

DMMReview

Information Is Your Business

July 2008/Volume 18, Number 7

www.dmreview.com



ANNUAL PRODUCT REVIEW ROUNDUP 2008

Product Review

Lehigh Valley
Hospital Uses
EventTracker
to Improve IT
Security and
Comply with
HIPAA

PRISM
MICROSYSTEMS



www.prismmicrosys.com

Lehigh Valley Hospital Uses EventTracker to Improve IT Security and Comply with HIPAA

REVIEWER: Brian Martin, CISSP, CHS-III, senior information security manager for Lehigh Valley Hospital and Health Network.

BACKGROUND: A premier academic community hospital, Lehigh Valley Hospital and Health Network comprises three hospital facilities - two in Allentown and one in Bethlehem, Pennsylvania. In 2007, *U.S. News & World Report* named Lehigh Valley Hospital one of America's Best Hospitals in six categories.

PLATFORMS: EventTracker from Prism Microsystems runs on Microsoft Windows 2003 server and collects log data from a complex IT infrastructure consisting of a mix of Windows, UNIX and Linux servers, Nortel and Cisco devices, workstations and applications. We currently monitor data in real time from about 150 systems at three main and two remote locations with the aim of deploying EventTracker network-wide to monitor data from over 5,000 devices.

PROBLEM SOLVED: Our plan of maintaining a HIPAA-compliant environment is to implement and maintain security best practices, of which event log management is a critical component. We needed a solution that would monitor and correlate critical log data from disparate geographically dispersed devices to detect unauthorized access, logon/logoff failures and other patterns of behavior that might suggest a security breach in progress. Real-time policy-based alerting was key in order to enable quick remediation and stop hostile behavior before it causes damage. To demonstrate compliance and conduct forensic analysis on security incidents, we also needed comprehensive reporting, with the ability to provide different functional groups with different privileges and access settings.

PRODUCT FUNCTIONALITY: We use Prism Microsystems EventTracker for reporting and alerting. It comes with a number of preconfigured reports mapped to HIPAA requirements that allow us to demonstrate compliance. We also use the reports as proof of evidence in legal situations and for forensic/historical analysis - we can use the predefined reporting templates for common security threats or to generate customized reports to pinpoint certain systems, users and/or time periods for in-depth investigation. We also depend on real-time correlation to improve security. Often, the clues to a security attack are spread out over a number of systems and can easily be missed - for example, log-on attempts to administrator accounts or multiple login failures by a single user across multiple systems often go undetected. Correlation allows us to spot these patterns of behavior and alerting enables us to respond to them in real time. EventTracker also allows us to insert customized business logic. With EventTracker, we are able to be instantly notified when a workstation accesses areas it is not authorized to access.

STRENGTHS: A main strength is scalability - EventTracker is expandable on a tiered system and allows us to separate the functional use of the software. We have separate groups that use the solution for compliance, security and IT operations, and with the help of granular role-based access, we can provide these groups with the functionalities they require without giving them full system administrator access. The collection point architecture allows each group to locally manage the resources they are responsible for, while at the same time enabling a network-wide rollup for compliance purposes.

WEAKNESSES: It would be nice to see improve-



ments in the rules authoring. Although the rule grammar is fairly simple, creating complex rules still takes some skill. Additional educational materials or a high-level scripting tool would make the solution easier to use by less experienced individuals and result in increased incorporation of business rules.

SELECTION CRITERIA: Prism provided us with a pilot to test EventTracker on our systems, and we found that it fit our requirements of real-time monitoring, role-based access, multi-tiered reporting, correlation and alerting extremely well. The implementation was quick and easy. Compared to other products we have tried and used, Prism was orders of magnitude ahead in our evaluation.

DELIVERABLES: EventTracker produces predefined and customized reports for us on a scheduled or ad hoc basis. Our main bread-and-butter reports are authentication activities and content review. In addition, we have access to all log data from varied devices across the network available to us for analysis and reporting at a central location. By using automation and rules, we eliminate the need for human review of the majority of our needs, which greatly increases our efficiency.

VENDOR SUPPORT: Support has been excellent. We have always gotten timely responses to our queries.

DOCUMENTATION: Documentation is complete and easy to understand.