Security Information and Event Management

An Emerging Opportunity for Telecom Providers

Prepared by

Security Information and Event Management: An Emerging Opportunity for Telecom Providers

Prepared by

The Shpigler Group
(404) 600-5480
www.shpigler.com

THE SHPIGLER GROUP
STRATEGY MANAGEMENT CONSULTING SERVICES

The Shpigler Group is a strategy management consulting firm offering our clients a full range of services. We have designed our practice to add value to our clients' organizations, identifying suitable opportunities and optimal solutions. We deliver custom consulting services to four major industry groups:

- Energy
- Water
- Telecom
- Smart Cities

Our services include financial and operational analysis, business case development, and detailed studies that examine best practices. We listen to our clients and incorporate their input alongside our own industry knowledge, ability, and experience to develop a comprehensive plan that addresses client needs while providing viable options that add value.

The Shpigler Group offers services to clients in a wide range of areas:

- Developing feasibility studies for program implementation
- Performing benchmarking studies to support performance enhancement
- Conducting financial analysis of operations and detailing areas for improvement
- Supporting network design and construction management
- Performing technical research relating to projects or solutions designed
- Conducting management and operational audits
- Implementing go-to-market strategies
- Developing comprehensive and fact-based business plans
- Developing complete network designs and performing economic analysis of chosen models
- Developing detailed operating analysis and managing deployment efforts

For more information, please visit www.shpigler.com.

Executive Summary

Data networks continue to grow in complexity as rapidly as the risks associated with viruses and intrusion attacks. As such, more focus has been paid to the practices of network security. Security Information and Event Management (SIEM) is a relatively new concept, with roughly 20 years of operation. The concepts behind SIEM may differ, but overall they typically include elements of:

- Log management – collection and storage of log messages and audit trails
- Information management – long-term storage and analysis/reporting of log data
- Event management – real-time monitoring, correlation of events, notifications and console views
- Security management – real-time analysis of security alerts generated by network hardware and applications

With the ongoing growth and prevalence of cyber-attacks and security breaches, IT departments of many companies across a wide range of industries have struggled with how to best respond. For many, the answer involves outsourcing – the opportunity to enhance security capabilities while still keeping budgets directed toward security at a manageable level. SIEM providers have deployed cutting edge solutions that keep pace with security threats, detect and manage real-time threats, and analyze large amounts of data in short periods of time. Many of the leading providers are large, specialized providers of SIEM products and systems – IBM, Splunk, Fortinet, LogRhythm, McAfee, Micro Focus International, RSA Security/Dell, Rapid7, Exabeam, Securonix, AlienVault, and Hewlett Packard.

Today, we see more and more enterprises seeking even more advanced solutions for SIEM. Beyond purchasing products and systems, more enterprises are looking to engage with providers that offer managed services in the SIEM sector. Telecom providers that already have a communications channel into the enterprise market are some of the leading providers that are actively promoting SIEM managed services. For many more, the field of SIEM offers a new market opportunity.

Security Information and Event Management – An Overview

SIEM investments are commonly driven by the need to quickly address regulatory compliance issues. As organizations overcome the compliance hurdle, they increasingly use SIEM to improve security monitoring capabilities to manage escalating threats. Most organizations desire baseline SIEM solutions that offer real-time collection and analysis of log data from host systems, security devices, and network devices.

Deployment of SIEM equipment offers the potential to centralize event and log management information from a variety of security devices and computers. However, enterprises often have to address concerns involving significant up-front costs, complex installations, and the need to hire experts to manage the function. Furthermore, the rapidly changing industry requirements are resulting in a heightened need for security services in industrial control systems:

- Cloud Computing – The market drive toward the increasing use of public cloud computing will result in a heightened need for security protection
- Mobile Devices – Increases in the volume of vulnerabilities disclosed in mobile devices and apps result in higher security concerns for enterprises
- Cyber Crime – Recent years have been the source of the highest increase of high profile targeted attacks against industrial control systems
- Web Applications – Web applications are estimated to be the source of roughly half of vulnerability disclosures

Security Information and Event Management services offer a robust solution to centralize the storage and interpretation of logs, or events, generated by other software running on the network. While the original SIEM programs started in 1999, programs are continuously evolving today. Many systems and applications that run on a computer network generate events which are kept in event logs. These logs are essentially lists of activities that occurred, with records of new events being appended to the end of the logs as they occur. Protocols can be used to transport these events, as they occur, to logging software that is not on the same host on which the events are generated. The better SIEMs provide a flexible array of supported communication protocols to allow for the broadest range of event collection.

Security Information and Event Monitoring involves real time monitoring and incident management for security-related events from networks, security devices, systems, and applications. The complex nature associated with the demands of SIEM services has resulted in significant growth in managed service approaches. As managed security services have grown in popularity overall during recent years, more and more enterprises are seeking outsourced solutions. Managed SIEM options range from as simple as centralizing log collection and reporting to as complex as event correlation and round-the-clock security-event monitoring.

Centralized SIEM programs offer a number of key benefits of interest to enterprise users:

- Access to all logs can be provided through a consistent central interface
- The SIEM can provide secure, forensically sound storage and archival of event logs (this is also a classic Log Management function)
- Powerful reporting tools can be run on the SIEM to mine the logs for useful information
- Events can be parsed as they hit the SIEM for significance, and alerts and notifications can be immediately sent out to interested parties as warranted
- Related events which occur on multiple systems can be detected which would be impossible to detect if each system had a separate log
- Events which are sent from a system to a SIEM remain on the system even if the sending system fails or the logs on it are accidentally or intentionally erased

The Managed Services Opportunity

The rapid growth in SIEM and the demand for managed services is enabling more communications providers to enter the space. As they do, telecom network operators are finding ways to leverage their capabilities to provide value-adding security capabilities. The challenge now lies in developing a managed services offering that complies with industry standards.

SIEM standards can be met by achieving compliance with both organizational and technical resources. To address organizational competence, a viable SIEM program will have management functions that enable successful program implementation by the enterprise. Key organizational issues that need to be addressed include:

- Stakeholder support – when developing requirements, the SIEM provider must be sure to collect them from the full range of groups that may benefit from collected log data
- Ease of use – creating correlation rules that help the enterprise staff focus on the areas of highest risk
- Deployment options – deploy systems that provide the data collection, analysis and correlation and use their own built-in databases to store copies of logs
- Management services – support log management capabilities, taking logs from the customer premises to a Security Operations Center and conducting archiving and reporting functions
- Vendor support – ensure full support for client needs on an ongoing basis
- Cost viability – the total system cost of ownership must be reasonable given the service provided

In order to achieve technical competence, the SIEM program needs to ensure that data management functions are properly accounted for. Key technical issues that need to be addressed include:

- Correlation capabilities – establish systems that normalize logs from various systems, which helps the user see the most important data needed from logs in a readable format
- System usability – establish systems that support easy set-up of policies and rules, create manual reports, and schedule automated reports
- Investigative capabilities – enable a view into not just network behavior, but also user and application behavior
- Console management – ensure that systems properly account for back-end intelligence and alerting
- Storage capacity – ensure that back-end IT and communications networks are adequate to support system functionality
- Scalability – allow for the collection of more data from more devices more quickly

Furthermore, managed service providers will need to account for a wide range of impending operational requirements. Providing a solution that offers full security while presenting the capabilities that allow an enterprise to achieve efficiency and flexibility is key. Some of the best practices in this respect include:

- Stakeholder support – Developing the SIEM in a way that provides support for each business unit and the underlying characteristics and requirements for each is key.
- Ease of use – Most systems are based on exceptions reporting, with threats measured against the relative intelligence of assets. This enables the user to easily operate the system despite the large amount of data being managed.
- Deployment options – SIEM providers will want to deploy systems at the exchange server and will want to identify systems at risk. They will need to quickly monitor critical systems based on the enterprise's changing requirements.
- Management services – Services should be structured to support flexibility given the relationship between SIEM provider and enterprise.
- Vendor support – SIEM system design should be based on the customer's needs and support systems should be provisioned accordingly. This offers a value proposition relative to common deployment systems that are not typically customized based on the user's needs.
- Correlation capabilities – A strong SIEM service provider will enable a seamless connection to internal systems without being intrusive. The required secure connections and authentication protocols will need to be accounted for.
- System usability – Systems should be customized to meet the enterprise's needs without resulting in higher costs to achieve customization.
- Investigative capabilities – The split in responsibilities for alarming needs to be laid out. Often times, the SIEM provider provides first level investigative function, or correlation service, while the enterprise's IT department could enjoy a seamless transition to corporate security for second level investigations.
- Console management – The SIEM provider needs to establish a Security Operations Center (SOC) with easy internal access.
- Storage capacity – Any good SIEM provider will need to establish a process to provide for regular capacity planning efforts. On a regular basis, the provider should analyze the capacity needs and report to the client, who will then procure the additional storage.
- Scalability – System functionality should be scaled easily given the nature of the ongoing relationship and system needs.
- Cost viability – In the end, the managed services offering needs to be priced competitively relative to that of competitive solutions.

System Design Considerations

According to Gartner, "innovation in the SIEM market is moving at an exciting pace to create a better threat detection tool."[1] This is certainly true, and more providers are being called upon to offer this valuable service. With many of these new providers emerging from within the telecom sector, some practices with respect to system design should be considered:

- Engineering
    - Patch and update system components as needed
    - Operate the SIEM Infrastructure
    - Plan capacity appropriate for long-term system needs
    - Tune/program filters to reduce number of events managed per day
    - Use rule-based correlation to select incidents for review as a central part of content development
- Correlation
    - Investigate the incidents identified by system against known system intelligence
    - Escalate suspicious incidents for detailed investigation
    - Perform further system tuning based on investigations conducted
    - Keep detailed case notes and change records for future reference
    - Prepare reports based on the "tuned" events
    - Perform ad hoc data extractions as requested by security operations
- Monitoring
    - Maintain continuous monitoring function of the SIEM program
    - Alert analysts of identified incidents flagged by system operations
    - Maintain performance statistics

[1] 2017 Gartner Magic Quadrant for Security Information and Event Management (SIEM), 2017.

Summary

The field of managed services within the SIEM sector promises to grow exponentially in the coming years. Telcos that have the capabilities to provide this needed offering stand to gain as the market clearly has a need to pursue dedicated Security Information and Event Management programs given the growing complexity of systems involved. For any emerging provider, it will be important that five key components be a part of any plan offering in order to ensure full usability:

- Log management functions must always be incorporated. This includes functions that support the cost-effective collection, indexing, storage and analysis of a large amount of information, including log and event data, as well as the ability to search and report on it. Reporting capabilities should include predefined reports, ad hoc reports and the use of third-party reporting tools.
- Compliance reporting must include key capabilities that include user and resource access reporting.
- Security Information and Event Management should always feature real-time data collection, a security event console, real-time event correlation and analysis, and incident management support.
- Deployment and support simplicity should be accommodated through the use of an architecture that supports scalability and deployment flexibility. Large volumes of event data will be collected, and a wide scope of analysis reporting will be deployed.
- User and resource access analysis defines access policies and discovers and reports on exceptions. It enables organizations to move from activity monitoring to exception analysis. This is important for compliance reporting, fraud detection, and breach discovery.

Going forward, there are some key recommendations for any designed program as future needs are accounted for:

- Correlation is a key aspect of SIEM systems, as they normalize logs from various systems, which in turn provides visibility into the most important data needed out of those logs in a readable format
- System usability is a key consideration, as the system operator needs to easily set up policies and rules, create manual reports and schedule automated reports
- System design should incorporate ease of building correlation rules, thereby focusing on the areas of highest risk
- Investigative capabilities are of key importance, including providing a view into not just network behavior, but also user and application behavior