Cyber Security Services for Middle Eastern Military

Implementation, design and managed services

SUMMARY: The organization sought the necessary tools and training to monitor their networks in order to identify and respond to cyber-threats. Following development of a Strategic Roadmap with the customer, 3eTI developed a robust solution with a readily scalable framework as the customer expanded coverage. The solution further involves classroom and hands-on training, a threat operations center (TOC) and a security operations center (SOC).

AT A GLANCE

Customer

Middle Eastern Military Force

Solution Components

- Threat operations center (TOC) and security operations center (SOC)
- Hands-on and classroom training for cyber awareness
- Policies and procedures consistent with global best practices and standards

Solution Benefits

- **Fully accredited solution recommendations,** consultation and guidance in full compliance with local and international information-assurance requirements
- **Flexible design for multi-vendor systems** to facilitate integration of disparate products and networks
- **Low-cost execution** by reusing the existing network infrastructure augmented with state of the art monitoring and defensive technology and equipment

Objective

The organization required a cyber-force sufficient to efficiently accommodate best-in-class cyber-secure technologies while maintaining full operational status. The scope includes advanced consultation and training to establish a highly skilled defense team.

Challenge

The customer lacks the expertise to establish an advanced cyber-secure operation. Highly skilled specialists are needed to design a security architecture and security solutions that existing staff will be able to proactively maintain for a cyber-hardened IT environment.

Solution

After extensive evaluation, the organization chose Ultra Electronics to provide the systems and training that resulted in a self-sufficient IT operation prepared to efficiently defend against advanced cyber-threats. The solution includes:

- **Cyber Awareness Training:** Develop and conduct tiered training for varying skill and responsibility levels.
- **Policies and Procedures:** 3eTI will work with the organization to develop comprehensive guidance reflecting global best practices relative to governmental and international standards. The purpose of these policies and procedures is to assure the confidentiality, integrity, and availability of their information assets, and to ensure that all cyber security policies and procedures are practiced on a daily basis as an ingrained part of operations. This includes external cyber-security related obligations to stakeholders.
- **Infrastructure Design:** 3eTI will advise on and manage the implementation of a secure-by-design series of enclaves to support sensitive information sharing and collaboration. A secure infrastructure will be designed to restrict unauthorized access, lateral movement by an attacker between network segments and systems, and the exfiltration of sensitive data.
- Threat Operations Center (TOC) and Security Operations Center (SOC): Ultra is tasked to build two main cyber-intelligence command day-to-day operation centers. The TOC will focus on proactively uncovering threats and deriving Indicators of Compromise (IoC) to mitigate them, while the SOC's mission is to continuously monitor, detect and isolate security incidents and the security management of the customer's network devices, end-user devices, and systems.

Why Ultra Electronics

Renowned for enabling information assured communications, 3eTI has an unrivaled heritage in solving operational security challenges for prominent government customers. 3eTI's cyber specialists understand ICS networks and work to add that vital security layer to new or existing systems that complement and support your solutions.

For more information contact 1-800-449-3384 or email sales@ultra-3eti.com