability to interpret arcane results and determine how to proceed with an investigation. A modern SIEM with machine-built timelines can offer a better interface for threat hunting that's easily used by a junior analyst. Instead of presenting discrete events, a machine-built timeline presents the results with context and risk scoring to help rapidly distill the essence of a threat – and how to fix it if needed.

The migration team will need to review and tune operational processes and their playbooks defined for the initial phase of migration. A critical component for automating elements of instant response playbooks are the integrations with third party vendors to orchestrate remediation actions. Example solution integrations include asset discovery, cloud applications, endpoint detection and response, email, firewall, identity and access management, mobile device management, sandboxes and threat intelligence. Exabeam SMP has incident response integrations with over 55 vendors.

Finally, the migration team should document new SIEM processes for SOC analysts, auditors and other stakeholders. Definitely not an implementer's favorite task, but it's one that will pay big dividends after the migration.

Timeline: It can take as little as 2 weeks to learn how to use a new SIEM. However, it can take much longer to change habits and processes that were formed using the legacy SIEM. Another factor impacting timing is the degree of effort involved in documenting new processes and mapping old ones over to new ways of working in your new SIEM. As a result, it can take up to 4 months before new operational processes are fully defined and internalized.

Establishing benchmark criteria for the new SIEM will help your organization measure and evaluate its performance. Benchmarks should employ criteria in the framework or frameworks currently used by your organization. This could be ISO for compliance, PCI DSS for payment security, and operational benchmarks such as search times, mean time to detection, mean time to response, number of alerts closed, and so forth. A modern SIEM's analytics will often dramatically reduce the number of alerts generated by a legacy SIEM, so it's important to chose metrics carefully in order to accurately gauge success.

Benchmark criteria can be used to score use cases in a manner similar to a heat map. As the migration proceeds, SOC managers may first see lots of reds for a short period of time. As machine learning analyzes log feeds, more colors will turn yellow; as analytics mature, greens will show good coverage. Color coding benchmark criteria will visually show SOC managers how well the SIEM is aligned with business objectives addressed by each use case.

Tuning is an important aspect to benchmarking, which entails supplementing Red Team attack exercises by

using the new SIEM to test use case assumptions. Testing will help identify where mis-configurations and other issues are hampering accurate detection. To a large extent, a modern SIEM uses analytics to mostly tune itself.

Timeline: Establishing benchmark criteria is a relatively quick step in a migration project, taking 2-4 weeks, as it is completely under control of the security team and goals and metrics are typically well established.

The last strategic step of SIEM migration is evaluating next steps. A legacy SIEM typically requires SOC analysts to constantly adjust thresholds and alerts to keep monitoring accurate. Migration to a new SIEM with behavioral analytics enabled with machine learning does away with rule tinkering. This will allow your SOC team to focus on developing new use cases as business priorities change.

We suggest a rotation of every few months to review the use cases, determine which are useful, and which may need additional tuning.

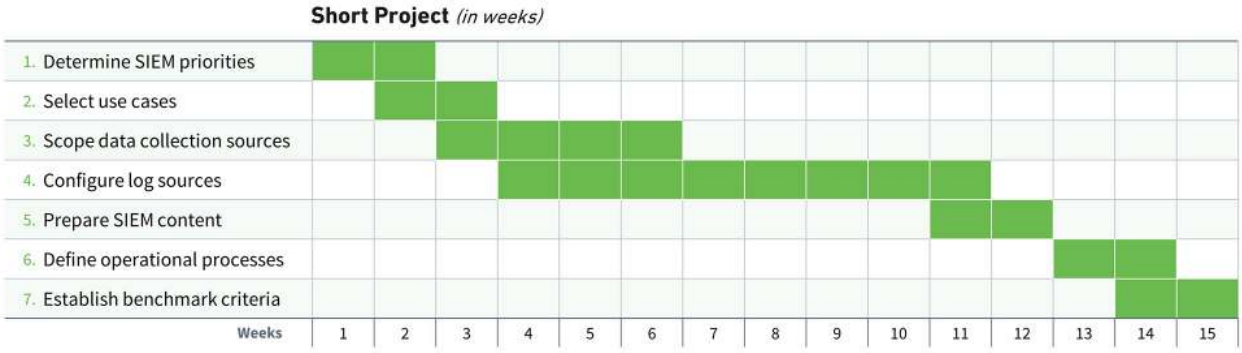
Attack simulations will help address improvements to achieve business objectives with the new SIEM. If your organization does not have Red Team capability in-house, consider turning to outside resources because attack simulations are essential for ensuring the quality of security processes.

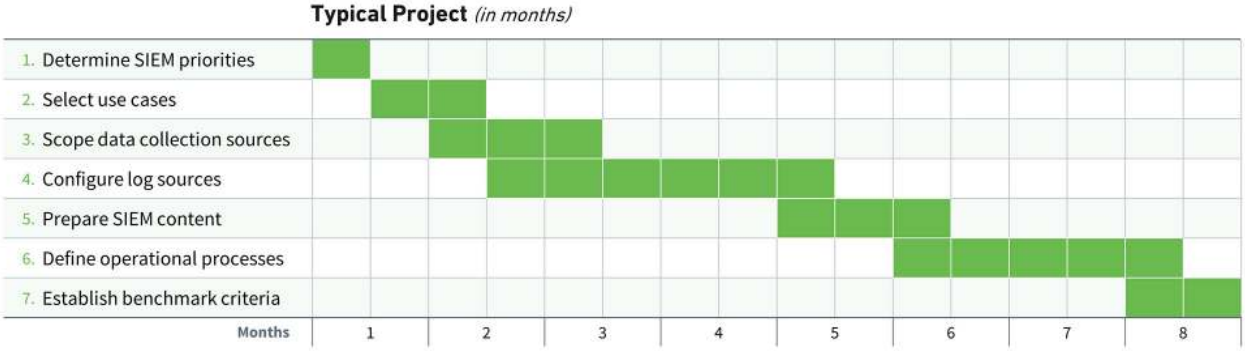
Finally, we urge your organization to use the eight-step SIEM migration model as a continuous process to help ensure strong security for your enterprise.

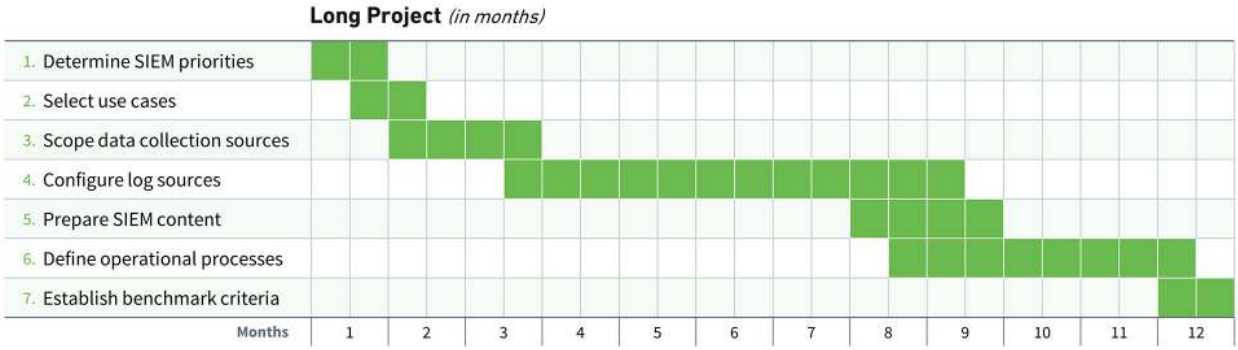
Timeline: Evaluating next steps is an ongoing task where the effort will wax and wane as circumstances change and new use cases are prioritized. Post-migration, you should be on the lookout for opportunities for constant process improvement.

TIMELINE

As this paper discusses, migrating a SIEM is a project that involves multiple steps and involves numerous people, processes and technologies. A typical migration takes 7-8 months. However, many factors can influence your timeline. A few of the most significant influences on timing are your choice of use cases, dependencies on others (including senior staff to outline the business priorities and other security and IT staff to provision log sources and infrastructure), and the willingness of the security team to change their work habits to take advantage of the capabilities of your new SIEM. As a result, the timeline for a SIEM migration can vary considerably, from 3-12 months. Example timelines for a short, typical and long migrations are outlined below.







CONCLUSION

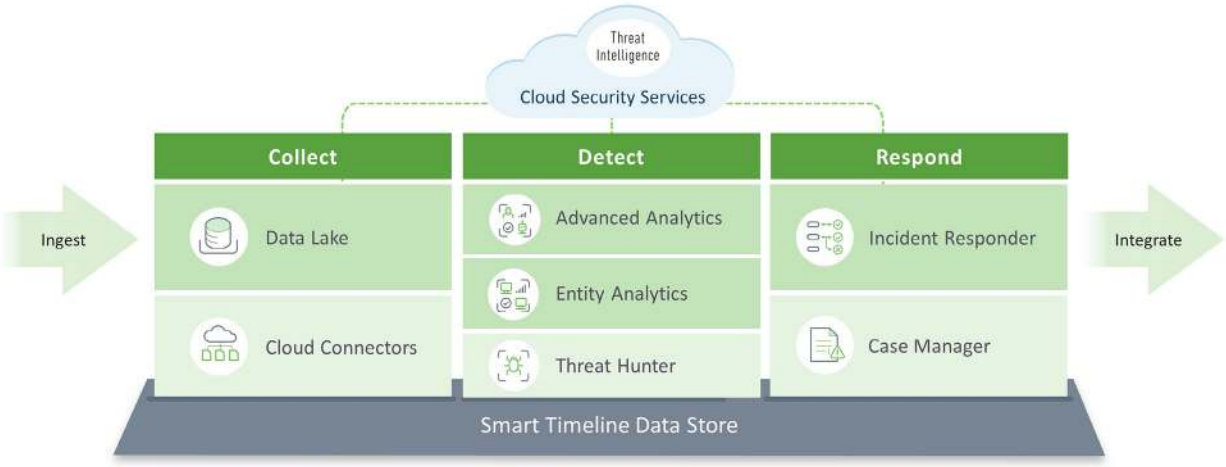
The executive decision to migrate a legacy SIEM will launch a journey touching many parts of the enterprise. This white paper has described eight steps to clarify how migration will proceed. The migration will entail people, process and technology, so planning and execution will need to address all three of those elements.

Process is an integral part of the eight considerations, and implementation will directly affect daily roles of some stakeholders – particularly people in the Security Operations Center. We encourage your organization to approach migration with a positive look to new benefits that will begin appearing during the course of this process.

By approaching security with a new SIEM, your enterprise will enable better security and compliance. As the technical enabler, the new SIEM will also help stakeholders be more productive and fruitfully engaged in this vital mission.

NEXT STEPS

A new SIEM will unlock fresh capabilities to bring stronger security to your enterprise. We hope Exabeam will play a prominent role in your choice. To learn more about migrating your SIEM, please contact Exabeam or one of our services partners. They can provide you with legacy SIEM-specific information to help guide the technical migration process.



THE EXABEAM SECURITY MANAGEMENT PLATFORM CONSISTS OF 7 PRODUCTS, A THREAT INTELLIGENCE SERVICE AND SMART TIMELINES

exabeam

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We empower enterprises to detect, investigate, and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines™, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques, and procedures. https://www.exabeam.com.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.