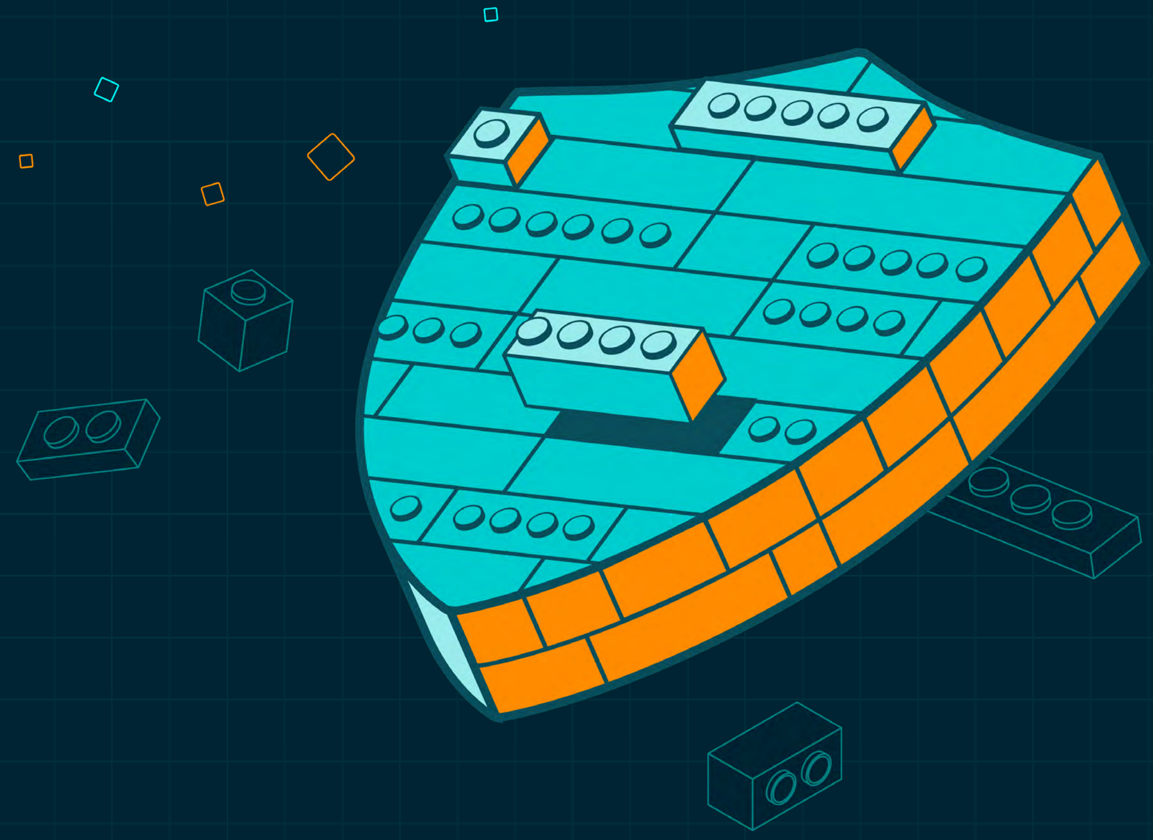
WHITEPAPER

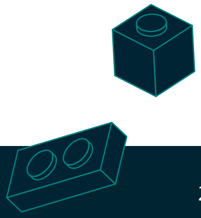
Eight Steps to Mastering Your **SIEM Migration**

Build a modern, vendor-agnostic security data strategy while de-risking your SIEM migration and enhancing threat detection.



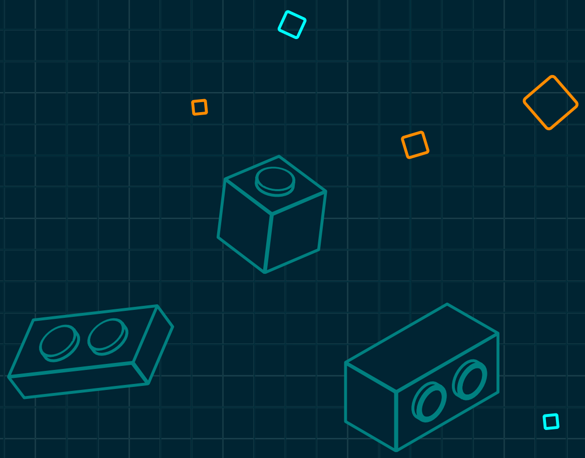
Cribl®

CONTENTS



2025

Organizations deploy Security Information and Event Management (SIEM) platforms as a foundational layer in their multi-tiered security architecture. These platforms enable real-time threat detection, incident response, and compliance enforcement.

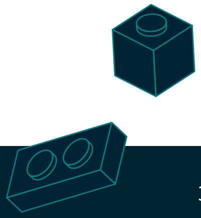


The cybersecurity landscape is changing. Evolving regulations, increasing telemetry, aggressive threats, and staff shortages are prompting security teams to rethink their SIEM architectures. Although SIEM is central to detection and response, its implementation overwhelms Security Operations Centers ("SOCs"), making overstressed analysts less effective and risking missed breach indicators. As outdated SIEM vendors struggle, new solutions promise better detection and automation. Security teams want to migrate, but few know how to do so efficiently, effectively, and without the risk of degrading the enterprise's security posture.

This whitepaper provides eight strategic steps to guide a SIEM migration, setting your organization on the course for an effective and efficient detection, response, and research program. It highlights the advantage of using Cribl's data engine for IT and Security data framework to:

1. **De-risk and accelerate** your SIEM migration
2. **Modernize** your security data strategy
3. **Decouple your SIEM** and, most importantly, your data from vendor lock-in

This guidance is tailored for leaders and key technical stakeholders to ensure the successful execution of a SIEM migration project and the long-term success of an organization's entire cybersecurity detection, response, and research program, which may include the SIEM, data lake, threat hunting, UEBA data platforms, and more.



Why migrate to a new SIEM?

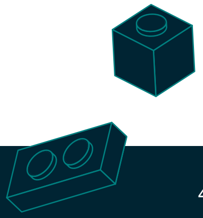
Cyberattacks are on the rise, but there aren't enough skilled security analysts to keep up. Telemetry data is also growing at a staggering rate of 28% CAGR, creating massive implications for storage and analysis. This exponential growth in data volume challenges organizations to find cost-effective ways to store, process, and derive value from their security telemetry.

At the same time, businesses are dealing with more security events and devices than ever before, putting a heavy strain on their SIEM systems. This further challenges security teams, who often waste valuable time responding to false alarms or irrelevant alerts. Many of these issues stem from outdated SIEM technology.

> According to a recent IDC Survey Spotlight, companies want to replace their SIEM for cost, functionality, ease of use and better data management.
>
> Source: IDC's Worldwide Views on SIEM Survey, January 2024.

Even though companies invest heavily in these systems, they often feel stuck with their existing tools due to budget constraints and vendor lock-in. Older SIEMs come with several significant drawbacks:

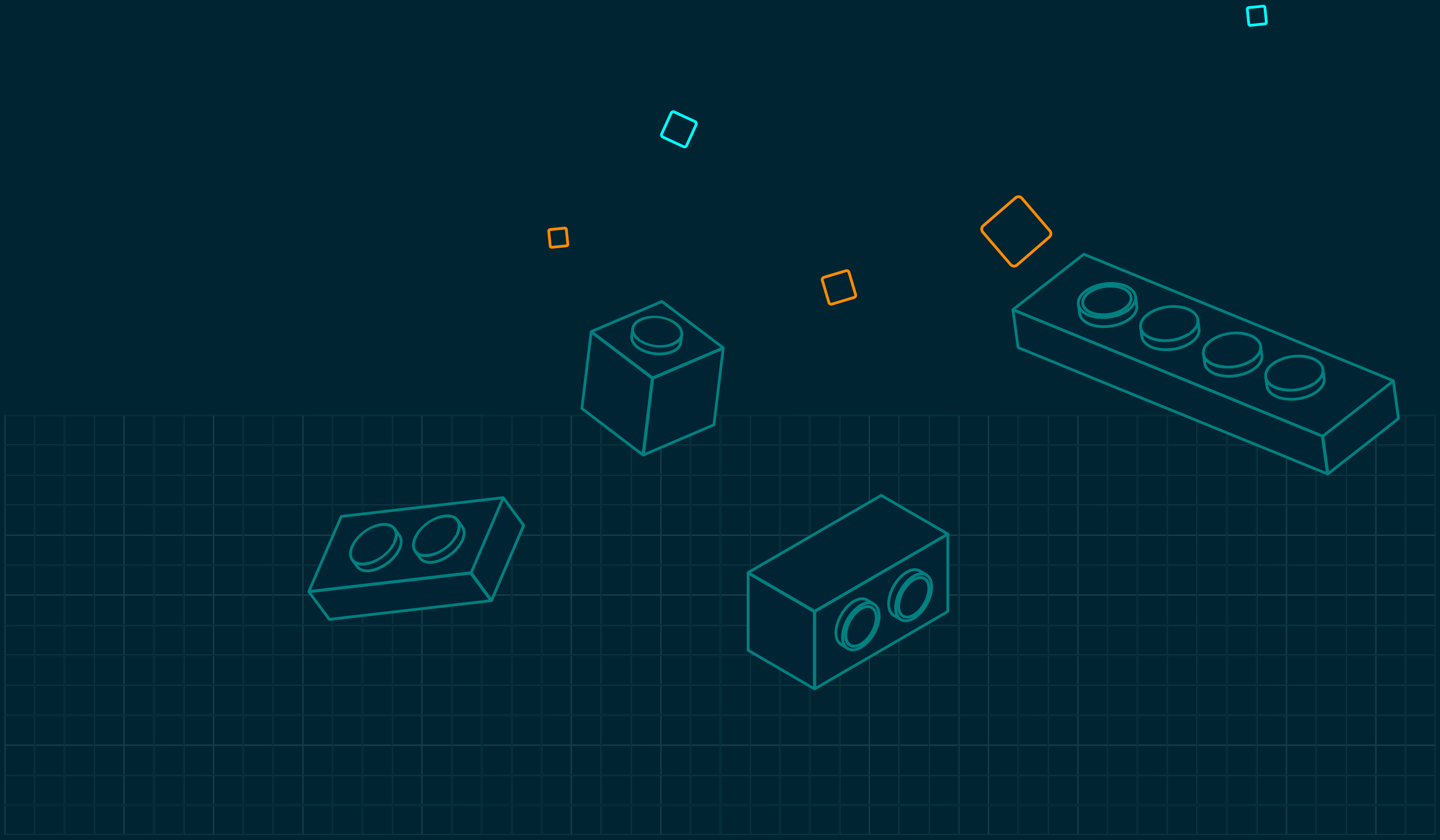
- **High storage costs**: As businesses adopt modern security approaches like zero-trust policies and cloud-based services, they generate massive amounts of security data. Older SIEMs store logs indiscriminately, leading to rising storage costs without adding meaningful security benefits.
- **Inability to track complex attacks**: Legacy SIEMs often fail to connect the dots when attackers move across different systems. Hackers may use stolen credentials to access networks in unrelated ways, making it harder for security teams to see the full picture. This fragmented approach increases the chances of missing serious threats.
- **Failure to detect new threats**: Many traditional SIEMs depend on basic rules and third-party alerts to identify risks. However, these outdated methods struggle to detect new and evolving cyber threats, making organizations more vulnerable.
- **Slow, manual investigations**: Older SIEMs lack automation for critical security tasks. As a result, security teams must manually piece together attack timelines and incident reports, which is time-consuming and inefficient. This slows down response times and increases the need for skilled analysts—who are already in short supply.



With these drawbacks, it is easy to see why enterprises are looking for better options. Legacy SIEM implementations are struggling to support effective detection and response processes. Teams need better options. While the desire to migrate is strong, organizations cannot simply hit a switch to move from one product to another. The business must still be protected. By using a telemetry pipeline, like Cribl Stream, security teams can migrate to a next generation SIEM while maintaining three core requirements:

1. Preserving full security posture during the migration process
2. Porting only optimized data to the new SIEM platform
3. Maintaining control over data ingest and data quality for the new SIEM platform

Before switching, stakeholders must consider how these changes impact existing workloads and plan accordingly. The following sections explore these factors in more detail.



Process of SIEM Migration leveraging a telemetry pipeline

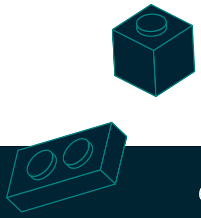
According to a recent IDC Survey, a top SIEM challenge is that data ingestion is too complex and expensive.

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

Any SIEM migration is a complex process. The data is often intricate, and SIEM content is vendor-specific, meaning that transitioning to a new platform requires time and training. Furthermore, security teams may not be the only users of the SIEM's capabilities. Years of effort have gone into legacy SIEM platforms, and it's not unusual for the scope to extend to non-security teams that utilize the data for operational purposes. These non-security workloads must be considered, and a decision needs to be made regarding where these workloads will exist post-migration. A SIEM migration requires extensive planning, and it is essential to develop a strategy around the process to ensure it is done correctly the first time and to minimize rework.

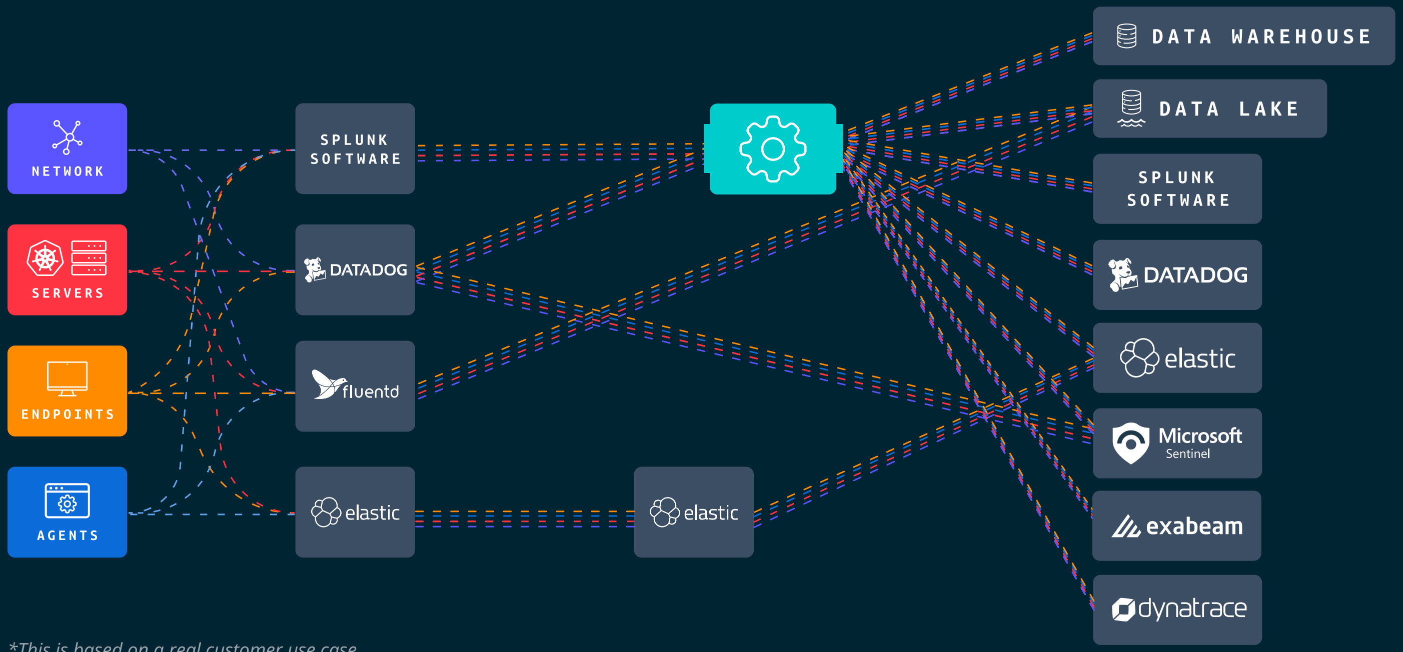
As organizations strive for greater agility and efficiency in their security operations, a modern data architecture—particularly when enabled by a telemetry pipeline—provides a flexible and scalable foundation. This approach allows teams to optimize their existing SIEM deployments, accelerate the adoption of new security tools, and seamlessly transition between platforms as their needs evolve. By decoupling data ingestion from specific SIEM solutions, security teams gain the freedom to adapt quickly to changing threats, improve resource utilization, and enhance overall system performance, regardless of their current SIEM infrastructure or future technology choices.

A telemetry pipeline accelerates and de-risks a SIEM migration because it sits between an organization's sources and destinations to support feeding the legacy SIEM and the new SIEM simultaneously. This enables the business to maintain its security posture in the legacy SIEM while cloning the full production dataset to your *new* SIEM. This powerful capability enables the migration team to build content in the new SIEM and thoroughly test everything without risk to its security posture. No ugly hacks or hard cutovers are required. No testing with sample data. The team knows its new content will work, materially lowering risk when the SOC cuts over to the new SIEM. Moreover, modern telemetry pipelines like Cribl Stream give teams a robust user experience that will accelerate every aspect of collecting and managing data, so less time is spent on data collection and more time is spent on getting value from the data.

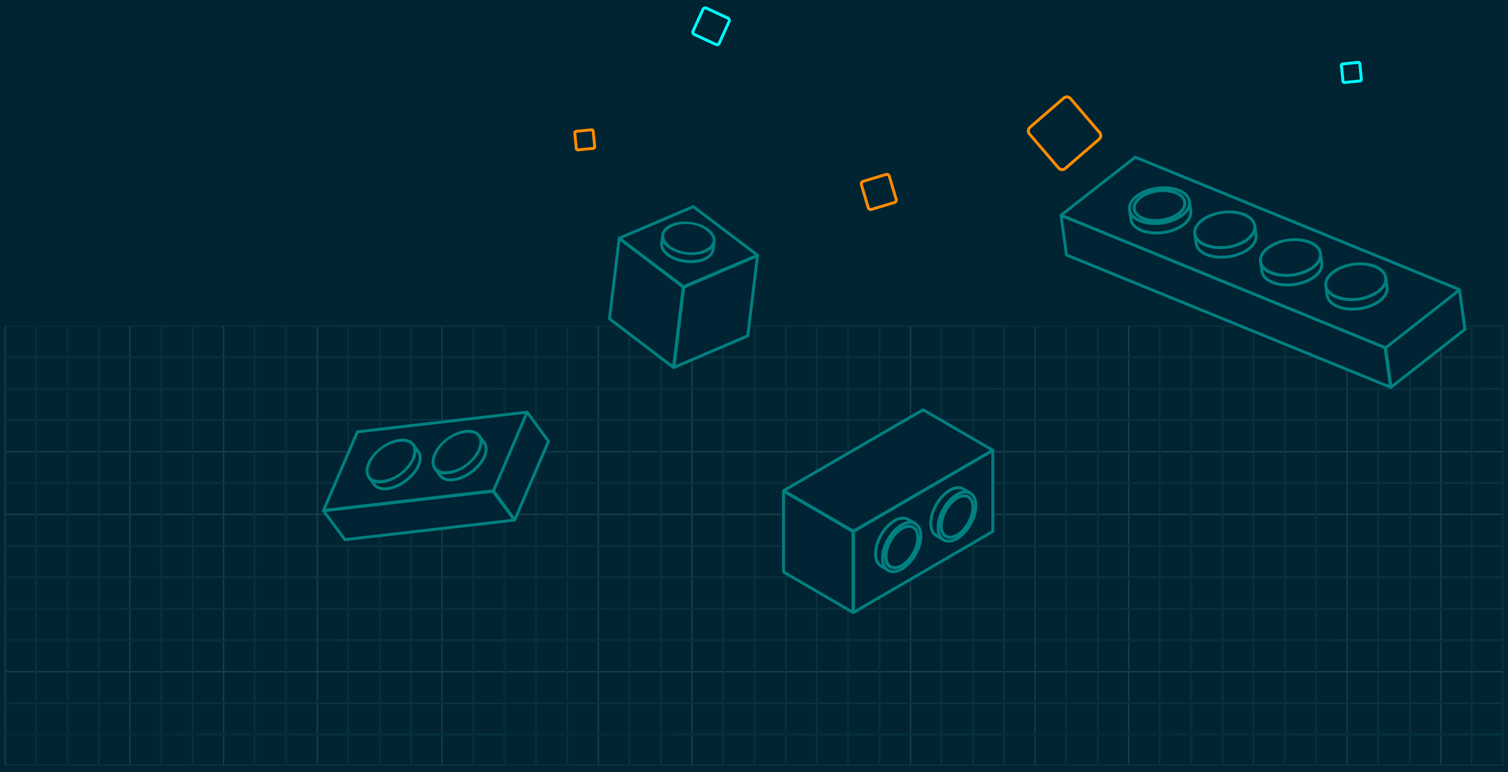


BEFORE

The Reality of Data Growth*

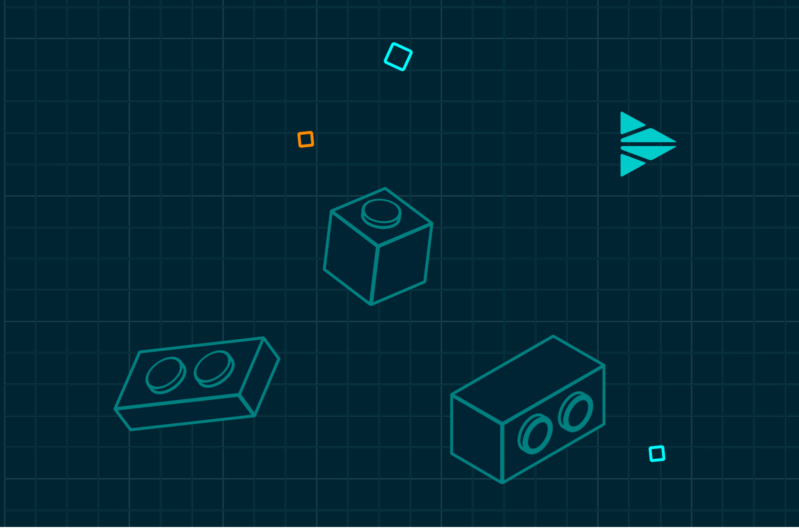


*This is based on a real customer use case.



2025

The Eight Steps of a SIEM Migration



STEP 1 Define SIEM Priorities

Setting clear SIEM priorities is crucial for a successful migration. These priorities define success criteria and guide the migration strategy. Before setting strategy, there are some important steps to address:

- **Collaboration and stakeholders:** Since SIEM migration impacts multiple areas of an enterprise, collaboration with stakeholders is essential to identify critical data, systems, and security assets—such as intellectual property, customer records, financial data, personnel files, and network infrastructure. Recognizing the organization's "risk assets" ensures protection against significant business risks.
- **Risk and Compliance:** Align SIEM priorities with risk management frameworks and regulatory requirements. Engaging executives early helps integrate business objectives with IT strategy, ensuring compliance and efficiency.
- **Existing Use Cases:** Understand all the workloads your legacy SIEM supports and if any non-security teams are involved. These workloads will need to be addressed and cannot be orphaned post-migration.

Migration Strategy

Define your migration approach. Will it be phased, modular, or a complete replacement? Some organizations enhance legacy SIEMs with new capabilities like behavioral analytics or automation, while others prefer a gradual transition. When planning decommissioning timelines, consider factors like legacy SIEM license renewals.

The best practice is a phased migration enabled by placing a telemetry pipeline, like Cribl Stream, between your sources and destinations. This will establish a common data plane that will give your Security Engineering team complete control over your data. Full data flow is maintained to your legacy SIEM with no changes. A second copy of your data is cloned to your new SIEM platform. This data is optimized for your new SIEM. This pattern enables a phased cutover and thorough testing of your content as it is rebuilt on the new platform while maintaining your security posture in the legacy SIEM. A telemetry pipeline also enables data to be shared outside of the SIEM to support non-security workloads so these teams are not forgotten post-migration.

Migration Strategy Timeline

Identifying stakeholders and aligning on priorities typically takes four to six weeks. This phase includes determining workloads and establishing change controls to manage upcoming transitions effectively.

STEP 2

Optimizing Use Cases for SIEM Migration

Legacy SIEMs may support dozens or even hundreds of use cases, but not all need replication in a modern SIEM. Newer systems enhance efficiency by reducing reliance on complex correlation rules and increasing automation. When deciding which use cases to carry over, prioritize those that align with the business's security objectives and address key threats. Do not carry over the technical debit of your legacy SIEM to your new SIEM.

Selecting Use Cases

Prioritize use cases based on business impact, event frequency, and potential consequences. Ignoring business relevance can lead to ineffective outcomes. Common use cases include detecting insider threats, compromised credentials, account activity, high-risk employee monitoring, endpoint analytics, and alert prioritization. Framing these within broader risk management initiatives—such as threat detection, process control, and asset protection—can engage executives who may not be familiar with technical specifics. The MITRE ATT&CK® framework is a valuable resource for mapping adversary tactics and techniques.

Strategic Implementation

Technical teams should focus on protecting critical business functions and sensitive data rather than replicating every previous use case. A phased approach starts with high-priority use cases, integrating others over time as the team gains experience with the new SIEM. Giving engineering time to master the new SIEM is critical to the migration process.

Each use case should clearly define the following:

People
Who will handle tasks?

Process
How will tasks be executed?

Technology
What capabilities does the new SIEM provide?

Evaluating how the new SIEM supports each use case ensures a smoother transition. Remember that this work can be done in isolation. A telemetry pipeline will be used to clone your production data to your new SIEM, allowing engineering to fully test your content to ensure it fits your framework and is optimized for your new SIEM. Since the new SIEM is getting the full production data stream, new content can be thoroughly tested for functionality and scalability.

Use Case Timeline

Depending on alignment with business and security needs, selecting relevant use cases typically takes two to four weeks. While security teams generally understand existing use cases, this period is crucial for assessing new capabilities that the legacy system may not have addressed.

STEP 3

Optimizing Data Collection for SIEM Migration

The primary goal of a SIEM platform is to help analysts quickly detect and respond to security threats by integrating telemetry data from various IT and security tools. Effective threat remediation requires collecting and correlating data from multiple sources, including:

- **Infrastructure**
  Servers, network devices, firewalls, endpoints, operating systems
- **Applications**
  Databases, directory services, cloud environments (public, private, hybrid)
- **Contextual Sources**
  HR systems, configuration management databases
- **Security tooling**
  EDR, WAF, CNAPP, XEM, DLP

PHASE A

Assess & Integrate Log Data

Start by evaluating your current log access and aligning data with key SIEM use cases:

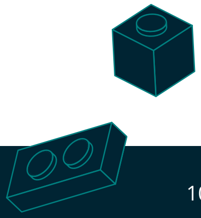
- **Insider threats:** Logs from DLP, email management, database activity, PAM, IAM
- **Compromised credentials:** Logs from authentication, IAM, CASB
- **Account creation and management:** Logs from PAM, IAM
- **Endpoint anomalies:** Logs from EDR, MDM, endpoint monitoring
- **Security alerts:** Logs from firewalls, cloud infrastructure, malware scanning, sandboxing, threat intelligence, VPNs, physical access systems

While some logs may contain overlapping data, the telemetry pipeline can handle data quality so the new SIEM is not flooded with confusing or duplicate data. This will improve data quality, leading to better outcomes and saving money. Evaluating how the new SIEM supports each use case ensures a smoother transition. Remember that this work can be done in isolation. A telemetry pipeline will be used to clone your production data to your new SIEM, allowing engineering to fully test your content to ensure it fits your framework and is optimized for your new SIEM. Since the new SIEM is getting the full production data stream, new content can be thoroughly tested for functionality and scalability.

PHASE B

Engage Stakeholders & Secure Access

Since SOC analysts may not control all forms of machine data or telemetry, collaboration with system owners is essential. Standards and business priority are vital so all teams will work with security to accomplish this complex task with as little friction as possible. Priority is critical and should be secured with some sort of mandate from leadership.



PHASE C

Plan Storage & Retention

The telemetry pipeline will enable engineering to align data cost with value by tiering data where it most makes sense. Decoupling is the key. Why lock up your data in your most expensive platform and in a vendor specific format? Critical data that is needed for detections is forwarded to the SIEM, but bulk data sources that are only needed occasionally are kept in data lakes based on object storage so that data is retained as required but stored at the lowest possible cost point instead of in the SIEM. The telemetry pipeline enables engineering to retrieve data as required from these data lakes back into the SIEM when and if needed. All of these functions are enabled and orchestrated by the telemetry pipeline. Ensure your new SIEM's pricing model aligns with your data collection needs and budget.

PHASE D

Data Collection Agents

A key question often forgotten is which agent will collect endpoint data. This is a nuanced question worth some thought. Usually, the legacy SIEM comes with an agent, but that agent won't let you send data to your target SIEM. Your options are limited to existing legacy data collection models. This is where a modern telemetry pipeline gives teams both choice and control over their data.

A vendor-agnostic telemetry pipeline like Cribl Stream can work with the agent you have in place, sending data to both your legacy and target SIEMs simultaneously. This minimizes your displacement costs since you can point the legacy agent at Stream and then get all the benefits with minimal complexity. This positions your team to get full value from your data with Stream and complete your SIEM migration. The issue is that SIEM decommissioning may require removing the agent. Check your license agreement since you do not want to be forced to pay a settlement because of an oversight.

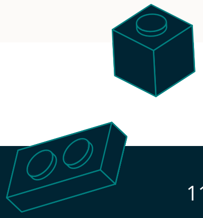
If the agent has to be replaced, your team has several options. Cribl Stream supports almost every available data collection agent, plus Cribl offers its own agent, called Cribl Edge. It is a flexible endpoint telemetry collection agent that is incredibly easy to use. Edge provides teams with a robust user experience, allowing admins to configure essential features like log and metrics collection and also to install pipelines for managing data at the edge. It offers remarkable flexibility that teams love to explore. One last piece of advice: Consider staging the agent replacement after implementing Stream. Teams that try to replace the agent and implement Cribl Stream at the same time tend to get bogged down with too much complexity. It is better to make one change at a time to manage the rate of change.

Data Collection Timeline

Mapping log sources to use cases typically takes four to eight weeks, depending on:

- Availability of pre-built integrations
- Changes in use cases during migration
- Updates to other security tools as part of broader security transformation
- Keeping your existing agent or replace it

A well-planned data collection strategy ensures a smooth SIEM migration, enhancing threat visibility and security operations.



STEP 4

Configuring Log Sources for SIEM Migration

Log source configuration is a critical and often time-consuming aspect of SIEM migration. It involves carefully setting up and optimizing the various data sources that feed your SIEM. This process ensures that your new SIEM receives all the necessary data in the correct format for effective threat detection and analysis. Proper planning and collaboration help streamline this process, ensuring seamless data integration and reliable security monitoring in the legacy SIEM while getting the new SIEM ready for cutover.

Now, let's dive into the specific steps for configuring SIEM log sources into your telemetry pipeline:

1. Onboard Required Data Sources

- Ensure telemetry is properly integrated into the telemetry pipeline. Cribl Stream supports numerous out-of-the-box data sources and offers nearly unlimited support for custom data sources.
- Infrastructure may need expansion to support log ingestion at scale.
- Given the complexity of this process, a dedicated team is recommended to maintain focus and consistency.

2. Develop and Implement Parsers

- Log parsing is essential for accurate threat detection, requiring field-specific parsers to interpret log data. This process ensures your data is fully aligned and optimized with your new SIEM.
- Logs often have unclear naming conventions, making parser development a technical challenge. Cribl Stream offers a range of options to best suit the team's needs and their new SIEM, including a rich UX that will help engineering normalize data sources faster than previously possible.

3. Clone and Synchronize Log Data

- Clone telemetry to the new SIEM, coordinating with storage, backup, IT operations, and compliance teams.
- Validate that all data is in scope and the data is optimized for the new SIEM. Engage your SIEM vendor to validate that data is optimized and being parsed as expected.
- Ensure the tiered data storage strategy is implemented and no extraneous data is forwarded to the new SIEM.

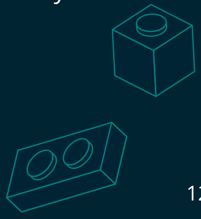
4. Telemetry Agent Replacement

- Roll out new agents in stages using Stream as the destination.
- Minimize change by keeping collection patterns and formats as close as possible to a one-for-one replacement.
- Validate formats and adjust Stream configs as required.
- Remove the old agent and enable the new agent.
- Validate SIEM content and test detections.

Log Configuration Timeline

Configuring log sources is one of the most time-intensive aspects of SIEM migration, typically taking two weeks to six months. The duration depends on:

- The number of log sources and their complexity.
- Coordination with IT and security teams across multiple locations.
- Setting up local collectors for geographically distributed environments.
- Replace the existing telemetry agent.



STEP 5

Preparing SOC Analysts and SIEM Content for Migration

Your SOC analysts must familiarize themselves with the new SIEM's capabilities. For example, a modern SIEM platform can:

1. Prioritize critical security events that require investigation
2. Provide a user-friendly dashboard to organize daily tasks
3. Generate reports for audit and compliance purposes

Analyst training is essential when transitioning from a rule-based alert system to one leveraging behavioral analytics and machine learning. Modern SIEM platforms leverage behavior and risk-based detections that require significant training. Yet again, having your production dataset cloned to your new SIEM enables realistic training and process validation without the on-the-job training that is typical when a telemetry pipeline is not powering a SIEM migration.

Training must be a focus for the SIEM migration to be a success and not compromise the company's security posture.

Configuring SIEM Content

To ensure effective migration, the SIEM content must support selected use cases, including:

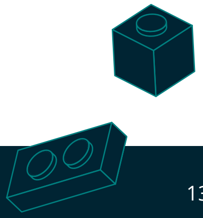
- **Dashboards & Reports**: Customizable for visibility into security trends and compliance
- **Correlation Rules & Anomaly Detection:** Aligning automated threat detection with security objectives
- **Case Management & Alerts:** Ensuring timely and relevant notifications

Compliance Considerations

The GRC team must confirm that the new SIEM meets industry-specific compliance requirements. Risk managers should define these criteria, and dashboards should be sortable by compliance categories to streamline audits.

Content Preparation Timeline

Configuring SIEM content typically takes four to ten weeks, depending on the complexity of the implemented use cases.



STEP 6

Optimizing SOC Analyst Productivity During SIEM Migration

Transitioning to a new SIEM requires adjusting productivity expectations for SOC analysts. This includes training on new tools, refining workflows, and updating operational playbooks to align with the modern system's capabilities.

Boosting Productivity with Faster Search & Automation

Legacy SIEMs often take hours to return search results, while modern systems deliver results in minutes. With automated response playbooks and real-time threat timelines, analysts can focus on high-priority security incidents instead of manual investigations.

Adapting to New Operational Processes

Migrating to a modern SIEM introduces changes in daily SOC workflows, leading to common questions such as:

- **Will analysts need to learn a new query language?**

  Many modern SIEMs offer intuitive point-and-click interfaces, reducing reliance on command-line queries. Some also use natural language processing (NLP) to simplify complex searches.

- **How does the alerting system compare to the old SIEM?**

  New SIEMs reduce false alarms, allowing analysts to focus on genuine threats rather than unnecessary alerts.

Enhancing Analyst Capabilities

A modern SIEM is easier to use, enabling Tier 1 analysts to handle tasks previously reserved for Tier 2 analysts, such as advanced query writing and rule creation. In contrast, legacy SIEMs often produce excessive or inaccurate alerts, forcing even senior analysts to spend time filtering out irrelevant data. By minimizing noise and automating repetitive tasks, a modern SIEM boosts efficiency across all analyst levels, leading to a more proactive security approach.

Refining Playbooks & Automating Response

During migration, the team must review and refine SOC workflows and incident response playbooks. Automating key response actions—including integrations with third-party vendors, ticketing systems, and IT teams—can significantly improve Mean Time to Respond (MTTR), a key measure of SOC efficiency.

Documenting New SIEM Processes

Comprehensive documentation ensures smooth post-migration operations. While not the most exciting task, documenting new processes for SOC analysts, auditors, and stakeholders is essential for maintaining operational continuity.

Training & Process Adoption Timeline

- Basic SIEM training: As little as two weeks
- Full adoption of new workflows: Up to four months, depending on how quickly teams adjust to new processes
- Operational efficiency improvements: Metrics should be carefully selected to measure alert reduction and analyst productivity gains

Migrating to a modern SIEM improves efficiency, accuracy, and automation, leading to a more agile and effective SOC.

STEP 7

Establishing Benchmark Criteria for SIEM Performance

Setting benchmark criteria for your new SIEM ensures measurable and effective performance evaluation. That which cannot be measured cannot be graded for effectiveness. These benchmarks should align with existing frameworks such as:

- ISO (compliance standards)
- PCI DSS (payment security)
- Operational metrics like search times, Mean Time to Detect (MTTD), and Mean Time to Respond (MTTR)

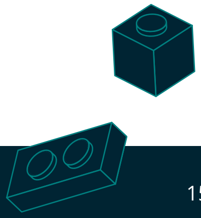
Benchmark criteria can be visually represented in a heat map to score use cases. Initially, SOC managers may observe many areas marked in red, indicating weaknesses that need improvement. Over time, as teams get more skilled, data quality improves and ML models learn, these areas will shift to yellow, reflecting gradual improvements. Eventually, as analytics mature and demonstrate effective security coverage, these areas will turn green, indicating that the SIEM is successfully meeting business objectives.

Tuning plays a crucial role in benchmarking. This process includes Red Team attack simulations to test and fine-tune the system. Regular tuning and testing help identify misconfigurations or weaknesses that could impact detection accuracy. Many modern SIEMs incorporate self-tuning analytics, which further optimize performance over time.

Benchmark Timeline

- **Setup Duration:** Expect two to four weeks, as this process is fully within the security team's control
- **Ongoing Review:** Evaluate use cases every few months to ensure effectiveness
- **Attack Simulations:** Test regularly to refine benchmarks to align with business objectives

If in-house Red Team capabilities are unavailable, consider hiring external security experts to conduct attack simulations, ensuring a robust security posture.



STEP 8

Evaluating the Next Steps in SIEM Migration

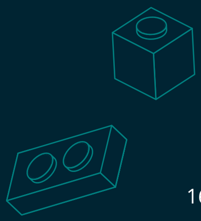
The final phase of SIEM migration involves evaluating next steps to ensure continuous security improvements. Unlike legacy SIEMs, which require constant manual adjustments to thresholds and alerts, modern SIEMs leverage behavioral analytics and machine learning to automate threat detection, reducing the need for manual rule adjustments. This shift allows SOC teams to focus on developing new use cases as business and security priorities evolve as long as data quality is high and represents the environment. Data quality makes these advanced processes work, so it is crucial to leverage the telemetry pipeline to monitor data drift and quality and take immediate action if an issue occurs. This has to be a continuous process, a proactive process, in order to not have a degraded security posture.

SIEM as an Ongoing Process

SIEM migration should not be viewed as a one-time project but as an ongoing process to maintain a strong security posture. Organizations should continuously review and refine processes, ensuring the SIEM adapts to emerging threats and business needs. Governance is everyone's job and cannot be forgotten.

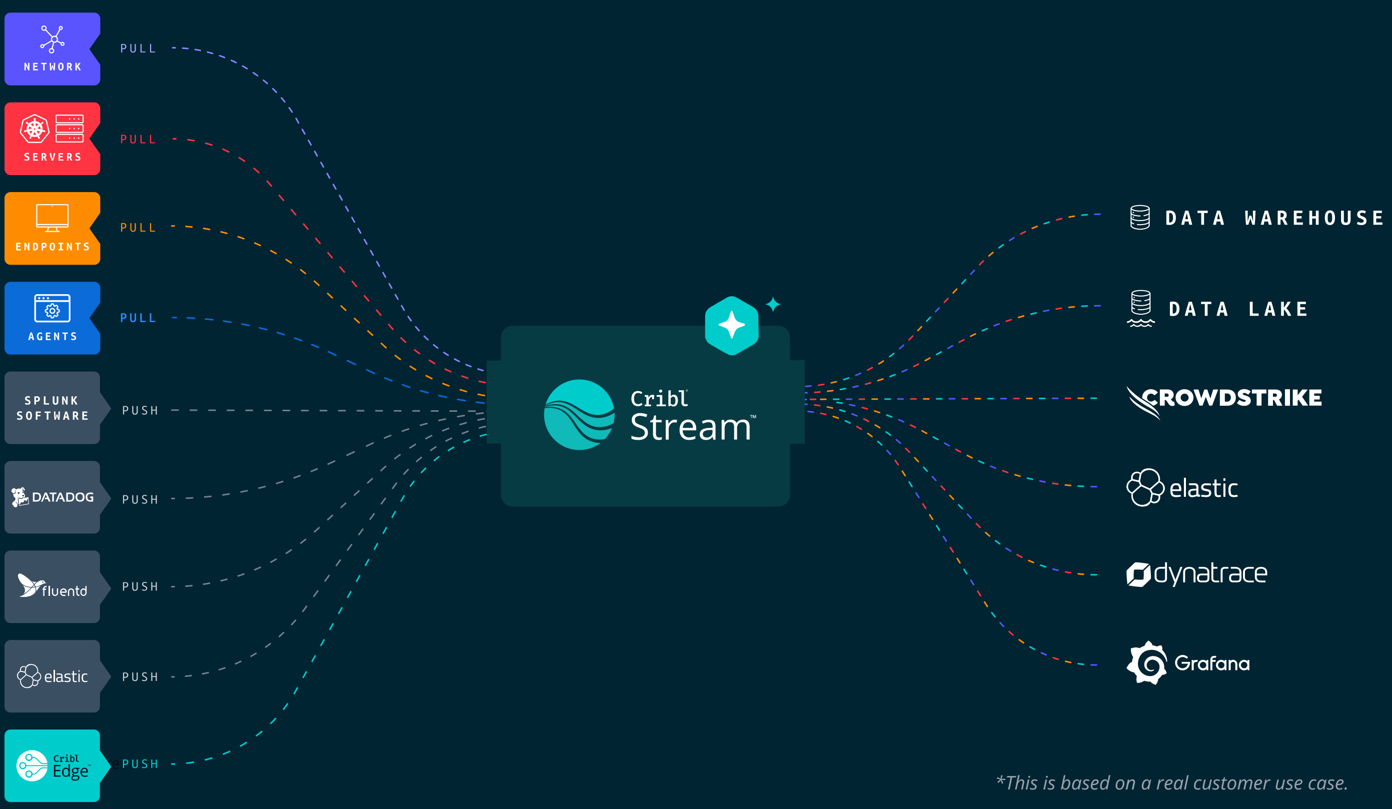
- **Ongoing Process:** The evaluation of next steps is a continuous effort, with the level of involvement varying based on changing security landscapes.
- **Post-Migration Improvements:** Regularly assess opportunities for process enhancement, ensuring the SIEM remains effective against evolving threats.

Organizations should initiate a SIEM migration project to jumpstart a broader security data strategy. This approach will prevent past mistakes from happening again, allowing organizations to maintain optimal security operations and improve their overall cybersecurity investment. Effective cybersecurity starts and ends with your data. It must be the focus of your program to ensure long-term success.

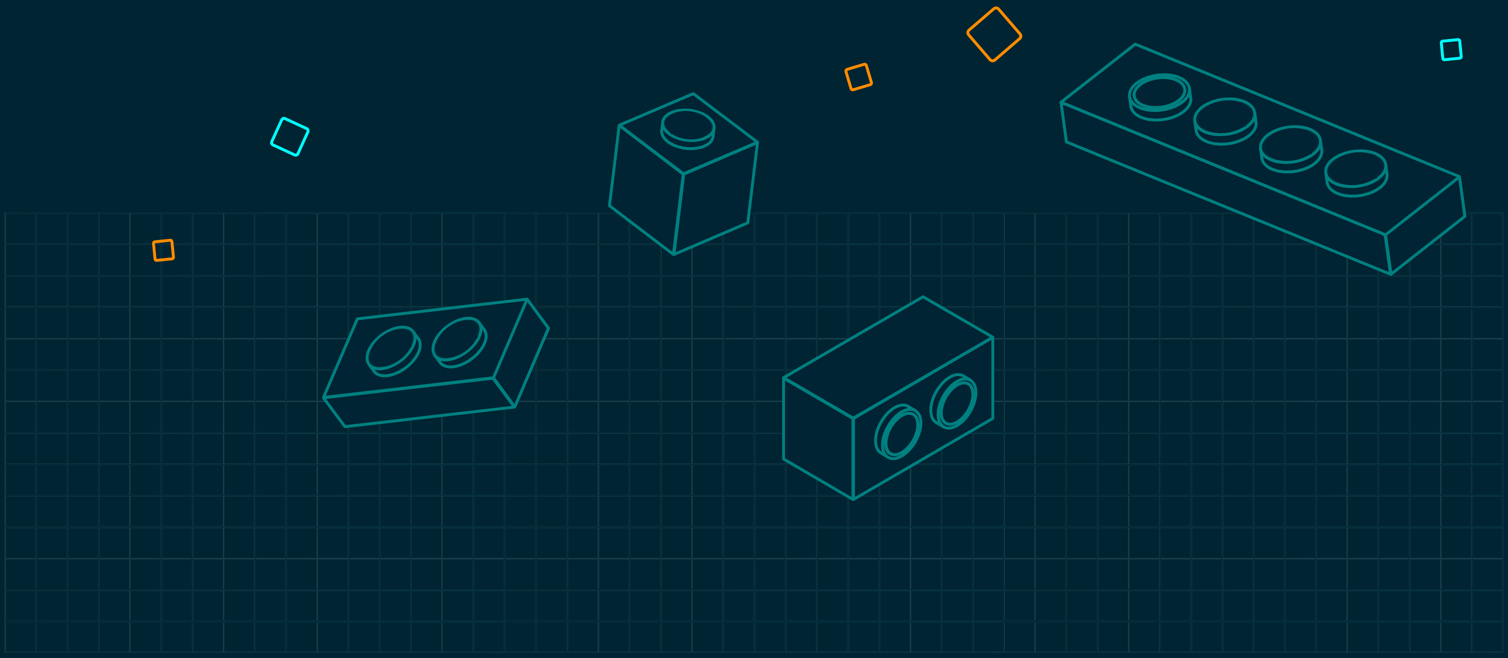


AFTER

Driving Security Outcomes Through Better Data*



*This is based on a real customer use case.



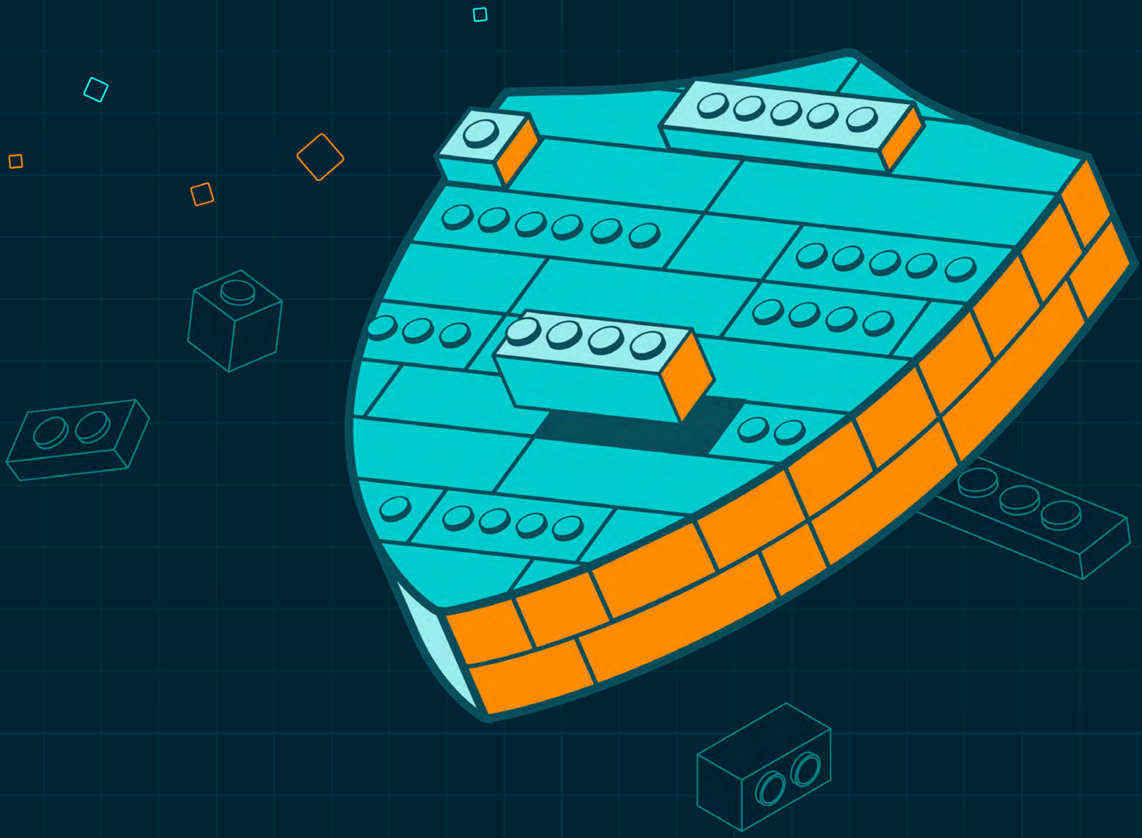
Conclusion

Migrating from a legacy SIEM is a significant decision that can potentially impact the entire enterprise. Instead of viewing it as just a technology shift, organizations should see it as an opportunity to unlock new efficiencies, enhance security, and streamline operations. The migration process offers tangible benefits, including improved threat detection, automation, and better alignment with evolving business needs. It also positions the organization to avoid the pitfalls of the past by using a telemetry pipeline to optimize costs and derive more value from its data moving forward.

Better results begin with better data, which is why every organization should consider developing a security data strategy as part of a SIEM migration. Seize this opportunity to address your technical debt and position your teams for future success by utilizing a telemetry pipeline like Cribl Stream, ensuring your teams collect the right data in the best possible format to derive maximum value from your new SIEM. This also enables your teams to enhance data portability and reduce vendor lock-in by decoupling your data ingestion process from your SIEM. With a telemetry pipeline implemented, your teams can on-board new data significantly faster and share information seamlessly across the enterprise. It is your data, and you are no longer constrained by your SIEM vendor.

The steps outlined above offer a framework for a successful migration, addressing the critical components of people, processes, and technology. A well-structured plan, combined with industry best practices, such as comprehensive documentation and a post-migration "lessons learned" review, ensures a smooth transition and long-term success.

Beyond technical implementation, the migration significantly impacts SOC teams and other key stakeholders whose daily workflows will evolve with the new SIEM's capabilities. By adopting a modern SIEM, organizations can strengthen security, ensure regulatory compliance, and boost SOC productivity, fostering a more proactive and engaged security environment.



Cribl

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Powered by a data processing engine purpose-built for IT and Security, Cribl's product suite is a vendor-agnostic data management solution capable of collecting data from any source, processing billions of events per second, automatically routing data for optimized storage, and analyzing any data, at any time, in any location. With Cribl, IT and Security teams have the choice, control, and flexibility required to adapt to their ever-changing data needs. Cribl's offerings—Stream, Edge, Search, and Lake—are available either as discrete products or as a holistic solution.

Learn more: cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter (X)