CYBERSECURITY, MEET BIG DATA

by Jenny Mangelsdorf

New security information and event management tools can help detect cyberattacks and theft, even when other methods can't.

Some compare the challenge of responding to today's cybersecurity threats to playing an extreme version of Whac-A-Mole: where the minute one focuses on destroying one mole-like threat, other moles are already popping up.

Take Adobe: This October, the company reported the cybertheft of more than 2.9 million customers' information. Even more disturbing for the company, and potentially others, was the theft of some of Adobe's source code, which may translate into further theft of personal information and other organizations' intellectual property.

While the theft's full damage is still unknown, the multipronged heist is another indicator that cyberattacks are wreaking increasingly greater damage. In Ponemon Institute's upcoming *2013 Cost of Cyber Crime Study*, the firm reports this year's average annualized cost of cybercrime was $7.2 million per company polled in its study — a 30 percent increase in mean value over last year. The report also says successful cyberattacks increased 20 percent over last year, with each company surveyed experiencing 1.4 successful attacks per week.

"We used to make statements, such as 'I have a firewall; I'm protected,' or 'I have antivirus software; I'm protected,'" says Todd Pedersen, a cybersecurity lead for CSC. "Now, the conversation is less about preventing an attack, threat or exposure, and more about how quickly you can detect that an attack is happening."

Data-guided defenses

There's a growing demand for security information and event management (SIEM) technologies and services, which gather and analyze security event data that is used to manage threats. Increasing numbers of regulations and mandates generated throughout the globe also are pushing the adoption of SIEM technologies and services.

"Both governments and industries are introducing more and more regulations and mandates that require the use of better data protection and security controls to help guard systems, information and individuals," says Matthew O'Brien, a global cybersecurity expert for CSC.

In the United States, the Federal Information Security Management Act, Health Insurance Portability and Accountability Act, Sarbanes-Oxley Act, and the Department of Homeland Security's Critical Infrastructure Protection guidelines, to name a few, all have requirements tied to collecting and logging information, events and activities that occur within an organization's environment — requirements that SIEM-related technologies and services help organizations meet.

> "Organizations need an automated approach to handle the collection, analysis and management of threat and log information because of the increased number and sophistication of threats they're experiencing."
>
> Matthew O'Brien, a global cybersecurity expert for CSC

For example, every second, more than 300,000 events generated by CSC and its customers run through CSC's Global Security Operations Centers.

"SIEM gives us the ability to take this massive amount of data and bring it all back to a central place, where it's combined with the other information we get from numerous security technologies," says Pedersen. "That gives us the ability to detect things that no individual technology in and of itself would have picked up, and create a picture to analyze, investigate and find security-related issues."

New levels of awareness

This SIEM capability also has become critical as organized crime, along with some nations' armed forces and intelligence services, moves center stage in the cyberarena, launching weapons-grade cyberattacks and advanced persistent threats.

At times these threats are global; at other times, attackers aim for specific industries. Ponemon's report says, "The average annualized cost of cybercrime appears to vary by industry segment, where organizations in defense, financial services, and energy and utilities experience substantially higher cybercrime costs than organizations in retail, media and consumer products."

"SIEM helps us create an environment that allows us to use a broad range of tools, some of which we select for a specific customer environment, and yet accrue data in a common environment and use that common environment for correlation and analysis," says Pedersen.

Increasing enterprise system complexity also creates a driver for SIEM. Today's organizations are adding greater numbers of connections, also known as endpoints, to their systems, either due to incorporating mobile devices, the bring-your-own-device trend, expanding supply chains, or a desire to link their IT systems with their industrial control systems.

"The number of integration points with other technologies and the processes that support them today can be overwhelming," says O'Brien. "As we ask our systems to do more, they also become more vulnerable, which means we need a level of awareness that wasn't required before." ■

JENNY MANGELSDORF is a writer for CSC's digital marketing team.

SIEM, AS A MANAGED SERVICE

Businesses are under pressure to detect and prevent cybersecurity threats. In addition, to facilitate forensic investigations and meet growing compliance and regulatory demands, companies must maintain extensive records of security events. These needs are driving demand for enterprise logging and security information and event management (SIEM) technology.

"During 2012, the SIEM market grew from $1.1 billion to approximately $1.36 billion, achieving a growth rate of about 23 percent," according to the May 7, 2013, Gartner, Inc. report *Magic Quadrant for Security Information and Event Management*, written by Mark Nicolett and Kelly M. Kavanagh.

In September, CSC expanded its managed security services to include a full SIEM solution managed through the company's global network of Security Operations Centers.

"While organizations recognize the essential value of SIEM functionality, the complexity and resources needed to deploy it have been a deterrent for many," says Samuel Visner, vice president and general manager, CSC Global Cybersecurity. "CSC's solution allows companies to manage their security through our global team of certified security analysts and adopt the technology in stages, from enterprise logging to the most advanced SIEM capabilities."

CSC's service utilizes HP ArcSight technology and provides comprehensive collection, aggregation, storage and correlation of logs across multiple networked devices, systems and applications. We supply customers with the infrastructure, processes and personnel needed to proactively monitor, report and escalate security events around the clock.

CSC provides multiple entry points into the SIEM service offering; at our Enhance tier, we simply provide logging for compliance or audit requirements. This Audit Log Assurance (ALA) component enables our clients to store log information and retrieve it later if required for audit or compliance requirements. We then add functionality to the service for compliance-based reporting and real-time event monitoring, correlation and management through CSC's Global Logical Security Operations Center.

Learn more at csc.com/cybersecurity.