

System*i*NEWS

A Penton Publication May 23, 2010

SIEM Solutions Ease Burden of Regulatory Compliance on IBM i

As I keep an eye on the security action in the IBM i world, and as regulatory compliance continues to become more—and not less—challenging, I realized SIEM solutions are becoming more and more important and should be on every IBM i pro's radar. For a quick explanation about what SIEM is and how it can benefit your shop, I reached out to Robin Tatam at PowerTech with a couple of questions.

System *i*NEWS: First, what exactly is a Security Information and Event Management (SIEM) solution? For IBM i–focused professionals, where do these fit beyond the built-in IBM i security?

Tatam: A simplified description of a SIEM (pronounced "sim") solution is an enterprise tool that collects and reports on security events generated by a number of technologies. This often entails the realtime, or near realtime, collection of events that trigger an alert and are stored for regulatory compliance.

While IBM i has a solid object-level security model and inherent event auditing capabilities, it requires a knowledgeable individual to generate reports and to perform manual analysis of that information. According to PowerTech's annual "State of IBM i Security" study, almost 20 percent of organizations perform no auditing, and even more have no procedures or software in place to analyze the data. In addition, this information often is stored locally on each individual server—a challenge for large organizations running with multiple partitions.

The deployment of a SIEM solution enables an organization to proactively report events to a centralized console. For IBM i shops, this allows important events to be reported together with other enterprise servers. The SIEM solution automates the burden of reporting and notification, which often leads to a significant improvement in incident response times (IRT).

In addition, an isolated event that occurs on one partition may not be a cause for concern; but if the same issue

occurs on many partitions in a small window of time, it might change the nature of the response. No IBM i security control is going to provide that cross-partition visibility.

SiN: Can you describe some key benefits of a SIEM solution—how can it pay off for an IBM i–focused organization and fit into the broader enterprise?

Tatam: The functionality varies greatly depending on the solution you work with, but features often include:

- + Filtering
- + Notification and alerting
- + Event correlation and rollup
- + Cross-device event correlation
- + Statistical analysis
- + Centralized log management and storage

Historically, IBM i has not participated in enterprise security initiatives, and this further reduces the visibility that the server has to security teams, and perhaps even its perceived value to management. Organizations today are running IT teams that are leaner than ever, and the burden of manual reporting not only involves expensive resources but relies on the ongoing analysis and clear identification of important events.

A failed server login attempt is a normal occurrence in any enterprise, but 100 of them in 5 minutes should sound an alarm. SIEM solutions permit the server to actively push security events out to ensure that they can be acted on in a timely manner, while reducing the chance of false positives. With the mission-critical data often stored on IBM i servers, reaction time can be the difference between a failed attack and a catastrophic breach.

—Linda Harty, executive editor & availability/
security/networking/connectivity editor