SIEM Solutions for Managed Security Service Providers

Selecting the Right Security Information and Event Management Solution
Choosing a Solution that Strengthens Your Competitive Position

Most MSSPs are not software companies at their core. They should rely on SIEM vendors to build their technology platform.

As IT becomes more complex and threats to important information assets grow more persistent, outsourcing security management becomes increasingly attractive. From legacy mainframe applications to social networking, all systems and applications need to be safeguarded from emerging threats and critical vulnerabilities.

A few years ago, most organizations could have survived by deploying simple firewalls and anti-virus solutions. Today, a dizzying array of security technologies—intrusion prevention system (IPS); unified threat management (UTM); data leak prevention (DLP); network access control (NAC); security information and event management (SIEM); governance, risk and compliance (GRC); to name just a few—is essential for survival. All of these technologies require skilled security personnel to manage and operate them. Yet the cost of acquiring and maintaining security personnel and technology has been rising dramatically.

These trends have driven the emergence of and high demand for managed security service provider (MSSP) solutions. Many organizations have no chance on their own of developing mature security monitoring capabilities that will cover their expanding IT landscape and deal with increasing attacker sophistication. MSSPs, however, provide a solution. At the core of every MSSP offering is a security management platform. Given how complex and uncertain the task of securing today’s organizations has become, outsourcing to an MSSP seems like an obvious solution. MSSP offerings may help organizations reduce costs, make internal security processes more efficient and even help with increasing regulatory burdens. Turning your complex environment over to a third party could also be cause for concern when you consider the MSSP is not familiar with your environment, and you are relying on a service level agreement (SLA) to protect your system.

To deliver reliable security services, MSSPs need powerful security technology platforms. While some choose to build their own, many MSSPs have been leveraging packaged SIEM technology for their operations. This paper helps MSSPs choose a SIEM technology platform that garners customer trust, optimizes operations and improves the MSSP’s competitive position.

SIEM Unveiled

SIEM solutions collect, aggregate, normalize and retain relevant logs; collect context data; analyze data, including correlating and prioritizing it; present findings, including reporting and visualization; manage security-related workflows; and manage relevant security content. SIEM solutions focus on information security, network security, data security and regulatory compliance. This functionality can be found in most commercial SIEM products on the market today.

Below we will discuss SIEM product features that are specific to an MSSP and illustrate how only select SIEM tools fit the needs of today’s sophisticated security service providers.

MSSP Unveiled

Organizations choose to outsource security to an MSSP for multiple reasons. Primarily, the decisions are made based on the perceived cost effectiveness of contracting for MSSP services compared to using the in-house security department to provide the services,
the organization’s culture regarding outsourcing the control of its security, security requirements, regulatory responsibilities and other business and technology factors. Some organizations trust their MSSP partners to make better security decisions while others want to retain both responsibility and control over their security decisions.

Because MSSPs focus on security, they are usually in a better position to train and retain good security personnel, and they have the advantage of learning from security threats they observe across their client base. As a result, their clients benefit from deep security expertise and improved security safeguards.

What sets MSSPs apart from each other is their service reliability, breadth of technology coverage, global reach, pricing flexibility and even their experience with technology platform interfaces.

Whatever the exact MSSP service bundle looks like, there is a technology platform under the offering. A scalable security monitoring and management platform takes years to build and even more time and resources to maintain. Such technology platform should be able to support the MSSP’s current and future service offerings, grow with their customer pool and address evolving IT regulations for MSSP global customers. To achieve MSSP cost advantages over internally sourced IT security, such platforms should automate routine tasks and enable MSSP analysts to perform most investigations without leaving their monitoring positions.

**SIEM Solutions for MSSPs**

SIEM is a strategic technology that allows MSSPs to deliver more value to their customers and develop more business. SIEM technology can boost MSSP service efficiency, reduce costs and improve service flexibility, all key competitive factors for MSSPs. For example, MSSPs that focus on device management can quickly build security monitoring and log management capabilities that can later be integrated with their existing device management offerings. Valued-added resellers (VARs) and consulting firms can build their own MSSP divisions or provide outsourced security operations consulting (SOC) services by building their platforms on top of commercial SIEM tools. Hosting and cloud providers can leverage the technology for selling additional security services to their current customers. SIEM tools can improve MSSP monitoring capabilities as well as provide more opportunities to offer new services.

SIEM tools can also serve the foundation for MSSP monitoring technology and help other businesses to further expand in the MSSP market. Even existing MSSPs with their own proprietary platforms can leverage SIEM solutions and log management tools to offer new services such as cloud SIEM or cloud log management.

**Key Business Criteria**

Before we address technology criteria for selecting a SIEM product, we need to address the broader business constraints that MSSPs face in their business. These directly apply to their process for selecting a SIEM solution.

- MSSPs are not software companies at their core. They have limited resources for developing new services, and whenever they develop new services or replace their main monitoring platform, their engineering and operations teams must dedicate resources. Most MSSPs will minimize any

Many SIEM products would not fare well with MSSPs, because MSSPs use SIEM solutions very differently from enterprises.
upfront engineering work constraining such work to just a few full-time employees and only for a few months before a service launch. This is not sufficient to develop a security monitoring platform but might be enough to customize the right SIEM solution for a job.

- MSSPs have limited development resources once their service is in routine operation. Tuning and updating their tools requires full-time commitment by both their engineering and operations teams. To better compete, the MSSP needs to focus these resources on expanding the MSSP’s services and not on maintaining the system. Many MSSPs have only a few full-time engineering employees for ongoing operations, and they need to optimize those employees’ time.

- MSSPs need to incur little or no costs to start up a new service for a customer. Ideally, the service should require no significant hardware purchases. Although there will likely be some costs, most MSSPs seek to minimize these costs by avoiding expensive hardware purchases for each new customer.

- MSSPs must leverage existing SIEM infrastructures for most customers to be profitable. Thus, their SIEM platform should never require in-person visits to a customer environment to manage on-premise components. Such troubleshooting visits quickly destroy any margin the MSSP earns.

- The offering must compete with the solutions from other MSSPs, including the early adopters that have spent years developing and perfecting their security platforms. They must also compete with enterprises using SIEM solutions in-house or via a co-sourced arrangement with a consulting firm or VAR. While customers seldom outsource security based on the strength of the MSSP portal, most providers prefer to use SIEM technology that is competitive in the marketplace.

- The MSSP must be able to demonstrate their service quickly to new and existing customers. Hauling in expensive and heavy appliances to demonstrate the service severely decreases its attractiveness and perceived value.

Overall, SIEM technology should enable MSSPs to run better and win more deals over other MSSPs and over software vendors that are set in the in-sourced security model.

Key Technology Criteria

MSSPs use SIEM solutions differently from enterprises. Many design decisions that SIEM developers have made over the years are perfectly logical for enterprise customers, but they might cause problems for globally managed security providers. Below are the main differences.

1. **SIEM tools.** MSSP customers and MSSP personnel use the same SIEM tools but in two different ways. The enterprise security team is likely the only entity deploying and operating the SIEM tool for monitoring its own environment—an environment the team knows well. With an MSSP involved, many enterprise security teams will use the SIEM product to monitor threats against its data. The team will work alongside the MSSP team in a multi-tenancy model. The difference in the way these two organizations use SIEM solutions should affect such product designs as user interfaces, access controls, privilege delegation and resilience against instabilities across one or more customer networks.

2. **Data segregation.** Data segregation is important to many enterprise customers. Enterprise SIEM will always contain the enterprise’s data. An MSSP SIEM platform will contain data from many different entities, and most of these entities will use the SIEM tools to guarantee their data is never seen by anybody but their team. Some enterprises will also request that data be physically separated, preventing the possibility of storing cross-enterprise data in the same
database. An MSSP can also host a dedicated SIEM installation for a particular customer. This solves data segregation challenges but also removes many of the advantages of relying on an MSSP.

3. **Data collection.** Traditional customer-owned SIEM solutions usually collect data from the entire environment using agent or agentless collectors deployed in various segments of the organization’s network. The MSSP relies on dedicated hardware or software, sometimes in the form of virtual machines, deployed in each customer environment for data collection. In this case, massive amounts of log data are likely moving across the Internet from the customer environment to the service provider data center. In most enterprise SIEM scenarios, local security teams or system administrators manage the collectors. With an MSSP platform, MSSP personnel must manage the collectors and other components remotely.

4. **Performance and reliability.** SIEM framework performance and reliability are essential to both enterprises and MSSPs. The MSSP likely has specific SLAs with its customers and any SIEM platform must be able to operate under such conditions without requiring ongoing support from SIEM vendor engineers.

5. **Scalability.** MSSPs require scalability and an ability to handle huge volumes of data. As new customers come online and as each customer’s data volume grows, the SIEM tool must grow with it—without expensive hardware upgrades.

6. **Support.** MSSPs handle support for custom and vertical applications differently. If a SIEM customer requires support for specific applications, the product management team can develop support on short notice. If an MSSP customer requires such support, the MSSP must petition its SIEM technology provider. This additional step can sometimes mean the difference between using an off-the-shelf tool and a homegrown framework.

7. **Access to system logs.** Many organizations that use MSSP services also request direct access to their system logs. This is in addition to accessing traditional service provider portals. Many organizations would prefer to use a log management service from a trusted service provider rather than deploy log management products in their own environment. This encourages managed service providers to deploy additional log management services alongside their SIEM platforms. As a result, tight integration between SIEM and log management become another critical requirement for the MSSP.

Because of these differences, MSSPs face serious challenges with some enterprise SIEM tools. Thus not every SIEM solution fits the MSSP bill.

**Key Questions MSSPs Should Ask SIEM Vendors**

In addition to the broader technical and business requirements outlined above, MSSPs must consider additional issues when selecting a SIEM solution. Here are some of the questions MSSPs should ask to gain assurance that the SIEM product will fulfill the MSSP’s needs for current and future service offerings.

- Which log sources does the vendor support for compliance reporting and other advanced features today? What constitutes a supported log source and how is such support maintained over time?
- Does the solution include a custom integration kit that includes a wizard, a software development kit (SDK), application programming interfaces (APIs), etc.? Can the MSSP use the kit to integrate log sources at no extra charge?
- What will the SIEM product do when unknown or custom application logs are fed into its collectors?
- How difficult is creating a new report or data view? What skill level is required?
Will reports and views be automatically updated when a new supported log source is added?

- Can remote components such as appliances, software and virtual machines (VMs) collect all required logs at each customer site without additional software? For example, some SIEM vendors require additional tools to collect Windows* logs, which are not managed centrally.

- Following the key technology requirements listed above, how complete is remote component and appliance management? How are configuration settings, parsing rules, application updates and operating system updates handled?

- Technology vendors often claim their remote components and appliances are low maintenance. What does that mean? Can maintenance be performed remotely?

MSSPs should start by determining their business and technology requirements. Then use the questions above to select the right SIEM product that meets their needs and enables them to offer new services, such as log retention and compliance log review, to their customers.

**Case Study: An MSSP Goes Shopping for SIEM**

In this example case study, a consulting firm decided to expand by building an MSSP practice. While its consultants already performed various security control deployments and configurations, the company had no managed service for security monitoring. The firm faced the following choices:

1. Provide monitoring services on customer equipment in a co-hosted model. The customer would purchase all necessary hardware and software, such as SIEM solutions. The firm’s MSSP consultants would then help operate and tune the system.

2. Build its own security monitoring platform and offer services on top of this. To do this the firm would have to hire and retain a dedicated engineering team.

3. Procure a commercial SIEM product and build a service on top of it. The firm’s MSSP practice would integrate the SIEM solution with an existing customer portal and a provisioning system.

Careful analysis of options and their comparative costs led the service provider to choose the third option. This firm decided the cost of purchasing hardware appliances for each customer would be prohibitive and decided it was not in the hardware business; it was in the services business. The firm thus purchased a SIEM solution from a major provider and deployed it at two data centers for redundancy, and it offered customers a choice of virtual systems or software for log collection.

As a result, the new MSSP was able to run a competitive service without developing any expertise in such esoteric areas as log parsing or scalable log data storage.

Later it realized that its SIEM platform allowed it to offer cloud log management and cloud SIEM services to its customers who were willing to handle monitoring themselves but who did not want to operate a SIEM solution. For these new services, customers paid for log management technology but retained the job of reviewing logs and monitoring security themselves, at a lower cost.

After the evaluation, the MSSP chose to deploy the following architecture based on a market-leading SIEM product.
Most of the SIEM components were deployed at the MSSP site. Log and other data were collected from customer environments and securely transported to the provider data center. The MSSP operated small, remotely managed collectors using customer premise equipment (CPE) in most customer environments. The collectors were deployed in the form of small Linux*-based virtual appliances. This architecture now enables the MSSP’s own personnel to monitor the customer environments and the customers to view their dashboards as well as access raw logs using searches and reports.

**Conclusion**

While it is clear that some managed service providers will choose to build their own security monitoring and log management platforms, they face a very competitive environment with well-funded players that have already spent years building their own products. As organizations outsource security to MSSPs, it only makes sense for MSSPs themselves to outsource software development to specialists—in this case to SIEM vendors. MSSPs should focus on their core competencies—offering high-value security services—and leave the platform development to SIEM tool developers.

To make use of commercial SIEM solutions as beneficial as possible, select SIEM vendors that have developed unique expertise in supporting their MSSP partners. Leading SIEM vendors such as Novell have already solved multi-tenant data storage, highly distributed collection and remote management problems.

On the other hand, it is clear that not every SIEM solution will work for an MSSP. Many of the SIEM players, even some that have been in business for years, will fail on both the business and technology criteria defined above.

As enterprises deploy more cloud applications, selecting the right SIEM solution will allow MSSPs to offer cloud security services such as cloud log management, cloud compliance log review and others. The MSSP can use these services to expand in the future to full security monitoring and device management services.