SIEM VS LOG MANAGEMENT: WHAT'S THE DIFFERENCE?

It seems that nearly every week, we hear about another major business who's just been a part of some data breach. Hackers have reached evidently secure information, often taking sensitive and financial information of employees and customers.

The problem is that we don't know what computer system attacks look like until after they occur. If we could miraculously know ahead of time, we'd be able to automate all security defenses, eliminating any need for humans to analyze security.

Often, the only way companies can detect attacks, even after one has occurs, is by knowing and understanding what's happening in logs and other secure areas. There are many software products and techniques that offer insight into the health of your company's security, but, as we'll see, these often provide only a narrow view of the whole picture.

Two popular terms, log management (LM) and security information and event management (SIEM), are often used in tandem, but there are significant differences in the definitions and approaches.

Security and Log Management

An important first step in establishing a security analysis protocol is managing your logs. Logs are computer-generated messages that come from all sorts of software and hardware – nearly every computing device has the capability of producing logs. The logs show, in detail, the varied functions of the device or application, as well as when users log in or attempt to log in.

These logs are often text-based, and they can be stored in local or remote servers. Logs are also known as audit records, audit travels, and event logs. Log management systems (LMS) can be used for a variety of functions, including: collecting, centrally aggregating, storing and retaining, rotating, analyzing, and reporting logs.

Companies primarily opt to store logs for security purposes. Reviewing these logs, whether before or after a security breach, are important in showing whether someone is an internal employee or an outside threat. After all, network and system administrators could look like hackers, if looking solely at the actions they regularly perform.

Regulation compliance and system and network management are also important reasons to maintain and manage logs.

The importance of these logs isn't in the logging itself. Instead, it's the analysis of these logs is what provides value. Logs are often used to detect weaknesses in security, and forward-thinking companies who employ strategic security analysts often are able to find and address these weaknesses before breaches can occur.

The larger the company, however, the more logs there are. In fact, companies can easily produce hundreds of gigabytes in logs per day! With this much data to sort through, several issues can impede manual log management, including:

- Volume and velocity – simply too much content, too quickly to view, let alone analyze
- Normalization – logs can vary in output format, so time may be spend normalizing the data output
- Veracity – ensuring the accuracy of the output

As the size of logs continues to grow, and companies becoming increasingly vigilant about security analysis, log management alone isn't enough – it's only a component of a holistic solution.

Security Information and Event Management

Any number of software offer a small window into the health of your security. For instance, an asset management system tracks only applications, business processes, and administrative contacts, and a network intrusion detection system (IDS) can only see IP addresses, packets, and protocols. Taken individually, these options cannot indicate what's happening in real time to your network.

Enter SIEM. Like log management, SIEM falls within the computer security field, and it includes both products and software that help companies manage security events and secure information.

SIEM, though, is a significant step beyond log management. Experts describe SIEM as greater than the sum of its parts. Indeed, SIEM comprises many security technologies, and implementing SIEM makes each individual security component more effective. In effect, SIEM is the singular way to view and analyze all of your network activity.

The term, coined in 2005, originates from and builds on several computer security techniques, including:

- **Log management** (LM), as previously described, which collects and stores log files from operating systems and applications, across various hosts and systems.
- **Security event management** (SEM), which focuses on real-time monitoring, correlating events, providing overarching console views, and customizing notifications.

- **Security information management** (SIM), which provides long-term storage, analysis, manipulation, and reporting on logs and security records.
- **Security event correlation** (SEC), which tracks and alerts designated administrators when a peculiar sequence of events occurs, such as three failed login attempts under the same user name on different machines.

Taken individually, these techniques cannot indicate what's happening in real time to your network. By combining the best of these techniques, however, SIEM provides a comprehensive approach to security.

Vendors may sell these as products and/or managed services, along with other security-related components. The most well-rounded SIEM products are those with the following capabilities:

- The aggregation, analysis, and reporting of log output from networks, operating systems, databases, and applications
- Applications that verify identities and manage access
- Vulnerability management and forensic analysis
- Policy compliance
- External threat notifications
- Customizable dashboards

Benefits of SIEM

Like log management, the goal of SIEM is security – and it is only as good as the data it accesses. But advantages of a SIEM approach are its real-time analysis and connecting disparate systems in order to unify the information in one console.

In essence, SIEM provides a wide, yet detailed view into your company's security. SIEM means your security analysts can continue doing what they do best – analyzing security in real-time – instead of spending time learning every single product under the security umbrella.

Additional Resources

Making Log Data Useful: SIEM and Log Management Together from **Anton Chuvakin**