What the Heck is a SIEM and Why Do Laws Firm Need Them?

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke
© 2024 Sensei Enterprises, Inc.

Explaining a SIEM Simply

It isn't easy. First, SIEM is pronounced "Sim." A lot of lawyers (and others) get it wrong. What does the acronym stand for? It stands for "security information and event management." In the simplest terms, it is a security solution that detects threat activities before your law firm is significantly impacted. SIEMs can detect, analyze and, most importantly, respond to security issues.

SIEMs harvest log data from many sources, performing the sorcerer's trick of identifying activity which is not normal with real-time analysis and, best of all, it can take action **without human involvement** – the need for human involvement slows everything down. Like so much technology, SIEMS have morphed over the last few years and now they detect threats and respond to them faster and with more assurance that they are taking the correct action with the aid of artificial intelligence.

Here's one example of what a SIEM can do quickly. It can flag a user account as suspicious when it generates 25 failed login attempts in 25 minutes but it would likely be regarded as a lower priority because the attempts were likely made by a user who forgot their log-in information. However, a user account that generates 130 failed login attempts in five minutes would be tagged as a high-priority event because the most likely explanation is that there is a brute-force attack taking place against your law firm.

Another example is impossible travel. After one successful login, there may be a second successful login from an IP address that would indicate impossible travel. Perhaps the second login is over 2500 miles away and occurred 5 minutes after the first one. It may be that the user is utilizing a VPN and the access is valid. It most certainly doesn't involve the use of a Star Trek transporter to cover the distance, but rather, it may be an attacker that obtained valid user credentials.

What are the Core Functions of SIEMS?

This is the hard part, so bear with us. SIEMs vary in their capabilities which means you must pay attention to what any particular SIEM offers. However, the core functions are these:

- Log management: SIEMs harvest vast amounts of data in a central location, organize it, and then they determine if there is data indicating a threat, an actual attack, or a breach.
- Event correlation: This basically means that the SIEM will sort the data to identify relationships and patterns, which allows it to identify security incidents across your law firm's network, which permits fast detection and response to possible threats.
- Incident monitoring and response. In brief, a SIEM will monitor security incidents across a law firm network, providing alerts and audits of all activity connected to an incident.

What are the Benefits of Using a SIEM for a Law Firm?

It's the best way to strengthen a law firm's cybersecurity, offering the following:

- A view of potential threats
- Real-time threat identification and rapid response, which minimizes damage to your law firm
- Highly advanced threat intelligence
- Regulatory compliance auditing and reporting
- A LOT more transparency monitoring users, applications and devices
- In the event of a breach, it can perform a detailed forensics analysis

How Does a Law Firm Implement a SIEM?

Law firms have an ethical duty to protect their confidential data. These days, you can get a SIEM at a reasonable price. Law firms of all sizes (not just the AmLaw 200) must take reasonable steps to reduce cybersecurity risks and meet regulatory compliance standards. Here are some of the elements involved in implementing a SIEM:

- Define YOUR requirements for SIEM deployment – you will likely need the assistance of your Managed Service Provider or your in-house IT/Cybersecurity employees.

- Once you install it, do some test runs.
- Make sure you've got a sufficient amount of data for testing purposes.
- Having a SIEM is NOT a guarantee that you won't have incidents or suffer a breach so make sure you have an incident response plan – just in case!
- As improvements become available for your SIEM, integrate them.

The Role of a SIEM for Your Law Firm

Having a SIEM is an integral part of your cybersecurity. Most law firms these days have a managed IT/cybersecurity provider. A SIEM gives that provider a central place to collect and analyze volumes of data, which streamlines security workflow. Additionally, it has operational capabilities such as compliance reporting, incident management, and sophisticated dashboards that prioritize threat activity.

How Much Will a SIEM Cost Your Small Law Firm?

Not as much as you might think. While pricing will vary for the various SIEM solutions, look for offerings that are cloud-based and priced on a per-user basis. Such solutions should cost around $10 per user per month, which is very affordable even for a solo attorney.

Final Words

We are endlessly frustrated by clients who choose not to install a SIEM for budgetary reasons. Though we sound like a broken record, we often tell them "If you can't afford security, you can't afford a breach." And trust us, the breach is far, far more costly.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* snelson@senseient.com

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* jsimek@senseient.com

Michael C. Maschke *is the Chief Executive Officer at Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security*

Professional (CISSP). He is a frequent speaker on IT, cybersecurity and digital forensics and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.