Guarding the Network

SecurIT360
The physics of securing IT

We know that it is critically important to have a well-defined cybersecurity program in place.

Once we have the correct policies, procedures, tools, and training in place, we still have a couple of important questions to consider every day.

- *Is anyone actively trying to get our information?*
- *How would we know if we are under attack by cyber-criminals?*

Unfortunately, this is one of the most over-looked or under-served areas of information security. This is especially true for small and medium sized organizations, which may not have the resources or expertise to manage it properly.

Security Incident and Event Management

The standard for security monitoring and alerting is a Security Incident and Event Management system, or SIEM.

In simple terms, a SIEM provides two main functions –

- *Monitor the traffic in and around the perimeter of the network*
- *Provide alerts about suspicious activity*

Security Incident and Event Management systems allow an organization to –

- *Meet compliance requirements*
- *Improve security*
- *Better understand how data moves through their perimeter*

SIEM is somewhat of a catchall for a system that collects, stores, analyzes, correlates and reports on events within a network. These events can include authentication, malware detection, intrusion attempts, suspicious outbound activity, system changes, and many other types.

According to the Verizon Breach Report, in 60% of cases, attackers can compromise an organization within minutes, but only 45% were discovered within days. A SIEM solution is always looking at the events within the network and can significantly decrease the time to discovery.

A major advantage to a SIEM solution is a centralized pane of glass. You can get alerts from firewalls, intrusion detection systems and other systems, but a SIEM product helps you to understand and correlate events from separate systems.

SIEM is a critical part of many compliance regulations such as **NERC CIP**, **HIPAA, PCI, GLBA, SOX** and others. On top of having its own SANS Top 20 Critical Security Control, it helps meet at least 15 other Critical Security Controls.

dburns@securit360.com

Guarding the Network

SecurIT360
The physics of securing IT

There are two ways to deploy and utilize a SIEM system for your information security.

- *Purchase, install and maintain your own SIEM system*
- *Hire an outsource SIEM provider to provide a managed SIEM service*

In determining whether to manage your own SIEM, or hiring an outsourced provider, it is important to understand the challenges.

Challenges of a Security Incident and Event Management System

Capital Investment	Most solutions require a sizable purchase of licenses and hardware.
Deployment	Installation and configuration may require professional services and installation of agents on endpoints. This can take weeks to months.
Staffing	SIEM systems often require additional staff or manpower to respond to alerts, and tune the system to get maximum value.
Total Cost of Ownership	As logs are produced, data grows from GB to TB. There must be a full-time owner or you will find that the system has not been functioning as expected.
Maintenance	As the network changes, log sources need to be updated. The system will also require security and software patches.
Expertise and Training	Not only will staff need to be trained on the solution itself, they will need to have or gain expertise in evaluating the alerts and understanding what to do with them.

If your organization has an IT staff to manage these challenges, you should consider managing your own SIEM. However, it is important to understand that it takes a significant amount of staff time to manage and maintain a SIEM system properly. That is one of the reasons that even large organizations often use an outsource provider for security incident and event management.

When considering the challenges above, many organizations determine that is less expensive and a better use of resources to hire a SIEM provider.

Consider all of the options and challenges to determine which is best for your organization.

As always, develop a “cyber-defense” mindset to protect yourself AND your company.

If you would like to learn more about Cybersecurity and how to protect your company, contact -

David Burns
Account Manager, SecurIT360
dburns@securit360.com
205.787.1250