maximus

Enhanced Cybersecurity at DISA Protects Against an Expanding Threat Network

Protecting our nation's most sensitive and critical communications infrastructure requires continuous technology advancements by dedicated and experienced professionals. The Defense Information Systems Agency (DISA), a U.S. Department of Defense (DOD) combat support agency, rises to this challenge every day by actively protecting our nation's systems and networks under a constant threat of cyberattacks. The DOD faces increasingly sophisticated and well-resourced cyber-attacks that must be stopped. In 2021, the average number of cyberattacks and data breaches increased by 15.1% from the previous year and cost American government entities nearly $19 billion in recovery costs and downtime. The DOD has made protecting our nation's data from these threats a priority.

Challenge

Effective data governance requires that government agencies share data. Every agency must adhere to stringent cybersecurity requirements when sending and receiving its most sensitive and classified information. This requires rigorous 24/7 monitoring of networks for external and internal threats, mitigating plans that can respond and contain them, and proactively preventing bad actors from compromising data integrity. Even with upgraded technology, successful cybersecurity relies on experts to evaluate anomalies and decide whether they need further investigation.

Services Provided:

- Deployed cybersecurity capabilities that enrich user monitoring and reduce the risk posture of DISA's Compartmented Enterprise Service Office (CESO)
- Provided scalable, modular cybersecurity services to detect, protect, respond and recover data security instances
- Increased CESO's Security Operations Center effectiveness by 50% with supplemental cyber risk and business technology experts

Success Achieved:

- Developed internal accreditation processes resulting in rapid approvals of multiple Authority to Operates (ATOs) for enterprise boundaries and applications
- Increased DISA's ESO's Security Operations Center effectiveness by 50%
- Established 24/7 protection of sensitive information and detection of advanced persistent, malicious insider threats

DISA needed staffing enhancements to connect the U.S. military and government through secure IT network, systems and communications support. The agency turned to a deeply trusted technology and consulting solutions partner, Maximus, to immediately assemble a team of certified technology specialists and cybersecurity experts who could meet the agency's operating objectives.

Approach

Maximus rapidly deployed 15 program team members with CSSP, CASP and CEH credentials and the necessary clearances. The unit got to work reviewing all cybersecurity activities to identify opportunities for applying system, application and data protection best practices. As an added value, the team used its collective experience to evaluate the Security Operations Center (SOC) and its compliance processes, paying particular attention to gaps in the Supply Chain Risk Management (SCRM) activities. With its comprehensive business view of the system environment, the team made several program recommendations and improvements:

- Complied with the Chief Information Security Officer's (CISO) SCRM requirements for standards and guidelines
- Outlined a risk and maturity assessment-based approach for operational improvements
- Analyzed suppliers and threat risks to establish workable supply chain controls
- Documented security impact results for agency leadership to make informed mission decisions
- Developed system dashboards for ease of access to critical data for documentation and informed decision making

Results

The collaboration of the Maximus and agency staff significantly increased the capability to successfully monitor five Authorization to Operate (ATO) boundaries. The combined team strengthened DISA's cyber defenses, ensured hardware and software compliance, and enhanced interoperability for sharing purposes, thus allowing the agency to maximize a heightened level of cybersecurity.

Expanding the view of the technology environment while anticipating future needs by utilizing trending data, Maximus advanced DISA's cybersecurity posture by:

- Reinforcing the agency's cybersecurity compliance requirements
- Developing and executing a Supply Chain Risk Management program
- Establishing a cyber team to investigate and mitigate current threats to the enterprise within 45 days
- Designing and implementing a cyber-centric dashboard for leadership to leverage for key decision making.
- Deploying cyber technology to remediate insider threats
- Establishing compliance scans to capture and secure recently deployed software and devices at speed to ensure critical data protection
- Developing a holistic process that ensured a secure system life cycle management schema that included patch management
- Maintaining the critical 24/7 monitoring support levels and thwarted cyber-attacks with a SOC environment

Aligned with the agency staff, Maximus guided the program to ensure DISA could establish and manage enterprise cybersecurity capabilities that protect IT systems and architecture when our nation's critical information is shared.