Trustwave®
Case Study

Department of Energy Continuous Monitoring of Controls

The mission of the Department of Energy is to advance the national, economic and energy security of the United States, as well as to promote scientific and technological innovation and ensure the environmental cleanup of the national nuclear weapons complex. Security plays a critical role in achieving the mission. One strategic goal is scientific discovery and innovation to make the U.S. more competitive and to improve our quality of life. This case study explains how one DOE research facility is able to provide a secure campus for 4,500 employees. Many of these employees are scientists that perform valuable research that involves collaboration with scientists from all over the world.

"A simple example of the value we find in Trustwave SIEM OE is we're able to identify an infected machine today rather than days or weeks out; the cost of remediation is significantly less."*

Not surprising is the fact that one challenge for this facility is allowing legitimate traffic from countries that often appear on dangerous watch lists. The security team at this DOE facility regularly receives questions and objections from scientists who perceive security controls for workstations are impacting their freedom to collaborate. Managing perceptions like this requires continuous education of the on-campus population and requires the security team have a real understanding of the scientific process in order to balance the level of control required to maintain a secure risk posture against the potential benefits of fewer controls.

This organization implemented Trustwave's Security Information and Event Management Operations Edition (SIEM OE) to automate continuous monitoring of controls determined to be essential to maintain a secure risk posture. There were three requirements for a SIEM solution:

First, it had to scale. The SOC (security operations center) at this facility benefits from centralized control over the campus and satellite facilities.
FACT: This SOC sees throughput of 220 million events per day or 7 billion events per month.

"Trustwave SIEM OE is one component that improves our effectiveness and efficiency... We could never afford all the staff it would take to monitor massive amounts of data. And even if we had the staff, it would be a difficult task without automation."

* All quotes are attributed to a spokesperson for this DOE facility.

70 W. Madison Street, Suite 1050, Chicago, IL 60602
www.trustwave.com
1.888.878.7817

Second, it had to adapt. There could be no limitation on what devices could be monitored, and the infrastructure is constantly changing.
FACT: Trustwave SIEM OE adapted quickly to monitoring 10,000 devices on the network including standard workstations, scientific workstations and network equipment – even handling one-off custom log sources. Trustwave supports their preferred syslog format.

Third, security monitoring had to be the focus. This SOC is deliberate about implementing controls to enforce policies and automating continuous operation as security monitoring is central to their security strategy.
FACT: Trustwave SIEM OE automates security event monitoring and has provided this organization support for Controls 6, 8 and 11 found in the Consensus Audit Guidelines.

Control 6

Maintenance, Monitoring and Analysis of Audit Logs

This organization relies on syslog for collecting audit logs, and Trustwave supports multiple protocols including syslog. Trustwave SIEM OE's architecture supports this organization's tiered approach for storing and sending audit logs. They like that SIEM OE alerts when events have not been seen for a specified length of time. Trustwave SIEM OE logs verbosely all VPN logs. Per the control, SIEM OE enables filtering of events but also provides access to "everything" for the purpose of forensic work. The SOC monitors all inbound and outbound traffic, even though the volume of firewall logs is overwhelming – Trustwave SIEM OE handles the volume. Trustwave SIEM OE aggregates and consolidates logs from multiple machines performing log correlation and analysis. Activity of regular vulnerability scanning is logged.

Control 8

Controlled Use of Administrative Privileges

This SOC follows the Federal Desktop Core Configuration (FDCC) standard for password administration and has removed user administrator privileges on Windows systems. Similarly FDCC guidelines are used for password changes and password for service accounts. Trustwave SIEM OE is used to monitor and report on any administrator account activity after business hours; monitor and alert when an account is added or removed from a domain admin group; and monitor and alert when an account is added to the admin group on local computers. Finally, spear-phishing tests are conducted monthly but training has improved the staff's ability to identify phishing e-mails.

> "We needed a SIEM that had 'crunching power' - to ingest all the data and still have the power to do the correlation - to get to the answers."

Control 11

Account Monitoring and Control

Trustwave SIEM OE generates daily summary reports of failed login attempts as prescribed by this control. Trustwave SIEM OE has the capability to report on locked out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. With the large user population (4,500) reporting on all of these is somewhat unwieldy. Audit logging using Trustwave SIEM OE can provide near real-time alerts or daily reports when attempts to access deactivated accounts are made. Trustwave SIEM OE also has the capability to monitor against a business day hours threshold. Using Trustwave SIEM OE, this SOC has alerts set up to monitor for any privileged user access to sensitive systems during off business hours or using special privileged accounts on systems on which they shouldn't be used.

Summary

The SOC benefits from Trustwave SIEM OE's real-time analysis of correlated events. It enables them to be proactive in identifying risk as soon as possible.