Defense Department Command Streamlines and Automates Cybersecurity Assurance with Xacta®

A Case Study in Risk Management and Continuous Compliance

Telos Corporation serves a command of the Department of Defense that must maintain security across seamless, worldwide information enterprise systems that connect joint and coalition forces and other agencies. This process includes analyzing the networks, identifying and categorizing risk, resolving potential security vulnerabilities, and assuring the compliance of systems on an ongoing basis.

Xacta: The Apex of Their Cybersecurity Regimen

At the apex of this command's cybersecurity regimen is Xacta, a suite of tools that supports security risk management, continuous compliance monitoring, and ongoing authorization of the command's information systems. Xacta is deployed enterprise-wide at the command and is their system of record for managing all of their Risk Management Framework for DoD IT packages as well as legacy DIACAP packages.

The Xacta Continuum® component of the suite has been deployed at the command's headquarters. This deployment includes both the integration of existing enterprise security tools such as Retina and Nessus as well as the Xacta HostInfo Agent. The resulting scans produced from these tools are imported into Xacta Continuum within the associated cycles of the RMF.

The Xacta risk management suite enables organizations to track the security state of a wide range of information systems on an ongoing basis and maintain their security authorization over time. Its elements work together to provide CISOs and other senior leaders with a dynamic view into the current status of security controls.

- Streamlines assessment and authorization (A&A) for the DoD RMF, CNSS, and NIST RMF
- Helps automate security processes for remediation and compliance reporting
- Correlates results from multiple security scans into a single view and maps them to the relevant controls
- Collects the diverse range of data needed for continuous monitoring and trend analysis
- Reduces the time needed to analyze and confirm findings across hundreds of assets
- Generates documentation and reports required for enterprise information assurance

The Xacta HostInfo agent is also being rolled out throughout headquarters to provide the command's cybersecurity team with near real-time authoritative information on assets included in associated Xacta 360 packages. Currently the organization has approximately 1,000 of the agents deployed through their Microsoft System Center Configuration Manager (SCCM) capability, which is used by network administrators to manage their groups of Microsoft Windows-based systems. In addition to asset awareness, the agent allows them to run scripts to validate compliance for individual vulnerabilities such as the recent OpenSSL Heartbleed bug.

Automation Helps Streamline Analysis and Enables Continuous Monitoring

The scan results collected from the Xacta HostInfo agents as well as information collected from existing security tools can be compared side by side to provide the cybersecurity engineer a complete overview of how the finding relates to particular controls within the governing regulation (such as CNSSI 1253) within an Xacta 360 package. Automating the analysis of these results enables the command to significantly reduce the amount of overhead required by its Security Control Assessors to analyze findings within the packages.

The combination of the Xacta 360 and Xacta Continuum toolsets provides the command an automated solution for not only developing their authorization processes within the workflow but also to address the continuous monitoring requirements included in CNSSI 1253. The systems built within Xacta 360 automatically update key fields on the organization's IT Registry, which is submitted through different channels as required to provide high-level compliance metrics for existing systems in the enterprise.

Telos solutions and services are available on a variety of federal contract vehicles:

- GSA Schedule
- ADMC-2
- ACCENT
- DOD ESI
- EAGLE II
- IMCS III
- ITES-3H
- NETCENTS-2
- OGP BPA
- RMF BPA

Xacta: An Essential Element in Information Security

For this command, information security is literally mission-critical. Xacta is empowering them to track the security state of a wide range of information systems on an ongoing basis and maintain security authorization for the systems over time. Its elements work together to provide the command's senior information security leaders with a dynamic view into the current status of security controls.

Telos®

For more information about Xacta, contact Telos Corporation

Telos Corporation | 19886 Ashburn Road, Ashburn, VA 20147-2358 | 1.800.70.TELOS | 1.800.708.3567 | Fax 703.724.3865 | www.telos.com