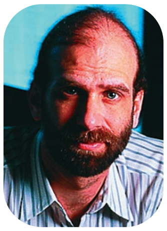
SIMS: Solution, or Part of the Problem?

The computer-security industry is guilty of overhyping and underdelivering. Again and again, it tells customers that they must buy a certain product to be secure. Again and again, they buy the products—and are still insecure.



Bruce Schneier
Counterpane Internet Security

Firewalls didn't keep out network attackers—in fact, the notion of "perimeter" is severely flawed. Intrusion-detection systems (IDSs) didn't keep networks safe, and worms and viruses do considerable damage despite the prevalence of antivirus products. It's in this context that I want to evaluate Security Information Management Systems, or SIMS, which promise to solve a serious network security problem: log analysis.

Computer logs are a goldmine of security information, containing not just IDS alerts, but messages from firewalls, servers, applications, and other network devices. Your network produces megabytes of these logs every day, and hidden in them are attack footprints. The trick is finding and reacting to them fast enough.

Analyzing log messages can determine how the attacker broke in, what he accessed, whether any backdoors were added, and so on. The idea behind log analysis is that if you can read the log messages in real time, you can figure out what the attacker is doing. And if you can respond fast enough, you can kick him out before he does damage. It's security detection and response. Log analysis works, whether or not you use SIMS.

Even better, it works against a wide variety of risks. Unlike point solutions, security monitoring is general. Log analysis can detect attackers regardless of their tactics.

But SIMS don't live up to the hype, because they're missing the essential ingredient that so many other computer security products lack: human intelligence. Firewalls often fail because they're configured and maintained improperly. IDSs are often useless because there's no one to respond to their alerts—or to separate the real attacks from the false alarms. SIMS have the same problem: unless there's a human expert monitoring them, they're not defending anything. The tools are only as effective as the people using them.

SIMS require vigilance: attacks can happen at any time of the day, any day of the year. Consequently, staffing requires five full-time employees; more, if you include supervisors and backup personnel with more specialized skills. Even if an organization could find the budget for all these people, it would be very difficult to hire them in today's job market. And attacks against a single organization don't happen often enough to keep a team of this caliber engaged and interested.

Back in 1999, I founded Counterpane Internet Security; we sell an outsourced service called Managed Security Monitoring, in which trained security analysts monitor IDS alerts and log messages. Because of the information our analysts received from the network—in real time—as well as their training and expertise, the analysts could detect attacks in progress and provide customers with a level of security they were incapable of achieving otherwise.

When building the Counterpane monitoring service in 1999, we examined log-monitoring appliances from companies like Intellitactics and e-Security. Back then, they weren't anywhere near good enough for us to use, so we developed our own proprietary system. Today, because of the caliber of the human analysts who use the Counterpane system, it's much better than any commercial SIMS. We were able to design it with our expert detection-and-response analysts in mind, and not the general sysadmin market.

The key to network security is people, not products. Piling more security products, such as SIMS, onto your network won't help. This is why I believe that network security will eventually be outsourced. There's no other cost-effective way to reliably get the experts you need, and therefore no other cost-effective way to reliably get security. □

Bruce Schneier is one of the world's foremost security experts and chief technical officer of Counterpane Internet Security. His most recent book is Beyond Fear: Thinking Sensibly about Security in an Uncertain World. *You can subscribe to his email newsletter,* Crypto-Gram, *at www.schneier.com.*