Enterprise Use of Security Information and Event Management Software

Bruce W. Barnes III

Class: ITEC 626

University of Maryland University College

1 May 2016

Abstract

This paper will analyze and justify the utilization of a security information and event management (SIEM) software. SIEM software is software that provides real-time monitoring of events, correlation of audit logs and notification of incidents to appropriate personnel. Large enterprises would benefit greatly from procuring SIEM software as it saves resources while researching potential incidents due to the correlation assembled by the SIEM. Conducting all the actions required to respond to an incident or actively monitor possible intrusions would require several full time employees in large organizations. This can be easily accomplished with the right SIEM software. By procuring a SIEM software, although expensive, it is a worthwhile investment in the defense of an enterprise network and fully justifiable if all duties were done manually. In addition, it meets regulatory compliance requirements such as Sarbanes-Oxley, Risk Management Framework or Health Information Accountability and Portability Act. It also assists in the identification and post-incident event management to implement lessons learned.

Keywords: SIEM, RMF, enterprise software, business case, SOX

Enterprise Use of Security Information and Event Management Software

In this day and age of persistent threats and advanced malware, there is increasingly a need for automated tools to assist in the defense and posture of networks. These tools range from the simple to the advanced. One of the most advanced tools available for commercial use today is Security Information and Event Management (SIEM) software. SIEM is software that "combines security information management and security event management functions into one security management system" (Rouse, 2014). SIEM software greatly enhances cybersecurity of an enterprise, helps with post incident event management, as well as, meets regulatory compliance requirements. These three uses are great reasons to procure SIEM software for an enterprise, but compared to performing these actions manually they are also more cost effective. For all these reasons, an appropriately configured SIEM should be part of the network tools a business enterprise network should maintain.

SIEM

What is SIEM and Examples

Security Information and Event Management software or SIEM is software that correlates log information from various sources and uses that information to create actionable data in real time. As stated above, SIEM is a combination of both security information management and security event management. Security Information Management is the collection of data and log files into a central location for analysis (Security Information Management, 2016). The central location or console is then monitored by a trained professional who responds to alerts. SIM typically is done on hosts, such as computers, servers, routers and switches. Security Event Management is "concerned with the 'real time' activities of network perimeter devices, like firewalls, proxy server, VPN, IDS etc." (ZOHO Corp, 2007). It may also

include some correlation and dashboards. SIEM, being the combination of the SIM and SEM, can be done by a single tool or multiple tools. The objective of SIEM is to help companies respond to incidents rapidly and make sense of the growing amount of logs (Detken, Rix, Kleiner, Hellmann, & Renners, 2015).

Prior to SIEM, logs were stored in many places. The Domain Controller had the audit logs for logon, the Exchange server had the email sent and receive logs, the SNMP viewer had packet loss information, the proxy had IP to website access and the firewall had blocked access attempts. As one can see in the event of an incident, it would be difficult to track down all the relevant information. Then came Syslog servers that allowed all these devices to push their logs to a single repository and perhaps perform some data normalization and alerts. This was a great step, but then what does one do with that information. This is where SIEM comes along and performs real-time data analysis to do more than alert, but actually make administrators aware of a problem when it occurs.

A few SIEM software solutions have risen to the top as leaders according to the Gartner SIEM 2015 Magic Quadrant, Figure 1. The leaders are those that match the general market requirements, show superior vision for anticipated requirements, strong customer support and a high market share. These include IBM Security QRadar, HP Arcsight, Splunk Enterprise and Cloud, and Intel Security's McAfee Enterprise Security Manager (Kavanagh & Rochford, 2015). As one can see, the marketplace is pretty competitive with at 13 vendors that made the cutoff criteria for the Gartner report.

Figure 1. The 2016 magic quadrant from Gartner comparing the competitors in the SIEM market against each other based upon

Enterprise Use and Requirements

In a business enterprise network a decision may be made about the necessity or requirement of having a SIEM software on the network. A review of the requirements of the business and its comparison to the SIEM solutions on the market is the best approach. The three primary reasons to have a SIEM software are for cyber security, log management and regulatory compliance. Many companies procure SIEM "to address regulatory compliance," but are used to assist in their cyber security posture (Kavanagh & Rochford, 2015).

Cybersecurity. 67% percent of a pool of 234 large companies stated a SIEM solution was procured or used for the "detection of security threats in real-time and better security threat awareness" (Netwrix, 2016). SIEM solutions offer this capability out of the box and a major reason for procuring it. Good cyber security is what prevents headlines such as "Billion Dollar Bangladesh Hack" and "Ugly data breach hits 'exclusive' Beautiful people dating site."

A significant portion of the capabilities of SIEM is to provide threat detection and prevention.

Log Correlation. As mentioned above, a form of log correlation exists in the form of a syslog server. Compared to a syslog server, how is a SIEM solution different? Fortunately, Solarwinds has a comparison chart, see Table 1, that shows how their SIEM solution compares to a standard Syslog server (Solarwinds). As one can see, the Solarwinds SIEM solution performs all the functions of a standard syslog server, but also provides dashboards, prebuilt filters, real-time filters and data normalization from varying sources.

The idea behind this log correlation is to bundle the events and information into easier and more manageable alerts. For example, say a user plugs in a thumb drive, remote logs on to another computer, installs software on the remote computer, transfers data and removes the thumb drive. A good SIEM product should be able to take all the information and bundle it together and immediately notify the administrators that a security incident has occurred. In a typical syslog environment, one may look at the logs daily and see that computer 5525 plugged in a USB drive for 5 minutes and that user ChrisX remoted into another PC. The SIEM takes the network, user and PC information and consolidates it into an event that is now actionable. What may have been missed before is now easier to see, and what may have resulted in 5 alerts may now give one or two and provide better information.

SIEM log correlation is the backbone of this solution. The effective log correlation also assists in other activities, like bandwidth usage, peak usage times, trends and uptime. All this information in one location expedites the recovery time from both security incidents and general issue and contingency response.

Regulatory Compliance. A 2016 survey by Netwrix stated that streamlined compliance reporting was one of their key drivers for 50% of respondents. There are multiple compliance requirements that include Health Information Accountability and Portability Act, Sarbanes-Oxley Act, Federal Information System Management Act and Payment Card Industry. Most include some form of requirement for maintaining logs to verify data integrity. As McAfeee's white paper on log management states, "log management has traditionally been the neglected stepchild of information security" (McAfee, 2013). With an appropriate SIEM solution, the regulatory requirements can be met with minimal effort.

The commercial sector is subject to a federal law called Sarbanes-Oxley Act (SOX) that "establish[es] verifiable security controls to protect against disclosure of confidential data, and tracking of personnel to detect data tampering that may be fraud related" (Correlog, 2011). The two main sections related to log analysis are sections 302 and 404 which detail these requirements. SOX requires protections against tampering of data and the ability to be verified by independent auditors. These requirements detail out that one must maintain logs that can verify any changes in data or information. SOCVue is EiQ's SIEM solution and has a handy chart for SOX compliance to include the critical security control of maintenance, monitoring and analysis of audit logs which it meets (EiQ, n.d.). Another SIEM competitor, Correlog has a whitepaper detailing out how they meet SOX requirements. Specifically be timestamping all data as received, tracking user access to PCs, high throughput rate, continuous monitoring, requires minimal training, and tests network and file integrity periodically (Correlog, 2011).

The federal sector includes a recently developed risk management framework (RMF) developed by the National Institute of Standards and Technology (NIST). This framework is mandated for use in all federal information systems. The idea is security controls should only be

implemented if it is right for the system. In the past, a system that could fire warheads was held to very similar standards of a map kiosk at a hospital. Because of this, an extensive review of understanding the system and enterprise is required.

In the category of Audit Review, Analysis and reporting AU-6 stipulate "the organization employs automated mechanisms to integrate audit review, analysis and reporting processes to support organizational processes for investigation and response to suspicious activities" (Joint Task Force Transformation Initiative, 2013, pp. F-45). It also stipulate being able to on-demand review and analyze logs after-the-fact. Outside the controls, the risk management framework requires organizations to continuously monitor and evaluate changes in the system.

These regulatory requirement under RMF essentially mandates the use of SIEM software for government systems. The one caveat to the automation is that it is only required for when the system processes any data that is considered moderate or high. This means if a system does not process financial records, personnel records, contingency planning, or other data than a SIEM may not be required. The United States Army, Air Force and the Defense Information Systems Agency have all procured various SIEM software to include EiQ SecureVue for regulatory compliance (EiQ, n.d.). The end aim is to meet the regulatory requirements for continuous monitoring per the NIST Special Publication 800-53.

Cost Analysis

According to ComputerWeekly, only 32% surveyed have SIEM installed and the key factors for purchasing are price and features. A respondent also stated that "unless fully integrated and deployed, it's basically a log manager" (Ashford, 2013). An efficiency survey came to the conclusion that the total cost of ownership is a main concern for procuring SIEM (Netwrix, 2016).

SIEM's are expensive for small and some medium business enterprises. In an IEEE conference in Warsaw, they showcased methods of using SIEM with opens source tools that would reduce the costs to be viable for small and medium business enterprises (Detken, Rix, Kleiner, Hellmann, & Renners, 2015). Table 2 includes a price comparison of various SIEM providers that had their pricing information available readily on their company's website. For a 500 user company, the average price for a SIEM annual is approximately $50,458.75.

Table 2

SIEM Solution Price Comparison

SIEM Solution	Price	Details
Solarwinds	$40,035	500 Nodes
Splunk	$57,000	50 GB/day
IBM QRader SIEM	$55,800[1]	Unknown
HP Arcsight	$49,000	500 PCs and 40 Network

Note. [1] Could not identify limits on this price, but was in comparable price range as others.

System Administrators make on average in the United States $65,273 (Glassdoor, 2015). A simple check of if the requirement and compliance reporting would require hiring an additional System Administrator, it is cost beneficial to procure a SIEM solution e.g. $65k versus $50k. The System Administrator salary is also not fully burdened, in that it doesn't include support and benefits of the position. It also doesn't address the total cost of ownership, including training, time saved, and deployment and installation.

From my experience, most training courses run about $5,000. So adding this to the SIEM column, brings the cost edge closer, but still in favor of a SIEM.

A typical incident may require two to six hours to research and identify the root cause. At 12 incidents a year, $50/hour is $2,400. One point that should be considered is that a SIEM may prevent a certain number of incidents. If we assume a 50% reduction, we are looking at a $1,200

savings for SIEM. In addition, with SIEM we may also see another 50% reduction in research time, revealing another $600 in savings.

Annual regulatory compliance reporting should also be considered. At $50/hour, a savings of a man-week can save $2,000 over manually finding and compiling a report. The reason this is possible is a main feature of SIEM products includes the regulatory compliance reporting. One just needs to ensure it is in the product features prior to procurement.

When all these numbers are added together, we obtain that a System Administrator would still cost $65,000 per year. The SIEM solution comes in at $51,200, making it a clear winner.

In the event a business was not looking to hire an additional employee to take on these roles, we are still looking at a potential 80 hours' worth of time saved. It must also be considered that although a SIEM solution might not produce a return on investment for every situation, it does reduce risk overall. What is the value in avoiding a news headline about a company data breach?

Conclusion

Security Information and Event Management software is software that performs the real-time, continuous monitoring and log correlation required to meet regulatory compliance, increase cyber security posture and expedite post incident management.

SIEM solutions all perform some form of log correlation and centralization. This is critical for most businesses.

The SIEM solutions also greatly support the auditing and regulatory requirements. Whether it is the Sarbanes-Oxley Act, Federal Information System Management Act, Risk Management Framework, Health Information Accountability and Portability Act, or even Payment Card Industry standards, SIEM satisfies the requirements for auditing.

As shown, SIEM software is also cost beneficial to a medium sized business that is comparing hiring an additional System Administrator with the annual cost of SIEM.

References

Ashford, W. (2013, January 28). *IT Security Purchasing Intentions 2013 - Europe*. Retrieved from ComputerWeekly: http://www.computerweekly.com/photostory/2240176697/Security-Media-Purchasing-Intentions-2013-Europe/6/Take-up-of-Security-Information-and-Event-Management-SIEM-technology

Correlog. (2011). *SOX-Compliance*. Retrieved from Correlog.com: https://correlog.com/support-public/SOX-Compliance.pdf

Detken, K., Rix, T., Kleiner, C., Hellmann, B., & Renners, L. (2015). SIEM approach for a higher level of IT security in enterprise networks. *8th IEEE International Conference on Intelligent Data ACquistion and Advanced Computing Systems.* Warsaw.

EiQ. (n.d.). *SecureVue Security Intelligence Platform*. Retrieved from EiQNetworks: https://www.eiqnetworks.com/federal/overview

Glassdoor. (2015, November 4). *Salary: System Administrator*. Retrieved from Glassdoor.com: https://www.glassdoor.com/Salaries/us-system-administrator-salary-SRCH_IL.0,2_IN1_KO3,23.htm

Gosier, G. F. (2009). Analyzing Malware Log Data to Support Security Information and Event Management: Some Research Results. *Advances in Databases, First International Conference*, 108-113. doi:http://doi.ieeecomputersociety.org/10.1109/DBKDA.2009.26

Joint Task Force Transformation Initiative. (2013, April). *Security and Privacy Controls for Federal Information Systems and Organizations (SP 800-53).* Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Kavanagh, K., & Rochford, O. (2015, July 20). *Magic Quadrant for Security Information and Event Management*. Retrieved from Gartner: https://www.gartner.com/doc/reprints?id=1-2JM104C&ct=150720&st=sb

Logrhythm, Inc. (2015, October 21). *Critical Capbilities Use Cases for Security Informaiton and Event Management.* Retrieved from Bitpipe.com: http://www.bitpipe.com/detail/RES/1444917356_20.html

McAfee. (2013). *Log Management - The Foundation for Federal Security and Compliance.* Retrieved from Mcafee White Paper - Log Management: http://www.mcafee.com/it/resources/white-papers/wp-log-management.pdf

NetForensics. (2009). *Essential Practices for Achieving Security Compliance Management.* Retrieved from Blackstratuc.com: http://www.blackstratus.com/assets/Whitepapers/WPnFXSCM.pdf

NetForensics. (2010). *SIEM in the Cloud: Cost-effective solutions for Taking Control of Data Overload and Scaling Security.* Retrieved from Blackstratus.com: http://www.blackstratus.com/assets/Whitepapers/nfxCloud.pdf

Netwrix. (2016). *2016 SIEM Efficiency Survey.* Retrieved from Netwrix: https://start.netwrix.com/siemsurvey2016.html

Nicolette, M. a. (2011, May 12). *Magic Quadrant for Security Information and Event Management.* Retrieved from Jameskaskade.com: http://jameskaskade.com/wp-content/uploads/2011/06/Magic-Quadrant-for-Security-Information-and-Event-Management.pdf

Rouse, M. (2014, December). *What is Security Information and event management*. Retrieved from TechTarget: http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

Security Information Management. (2016). *Security information management.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Security_information_management

Solarwinds. (n.d.). *Comparing SolarWinds Log & Event Manager to Kiwi Syslog Server.* Retrieved from Solarwinds.com: http://www.solarwinds.com/log-event-manager/kiwi-vs-lem.aspx

ZOHO Corp. (2007). *Analyzing Logs for Security Information Event Management - Whitepaper.* Retrieved from Manageengine: https://download.manageengine.com/products/eventlog/Analyzing-Logs-for-SIEM-Whitepaper.pdf

Tables

Table 1

Feature Comparison between Syslog and SIEM

Use Case	Syslog	Log and Event Manager
Consolidates Log events across multiple Systems	Yes	Unlimited
Filtered views base on event criteria	Yes	Yes
Long term log archival and search	Yes	Yes
Real-time dashboard with visualizations	No	Yes
Consolidates log events across Syslog, SNMP, flat log files, databases	No	Yes
Filter Log events on multiple criteria	Yes	Yes
Real-time log and environment information filters	No	Yes
Over 700 rules, alerts filters & reports for security & compliance best practices	No	Yes
USB Detection & Prevention	No	Yes
Cost	$295	$4495