ISSN: 2321-8169
6459 - 6463

# A Study on Capabilities and functionalities of Security Information and Event Management systems(SIEM)

Dhawal S. Shah
Student, Department Of IT,
K J Somaiya College of Engineering,
Mumbai, India.

***Abstract*—**Security Management is the important issue in the IT Industry. IT industries is in need of a tool which can help in managing the information and events and increase the grade of security. Security information and event management (SIEM) offers a new approach to security management by providing a holistic view of the business information technology security. SIEM tools can be reviewed on the basis its critical capabilities as for any product. This paper discusses about some of the important capabilities for any SIEM product, also few current vendors for SIEM tool are evaluated in terms of those critical capabilities of SIEM.

***Keywords:*** *Compliance, Threat Intelligence, Event Management, log analysis, log management, Security Information and Event management*

*****

## I. INTRODUCTION

Security information and event management (SIEM) technology is an important asset of an organization's security infrastructure, because it cover all points for all forms of security monitoring. It can be used to detect a targeted attack in its early phases to minimize damage. SIEM tools provide monitoring of user activity data access along with reporting for threat detection. It also helps to satisfy audit requirements.[1][2]

SIEM technology has features for threat management, security incident response, incident investigation and security policy compliance monitoring with the collection and analysis of security events and reporting on historical data from these sources. The core capabilities of SIEM technology are the event collection and the ability to correlate, further analyze events across distinct information sources. The technology is typically deployed to:

- Identify external and internal threats
- Trace the activities of users
- Monitor IT infrastructure resource access
- Support compliance reporting
- Investigate and present analytics, workflow to support incident response

SIEM technology collects and helps to further analyzes the event data produced by devices, systems and applications. The primary data source is log data, because they provide powerful visibility and network security intelligence of user behaviors, network anomalies, system downtime, policy violations, internal threats, etc. The data first undergoes normalization, so that events from distinct sources can be correlated and further analyzed for specific purposes, like network security and user activity monitoring.[1][2]

In this paper, the challenges faced by IT administrators while dealing with terabytes of log data to ensure IT security are discussed. It also focus on critical capabilities which are found common to most SIEM solutions. Finally, the comparison of various SIEM solution are discussed in terms of capabilities.

## II. NEED FOR SIEM SYSTEMS

The following are the few key log management challenges that organization's face.

### *A. Analyzing Logs for Security Intelligence:*

Fetching relevant information in real time from terabytes of log data is the greatest challenge usually faced by network administrators. Performing manual analysis and correlation of log data for IT security is difficult and prone to human error.[1]

### *B. Centralizing Log Collection:*

Collecting log data from disparate sources (Operating systems, applications, databases, routers, switches, firewalls, etc.) at a central place can be a difficult task for IT administrators. Using different tools to manage different log formats from numerous devices, systems, and applications is not an impressive way to manage the logs in an enterprise.[1][2]

### *C. IT Compliance Requirements:*

Compliance Auditors always remained a challenge for the IT administrators, as they have to provide compliance data to them. Compliance reports have to be ready, and the reports should remain backed up with the appropriate log data and with the data management tools used. Meeting compliance requirements laid down by regulatory bodies such as FISMA, PCI DSS, SOX, HIPAA, ISO 27001, etc. is impossible without effective log management and compliance tool[1][2]

### *D. Investigating Root Cause Analysis:*

Searching across logs to spot the root cause of any network or event based problem has been difficult task for the administrators. They struggle for search capabilities that should help them to conduct log forensics, which may help them to find and remediate any network issues or anomalous behavior quickly. [1][2]

### E. *Visualizing log data:*

Viewing and presenting any data graphically is usually preferred. Network administrators always struggle to have better data representation in different graphical formats, reports, and dashboards. The dashboard is one of the most preferable components of an IT security solution. It acts as the primary interface to monitor real-time events and perform log data analysis.[1][2]

### F. *Tracking Suspicious User Behavior:*

IT administrators find it difficult to monitor user activities in real time across the IT infrastructure. It help to detect data thefts, outages, and system crashes and prevent monetary loss for enterprise Enterprises struggle for real-time monitoring and notifying mechanism when any anomalous activity occurs on their network devices, applications, systems, files, and more. [1][2]

## III. Basic SIEM Capabilities

Today most of the SIEM vendors option's available in the market comprises of the basic capabilities described below:

### A. *Log collection:*

A SIEM solution has the capability to collect logs from various sources and aggregate at a central location. It acts as a central repository to analyze any log data format from any source.[1]

### B. *Log Analysis:*

Parsing raw log data and fetching intelligence from IT security devices in real time is the core function of any SIEM solution. The raw log data is parsed and analyzed to fetch relevant actionable security data and represented in easy-to-understand charts, graphs, and reports. [1]

### C. *Event Correlation:*

Correlation of events provide organization a platform to increase visibility of their network security by processing millions of events simultaneously to detect threats and anomalous events on the network.

### D. *Log Forensics:*

SIEM solutions provide security professionals a platform to conduct log forensic investigation by allowing them to investigate a root cause analysis to track down a network intruder or the event activity that caused the network problem.

### E. *IT Compliance:*

SIEM solutions provides a platform for IT compliance reporting. Few SIEM solutions offers regulatory compliance reporting functionalities to cover various regulatory compliance standards, such as PCI DSS, FISMA, GLBA, SOX, HIPAA. [1]

### F. *Dashboards:*

SIEM solutions provides dashboards which help IT administrators to perform timely action and take the right steps during incidents. It helps to present security data in a very graphical manner. The dashboards are fully customizable so that IT administrators can add and view the security information as per their need. [1]

### G. *System and Device Log Monitoring:*

The log data generated by your network and IT security device contain crucial information that can be use to mitigate security incidents. It also helps to reduce network downtime, increase network performance, and strengthen network security.

### H. *Log Retention:*

Log retention or archiving is very important for organizations, as log storage has became a part of various compliance regulatory requirements.[1][2]

## IV. Advanced SIEM Capabilities

As already mentioned, the above mentioned capabilities are generally found in every SIEM options available today. The current market players provide advanced capabilities, which leads to competitive environment among them, few of such advanced capabilities along with details of the component available in current SIEM vendors are as follows:

### A. *RealTime Monitoring*

RealTime Monitoring is important for threat detection and for user activity monitoring. Event correlation helps to derive relationships among logs or events that are generated by devices, systems or applications, based on characteristics like the source, target, protocol or event type. The SIEM should have a library of predefined correlation rules which are common to most organizations and also the ability to easily customize those rules. A security event console should provide the realtime presentation of security incidents and events. [4][5][6]

- HP Arcsight: ArcSight ESM provides the capabilities needed for large scale, SEM focused deployments, but it has been complex to implement and manage. ESM replaced a major source of complexity and cost “the Oracle Database” with the purpose built Correlation Optimized Retention and Retrieval (CORR) Engine.[4][12]
- IBM Qradar: The QRadar technology provides an integrated view of the threat environment using NetFlow and direct network traffic monitoring, in combination with log based event sources.[4][7][9]
- LogRhythm: LogRhythm has more than 500 Predefined monitoring rules, and new modules providing specialized correlation rules, saved searches and dashboards for specific threats and topics such as privileged user monitoring, network anomaly detection and advanced persistent threats (APTs) were added. Network Monitor adds network traffic monitoring and forensic capabilities and allows correlation with log based sources. [5][10]
- Splunk: The Splunk App for Enterprise Security includes predefined mapping for security event sources, security specific correlation searches, reporting and security monitoring dashboards. [4][8]

- Mcafee: McAfee ESM supports rule based and risk based correlation. Data from event and log sources, dynamic watch lists and threat intelligence can be used for correlation. The McAfee Advanced Correlation Engine (ACE) adds the capability to correlate NetFlow and event data, and run correlations against historic data.[5][11]

### B. *Threat Intelligence*

Live information on threats and attack patterns can help an organization recognize abnormal activity. For example, a small amount of outbound activity to an external IP address might look normal and would be easily ignored. Everything changes if there is threat intelligence that indicates that the destination is associated with a botnet command and control center. Information about the current threat environment exists in a variety of sources, including open source lists, the threat and reputation content developed and maintained by security research teams within security vendors, and data developed by managed security and other service providers. Threat intelligence data can be integrated with a SIEM in the form of lookups, correlation rules and queries in ways that increase the success rate of early breach detection. [4][5][6]

- HP Arcsight: Arcsight provides support Threat response manager as an addon component that can perform network threat mitigation based on event triggers from ArcSight RepSM(Reputation Security Monitor) and other third party security solutions, such as iDefense and DeepSight. HP Reputation Security Monitor (RepSM) is an optional component that receives near realtime reputation feeds from HP research labs. [4][13]

- IBM Qradar: QRadar includes an auto update service that maintains current threat information such as top targeted ports, botnets, emerging threats, bogon IPs, hostile nets, darknets and anonymous proxy. In addition, IBM Security provides an integration of XForce IP Reputation data into QRadar that can be refreshed on a daily schedule. [4][7][9]

- LogRhythm: LogRhythm provides its own threat intelligence via the LogRhythm Advanced Intelligence (AI) Engine, but there is no specific support for commercial feeds.[5][10]

- Splunk: Splunk has released the threat intelligence framework, which maps multiple feeds into a single framework to enable deployment into common watchlists. Splunk supports a broad range of threat intelligence feeds. Users can add additional threat intelligence sources. On demand lookup is supported for databases, including DShield and CentralOps.net's Domain Dossier, Norse intelligence feed.[4][8]

- Mcafee: McAfee Global Threat Intelligence for ESM provides threat context and is available as an additional module. McAfee ESM also supports the integration of third party threat intelligence services via dynamic watch lists.[5][11]

### C. *Behavior Profiling*

When abnormal conditions are well defined, it's possible to define correlation rules that look for a specific set of conditions. However such signature based approach proves insufficient to cover all the abnormal conditions. Anomaly detection can comes to help under such condition, because it alerts organizations to deviations from normal. Anomaly detection is emerging capabilities in SIEM that complement rule based correlation. Behavior profiling is 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. [4][5][6]

- HP ArcSight: ArcSight provides two functions for behavior analysis. IdentityView has a set of detection rules to issue alerts in real time. The second is ThreatDetector, which performs historical analysis of logs to detect and graphically display statistically significant patterns.[4][12]

- IBM Qradar: Qradar has ability to perform network anomaly detection in such a sophisticated manner that complements SiteProtector deployments by adding NetFlow and anomaly detection to the SiteProtector IDS. [4][7][9]

- LogRhythm: LogRhythm supports monitoring against whitelists, average trends, rate trends and histogram trends. It also has the ability to create behavioral whitelists and baselines from host, application and user data, as well as Network Monitor session data.[5][10]

- Splunk: Splunk statistical analysis functions (over 100 commands) can be used to identify anomalies and deviations from normal behavior. User has to create conditions and use cases to detect anomalies with the use of such commands.[4][8]

- Mcafee: The McAfee ESM correlation engine supports statistical and baseline anomaly detection, as well as risk based correlations. McAfee Application Data Monitor provides network anomaly detection, and McAfee Advanced Correlation Engine can be used to correlate and profile network and event data. [5][11]

### D. *Data and User Monitoring*

User and data activity monitoring should have capability to establish user and data profiles, and enables data access and activity monitoring. Functions may include integration with Identity and access management(IAM) infrastructure, File integrity management(FIM) and Data loss prevention (DLP). DBMS monitoring should cover DBMS audit logs, integration with third party DAM functions or embedded DAM functions. [4][5][6]

- HP ArcSight: ArcSight supports integration with Active Directory and network authentication sources, major DLP and FIM products. However integration with Identity and access management (IAM)systems is separately chargeable. ArcSight also maintains connectors with database audit and protection (DAP) products, and supports direct collection from database audit logs. There is no native FIM or DLP capability. [4][13]

- IBM Qradar: QRadar provides support for integration with Active Directory and network authentication devices, QRadar also integrates with IAM technologies from few third party technologies. DAM is supported through direct monitoring of major DBMS logs and through integration with third party database monitoring products from IBM InfoSphere Guardium, Imperva, McAfee and Application Security. This also integrates with third party FIM and DLP products.[4][7][9]
- LogRhythm: In addition to integration with Active Directory and standard network authentication sources, there are integrations with IAM technologies from few third party technologies. The Identity Inference Engine adds missing identity information to anonymous log data. There is also support for integration with Symantec's DLP technology. LogRhythm can also monitor database audit logs, and there is scope for integration with third party DAM technologies.[5][10]
- Splunk: Splunk provides a Windows Management Instrumentation collector for Active Directory, integration with LDAP, IAM event sources. Splunk agent provides basic FIM functions (essentially change detection). Splunk has released predefined mapping support for third party DLP products. [4][8]
- Mcafee: Mcafee ESM provides support for Active Directory and LDAP. McAfee ESM can also directly monitor database audit logs. ESM can be integrated with McAfee Vulnerability Manager for databases. For FIM and DLP, there is also support for various Mcafee and third party products. [5][11]

### E. *Application Monitoring*

This is critical because application vulnerabilities are frequently exploited in targeted attacks, and abnormal application activity may be the only signal of a successful breach or of fraudulent activity. SIEM should have ability define and parse activity streams from packaged or custom applications upto application layer. 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. [4][5][6]

- HP Arcsight: HP Arcsight provide connectors for major packaged and service as a software (SaaS) applications like Oracle, SAP and salesforce.com. There is support for event collection from custom online applications and correlation across other fraud products to evaluate device, destination, account and transaction risks. HP Fortify Runtime technology is used and implements a JAR file that runs with the application on the application server. It monitors method calls by the application, with many activities monitored out of the box. There is also a customization interface for transaction monitoring. [4][5]
- IBM Qradar: There is integration with a variety of applications, including major Web application firewall and Web server technologies. There is also an integration with the SAP audit log, and a capability to monitor application behavior from the network using QFlow sensors.[4][7][9]
- LogRhythm: LogRhythm integrates with a large number of packaged applications, including SAP, Oracle's PeopleSoft, and a variety of other ERP and HR applications. There are also integrations with Web application servers and firewalls. Network Monitor adds application awareness via deep packet inspection and application identification for more than 2,000 applications.[5][10]
- Splunk: Splunk provides specialized add ons for a number of commercial applications, but only a few of these sources are supported with event mapping, predefined searches and reports. [4][8]
- Mcafee: The McAfee ADM component provides network based activity monitoring for an extensive list of applications. Direct Web server log integration is limited to Apache and Microsoft IIS. SAP and Oracle's PeopleSoft are supported via a direct integration. Support for industrial control systems and SCADA servers is also provided. [5][11]

### F. *Analytics*

When suspect activity is detected 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.[4][5][6]

- HP Arcsight: Arcsight ESM provides trend analysis functions. Arcsight ESM query performance and resource efficiency has been improved via the CORR-Engine. ArcSight has integrations with Business Service Management, and there are ArcSight connectors for Hadoop and Autonomy.[4][12]
- IBM Qradar: Analytics are supported directly from QRadar distributed event data. QRadar has two way integration with InfoSphere BigInsights (IBM's commercialized Hadoop offering) and also with IBM's analytics and data visualization technologies (InfoSphere BigSheets and i2 Intelligence Analysis). [4][7][9]
- LogRhythm's: Search and structured analysis can be done directly via query language, or by drilling down from dashboard widgets. These can be customized to provide usecase specific views, visualizations and analytics, and can accommodate data point pivoting and filtering.[5][10]
- Splunk: The Splunk App for Enterprise Security provides predefined dashboards that support drill down

to intermediate data aggregations, raw data, and pivoting to look at the data from different perspectives. During 2013, Splunk introduced new visualizations for security metrics, threat analytics and predictive analytics. Hunk: Splunk Analytics for Hadoop and NoSQL Stores uses batch loading and does not require Splunk event collection infrastructure

- Mcafee: ESM includes proprietary high speed event storage and query technology. Customer references give high marks for ad hoc query performance, even for deployments that must support high data acquisition rates and storage volumes. A Hadoop connector is available.[5][11]

### *G. Log Management and Reporting*

Log management has become significant part of the standard of due care for almost every 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. SIEM should have capabilities for storage and analysis of a log information 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. [4][5][6]

- HP Arcsight: ArcSight Express provides predefined monitoring rules and reports, as well as a simplified data model.[4][13]
- IBM Qradar: Qradar technology has 1,300 predefined reports covering all major regulations. These reports can be augmented with security configuration compliance reporting via Risk Manager and vulnerability reporting with Vulnerability Manager (or third party vulnerability scanning products).[4][7][9]
- LogRhythm's: LogRhythm's appliances provide horizontally scalable log management functions. Knowledge Base has more than 950 predefined security monitoring and compliance reports, plus more than 160 additional report templates that can be used to create custom reports.[5][10]
- Splunk: Security organizations use Splunk to provide log management functions for SIEM deployments, ad hoc query and compliance reporting. Reporting has been improved through predefined data models and pivot tables.[4][8]
- Mcafee: The McAfee Event Receiver component is an event log collector, and McAfee Enterprise Log Manager (ELM) provides log management. A large number of customizable predefined reports are provided.[5][11]

## V. CONCLUSION

Organizations looking for security information and event management (SIEM) solution should have create a checklist based on the requirements definition comprising of IT security, IT operations, internal audit and compliance. In addition, organizations should also assess based on the deployment and support capabilities of products and identify products which prove are best fit matches to internal projects and support capabilities. However considering above usecases it can be justified as IBM Qradar is best suited in scenarios like real time monitoring and threat intelligence is considered. It's followed by HP Arcsight for data, user or application monitoring is considered. Whereas Splunk leads in scenarios like Analytics and Reporting.

## REFERENCES

[1] Joel John Fernandes, SIEM Your Complete IT Security Arsenal,, ManageEngine Whitepaper "https://www.manageengine.com/products/eventlog/manageengine-siem-whitepaper.html,"

[2] Kelly M Kavanagh, Oliver Rochford, Magic Quadrant for Security Information and Event Management , 20 July 2015.

[3] Kelly M Kavanagh, Mark Nicolett, Oliver Rochford, Magic Quadrant for Security Information and Event Management, 25 June 2014."www.gartner.com" .

[4] Mark Nicolett, Kelly M Kavanagh, Oliver Rochford, Critical Capabilities for Security Information and Event Management Technology, 25 June 2014

[5] Mark Nicolett, Kelly M Kavanagh, Critical Capabilities for Security Information and Event Management Technology , 7 May 2011

[6] Kavita Agrawal, Hemant Makwana ,"A Study on Critical Capabilities for Security Information and Event Management,", International Journal of Science and Research (IJSR) Volume 4 Issue 7, July 2015

[7] DataSheet on 'IBM QRadar Security Intelligence Platform'

[8] Splunk Manuals, "http://docs.splunk.com/Documentation"

[9] IBM Security QRadar documentation,"http://www-01.ibm.com/support/docview.wss? uid=swg21614644"

[10] Datasheep on "LogRhythm Security Intelligence Platform","https://logrhythm.com/resources/datasheets/"

[11] Mcafee ESM user guide "https://kc.mcafee.com/corporate/index page=content&id=PD23998&actp=LIST_RECENT".

[12] Datasheet on "HP ArcSight Enterprise Security Manager","http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA4-3483ENW.pdf"

[13] Datasheet on "HP ArcSight ESM Express"," http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA4-1163ENW.pdf"