Netelligent

SIEM USE CASES FOR THE ENTERPRISE

Kevin Van Mondfrans, Director of Product Management, Netelligent

20 February 2016

As organizations recognize the value of their data and face the increasing complexity of security and compliance that should be in place, implementing a Security Incident and Event Management (SIEM) platform or managed services has become an attractive option to address various security-related business objectives. Typically two primary drivers exist for deploying a Security Incident and Event Management (SIEM) platform or managed service. The first driver is the requirement to be compliant with industry or government regulations such as PCI-DSS, HIPAA/HITECH, FFIEC/GLBA, NIST, ISO27001 and others. The second driver is the need to improve an organization's security detection and threat visibility. Either of these objectives merits implementing SIEM to secure business operations.

A modern SIEM platform or service combines log management with a powerful analytics engine. The analytics engine can run complex rules and advanced correlations against log and event data coming into the platform. This advanced SIEM platform can detect patterns of behavior on your network or within your devices that may be undetectable by your perimeter or end point security. It also enables the detection of threats that may originate within the organization and bypass the some of the traditional threat prevention and detection points. Finally, a certain behavior may not be alarming when occurring on a single device, but when detected across multiple devices, may signal a threat.

Let's dig a bit deeper by looking at the top uses cases of a well-tuned SIEM service.

1. DETECTION OF BRUTE FORCE ATTACK

With the evolution of faster and more efficient password cracking tools, brute force attacks are increasing against the services of an organization. When configured, SIEM will count the frequency of login attempts (failed or successful), multiple logins from the same IP address or geo-location, and any modification to system files, etc., so that a possible attack underway will get noticed and cangenerate an alert before the attack succeeds. Given the correlation of login attempts across the network, SIEM can uniquely identify patterns that would be missed on an individual device.

2. DETECTION OF MALWARE ACTIVITY

Organizations believe in protecting their network end to end; from their network perimeter, with devices like firewalls and Intrusion Prevention Systems (IPS), to the endpoint devices with security features like antivirus and multi-factor authentication. Most organizations collect reports of security incidents from these security products in a standalone mode, which brings problems like false positives and an overwhelming amount of raw events.

Correlation logic is the backbone of a modern SIEM solution, and correlation is more effective when built over the output from disparate log sources. For example, an organization can correlate various security events like unusual port activities in firewalls, suspicious DNS requests, warnings from Web Application firewalls and Intrusion Prevention System (IPS), threats recognized from antivirus, Host IPS, etc. to detect a potential threat. Malware activity can be detected in the following ways:

- Traffic/queries to malware domains/IPs
- Unusual network traffic spikes to and from sources
- Endpoints with maximum number of malware threats
- Top trends of malware observed; detected, prevented, mitigated
- Brute force pattern check on Bastion hosts

3. DETECTION OF SUSPICIOUS USER BEHAVIOR

Reportedly, more than 30 percent of attacks initiate from malicious insiders within an organization. Insider behavior may be more challenging to detect given they already have access to the network. It is imperative that SIEM rules discover activity patterns of insiders that can alert on suspicious behavior.

To counter such insider threats, a well-configured SIEM collects and correlates the following to determine if there is a possible threat:

- Account creation, deletion, and login patterns
- Multiple system logins
- System changes by user
- Data exfiltration
- Anomalous traffic patterns

4. DETECTION OF SUSPICIOUS NETWORK BEHAVIOR

IT networks are growing ever more distributed, complex and difficult to manage. This makes it harder to visualize traffic and exploitation attempts across the network and its many ingress and egress points. SIEM can be a valuable link to discovering the suspicious inbound and outbound connectivity and enrich that traffic information with details such as geo-location to make the traffic more meaningful. This suspicious traffic can indicate possible attacks underway including account compromises, data exfiltration, malware activity, DDoS events, and connectivity to known bad sites.

To discover the true nature of the network traffic, a well-configured SIEM collects and correlates the following information to identify the suspicious behavior:

- Suspicious connections, connection patterns, and geo-locations
- Suspicious data transfers
- Excessive connections
- Account access attempts
- Connectivity to blocked and backlisted sites
- Backdoor connections
- IDS/IPS exploits
- Spyware activity
- Man-in-the-middle activity

5. SUSPICIOUS DEVICE BEHAVIOR

Log sources are the feeds for any SIEM solution. For SIEM services, logging levels are set in the system registry to an on premise collector or the SIEM manager for analysis.

An attacker, after gaining control over a compromised machine/account, tends to stop or reduce logging services so that their unauthorized and illegitimate behavior goes unnoticed. To counter such malicious actions, SIEM is configured to raise an alert if a host stops or dramatically reduces forwarding logs after a threshold limit.

Another common pattern found among compromised log sources is that attackers tend to change the configuration files of endpoint agents installed and forward alot of irrelevant files to the SIEM Platform, causing a bandwidth choke between the endpoint agent and manager. This affects the performance of real time searches, storage capacity, dashboards and reporting. SIEM rules and analytics can be implemented to handle this suspicious behavior of log sources.

6. TRACK SYSTEM CHANGES AND AUTHENTICATION

Attackers will install files, modify systems, use existing accounts or create new accounts to execute their attack. The attacker will leave a bread crumb trail of user authentication, source locations and system and file changes. All of these factors can be evidence that an attack is underway.

SIEM rules are developed to track changes and administrative actions across internal systems and matching them to allowed policy. Detection of policy violations or behavior that is not normal is well within the scope of the SIEM detection capabilities. Here is a classic case that a well configured SIEM will easy pick up: "root access from an unknown IP in a foreign country that you do not do business with at 3AM, leading to system changes". This will raise alarms in SIEM and provide specific actions such as black listing IPs or communications from geographies, as well as a forensic trail to undo the specific changes. Furthermore, user login information is captured so accounts can be suspended, deleted or watched closely for additional activity.

7. CONTINUOUS COMPLIANCE MANAGEMENT

Almost every business is bound by some sort of regulation, such as PCI-DSS, HIPAA, FFIEC/GLBA, and Sarbanes-Oxley (SOX). Attaining and maintaining compliance with these regulations can be a daunting time and resource intensive task. SIEM technologies can address compliance requirements, both directly and indirectly.

Virtually every regulatory guideline requires some form of log management to maintain an audit trail of activity. SIEMs provide a mechanism to rapidly and easily deploy a log collection infrastructure that directly supports this requirement, and allows instant access to recent log data, as well as archival and retrieval of older log data. Alerting and correlation capabilities also satisfy routine log data review requirements, an otherwise tedious and daunting task when done manually.

In addition, SIEM reporting capabilities provide audit support to verify certain requirements are being met. Most SIEM platforms provide reports that directly map to specific compliance regulations. These can be run with minimal configuration and will aggregate and generate reports from across the enterprise to meet audit requirements.

8. DETECTION OF UNKNOWN THREATS

Many threats may allude your perimeter or end point security. Advanced persistent threats (APT) which target a specific piece of data or infrastructure utilizing a sophisticated combination of attack vectors and methods to elude detection. For example with Zero Day Threats the specific Malware is often not yet discoverable by the perimeter or endpoint protection.

Given the sophistication of APTs, enterprises must have an in-depth defense strategy to block activity beyond the perimeter (perimeter FW, IDS/IPS, internal FW, AV, multi-factor, etc). All of these devices generate a huge amount of data that is difficult to monitor. A security team cannot realistically have eight dashboards open and correlate events among several components fast enough to keep up with the packets traversing the network. SIEM technologies bring all of these controls together into a single engine capable of continuous, real-time monitoring and correlation across the breadth and depth of the enterprise.

But what if an attack is not detected before entering the network or system? After a host is compromised, the attacker must still locate the target data and extract it. Well configured SIEM correlation engines are able to monitor for a threshold of unique values. For example, a rule that looks for a certain number of unsuccessful access attempts on port 445 (or ports 137, 138 and 139 if NetBIOS is used) from the same host within a short time frame would identify a scan for shared folders. A similar rule looking for standard database ports would indicate a scan for databases listening on the network.

New attack vectors and vulnerabilities are discovered every day. Signature based detection solutions (FW, IDS, AV, etc.) are not equipped to detect zero day attacks. A SIEM can detect activity associated with an attack rather than the attack itself. For instance, a well-crafted spear-phishing attack using a zero-day exploit has a high likelihood of making it through spam filters, firewalls and antivirus software, and being opened by a target user. When well configured, SIEM is configured to detect activity surrounding such an attack. For example, a PDF exploit generally causes the Adobe Reader process to crash. Shortly thereafter, a new process will launch that either listens for an incoming network connection, or initiates an outbound connection to

the attacker. Many SIEMs offer enhanced endpoint monitoring capabilities that keep track of processes starting and stopping and network connections opening and closing. By correlating process activity and network connections from host machines, a SIEM can detect attacks without ever having to inspect packets or payloads. While IDS/IPS and AV do what they do well, a SIEM provides a safety net to catch malicious activities that slip through traditional defenses.

CONCLUSION

These use cases represent key examples for a well-configured SIEM platform. However, the time, complexity and maintenance of a SIEM platform should not to be underestimated. Developing the rules and then fine-tuning them to deliver meaningful results and achieving just the right level of alerting to avoid false positives and to avoid missing critical alerts, is time consuming and can take months or years of continuous development. With changing threats and growing infrastructure, the SIEM platform tuning is never ending. Additionally, continuous log reviews are essential to threat discovery, platform tuning and meeting many compliance requirements.

For these reasons, most mid- to large-sized enterprises seek an experienced managed security service provider (MSSP) to provide security monitoring and management services. The tangible benefits of offloading infrastructure management and security operations to a managed services provider include an improved security posture with a proactive approach with expertise to detect threats and defend your organizations faster, reduce expense, and gain a peace of mind.

ABOUT NETELLIGENT

Netelligent is a technology solutions company. With a robust hybrid IT solutions portfolio ranging from on-premises equipment to innovative managed services to complete cloud solutions, Netelligent offers mid-sized to large enterprise creative ways to transform their environments and deliver improved business outcomes. Named to the CRN Managed Services Provider (MSP) 500 list in the Elite 150 category three consecutive years, Netelligent demonstrates its expertise in cutting-edge approaches to delivering managed security services. On average it manages nearly 20,000 devices for its clients. Additional information about Netelligent can be found on their website http://www.netelligent.com.

REFERENCES:
http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up

SOURCES:
http://resources.infosecinstitute.com/top-6-seim-use-cases/
http://www.networkworld.com/article/2180119/tech-primers/5-reasons-why-siem-is-more-important-than-ever.html