CASE STUDY

tenable DPAA

Defense POW/ MIA Accounting Agency

"We feel extremely confident about our choice to go with Tenable. The company's reputation and proven success across the DoD and federal civilian agencies are unmatched... not to mention the significant number of Tenable deployments in the private sector."

The **Defense POW/MIA Accounting Agency (DPAA)**, is part of the U.S. Department of Defense (DoD). Its mission is to recover the remains of POWS and others missing in action from all past wars and conflicts, and provide the fullest possible accounting for these military personnel to their families and the nation.

KEY BUSINESS NEEDS

The Defense POW/MIA Accounting Agency (DPAA) required a unified solution capable of quickly and accurately identifying, visualizing and assessing asset vulnerabilities across all DPAA networks.

PRODUCTS USED

The foundation of ACAS is comprised of the **Tenable.sc™** platform (formerly named SecurityCenter®) integrated with **Nessus® Network Monitor** and **Nessus®**, the most widely deployed vulnerability and compliance scanner in the world. In addition to ACAS, DPAA also deployed Nessus on its classified networks.

CHALLENGES

Federal government agencies like DPAA face many of the same cybersecurity challenges as commercial enterprises. The IT landscape is becoming more complex by the minute as new systems, devices and users stretch the borders of the ecosystem. Cyber adversaries and their methodologies are increasingly sophisticated and successful. Attacks are frequent and expertly designed to target vulnerabilities that yield unauthorized access to proprietary mission-critical information.

DPAA recognized the need for an ironclad cybersecurity defense that would span and protect its highly distributed environment. The agency required a unified solution capable of quickly and accurately identifying, visualizing and assessing asset vulnerabilities across all DPAA networks.

DPAA sought a **flexible and scalable vulnerability management platform that could be easily deployed** in all critical business areas for:

- Continuous enterprise-wide network security and risk assessment
- Increased accuracy of risk assessment and standards compliance verification
- High scalability and ease of deployment at all levels, from senior commanders to warfighters on the front lines
- Essential situational awareness to enable risk-based management decisions consistent with existing and emerging federal guidelines

The DPAA mission encompasses diverse objectives including national security, privacy protection and warfighter support. Success mandates complex operational capabilities, so solution requirements extended well beyond standards dictated by compliance regulations.

SOLUTION

As part of DoD, DPAA was eligible to leverage the department's **Assured Compliance Assessment Solution (ACAS)** for vulnerability management and configuration. The DoD ACAS program fulfills a combination of operational and strategic objectives:

- Providing an innovative technical solution with a flexible cost structure
- Employing a commercial solution that can be easily ordered and quickly deployed across DoD infrastructure
- Supporting enterprise-wide deployment with the ability to tier system evaluation and management throughout the organization

The foundation of ACAS is comprised of the **Tenable.sc** platform integrated with **Nessus Network Monitor** and **Nessus**, the most widely deployed vulnerability and compliance scanner in the world. In addition to ACAS, DPAA also deployed Nessus on its classified networks. Tenable's approach delivers a proactive network defense for DPAA, designed to scale easily while maintaining cost-effectiveness.

tenable.sc™

Tenable.sc provides continuous asset-based security and compliance monitoring, unifying the processes of asset and vulnerability discovery, and configuration auditing. It delivers a central point for visualizing assets, managing events, and conducting audits.

Tenable.sc is the first agent-less scanning solution to be certified by FDCC and SCAP.

The Tenable.sc console works with Nessus® scanners to look for policy changes. This on request provides the ability to assess an organization's vulnerability and compliance posture, and to deliver analysis and workflow tools that allow the user to perform reporting, auditing and remediation tasks.

Tenable.sc's reporting engine produces the common reports DPAA needs – without advanced scripting. ACAS users quickly gain access to relevant data.

nessus Scanner

A high-quality, full-function scanner covers a breadth of vulnerability and configuration checks across a broad range of different workstation, server and network devices. The Tenable Nessus scanner supports more than 87,428 plug-ins and covers more than 38,439 unique Common Vulnerabilities and Exposures (CVEs). The scanner is fast and accurate, giving clients the greatest possible visibility into the status of connected devices and systems.

nessus Network Monitor

Traditional active scanning systems miss transient devices – like smartphones – as well as many cloud-based services, resulting in dangerous gaps in coverage and visibility. Sophisticated security professionals complement active scanning with passive scanning. Nessus Network Monitor (formerly Passive Vulnerability Scanner or PVS) uniquely overcomes these limitations, effectively extending scanning visibility to resources that would otherwise be missed in assessments. It introduces continuous monitoring, identifying devices and systems, applications and services, and network connections, as well as eliminating the restrictions and limitations of traditional, schedule-based scanning. The inclusion of passive vulnerability scanning provides a comprehensive solution for DPAA.

BENEFITS

With Tenable tools and technologies providing cybersecurity firepower, DPAA was able to sharpen its focus on mission objectives and operational excellence. Tenable solutions deliver the broad range of capabilities DPAA needs to maintain a stealthy defense:

- Instant Asset Discovery
- Continuous Monitoring
- Comprehensive Visibility
- Situational Awareness
- Advanced Analytics
- Automated Compliance
- Interactive Dashboards
- Customized Reporting
- Risk-based Management Decisions

The Tenable Advantage

Flexibility
The option to deploy unlimited consoles and scanners enables DPAA to build the optimal scanning strategy, reflecting environmental, architectural and organization requirements.

Scalability
Individual Tenable.sc consoles can scan hundreds of thousands of IPs based on mission requirements, not technology constraints.

Accuracy
The comprehensive Nessus library helps eliminate missed events (i.e., false negatives), while the popularity of Nessus provides an immediate feedback loop and an extra layer of quality assurance.

Ease of use
The Tenable platform does not require a relational database or agents.

Continuous Monitoring
Passive scanning capabilities, unique to Tenable, help DPAA move beyond static, point-in-time assessments.

Experience

The combination of one of the world's largest technology companies with one of the most widely used vulnerability scanners gives DPAA a partner it can trust.

Relying on best-of-breed technologies, DPAA is now poised to anticipate, prioritize and neutralize cyber threats as they arise, in real time. Tenable tools set the global standard for enterprise visibility of digital systems and connected devices, as well as the rapidly expanding attack surface, delivering the richest data and insights available in the market.

"The decision regarding product selection was simple. The trifecta of Tenable.sc, Nessus and Nessus Network Monitor was the only solution that delivered on all of our mission requirements."

To learn more, visit: **tenable.com** and **http://www.dpaa.mil**
Contact Us: **marketing@tenable.com**