

Anchors Aweigh

U.S. Navy Brings in the Big Guns with Novell Sentinel

This article first appeared
in the February 2009 issue of
Novell Connection magazine.

Maintaining the security of U.S. Navy networks is critical to the security of the country. Using Novell Sentinel as part of its PROMETHEUS system, NCDOC has automated and centralized security monitoring across hundreds of diverse locations worldwide. NCDOC personnel now have a real-time, holistic view of all network activities and can prioritize them to focus on what is most critical.

> Overview

The Navy Cyber Defense Operations Command (NCDOC) is one of several military cyber defense teams in the Department of Defense (DOD) which maintains the largest computer network in the world. Based in Norfolk, Va., NCDOC is responsible for around-the-clock protection of the Navy's computer networks, with more than 700,000 users worldwide. NCDOC is the first and only certified computer network defense provider within the DOD to be awarded top-level accreditation.

“Our job 24/7 is to secure and defend Navy networks worldwide against a persistent and adaptive threat. Novell Sentinel helps us accomplish that.”

-Jim Granger

**Director of Capabilities and
Readiness**

**Navy Cyber Defense Operations
Command**

> Challenge

The 180 personnel at the NCDOC are responsible for analyzing huge volumes of network information gathered from hundreds of locations worldwide including ships, medical clinics, headquarter offices and research facilities. NCDOC personnel monitor these networks 24/7, 365 days a year.

NCDOC was experiencing data overload from an increasing number of cyber security sensors and corresponding alerts, but had insufficient personnel to monitor them. Because all network activity needs to be carefully evaluated, NCDOC wanted to automate the

monitoring across hundreds of security sensors, including firewalls, intrusion protection systems and other security-related systems. The solution needed to be vendor-independent to accommodate a variety of platforms and systems, as well as scalable enough to handle continued growth in the number of sensors.

> Solution

NCDOC created PROMETHEUS, a suite of tools that monitors, reports and thwarts malicious network activity. PROMETHEUS uses the SAS Intelligence Platform as the data warehouse back end, and Novell Sentinel as the security event management front end to monitor tens of thousands of network events per day.

“We always choose the top tools in the industry and Novell Sentinel is a market leader,” said Jim Granger, Director of Capabilities and Readiness at NCDOC. “The product works well with SAS and met our requirements of being open and scalable.”

The PROMETHEUS system accesses and aggregates data from all portions of the network—including system logs, Web logs, e-mail logs, firewall logs and router logs—and prepares and stores the data for analysis and reporting. Novell Sentinel presents and prioritizes all security events in a centralized dashboard for security operators.

“With Novell Sentinel, we have a unified, real-time view of security activity across our diverse global environment from a central console,” said Keith Rohwer, NCDOC director of Research, Development, Testing and Evaluation. “We can customize what we want to see and prioritize everything according to the seven standard security levels of the DOD.”

NCDOC can easily customize information, such as by region or type of system, and scale to meet increasing volumes of data. The Novell Sentinel interface remains consistent, despite the addition of more sensors. The NCDOC team can also operate the Sentinel system from other locations, so that there is no central point of failure.

“It would have been impossible to keep up with the dramatic increase in network security activity without at least 10,000 personnel,” said Granger. “Novell Sentinel gives our centralized monitoring team a comprehensive and holistic view of security events so we can immediately act on what is most critical.”

Novell Sentinel also simplifies daily reporting with the ability to generate reports in all levels of detail for different audiences, whether commanders, other agency partners or a joint security task force.

“As a government entity, we have high expectations as a customer,” said Rohwer. “We have an outstanding business relationship with Novell.”

“With Novell Sentinel, we have a unified, real-time view of security activity across our diverse global environment from a central console.”

-Keith Rohwer

**Director of Research,
Development, Testing and
Evaluation**

**Navy Cyber Defense Operations
Command**

> Results

With Novell Sentinel as part of its PROMETHEUS system, NCDOC has automated and centralized security monitoring for thousands of sensors and corresponding alerts across multiple geographically dispersed networks. The ability to prioritize security events allows the command to focus on those that require the most

attention, such as the network aboard a ship entering a battle zone.

NCDOC can now create real-time reports in minutes or hours, instead of weeks or months. As network security is vital to the nation's defense, this information is a top priority for military leaders at the highest levels.

“Our job 24/7 is to secure and defend Navy networks worldwide against a persistent and adaptive threat. Novell Sentinel helps us accomplish that,” said Granger. “The biggest military advantage is the power of information. We rely on the security of our networks to get the right information to the right people quickly.” **N**

**Products and Services:
Novell Sentinel**

Results:

- Centralized and automated security monitoring for thousands of sensors and alerts across geographically dispersed networks
- Increased ability to prioritize security events and focus on most critical
- Can create customized reports and prioritize according to the seven DOD standard security event classifications