How to Define SIEM Strategy, Management and Success in the Enterprise
Security information and event management technology has traveled a long and winding road, but today enterprise SIEM technology is as functional, manageable and affordable as it’s ever been. Yet many enterprises haven’t implemented a modern SIEM product, and others that have aren’t taking full advantage of the advanced capabilities of contemporary products. In this Essential Guide, learn to develop or refresh your enterprise SIEM strategy to set the stage for SIEM success today and tomorrow according to how you best define SIEM for your business.

Jane Wright, Site Editor

Security information and event management (SIEM) products grew out of two narrower product categories in the past decade. Security information management (SIM) software and appliances were used to collect and review logs of data from host systems, network devices, security devices and applications. Security event management (SEM) products came next, providing automated reviews of log data in real time, looking for anomalies or event correlations that signaled a security threat or a compliance violation. Gradually, SIM and SEM vendors merged these tools into SIEM technology platforms.

SIEM platforms recently evolved further to collect data about users’ behaviors and data access. SIEM platforms may collect data from hundreds of sources, including hardware devices, virtual machines and applications such as Microsoft Exchange and Oracle databases.

Rocky start for SIEM technology

The earliest SIEM deployments were often a disappointment, according to Jessica Ireland, research analyst for Ontario-based Info-Tech Research
Customers tried to implement all of the SIEM functions with all available sources, which added more complexity than most customers could absorb in a short time. As a result, most of the logs collected by the SIEM sat unviewed, and many customers would label their SIEM project as a failure. Over time, customers were encouraged to start their SIEM project with just one objective (threat monitoring or compliance reporting, but not both) and just a small set of sources (for example, just the network devices), to gain skills and experience and gradually grow their SIEM project at a manageable pace.

Current SIEM technology offerings

SIEM platforms have improved significantly in the past few years. “The products keep getting better,” Ireland said. “We’re seeing a lot of fluid and intuitive interfaces, which make SIEM easier for clients to use.”

One example of the easier interface is the “replay” function. This enables the administrator to recreate a past incident or attack and develop a new policy for times when a similar incident occurs in the future.

Alerts and responses have also improved in most SIEM platforms, according to James McCloskey, senior research analyst at Info-Tech Research Group. Early implementations of automated responses caused problems, such as actions being taken when the alert was actually a false positive. “A lot of the kinks in automatic response systems have been worked out,” McCloskey said. “More people are comfortable that their SIEM will properly correlate an attack with information from other tools, such as a Web content filtering product, and respond appropriately.”

Major SIEM technology vendors

There are approximately two dozen vendors actively selling in the SIEM space. In its 2011 Magic Quadrant for SIEM report, Gartner Inc. placed HP/ArcSight LLC, Q1 Labs (acquired by IBM), RSA (the security division of EMC), Symantec Corp., LogLogic Inc., NitroSecurity Inc. (acquired by McAfee) and Novell Inc., in the leaders quadrant. Vendors such as NetIQ
Corp, elQnetworks Inc. and others fill the remaining quadrants of Gartner’s report.

The majority of SIEM vendors are particularly active in North America, where most of the first SIEM platforms were sold. In recent years, interest in SIEM technology has expanded to Europe, Latin America, Australia and Asia/Pacific regions.

**SIEM market**

According to the Gartner report, the SIEM market is mature, with many customers having their SIEM implementations in place for more than a few years, and some shopping for an upgrade or replacement to their initial SIEM choice.

Large enterprises continue to be the predominant purchasers of SIEM platform products, Ireland said. SMB customers are more likely to employ a managed security services provider (MSS) for SIEM functions. Some SIEM vendors now offer scaled-down versions of their platforms, supporting a small number of logs from a limited number of log sources, to provide a lower price point for SMB customers.

**SIEM technology: Typical uses**

Customers typically use SIEM products for two reasons: to spot evidence of security threats or security breaches, and to ensure their organization is complying with regulatory standards. A 2011 Forrester Research survey (sponsored by SenSage) showed most customers are currently using their SIEM tool for both threat management and compliance reporting.

While the decision to install a SIEM platform may be made by the IT department, the compliance manager, or a business unit within an organization, Gartner’s report stated ownership and management of the SIEM platform usually goes to the IT team.
The future of SIEM technology

All those logs of data captured by the SIEM are growing, especially as SIEM platforms begin to capture usage and incidents from mobile devices. For this reason, some vendors are working to connect business intelligence and analytics tools to SIEM data. In its 2011 report, How Proactive Security Organizations Use Advanced Data Practices to Make Decisions, Forrester said the IT industry is currently poised at the intersection of SIEM, data warehousing and business intelligence, which could potentially unlock the ability to discover and respond to new threats.

In addition, many of the larger SIEM vendors are working to integrate their SIEM platforms with GRC (governance, risk and compliance) products, or with identity and access management products.

Ireland believes some vendors will accomplish this three-pronged approach of SIEM, GRC and security infrastructure through acquisitions. "We expect further consolidation as more vendors try to pull these three prongs of SIEM, GRC and security infrastructure together," Ireland said. "Some of the larger vendors may grab up the few remaining niche players."

Unlocking the opportunity of SIEM technology

Unlocking the opportunity of SIEM technology
Andrew Hutchison

Ensuring the ongoing integrity of an enterprise information technology environment is a formidable task, and one that requires every advantage a delivery management team can harness. Security information and event management, or SIEM, can create a significant advantage in providing enterprises with a comprehensive, coordinated view of the security status of their environment. The challenge in security is always to remain one step
SIEM technology

Unlocking the opportunity of SIEM technology

Security information management systems aspire to real time security

Five tips to improve a threat and vulnerability management program

Is centralized logging worth all the effort?

---

The opportunity of SIEM is to establish a centralized, coordinated view of security-related information and events. The underlying principle is that such inputs are produced in multiple locations, but without seeing "the big picture," it may not be obvious that trends or patterns are occurring. By establishing a collector network, the security-related events from end-user devices, servers, network equipment -- and even specialized security equipment like firewalls, antivirus or intrusion prevention systems -- can be gathered and inspected.

In this article, we examine how a SIEM system works and what types of events can be integrated, including new data sources such as fraud detection systems and network access control technologies that haven’t always been in scope for a SIEM deployment. We also look at the process for detecting actual security threats or incidents and steps organizations can take to develop a SIEM capability.

### SIEM components

As indicated, the opportunity of SIEM is that information from diverse sources and systems can be collected. Often the volumes are very high and the SIEM system needs to ensure it is capable of handling the events without becoming overwhelmed. SIEM systems are typically constructed in a hierarchical manner so collection can be done at multiple levels. Some sort of agent is often deployed in multiple locations, communicating back to a central SIEM management node at which detailed analysis takes place.

In some systems, pre-processing may happen at edge collectors, with only certain events being passed through to a centralized management node. In this way, the volume of information being communicated and stored can be reduced. The danger, of course, is that relevant events may be filtered out too soon, so a balance is required and this is the challenge of SIEM designers and implementers. At the central node, analysis techniques are applied to interrogate, aggregate and correlate the incoming information. The
better the analysis techniques, the more value can be derived from the SIEM environment.

**Feeding the SIEM**

Depending on the level at which security-related information and events are collected, a SIEM can be quite versatile. Traditionally, it is the infrastructure-related events that are collected by SIEM systems. The operating systems running on end-user devices and servers can forward information like logins (successful or not, user information, administrator logins, Kerberos events etc.), antivirus system alerts (successful/unsuccessful updates, repairs, infection details, etc.), and communication subsystem information (port connection attempts, blocked connections, IP address information, etc). Additional information from network devices such as routers, firewalls, and intrusion prevention systems can also be forwarded to a SIEM to provide information relating to these aspects of the infrastructure, too.

To be able to identify anomalous events, it’s important the SIEM can also build a profile of the system under normal event conditions. For this reason, items such as successful system logins are also typically recorded to establish a norm against which abnormal logins can be detected. Rich events relating to access of the network can also be integrated in environments where network access control (NAC) is enabled. It may be possible to pick up patterns of denied access, or to detect patterns of network access by virtue of the NAC mechanisms of checking credentials, device addresses etc. to prevent unauthorized devices from connecting to an enterprise LAN.

Sometimes it is also useful to have knowledge of other system information, such as processor or memory utilization to determine whether there is an unexpected change in the status of a system. For this reason, it is useful to have other contextual information available for the SIEM management team. While we are suggesting that SIEM has a special focus and separateness, it’s often this kind of system information that exhibits the effect of an incident. So SIEM should also be viewed as part of an overall, comprehensive systems management approach.
When talking about the business impact of security incidents and where the real damage occurs, corporations often say the transactional level is the most dangerous. Fraudulent transactions can result in direct costs for organizations, and this can come at a very high price. An opportunity for SIEM systems is to collect information that is above the infrastructure level and which derives from application and business systems. Being able to intercept a transaction where an approver is the same person as the requestor, or where other separation-of-duty requirements are compromised, could be of high relevance to an organization. The difficulty with application generated events is they tend to be non-standard, whereas a whole population of operating system devices generate events of similar format and semantics [meaning]. Although application events may require some work to integrate and interpret, this is effort well spent in terms of taking the SIEM from the engine room to a system that also incorporates business process information.

As a final word on the type of events a SIEM should aim to incorporate, it’s also necessary to interpret system or application events in the context of external events. Unusual behavior patterns may be detected by security staff, based on SIEM alerts, but these could relate to system modifications in change control windows (with, for example, more privileged logins than usual), the time of day or seasonal variations such as increased trading volumes from a Black Friday or pre-Christmas rush.

Detecting threats with SEIM systems

From the multitude of security information presented, SIEM systems have to make sense of the feeds received and determine whether alarms need to be raised, operators need to intervene or if warnings should be provided. The task is a bit like finding a needle in a haystack. Overall though, the accuracy aspect of a SIEM should be to reduce false positives, whereby patterns that don’t relate to an attack or malicious behavior are reported as such.

At the most basic level, static rules can be configured in SIEM systems and, based on logical expression evaluations, these will either be activated or not. A similar approach is to configure thresholds, whereby identification of
certain numbers of events (or some combination of event types) will result in a flagging of this occurrence.

Much of the focus of future SIEM work is on moving from static detection techniques to dynamic ones that are capable of identifying behaviors not seen before. The latter type of system uses techniques such as anomaly detection based on artificial intelligence. Through employing techniques of finding anomalous points or anomalous series, depending on the types of data, statistical or time series analysis can be performed to find deviations from a norm. Experimental systems based on such techniques are showing promise, and such learning type systems will increasingly be incorporated in commercial systems too.

In addition to techniques that can detect anomalies and outliers, security vendors, managed service providers, researchers, and universities are working to enhance prediction of attack situations. Through various attack modeling techniques, systems can compare incoming events with certain patterns and determine whether an attack pattern is being observed. This is particularly powerful, specifically for dealing with zero-day type attacks. Responses to incidents can be characterized as reactive or proactive, but identifying attacks in advance can be challenging. Where attack patterns have been seen before these can be incorporated into rule-bases or correlation engines. In this way, rules can be changed to add or adapt a static/threshold response. Post-event analysis can help to prevent future occurrences.

As a final word on detection, it is important to recognize that the SIEM system needs to form part of an overall security process. It is arguably just as important to have appropriate interfaces, channels, alerts and inspection capabilities available to SIEM operators, as it is to have the relevant security source information and events collected by the SIEM.

**Developing a SIEM capability**

In terms of establishing a SIEM capability, an organization may either do this directly through its IT function or retain a service provider to perform this
service along with other systems or security services. Various products are available from major vendors and there also are open source options such as Alien Vault.

A project to establish SIEM functionality requires the incorporation of many heterogeneous devices. In some cases, SNMP information feeds may exist, in other cases syslog information is derived and fed to the analysis engine. Overall, though, a careful mapping of events, incorporating all operating systems and devices needs to take place. This should be done with a dedicated, external team. In one large SIEM deployment studied, there were significant delays because the same team running day-to-day security also tried to build the SIEM capability.

When collecting and scrutinizing events via a SIEM deployment, other problems in the IT environment may surface. For example, inconsistent configuration can lead to one device generating huge volumes of event information, in contrast to other devices emitting very little (or no) information. This can lead to an anomaly based system flagging this difference immediately. To counter this, servers and domain controllers can be configured for how “verbose” they are with their logging information. The establishment of a SIEM environment has the additional benefit of creating a real bottom-up view of an environment, and for giving security operation center teams a feel for the norms that should be seen. Documentation and mapping of security events are other useful by-products of a SIEM deployment.

### Looking ahead: Future of SIEM

The future of SIEM systems is promising, especially with additional detection techniques being developed and incorporated into SIEM analysis engines.

The evolution to an “Internet of things” means many more devices will be IP enabled, and it will become increasingly difficult to manage and ensure the operation of all these components without SIEM techniques. Trends with cyber-physical systems make the stakes even higher, in that connected vehicles, energy grids, health systems, or manufacturing environments.
create the potential for life-threatening impact of security attacks. For this reason, another avenue of exploration for SIEM systems is to make them more tightly coupled with the architectures of the environments they are supporting. For example, various smart grid and smart car architectures make use of a systems bus for intercommunication and connection of supporting modules. Building SIEM-type capabilities into these environments directly could be a promising (and reassuring) approach to complement the technology advances in these environments with strong supporting security monitoring modules. As systems evolve, and attack scenarios are considered, misuse cases can be developed. We also need to understand misuse cases better to assist designers of future SIEM-supporting technologies to make analysis approaches as effective as possible.

Other emerging trends include experimentation with cloud-based delivery of SIEM services. While there is debate on the security of cloud services in general, SIEM-based cloud systems may still have some concerns to alleviate before becoming widely accepted.

The security of the SIEM system itself is something that also needs to be considered. An attacker may have reason for wanting to modify or block messages within the SIEM. The integrity of the SIEM system itself is critical: If the security monitoring system can be undermined, then system management can be compromised. Researchers are trying to develop resilient collector agents (with smart routing) that could prevent parts of an SIEM from becoming partitioned.

Overall, SIEM is a technology and approach that can provide powerful insights, through separating and focusing on security information and events. Organizations should work towards developing a SIEM service that is distinct from the normal management and monitoring activities that track availability, performance, capacity, etc. within an IT environment. In combination with a security operations center type approach, the SIEM will help an organization consider patterns that may suggest or reflect a security incident. Advances in analysis and correlation techniques provided in SIEM tools will assist operational staff to interpret the large volumes of information even better, and SIEM will increasingly play an important role in helping
retain the advantage of safe, secure systems of integrity -- despite those who may try to undermine the intended operation in some way.

Security information management systems aspire to real-time security

Michael S. Mimoso

Big data is coming to information security. And it’s forcing security managers to take a critical look at their existing technology investments, in particular data collection points such as security information management (SIM) systems, to determine if they’re up to the task of helping with real-time security analysis of event data.

Enterprises need to understand what’s happening on networks in as close to real time as possible. Yet experts agree that real-time analysis might be a bit ambitious at this juncture, for SIM especially. Security teams should temper their expectations of what “real time” means, what SIM and other analytics technologies are capable of, and the resources needed to observe and react to security incidents in real time.

“It is ambitious, especially for SIM, because the event has to happen to get logged, sent to the SIM or log aggregator and run through the rules engine,” said Diana Kelley, founder of Security Curve, a consultancy in New Hampshire. “All of this takes time and it’s not real time. You’re not looking at live traffic like an IPS or next-generation firewall would. That’s closer to real time than an event going through a log management system that parses the data and sends it to a SIM where correlation rules are run.”

Actionable information has always been the pot of gold at the end of the SIM rainbow, but finding the treasure often gives way to painful rule writing and integration exercises. SIM rules can be a hardship because, like all
signature-based defenses, security teams need to understand what they're looking for in order to establish proper alerting thresholds.

“If your thresholds are too high, you’re not alerted quickly enough,” Kelley said. “If they’re too low, your SIM is slamming you with alerts. Figuring out those thresholds is what makes rule writing so complicated.

“Log management or SIM can be great for forensics—going through and finding needles in haystacks,” Kelley added. “If you don’t know where to start, it gets problematic.”

The end result has often been frustration with the product; companies sometimes end up shutting off the analytics and are left with a compliance and reporting tool that in some cases may have cost more than six figures to buy, install and maintain. However, using SIM to its fullest may not be a luxury for much longer. Not only do regulations require log analysis and reporting tools, but the crush of targeted, persistent attacks against high-value government, manufacturing and financial targets could inject renewed interest in maximizing SIM investments.

**Extended security information management system capabilities for real-time security**

Robert Capps, senior manager of trust and safety at online ticket broker StubHub, augmented his company’s SIM and monitoring technologies with fraud detection technology from Silver Tail Systems that looks for anomalies in how users interact with the site versus a baseline of normal traffic. He cited frustration with the inability of SIM and other network security devices to pick up abuses of legitimate StubHub services perpetrated by attackers. Intrusion prevention systems (IPS), for example, saw only legitimate network traffic, while SIM recorded successful logins with legitimate accounts created by attackers for the purposes of fraud.

Capps said he believed IPS, SIM and other analytical tools weren’t effective at analyzing security events, but didn’t have the data to support it. By taking a real-time analytics approach, he said he was able to identify problems and
change his company’s security response without changing the customer experience.

“IPS is great if someone is trying to attack your firewall; it’s not real good at identifying bad actors who are getting in with good traffic, especially if they’re using your Web application like everyone else,” Capps said. “I’d rather have a tool that says, ‘This looks odd and doesn’t fit with my transaction flows.’ That was the direction I needed to identify zero-day attacks.”

Leading SIM vendors such as ArcSight, an HP company, Sensage and Q1 Labs (IBM) are talking about extending the capabilities of their products in the direction of business analytics and data warehousing in order to accommodate big data analysis, essentially bringing real time into the equation. Security analysts are burdened with a virtual landslide of data from not only network security devices, but operating systems, applications and even user behaviors. Sensage President and CEO Joe Gottlieb says his company’s tools already give organizations the option of pulling security data from particular sources into a data warehouse where correlation rules are run against smaller subsets of data flows.

“The data is no more than five minutes old,” Gottlieb said. “Real time is really about a mix of sources and freshness (of data). The least common denominator is the oldest data you have in a state machine. That indicates how real real-time is… In general, the industry has needed to manage expectations on real time. Deep-packet inspection technologies set the tone for prevention, and they expect the same level of situational awareness from SIM, but don’t tend to get it.”

Data overload threatens SIM’s real-time security ability

Clearly, as monitoring and reporting technologies move closer to real time and more data sources are involved, the complexity involved in querying and processing events and maintaining thresholds grows too.

“If it’s too ambitious, it could come back to what you are trying to accomplish. There’s no reason why any organization wouldn’t want to do real-time
analysis, but you need to balance that with what your environment looks like and what real time means to you and how you want to manage risk,” said Michael Callahan, vice president of worldwide product and solution marketing for HP ESP.

ArcSight also is heading toward real time via improved analytics and correlation for its SIM. Callahan said customers want enhanced performance and scalability – faster analytics and correlation from more sources – as well as more context from security events and what’s happening in IT operations.

“The next piece is to broaden it to the entire organization; this gives you the opportunity to look at what is your business’ overall risk,” Callahan said.

Experts caution that enterprises need to narrow their real-time scope, understand their environments and what attacks mean to different parts of their IT infrastructure.

“Every security team is drowning in data; another problem with real time is that it puts more data into a data overload situation,” said Mike Lloyd, chief technology officer at Red Seal Networks. “Enterprises are already drowning in way too much data, and building more sensors with more data is not a great path forward. Making the human scale along with the data so that we can take action is hard and another real-time problem.”

Red Seal’s products promise continuous visibility into an IT infrastructure by mapping interactions between security devices and highlighting access points that could be vulnerable. Lloyd said companies should avoid the temptation of over-investing in any area of security, such as analytics, at the expense of prevention or forensics.

“That’s a big mistake in the enterprise,” Lloyd said. “You can’t know everything at a high scale.”

Security Curve’s Kelley said SIM needs to provide better rule sets and intelligence on attacks to its customers.
“SIM is very strong in forensics and piecing events back together,” Kelley said. “And it’s good at alerting in near real time on simpler, less complex issues.”

Five tips to improve a threat and vulnerability management program

Diana Kelley, Contributor

Modern enterprise cybersecurity teams must be prepared to deal with a barrage of new and rapidly evolving threats. From script kiddies to sophisticated hackers working for criminal organizations, if an enterprise doesn't have plans in place to deal with such threats, it will pay the price in expensive, embarrassing data breaches.

An effective threat management program is undoubtedly a vital ingredient for any enterprise security team dealing with the modern threat landscape, but keeping such a program running smoothly takes time and ongoing planning. Resources must be allocated to put a program in place that can deal with a multitude of attacks.

In this tip, we will offer five best practices that companies can implement to increase the effectiveness of their threat and vulnerability management program.

No. 1: Manage alerts

If a tree falls in the woods and no one is there to hear it, does it make a sound? This old philosophical question comes to mind when thinking about threat management. Like that tree, are alerts about suspicious activity and anomalous behavior that can signal an attack in progress that an administrator doesn't see or review really alerts? The most important thing a company can do to get a handle on threat management is to ensure that someone is there to review and respond to an alert that's been triggered. To
meet this requirement, most organizations should assign a dedicated resource, or resources, with the remit to review log and alert consoles on a daily basis.

At the daily alert review level, it's not uncommon to see organizations assign different specialists to review different alert consoles. For example, a firewall operations expert may be in charge with reviewing firewall rule changes and alert logs, while an applications engineer may be responsible for reviewing the logs and alerts from the Web application firewalls and Web app scanners.

**No. 2: Take a holistic view**

In the realm of detection evasion, attackers are growing increasingly sophisticated, as can be seen with their use of multi-channel attacks and other techniques that are designed to fly below security radars. An example of a multichannel attack is the seemingly innocuous spear SMSish (SMS phish to a smartphone), which fools the user into clicking on a link that leads to a rogue site that has been designed to look legitimate. The user may then be tricked into entering sensitive data or clicking on a link that infects the targeted machine with a bot. Once the user's sensitive information has been collected, the attacker attempts to log in to a system and dig deeper into the corporate network for more valuable information.

Most organizations already monitor for threats and suspicious activity on most devices, including wired desktops, wireless tablets, smart devices, laptops, Web applications, databases and servers. To catch multichannel attackers, organizations should corral alerts from all of those systems into a single console where correlation rules can filter the seemingly innocuous activity that, when combined, creates a single, organized attack.

**No. 3: Reduce false positives**

Excessive alerts and false positives ratchet up the "noise" ratio so high that it can be difficult (if not impossible) to sift through all the available data to find the truly malicious events. If an organization's administrators can't discern
important alert signals through all the less insignificant events, the alert system becomes useless. To reduce the number of false positives produced, an enterprise should first analyze the alert output of its threat-warning console, or consoles, and determine if the rules can be tuned to reduce the false positive noise, or filter alerts by level of confidence so that admins can see which ones are more likely to be relevant.

One way to lower those levels without losing critical alerts is to set threshold levels that match normal activity on the network. For example, a company that forces all users to change passwords on the same 90-day cycle might find that failed logins increase significantly on the day after the end of a cycle. To account for this occurrence, a rule that normally signals an alert after three failed logins could be increased to five failed logins on days following the password change. The logins could also be linked to other threat indicators, such as attempts to log in using the same ID from different IP addresses, to increase accuracy.

Keep in mind that over-tuning or setting thresholds too low will result in false negatives, so test thresholds carefully before implementation.

No. 4: Integrate with the SOC

As mentioned above, aggregating threat information into a single console gives organizations threat visibility across the whole enterprise. To gain even deeper visibility, a company can integrate that single-console(or multiconsole) view with its security operations center (SOC). At most companies, the SOC's main purpose is to monitor security activity and respond to attacks quickly, which makes integrating the threat management program with the SOC something of a no-brainer.

To integrate threat information with the SOC, filter alert information into a SIEM system and log data into either the SIEM or whatever is being used for log centralization. Next, create rules in the SIEM, log aggregation tool, or both to parse through alert information and flag legitimate attack activity for further investigation or response. To integrate effectively, make sure that engineers and administrators in the SOC have access to the standard
operating procedures for incident response, so that the team knows the correct escalation paths, communication protocols and approved response activities.

**No. 5: Validate remediation activities**

In the heated atmosphere of an incident response, organizations can easily overlook validating the remediation activities. Even during routine activities like patch management, many companies fail to close the remediation loop with validation. Did the patch get loaded properly? Did it close the intended vulnerability? Without testing, an organization can't be certain that the remediation was successful and the threat exposure was closed.

Complete the threat management cycle with steps for validation. These can include rescanning systems to validate patches and performing application and network penetration testing to confirm that fixes or controls are blocking vulnerabilities as expected.

**Conclusion**

The modern threat landscape is complex and attacks come in from multiple channels and sources. Organizations need to have a multichannel approach to managing and responding to threat activity. Rolling up activity data into the SIEM, or other management console, and having trained professionals review the alert data will increase situational awareness and improve response time and efficacy. And when patches or controls are in place for remediation, don't forget to validate that they are installed and working. Stopping all attack activity is impossible, but by taking steps to improve a threat and vulnerability management program, businesses can avoid a incident becoming catastrophic.
Is centralized logging worth all the effort?

Mike Chapple

Is the work involved in implementing a centralized logging infrastructure worth the security benefits?

Absolutely! Network log records play an extremely important role in any well-constructed security program. They help in the detection of anomalous activity both in real-time, as well as reactively during an incident-response event. Centralized logging provides two important benefits. First, it places all of your log records in a single location, greatly simplifying log analysis and correlation tasks. Second, it provides you with a secure storage area for your log data. In the event that a machine on your network becomes compromised, the intruder will not be able to tamper with the logs stored in the central log repository -- unless that machine is also compromised.

Once you establish a central log repository, the next step is to introduce centralized analysis techniques. Many organizations fulfill this requirement through the use of a security incident management (SIM) device. A SIM allows you to add a degree of automation to your log analysis process. You can create rules that analyze logs, aggregated from various devices, for patterns of suspicious activity.

The main stumbling block many organizations face when deciding whether to implement centralized logging and/or SIMs is the investment of time and resources necessary to get such an implementation off the ground. Depending upon how long you decide to retain records (many organizations choose to keep them for at least a year), logs can consume massive quantities of disk space. Additionally, SIMs require a significant amount of configuration and tuning to optimize for a particular enterprise.
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