E-Guide

How to Define SIEM Strategy, Management and Success in the Enterprise

Contents

Security information and event management (SIEM) projects continue to challenge enterprises. The editors at SearchSecurity.com have compiled essential resources to help you tackle these projects once and for all.

A full-service model for SIEM

George Do

Organizations continue to struggle with a rise in security incidents, and CISOs and their IT teams often lack the resources to meet the challenge. Like most information security programs, we are being asked -- and, in many cases, forced -- to do more with less.

Enter a concept that hasn't been a focus in the industry until recently: Developing a security information and event management (SIEM) system, which addresses not only the high costs of setup and ownership, but the most important use cases.

SIEM promises to improve the security incident response lifecycle by collecting and analyzing data from a myriad of sources (network and security devices, security programs and servers). SIEM technologies provide log management, event monitoring, alerting and compliance reporting through complex infrastructure involving hardware, software, custom processes and analytics. Given the push towards the cloud, there's a unique opportunity to deliver SIEM in a way that adds far greater value to users.

What is the goal of a SIEM? That depends on the organization, but the common use cases are to detect, validate and adequately respond to system compromises, data leakage events, malware outbreaks, investigations into a particular user and service outages. At least that's what it is for my organization. Simplistic as it may sound, I expect that this would be the answer from most other organizations, too.

Contents

Much has been researched, written and deployed in practice regarding SIEM. However, the industry still fails to recognize the valid need for cloud-based SIEM services. A full-service SIEM would not only leverage the commonly accepted benefits of the cloud, it would address the complete incident response lifecycle. After all, a SIEM's output is basically a correlated event that responders use to investigate incidents. When and how the event is used is the key to adding greater value to any SIEM investment.

Consider a subscription-based SIEM service that is straightforward to deploy and goes beyond just spitting out events by taking it several steps further. The complexity of log and event management (collection, storage and analysis) is significantly reduced because users no longer have to invest heavily in these security activities in terms of human or monetary capital. Because all these complex infrastructures live in the cloud, the model can be as simple as forward all your logs/events to the cloud, execute a basic security baseline exercise during setup and agree to a service-level agreement (SLA) for event alerting. In addition, the service would offer 24/7 security operations center coverage, in which frontline responders analyze each SIEM event and escalate it to users only if necessary based on SLAs.

The value proposition for such a service is vastly more attractive compared with traditional on-premises SIEM systems. The goal of SIEM in the cloud is to have 100% in the cloud with nothing on-premises.

As with most options that marry complex technology and processes, the devil is in the details. SIEM systems store and process highly sensitive data (security logs and events) for an organization and may even contain personal data.

Cloud SIEM users are required to have an extremely high level of trust with the SIEM provider. Key security challenges, such as the following, need to be addressed:

1. Security level and posture of the vendor
2. Limits of liabilities (customer data compromise)

3. Governance, risk and compliance requirements (consider companies that comply with EU regulations)
4. Compliance with privacy policy (user and corporate data leaving the premise)

Contents

There's help out there for many of these issues. Companies such as Skyhigh Networks offer cloud security software to help organizations efficiently assess the security level and posture of cloud services. This enables organizations to quantify the risk of cloud services with hard data to back up their assessments. CISOs can then make an informed decision about whether to engage with the cloud vendor based on these merits.

The SIEM field is crowded and contains a mash of providers from traditional players -- RSA enVision, HP ArcSight, McAfee and Splunk -- to innovative log management companies, such as Sumo Logic. Each offering has strong as well as weak points. However, no one has really crafted an offering for a full-service SIEM in the cloud that includes a security operations center (SOC) with human eyes to proactively monitor events. Managed security service providers, such as AT&T and IBM, have offerings that cobble pieces together. However, these services are targeted at managing or leasing SIEM infrastructure.

A full-service SIEM should offer the following:

1. Zero (or negligible) investments in on-premises hardware and software
2. Quick to deploy: Just forward logs from your existing infrastructure
3. SOC coverage, 24/7
4. Packaged common use cases and SLA (out-of-the-box configuration)

Hopefully, the industry will come to recognize this as an issue and, more importantly, develop complete options for SIEM in the cloud. It's time security technology started taking advantage of the scalability and cost benefits realized by other services.

SIEM analytics: Process matters more than products

Anton Chuvakin

Security information and event management (SIEM) projects—still in the early stages for some organizations—have a long and somewhat tortuous history. After two decades, many of the remaining challenges concern SIEM-related processes and practices rather than the tools themselves. Organizations can procure next-generation SIEM products from numerous vendors, but buying the security monitoring capability is impossible.

SIEM tools collect, correlate and analyze a wide variety of security-related data. This information can include logs, alerts and flows as well as vulnerability, asset and user contexts.

Security monitoring refers to the set of operational processes that are built around the tool. SIEM processes, which can apply to multiple security monitoring and data analysis technologies, depend on the usage of the product. Is it for security or compliance-driven monitoring? If there's no process whatsoever, the IT budget that's spent on SIEM technology is likely wasted.

Use-case-independent processes

Many processes and practices are mandatory for getting any value out of a SIEM. A few procedures are compulsory for utilizing advanced functionality, and only become necessary at high maturity stages.

Use-case-independent processes are mandatory for all SIEM deployments. The core set of processes includes the following:

- Collector and log source configuration process
- SIEM program checkpoint process

- Content tuning and customization processes

The collector and log source configuration process enables the SIEM team to get to log sources to send data into the SIEM product. Together with collection and parsing, the monitoring process enables the team to know when log sources stop reporting data or stop reporting the correct data, which enables the SIEM to actually function. This process should include steps aimed at planning, configuring, testing and tracking the changes of log source configurations.

The SIEM program checkpoint process (biannual or annual) is a health-monitoring indicator for an entire SIEM program, not just the tool. This process allows an organization to track its successes with SIEM and plan deployment expansion.

Content tuning and customization are critically important for SIEM success. If an organization does not have some sort of tuning process (initial and ongoing) to adapt a SIEM product to a changing environment, the chances of getting security value that's equivalent to the software purchase price are minuscule. "Off the shelf" SIEM content, while somewhat useful, needs to be customized and adjusted to solve the tougher problems for which modern SIEM tools are built.

Today's SIEM products come with reports, dashboards and correlation rules, which are created to address regulatory compliance (such as PCI DSS, HIPAA and many others) as well as common scenarios for security (such as reduction of false positives and user authentication analysis). Some vendors claim that such content is useful "out of the box" with no customization. Customer experience has shown that most content is useful only when it is applied to specific systems (thus customized by adding filters) or tweaked to better match the environment.

As SIEM deployments move up on the maturity scale, however, the process for customizing content, and eventually creating content, essentially becomes mandatory. For example, an organization that just purchased its first SIEM tool might only customize the reports for PCI DSS compliance so

Contents

that they only run on systems in scope for PCI (a task of minimum difficulty). More mature organizations can modify the parameters (such as counts or timings) of vendor-provided correlation rules to increase their applicability for specific segments of the environment. Mature organizations that seek to extract maximum value from their SIEM tools will ultimately grow to create their own content based on defined use cases, thus making the SIEM tools deliver the value they were designed to provide.

Content tuning and customization processes need to be built during the deployment stage or shortly thereafter, before routine SIEM operation commences.

Regulations and compliance

Compliance adds little to a core SIEM process set:

- Report review process
- Compliance issue remediation process

Report review presents the core of the periodic workflow dedicated to compliance. PCI DSS (see Requirement 10.6) prescribes daily log reviews; other regulations also call for activity audits and reviews. For example, HIPAA calls for "procedures for monitoring log-in attempts and reporting discrepancies" and for covered organizations to "implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports."

Compliance control weakness remediation enables the organization to close the loop on discovered compliance weaknesses, and thus, act on the results of monitoring. This is an equivalent to security incident response processes, but applied to compliance incidents. Admittedly, the process does not reside inside the SIEM tool, but it is closely tied to SIEM-generated reports and alerts.

Real-time monitoring and investigations

Security processes are split into two distinct kinds: real-time monitoring and investigations. Some SIEM products excel at both, a few derive their lineage from investigative tools, and others retain their focus on real-time monitoring.

However, one process reigns supreme and presents a foundational element for any SIEM security use: the security incident response process.

If an organization does not have an incident response process that outlines what will happen if there is a security incident, procuring a SIEM tool is likely a mistake. In fact, "75% of chief information security officers (CISOs) who experience publicly disclosed security breaches and lack documented, tested response plans will be fired," according to Gartner research. Thus, organizations should put an incident response process in place before putting a SIEM tool into operation.

Monitoring processes include the following:

- Alert triage process
- Activity baselining process

The alert triage process happens between the moment when an alert is triggered and the time when an incident response process is initiated. Not every alert generated by a SIEM product triggers an incident, some might prompt refinements of SIEM content or changes in security policy. This process should include steps that allow security personnel to unambiguously determine whether the alert is an indicator of an incident, needs to be suppressed in the future, or requires further investigation or escalation.

The activity baselining process is inherently followed by most analysts that use a SIEM tool to review logs. This means that somebody learns what "normal" is for a particular network or system, and then tracks when some activity deviates from it. A dedicated process to profile users and system behaviors, and build a baseline is recommended for mature deployments.

Investigative processes include the following:

- Indicator analysis process
- Remediation process

The indicator analysis process is triggered when a security monitoring team receives an indication from outside a SIEM tool that something is amiss. Such a process will involve search results and report review in order to understand whether an indicator calls for activating an incident response process.

The remediation process is most commonly triggered outside of a SIEM tool, but based on investigation or alert triage. This process actually causes changes in an environment, either on monitored systems or in a SIEM itself. Many successful SIEM projects treat this as a closed loop from detection to issue resolution. Remediation is unlikely to be fully automated and may never fully reside inside the SIEM tool.

Many other processes can be built and should evolve in more mature environments. However, this base set of processes presents a reliable indicator of SIEM program success.

Contents

TechTarget

Contents

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

- SearchCloudSecurity
- SearchSecurity
- SearchMidmarketSecurity
- SearchFinancialSecurity