CASE STUDY

Cybersecurity Services: Sovereign Military Force
Implementation, design and managed services

SUMMARY: A large Middle Eastern military force required a cybersecurity solution sufficient to efficiently accommodate best-in-class technologies while minimally impacting operational status. The scope included expert consultation and extensive training to establish an internal defense team of skilled cybersecurity specialists.

OBJECTIVE
Knowing they lacked the appropriate expertise internally, a large Middle Eastern military force sought an experienced company to help establish an advanced cyber-secure operation. Following the development of a strategic roadmap, the organization required a robust solution with a readily scalable framework to expanded cybersecurity coverage. Classroom and hands-on training also were required, as were a threat operations center (TOC) and a security operations center (SOC). Training and security facilities were needed to enable the military force to establish a strong cybersecurity team internally.

The specifications necessitated the design of a security architecture with associated solutions that existing staff would be able to maintain for a cyber-hardened IT environment. The organization also needed necessary tools and training to monitor networks and address cyber-threats.

SOLUTION
After an exhaustive review process, the organization chose to partner with Ultra Electronics, 3eTI for system design and implementation, supported by training to establish a self-sufficient IT operation. The solution included:

- **Policies and Procedures**: 3eTI provided comprehensive guidance reflecting global best practices relative to governmental and international standards. The purpose of these policies and procedures was to assure the confidentiality, integrity and availability of information assets, and to ensure that all cybersecurity policies and procedures are practiced on a daily basis as an ingrained operational function.

- **Infrastructure Design**: 3eTI managed the implementation of a secure-by-design series of enclaves to support sensitive information sharing and collaboration. The design restricted unauthorized access, lateral movement by an attacker between network segments and systems, and the exfiltration of sensitive data.

- **TOC and SOC**: 3eTI was tasked with building two main command centers for day-to-day cyber-intelligence operations. The TOC focuses on proactively uncovering threats and indicators of compromise (IoC) to mitigate them. The SOC’s mission is to continuously monitor, detect and isolate security incidents. It oversees the security management of the network devices, end user devices, and systems.

- **Cyber-Awareness Training**: 3eTI developed and conducted tiered training for varying skill and responsibility levels.

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

AT A GLANCE

Customer: Sovereign Military Force

3eTI Solution

- Strategic plan development
- TOC and SOC deployments
- Managed services
- Training for cyber awareness
- Policies and procedures compliance

Key Benefits

- **Fully Accredited**: Solution recommendations, consultation and guidance were in full compliance with local and international information-assurance requirements.

- **Flexible Design**: Multivendor-compatible systems facilitate integration of disparate products and networks.

- **Low-Cost Implementation**: Reusing the existing network infrastructure, augmented with state-of-the-art technology and equipment, resulted in significant savings.

Since 1995, 3eTI has been a trusted supplier for the defense, government, energy and industrial automation markets worldwide. We connect and protect critical information and infrastructure systems through advanced cybersecurity, secure wireless, perimeter management, and security services.

ultra-3eti.com
linkedin.com/company/3eTI
twitter.com/ultra_3eti
Copyright © 2018 v0518