Security Information and Event Management

PMI-SVC Technology Forum

Tom Carlos

5/30/2017

Problem Identification and needed solution for:

- Monitoring critical S/W applications
- Security and Access - Identity and Access Management applications
- Operating-system, database and application logs
- External threat data, breaches
- Compliance – HIPAA, Regulatory
- Investigations

What is SIEM?

Security Information and Event Management (**SIEM**) software technology combines SIM (security information management) and SEM (security event management).

"The term *security information event management* (SIEM), coined by Mark Nicolett and Amrit Williams of Gartner in 2005."

What is SIEM?

SEM provides real-time analysis of security alerts by monitoring network hardware, security devices, and software applications correlation of events, system notifications and console views.

SIM provides long-term “secured” storage of log files, analysis, manipulation, and reporting of log data and security records collated by SEM software.

SIEM Capabilities

- **Data aggregation**: Log management aggregates data from multiple sources (ie network, security, servers, databases, applications) to consolidate monitored data to detect crucial events.
- **Normalization:** The process of taking raw input events and extracting individual fields, allowing data from different system to “look alike.”
- **Correlation**: Uses common attributes from log files, and links events meaningful groupings. This allows for a variety of correlation techniques to integrate different sources and transform differing data into useful information.

SIEM Capabilities

- **Alerting**: Automated alerting of correlated events to notify recipients of real time issues (via dashboards or email).
- **Dashboards**: Converting event data into informational charts and views, to assist in visualizing patterns and identifying activities that are of an unusual pattern.
- **Compliance:** Automation of gathering compliance data, producing reports for security requirements, governance, and auditing processes.
- **Retention**: Long-term storage of historical data, critical in forensic investigations and network breaches, to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements.

SIEM Capabilities

- **Forensic Analysis:** Ability to search across logs on different nodes of different time periods based on specific search criteria. This eliminates manual searching through volumes (thousands) of logs and data, prone to error, and moving the search to the software for accuracy and timely reporting.
- **Non-Repudiation:** (1) “Nonrepudiation is the assurance that someone cannot deny something” and (2) That the sender of the data is provided with the transmitted data in a way that prevents both the sender and consumer from denying that the transaction occurred.

Top Security Controls

- **SANS** (SysAdmin, Audit, Network and Security) Institute: Implementing the 20 Critical Controls with SIEM in the following categories.
  - Authentication and Authorization Reports
  - Systems and Data Change Reports
  - Network Activity Reports
  - Resource Access Reports
  - Malware Activity Reports
  - Failure and Critical Error Reports
- **CIS** (Center for Internet Security) critical security controls.

Gartner Group Magic Quadrant SIEM 2016

SIEM Leaders

- **IBM:** Q-Radar
- **Splunk:** Enterprise Security Application
- **LogRhythm:** Security Intelligence Platform
- **Hewlett Packard Enterprise:** ArcSight Enterprise Security Manager
- **Intel Security:** McAfee Enterprise Security Manager
- **EMC (RSA):** RSA NetWitness Suite

SIEM Endpoints

- **Endpoint:** A hardware device or software application that will be monitored by the SIEM solution. Each endpoint must be able to generate log files that will be ingested and recognized by the SIEM solution.

Components of SIEM

- **S/W Applications**
  - Standard or Custom Applications
  - Web, DB
  - Generating Log files
- **Hardware**
  - Servers, Desktop PCs, Routers, Firewalls, Switches
- **Network Bandwidth**
  - Must be able to handle data transfer

Components of SIEM

- **SIEM Software**
  - Main software applications
  - Agents/Collectors on key endpoints
- **SIEM Hardware**
  - Servers, Routers,
  - Will use Agents / Forwarders /Collectors to send log files to SIEM
- **SIEM Storage**
  - Hot / Cold / Frozen

Logging Sources of SIEM

Logging Sources

- Syslog and SNMP Trap
- Network
  - Cisco IOS
  - Snort IDS/IPS
- Servers/Workstations
  - Enterprise Linux 3/4/5
  - Microsoft Windows
- Applications
  - BIND (DNS)
  - Exchange
  - MS SQL
  - Host Intrusion Detection

Logging Services

- SYSLOG
  - SYSLOGD
  - SYSLOG-NG
  - RSYSLOG
- SNMP TRAP

Source: https://www.sans.edu/student-files/projects/JWP-Presentation-Slides-davis-horwath-zabiuk.ppt

SIEM Pre-Project

- **Read “Dr. Anton Chuvakin”**
  - “Five Best and Five Worst Practices of SIEM”
- **Establish Stakeholders**
  - Include Business and Technology
- **Identify problem to be solved**
  - Requirements must have an owner
- **Research SIEM solutions and Costs**
  - Is this the best way to attack the problem?
  - Hardware, Software, Human Capital
- **Estimate Sizing Requirements**
  - Events Per Second vs Daily Average in GB

SIEM Options

- **Self Hosted, Self Managed**
  - Buy it, control it
- **Self Hosted, Outsource Management**
  - Bring in the experts
- **Cloud MSSP Management**
  - Managed Security Service Provider
- **Hybrid Model**
  - Work with vendor to customize solution

Team Formation

- **IT Security Information Office**
- **IT Security Engineering**
- **Database and Network**
- **Business partners and s/w applications**
- **Organizational project champion**
- **Executive project sponsorship**

SIEM Project

- **Charter**
  - Clear definition of your scope
- **Start slow, start small, easy wins, and add endpoints over time**
- **Show results**
  - Generate reports
  - Storage of data
- **Document installation and Configuration**
- **Repeat process with next endpoint**

Major Challenges

- **Budget and Unexpected Costs**
- **Limited human capital resources**
- **Lack of buy-in from business partners**
- **Lack of planning – especially long term**
- **Uncoordinated deployment strategies**

Lessons Learned

- **Must have 100% dedicated resources (with designated backups)**
- **Every requirement needs an owner**
- **Trust and utilize vendor resources**
- **Pilot phase may not be practical**
- **Avoid convoluted procurement processes that may lead to selecting the wrong solution**

Questions?

Thank you!

Thomas Carlos Consulting Inc.
Roseville, CA.
www.carlosconsulting.com
(916) 521-2520

Tom Carlos is the owner and principle consultant for Thomas Carlos Consulting Inc., a company offering Project Management and Business Operations Consulting. He has worked in Public and Private Sector arenas, on Technical and Non-Technical projects, and managed a $1.5M SIEM Implementation.

References

- https://en.wikipedia.org/wiki/Security_information_and_event_management
- https://www.owasp.org/index.php/Logging_Cheat_Sheet
- http://searchsecurity.techtarget.com/definition/nonrepudiation
- https://www.splunk.com/blog/2010/05/26/splunking-your-way-to-information-assurance/
- https://www.sans.org/reading-room/whitepapers/analyst/implementing-20-critical-controls-security-information-event-management-siem-systems-34965
- http://www.splunk.com/web_assets/pdfs/secure/Splunk-and-the-SANS-Top-20-Critical-Security-Controls.pdf
- https://www.cisecurity.org/controls/cis-controls-faq/
- https://techbeacon.com/highlights-gartner-magic-quadrant-siem-2016
- https://www.slideshare.net/anton_chuvakin/five-best-and-five-worst-practices-for-siem-by-dr-anton-chuvakin
- https://www.slideshare.net/k33a/security-information-and-event-management-siem
- http://www.buzzcircuit.com/guessing-game-planning-sizing-siem-based-on-eps/
- http://content.solarwinds.com/creative/pdf/Whitepapers/estimating_log_generation_white_paper.pdf
- https://splunk-sizing.appspot.com/
- https://www.sans.edu/student-files/projects/JWP-Presentation-Slides-davis-horwath-zabiuk.ppt
- https://securosis.com/assets/library/reports/Securosis_Understanding_Selecting_SIEM_LM_FINAL.pdf
- Williams, Amrit (2005-05-02). "Improve IT Security With Vulnerability Management". Retrieved 2016-04-09. Security information and event management (SIEM).