Security Information and Event Management Project

Proposal Submission:
Mr. Ken Foster

Contents

Recommendation:.....3
What is Security Information and Event Management:.....3
Business Case for SEIM Deployment:.....3
Core Functions of an effective SEIM:.....4
To be effective a SEIM solution must be able to consume:.....4
Examples of an Attack with and without SEIM integration:.....5
References:.....8

SEIM Procurement Project:

Recommendation:

Today's security infrastructure is comprised of stand-alone security solutions, designed to provide a defense in depth approach. The solution lacks a central point of analysis for the identification of complex blended attacks and the ability to implement consistent polices for event handling across networks. This organization must implement a Security Information and Event Management (SEIM) solution to identify and inhibit blended attacks from successfully penetrating and remaining undetected within the existing network infrastructure.

What is Security Information and Event Management:

A Security Information and Event Management (SEIM) appliance provides an automated analysis of multiple events from across the network seeking relationships which may indicate an effort to attack or exfiltrate sensitive data. SEIM appliances are able to handle events based on levels of severity and pre-determined policies. These policies determine severity of event, pre-determined isolation and action requirements, and report notification procedures. These policies in addition to increasing the overall security of the network may be utilized for mandatory auditing compliance verification and provide additional forensic evidence which may be provided to authorities for prosecution.

Business Case for SEIM Deployment:

There are two compelling business cases for deployment of a SEIM in our environment.

1. Counter-Measure Effectiveness: SEIM's provide enhanced operational awareness of our attack surface and their effectiveness against both internal and external penetration attempts. These devices provide both a preventative (perimeter) and reactive (post-intrusion) solution to policy-based violations. Currently a typical organization with an OC3 connection see's an average of 2,204 critical/major alerts each month on its intrusion detection/prevention systems. This equates to one serious event every 19 seconds on average. These alerts do not include denials on the firewalls which occur prior to the IPS's visibility but should a SEIM be integrated would provide a more detailed overview of the attack vectors used.

2. Compliance Monitoring, Reporting, and Scoring: SEIM's provide both prebuilt and optional custom built reports to provide an overview of the effectiveness and security posture of the network. These reports can be used as tools for determining activity trends, compliance ratings, document post-intrusion event analysis, and provide metrics for policy review and improvement. Dependent upon the sector of the organization, these reports may be mandated by SOX, HIPPA, and other compliance requirements.

Core Functions of an effective SEIM:

A SEIM has five primary functions that is must address to be considered an effective Security Information and Event Management tool:

- Log Consolidation: Centralized log collection based on standardized formats and consumption. This includes deployment and monitoring of collector devices / sensors on sources.

- Event Normalization: Events come from many sources and in many formats. The SEIM must be able to consume the logs and analyze the data elements to cross correlate the native values from one vender to the equivalent from another source. For example the exploit *Sasser Worm* is:

    - Cisco event 3338: IDS Signature Windows LSASS RPC Overflow
    - Symantec anti-virus exploit: W32/Sasser.worm
    - SNORT IDS event 2512: NETBIOS SMB-DS DCERPCLASS bind attempt.

- Threat Correlation: An artificial intelligence engine that uses collected events and either event signatures or anomaly-based detection algorithms to identify policy violations.

- Incident Management: Execute a workflow that occurs as the result of policy violation detection. These workflows may include any combination of:

    - Notification Facilities (e.g. Email, SNMP Traps to Network monitoring software, etc…)
    - Trouble Ticket Creation
    - Execution of Automated Scripts
    - Policy-based Response and Remediation
    - Correlated Event Logging

- Reporting: Product generation of events that comply with FISMA, HIPPA, and Forensics Investigation formats in addition to actionable metrics for performance measurement.

To be effective a SEIM solution must be able to consume:

- Firewall Events
- IDS Sensor Events
- AAA
- LDAP or AD (as applicable)
- Vulnerability Scanner results
- Server and Workstation event logs
- Anti-Virus / Malware
- Host-base Intrusion Detection Logs

Examples of an Attack with and without SEIM integration:

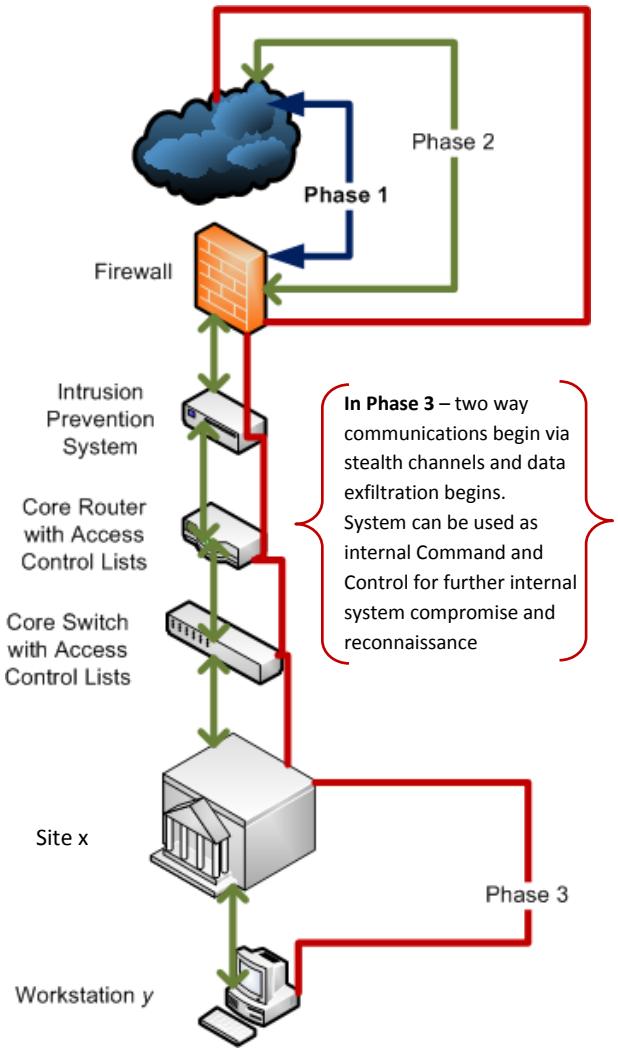
Discussion of SEIM's is best undertaken through the visualization of a simulated attack against a network. Using the common industry established practices for network penetration; a standardized process can be analyzed. Below are two examples of a simulated common exploitation of a network from the perimeter. In example one, the network provides common anti-penetration tactics without any event correlation. In example two, a SEIM is integrated into the solution to demonstrate how policies and applied based on artificial intelligence engine and combined log analysis (which occurs in near-realtime).

Example 1: Current Network (IPS w/o SEIM):

Phase 1 – Reconnaissance:
Attacker uses HPING, NMAP, or Firewalker to execute a scan of the firewall to determine which ports are open. Once open ports are determined, OS and infrastructure fingerprinting attempt to identify devices for targeted attacks. In the reconnaissance phase these probes are done slowly to attempt to avoid firewall and IPS exploit signatures.

Phase 2 – Stealth Targeting Payloads:
Once the attacker has selected a target for compromise, they must send packets to the target that will provide them a mechanism to launch their compromise. This must be done in a manner that prevents the Intrusion Prevention System from detecting this action. Common tools in this space include nemesis, fragroute, admutate, and metasploit.

Phase 3 – System Compromise:
The packets arrive to the host causing a buffer overflow and allowing for the installation of backdoors, rootkits, and botnets. The compromised system then reports in that it is ready for control to the attacker. This portion may include fouling Anti-virus /Malware detection mechanisms.

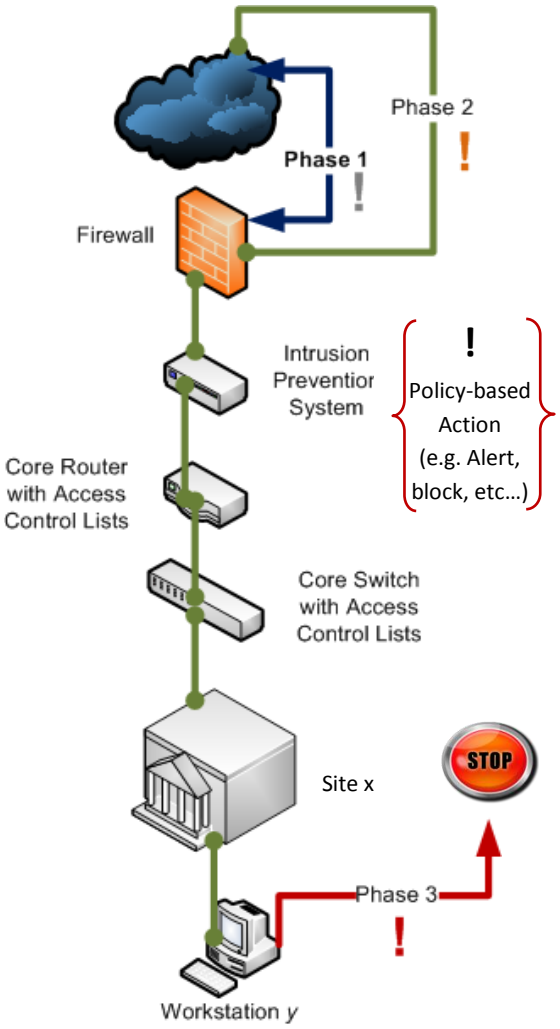


Example 2: Current Network (IPS with SEIM Intergration):

Phase 1 – Reconnaissance:
Attacker uses HPING, NMAP, or Firewalker to execute a scan of the firewall to determine which ports are open. Events are sent to the SEIM which using artificial intelligence detects the port scans and creates an event at the minor / warning level. It tracks this event. When OS and infrastructure fingerprinting begin, the SEIM correlates this event with the previous tracked event and raises the event the elevated, triggering a workflow alert to the security team.

Phase 2 – Stealth Targeting Payloads:
The firewall reports fragmented packets or the IPS detects possible exploit patterns. The SEIM raises the event to critical, and executes the Policy and workflow for the event. This may include port or IP blocking, system isolation, and security team notification.

Phase 3 – System Compromise:
If the attacker is successful in evading the Firewall, IPS, and Anti-virus in order to deploy a payload on the system, communication traffic back from the compromised host to the attacker would trigger a Major Threat event and the Major Event Policy and notification actions would be executed.



References:

Information Security Magazine. (nd). *SIM and Log Management.* Needham, MA: Garland, Josh.

Swift, D. (2006). *A Practical Application of SIM/SEM/SIEM - Automating Threat Identification.* Bethesda, Maryland: SANS Institute.