EVENTSENTRY

# Engvall Security Intensifies Its Security Focus with EventSentry

Engvall Security is part of a Swedish authority tasked with supporting IT services for various projects. The company prides itself on the quality and clarity of its service delivery—as well as its customer service.

ENGVALL SECURITY

Jonas Haglund, chairman and head of security at Engvall Security, is a CISSP, CISA, and PowerShell and VBScript scripter. In his spare time, he enjoys backcountry skiing, mechanics, and carpentry. But at work, Haglund is faced with the daily challenge of dealing with the extensive security requirements of the entities his company services. Engvall Security needed a tool that automated the analysis of security logs, consolidated and commonly analyzed logs from various system components (and different systems), and normalized all logs during consolidation.

After evaluating several products on the basis of broad functionality and price, Engvall Security chose NETIKUS.NET EventSentry in 2008, and the company hasn't looked back. Haglund uses EventSentry primarily for monitoring events from Windows event logs and Syslog output, and alerting through SNMP and email as well as a weekly log review. EventSentry also provides Haglund with **strong log consolidation and archiving functionality.**

Haglund points to EventSentry's customizable alerting functionality as a particular benefit. "Our users were experiencing login failure while attempting to access web services that were authenticating to Active Directory in the background," he says. "When the login failed—because of an expired password, account lockout, and so on—the website wasn't providing those failure details to the user. So we used an EventSentry filter that **parses text from the login failure events, triggers a script, and sends an email message** telling the user what happened."

In the Engvall Security administration room, the EventSentry network status screen is always on for all administrators to observe. "From there," Haglund says, "we have been able to avoid out-of-disk situations and failing services. EventSentry has definitely prevented us from experiencing downtime."

Although Engvall Security hasn't experienced a great number of security issues, EventSentry has helped the company become faster at **determining whether certain symptoms of intrusion are signs of actual malicious activity.** "With EventSentry, several times we have been able to detect hardware errors early and thus avoid issues," Haglund says. "For example, we've avoided failing hard drives (exchanging faulty drives before the entire RAID array failed), as well as a failing management blade in our blade server solution."

Haglund points to several other EventSentry features that stand out. "I really like the customizable status views in the web reports," he says, "and the possibility to script local actions for certain events is indispensable."

EventSentry support has been responsive, polite, and accurate, according to Haglund, who would recommend the product to other systems administrators. **The product's return on investment (ROI) is excellent,** especially when compared with market competitors.

**For more information call 312.624.7698**
**www.eventsentry.com**