Information Security Decisions

TechTarget

It’s Finally Time to Love SIEM

Karen Scarfone
Principal Consultant
Scarfone Cybersecurity

events.techtarget.com

Agenda

- The motivation behind SIEM
- Early SIEM issues and their resolution
- How to improve SIEM effectiveness
- SIEM issues to be addressed

Background

- Log management has always been a “best practice”
- Regulations and standards in late 1990s/early 2000s
  - Federal Information Security Management Act (FISMA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Payment Card Industry Data Security Standard (PCI DSS)
- Three groups of challenges to log management
  - Initial generation and storage of logs
  - Protection of generated and stored logs—preventing breaches of confidentiality, integrity, and availability
  - Inadequate preparation and support for log analysis

Initial Generation and Storage of Logs

- Too many log sources
  - Hosts throughout an organization
  - Multiple logs generated by each log source
- Inconsistent log content
  - Host IP addresses, usernames, other fields
  - Value representation (“FTP” versus “ftpd” versus “21”)
- Inconsistent timestamps
- Inconsistent log formats
  - Text files, databases, syslog, SNMP, XML, binary files, etc.
- Sheer volume of logs

Log Management Infrastructure Functions

- General
  - Log parsing
  - Event filtering
  - Event aggregation
- Storage
  - Log rotation
  - Log archival
  - Log compression
  - Log reduction
  - Log conversion
  - Log normalization
  - Log file integrity checking
- Analysis
  - Event correlation
  - Log viewing
  - Log reporting
- Disposal
  - Log clearing

From NIST Special Publication 800-92, *Guide to Computer Security Log Management*

General Functions

- Fundamental principle of not editing original logs
- Log Parsing: Extracting data from a log so the parsed values can be used as input for another logging function
- Event Filtering: Suppression of log entries from analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest
- Event Aggregation: Consolidation of similar entries into a single entry containing a count of the number of occurrences of the event

Storage Functions

- Log Rotation: Closing a log file and opening a new log file when the first file is considered complete
- Log Archival: Retaining logs for an extended period of time
- Log Compression: Storing a log file in a way that reduces the amount of storage space needed without altering the meaning of its contents
- Log Reduction: Removing unneeded entries from a log to create a new log that is smaller
- Log Conversion: Parsing a log in one format and storing its entries in a second format
- Log Normalization: Converting each log data field to a particular data representation (e.g., dates, times)
- Log File Integrity Checking: Calculating a message digest for each log file and storing the MD securely to ensure that changes to archived logs can be detected

Analysis and Disposal Functions

- Event Correlation: Finding relationships between two or more log entries
- Log Viewing: Displaying log entries in a human-readable format
- Log Reporting: Displaying the results of log analysis
- Log Clearing: Removing all entries from a log that precede a certain date and time

Centralized Log Management Infrastructure Architecture

- Tier 1: Log Generation
  - The hosts that generate the original log data
- Tier 2: Log Analysis and Storage
  - One or more log servers that receive log data from Tier 1
  - May store log data on the log servers or database servers
  - May have multiple levels of log servers
- Tier 3: Log Monitoring
  - Consoles for
    - Monitoring and reviewing log data and the results of automated analysis
    - Performing their own analysis
    - Generating reports
    - Managing log servers and clients

SIEM Basics

- Receives log data from Tier 1 (and optionally Tier 2) through agents or agentless methods
- Analyzes data from all the different log sources
- Correlates events among the log entries
- Identifies and prioritizes significant events
- Initiates responses to events if desired

Early SIEM Issues

- Deployed too aggressively
  - Too many hosts and log sources
  - Too many objectives
    - Incident investigation
    - Compliance reporting
- Poor interfaces
  - Weak support for user analysis
- Poor event correlation and incident response
  - False positives, false negatives
- Lack of dedicated SIEM support
  - Operational staff expected to implement and deploy SIEM
  - Heavy reliance on external professional services
- Overall, just too complex

How Issues Have Been Addressed, and What Remains

- Significant improvements to SIEM technologies
  - Better data collection, better correlation, better performance
  - Better interfaces
  - More scalable solutions to meet enterprise needs
- Still a lot of complexity in SIEM policies
  - Unavoidable—nature of the rule sets
  - Not an “out of the box” technology
  - Needs constant monitoring and maintenance
- Increased focus on using SIEM for incident detection and investigation
  - Less focus on compliance reporting

How to Improve SIEM Effectiveness

- Collect as much data as possible *
  - Infrastructure
  - Applications
  - Environment
- Build the rules **
  - Model the threat
  - Refine the rules
  - Optimize the thresholds
  - Wash, rinse, repeat

* http://searchsecurity.techtarget.com/tip/Why-focus-on-SIEM-integration-coverage-maximizes-anomaly-detection
** http://searchsecurity.techtarget.com/tip/SIEM-best-practices-for-advanced-attack-detection

SIEM Issues to Be Addressed

- Mobility
- Applications
- Cloud and virtual environments
- Industrial Control Systems (ICS)
- Big data

Mobility

- Sharply increased use of mobile devices
- Wide variety of mobile OSs and applications, and incredibly short lifecycles
  - Lack of logging standards
- Devices not directly connected to organization networks
- Devices often not centrally managed
- Bring Your Own Device (BYOD)
  - Performance, reliability, privacy
- Lack of security controls for mobile devices at this time

Applications

- Similar problems to mobility
  - Large number of applications, especially mobile apps
  - New applications and application updates constantly available
  - Lack of standards for application logging
- Most apps are written by third parties
- Generally more challenging to understand application events than OS events

Cloud and Virtual Environments

- SIEM supporting logging…
  - In the cloud
  - In other virtual environments
- SIEM being run within the cloud
  - SaaS

Industrial Control Systems (ICS)

- Increasing interest in including ICS/SCADA systems in enterprise logging
  - ICS systems adopting more mainstream technologies
  - Significant threats against critical infrastructure
- Different security objective priorities and operational requirements for ICS

Big Data

- Movement toward using big data analysis techniques on SIEM data
  - Incident detection and investigation
  - Forensics
  - Compliance reporting
- Scalability and performance concerns

Conclusions

- SIEM plays a critical role in log management
- Early issues in the technology have been addressed
- Known ways to improve SIEM effectiveness
- Future of SIEM weighs heavily on resolving issues:
  - Mobility, applications, cloud/virtual environments, Industrial Control Systems (ICS), Big Data

Thank You! Questions?

Karen Scarfone

karen@scarfonecybersecurity.com

http://www.linkedin.com/in/karenscarfone

TechTarget

TechTarget
Speaker
Bureau 2013