International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Study on Critical Capabilities for Security Information and Event Management

Kavita Agrawal[1], Hemant Makwana[2]

Department of CS, Institute of Engineering & Technology, D.A.V.V., Indore, India

Reader, Department of IT, Institute of Engineering & Technology, D.A.V.V., Indore, India

Abstract: ***Security Management is the crucial issue in the IT Industry. IT industries require a tool which can help in managing the information and events and enhance the level of security. Security information and event management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security. SIEM tools can analysis on the basis critical capabilities for any product. In this paper, discussed about some of the important critical capabilities for any product and vendors for SIEM tool. Each of the products/services for different tools has been evaluated on the critical capabilities.***

Keywords: Compliance, Threat Intelligence, Event Management, log analysis, log management

1. Introduction

Security information and event management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security. The underlying principle of a SIEM system is that relevant data about an enterprise's security is produced in multiple locations and being able to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary. SIEM combines SIM (security information management) and SEM (security event management) functions into one security management system. A SEM system centralizes the storage and interpretation of logs and allows near real-time analysis which enables security personnel to take defensive actions more quickly. A SIM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralized reporting. By bringing these two functions together, SIEM systems provide quicker identification, analysis and recovery of security events. They also allow compliance managers to confirm they are fulfilling an organization's legal compliance requirements. A SIEM system collects logs and other security-related documentation for analysis. Most SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network equipment and even specialized security like firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies. To allow the system to identify anomalous events, it's important that the SIEM administrator first creates a profile of the system under normal event conditions. [1][2]

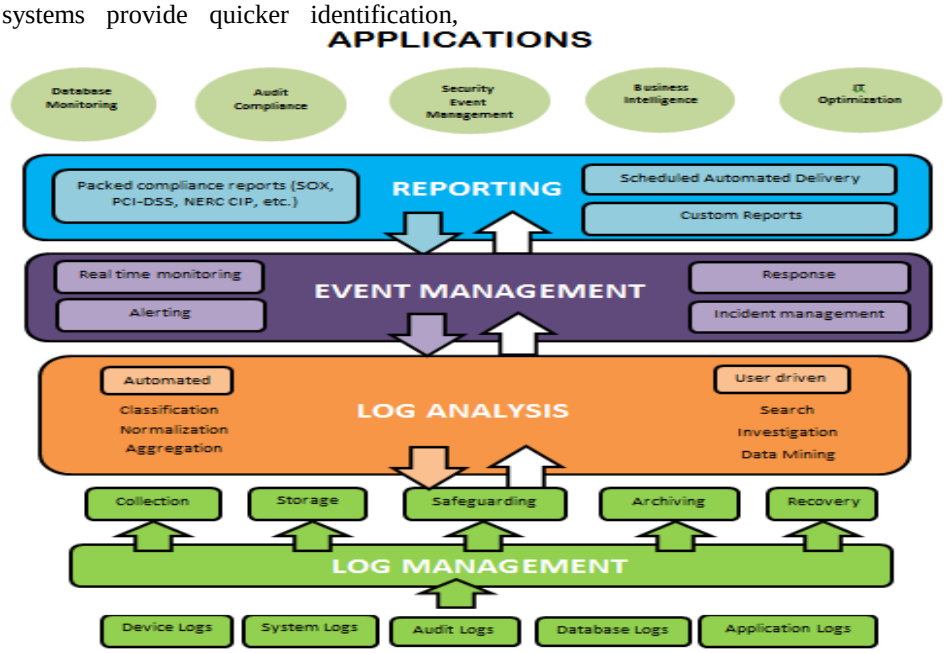

Figure 1: Flowchart of working of SIEM tools [3]

vendors, and data developed by managed security and other service providers. Threat intelligence data can be integrated with a SIEM in the form of watchlists, correlation rules and queries in ways that increase the success rate of early breach detection.

- **Behavior Profiling**

When abnormal conditions are well-defined, it's possible to define correlation rules that look for a specific set of conditions. It is very difficult to cover all the conditions that are abnormal with a rule-based approach. Anomaly detection can complement rule-based approaches, because it alerts organizations to deviations from normal. Profiling and anomaly detection are emerging capabilities in SIEM that complement rule-based correlation. Behavior profiling employs a learning phase that builds profiles of normal activity for various event categories, such as network flows, user activity and server access. The monitoring phase alerts on deviations from normal. Profiling and anomaly detection are emerging capabilities in SIEM that complement rule-based correlation.

- **Data and User Monitoring**

User and data activity monitoring that includes user and data context is needed for breach and misuse discovery. Privileged user and sensitive data access monitoring is also a common requirement for compliance reporting. This capability establishes user and data context, and enables data access and activity monitoring. Functions include integration with IAM infrastructure to obtain user context and the inclusion of user context in correlation, analytics and reporting. Data access monitoring includes monitoring of DBMSs and integration with FIM and DLP functions. DBMS monitoring can take three forms — parsing of DBMS audit logs, integration with third-party DAM functions or embedded DAM functions. FIM can be provided by the SIEM product directly or through integration with third-party products.

- **Application Monitoring**

This is critical because application weaknesses are frequently exploited in targeted attacks, and abnormal application activity may be the only signal of a successful breach or of fraudulent activity. The ability to parse activity streams from packaged applications enables application-layer monitoring for those components, and the ability to define and parse activity streams for custom applications enables application-layer monitoring for in-house-developed applications. Integration with packaged applications, an interface that allows customers to define log formats of unsupported event sources, and the inclusion of application and user context are important capabilities that enable the monitoring of application activities for application-layer attack detection, fraud detection and compliance reporting.

- **Analytics**

When suspect activity is surfaced by security monitoring or activity reporting, it is important to be able to analyze user and resource access in using an iterative approach to start with a broad query about an event source, user or target, and to then initiate increasingly focused queries to identify the source of the problem. Security event analytics are composed of dashboard views, reports and ad hoc query functions to support the investigation of user activity and resource access in order to identify a threat, a breach or the misuse of access rights.

- **Log Management and Reporting**

Log management has become part of the standard of due care for many regulations. Compliance-oriented deployments are simplified when the SIEM technology includes predefined and modifiable reports for user activity, resource access and model reports for specific regulations. Functions supporting the cost-effective storage and analysis of a large information store include collection, indexing and storage of all log and event data from every source, as well as the capability to search and report on that data. Reporting capabilities should include predefined reports, as well as the ability to define ad hoc reports or use third-party reporting tools.

- **Deployment/Support Simplicity**

Compliance and security requirements have extended the SIEM market to organizations that have smaller security staffs and more-limited system support capabilities. For these buyers, predefined functions and ease of deployment and support are valued over advanced functionality and extensive customization. Deployment and support simplicity is achieved through a combination of embedded SIEM use-case knowledge, and a general design that minimizes deployment and support tasks. Embedded knowledge is delivered with predefined dashboard views, reports for specific monitoring tasks and regulatory requirements, a library of correlation rules for common monitoring scenarios, and event filters for common sources. There should also be an easy way to modify the predefined functions to meet the particular needs of an organization.

2. Vendors for SIEM

Few vendors for SIEM are listed in random order, not in order of performance or capabilities.

4.1 HP (Arc Sight)

HP ArcSight provides three SIEM offerings:

- ArcSight Enterprise Security Manager (ESM) software for large-scale event management
- ArcSight Express: Appliance for SIEM functions for small and midsize deployments
- ArcSight Logger: Line of appliances, software and connectors for log management and reporting

The capability to deploy Logger in combination with ArcSight Connectors provides additional options for normalized data analysis and application-layer data collection. HP is using ArcSight to unify event management across its security technologies, and to provide an integrated view of operations and security events. There is integration among ArcSight, Fortify, TippingPoint and IT Performance Suite (Operations Manager and Network Node Manager) products. ArcSight is also integrated with HP EnterpriseView, which provides a business-centric view of IT that includes security assessment, security event and compliance data. [7]

4.2 IBM Security (QRadar)

IBM Security QRadar can be deployed as all-in-one solutions for smaller environments, or it can be horizontally scaled in larger environments with specialized event collection, processing and console appliances. A distinguishing characteristic of the technology is the collection and processing of NetFlow data to provide network and application behavioral analyses, and behavior analysis capabilities for all events collected from any source. IBM Security also provides an optional component, QRadar Risk Manager, which adds network and firewall configuration monitoring and configuration context to event analysis. [8]

4.3 McAfee (ESM)

McAfee Enterprise Security Manager (ESM) combines SIM and SEM functions and is available as stand-alone, all-in-one, virtual appliances and is delivered as a managed service by partners. Capabilities can be extended and enhanced with a range of specialized add-on products, such as Database Event Monitor (DEM), which provides database activity monitoring and analysis, Application Data Monitor (ADM) for application monitoring, and Global Threat Intelligence (GTI). McAfee is further developing integration of ESM with its wider security portfolio to enable context about vulnerabilities, endpoint state and threats, and to enable automated response and blocking. [9][10]

4.4 Splunk

Splunk provides log management, analytics and statistical commands that facilitate real-time correlation and visualization. Running on Splunk Enterprise, the Splunk App for Enterprise Security provides predefined dashboards, searches, reports, and alerts to support security monitoring and analytics use cases. Splunk is most often deployed by IT operations and application support areas to gain log management and analytics for availability-oriented use cases and, because of these deployments, the vendor is often on SIEM shortlists as an incumbent vendor.[11][12]

4.5 LogRhythm

LogRhythm provides SIEM appliance and software technology to midsize and large enterprises. The SIEM technology can be deployed as a single appliance or software instance in smaller environments —configured to provide log management, event management and real-time analytics. In larger environments, it can be scaled as a set of specialized appliances and/or software instances (log management, event management and real-time analytics).Network forensic capabilities such as deep packet inspection and flow monitoring are supported via LogRhythm's Network Monitor. The technology also includes optional agents for major OSs that can be used for filtering at the source and to provide capabilities such as file and host activity monitoring. [13]

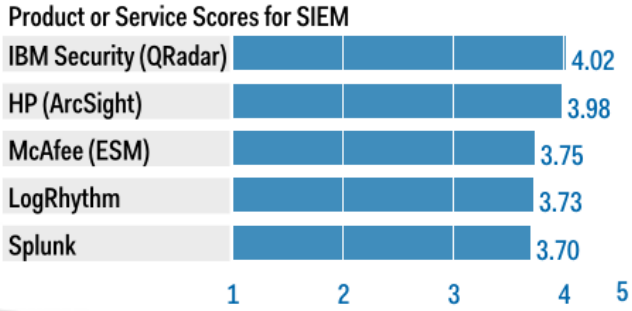

Figure 2: Vendors' Product Scores for SIEM [14]

3. Conclusion

Organizations evaluating security information and event management (SIEM) tools should begin with a requirements definition effort that includes IT security, IT operations, internal audit and compliance. Organizations must determine deployment scale, real-time monitoring, postcapture analytics and compliance reporting requirements. In addition, organizations should identify products whose deployment and support requirements are good matches to internal project and support capabilities.

The methodology requires analysts to identify the critical capabilities for a class of products. Each capability is then weighted in terms of its relative importance overall as well as for specific product use cases. [15]

Each vendor’s product or service is evaluated in terms of how well it delivers each capability, on a five-point scale.

Critical Capabilities Rating

Each of the products/services for different tools has been evaluated on the critical capabilities on a scale of 1 to 5

1 = Poor (most or all defined requirements not achieved)
2 = Fair (some requirements not achieved)
3 = Good (meets requirements)
4 = Excellent (meets or exceeds some requirements)
5 = Outstanding (significantly exceeds requirements)

Table 1: Product/Service Rating on Critical Capabilities [4][14][15]

Critical Capabilities	HP (Arc sight)	IBM (QRadar)	McAfee (ESM)	Splunk	LogRhythm
Real-time monitoring	4.1	4	3.8	3.7	3.8
Threat intelligence	4	4	4	3.5	3.2
Behavior profiling	4	4.5	3.5	3.6	3.4
Data and user monitoring	4.2	3.8	4.4	3.3	3.4
Application monitoring	4.5	4.3	4.2	4.3	4.1
Analytics	3.8	3.7	3.6	3.8	3.3
Log management and reporting	4	3.8	3.2	4	3.8
Deployment/Support Simplicity	3.7	4.3	4	3.4	4.2

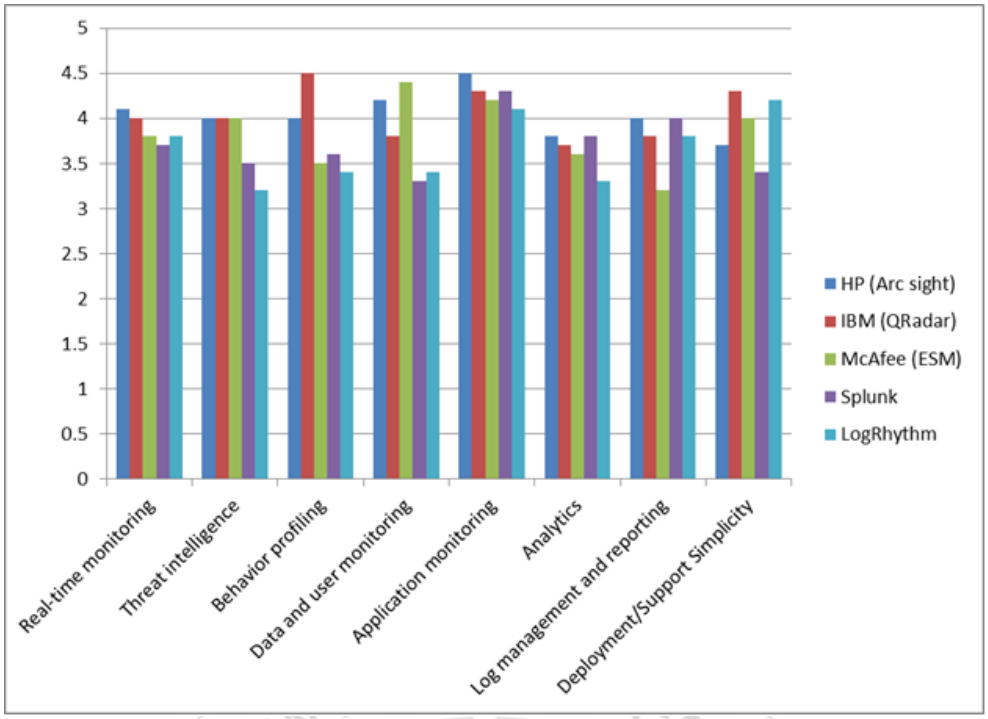

Figure 3: Graph showing Product/Service Rating on Critical Capabilities [4][14][15]

The critical capabilities selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Organizations should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision. It is also recommended that users/ organizations consider the set of critical capabilities as some of the most important criteria for acquisition decisions.[16]

References

[1] http://searchsecurity.techtarget.com/definition/security-information-and-event-management- SIEM
[2] https://en.wikipedia.org/wiki/Security_information_and_event_management
[3] http://www.ip-performance.co.uk/logeventmanagementfileintegritymonitoringendpointmonitoringcontroloneintegratedsolution_132.php
[4] Critical Capabilities for Security Information and Event Management by Mark Nicolett, Kelly M. Kavanagh, 7 May 2013
[5] http://www.gartner.com/technology/research/methodologies/research_critcap.jsp
[6] http://www.sans.org/reading-room/whitepapers/analyst/real-time-approach-continuous- monitoring
[7] http://www8.hp.com/in/en/software-solutions/siem-security-information-event-management/
[8] DataSheet on 'IBM QRadar Security Intelligence Platform'
[9] http://www.mcafee.com/in/products/enterprise-log-manager
[10] http://www.mcafee.com/in/products/enterprise-security-manager.aspx
[11] http://www.slideshare.net/sbelyaeva/2-21677-splunkbigdatafutureofsecurity
[12] http://www.decisionreport.com.br/download/WhitePaper_Splunk.pdf Splunk, Big Data and Future of Security
[13] https://www.logrhythm.com
[14] Magic Quadrant for Security Information and Event Management by Kelly M Kavanagh, Mark Nicolett, Oliver Rochford, 25 June 2014
[15] Critical Capabilities for Security Information and Event Management Technology by Mark Nicolett, Kelly M Kavanagh, 12 May 2011
[16] http://www.gartner.com