Case Study: Operational Technology Cybersecurity & Incident Response for DLA

Client: Defense Logistics Agency (DLA)
Industry: Federal Government / Cybersecurity / Operational Technology
Services Provided: CND Analysis, Vulnerability Management, Incident Response, Cybersecurity Content Development, Fly-Away OT Missions

Project Overview

Horizon delivered **full-spectrum cybersecurity support** to DLA, with a specialized focus on **Operational Technology (OT)** environments. Acting as a key partner to the DLA Cybersecurity Service Provider (CSSP), Horizon provided **incident response, vulnerability management, content development**, and cyber threat analysis services, specifically designed to secure DLA's growing OT footprint.

Our work included coordination with DLA internal teams and external agencies (e.g., **USCYBERCOM, DIA, Law Enforcement**) to ensure timely mitigation of incidents and the implementation of DoD-mandated security directives across enterprise networks and OT systems.

Solutions & Capabilities Delivered

24x7 Incident Response & Cyber Defense

- Provided full-time coverage supporting DLA CERT operations
- Monitored and defended DLA's OT infrastructure from evolving cyber threats

Fly-Away OT Cybersecurity Kits

- Designed and deployed mobile cybersecurity response kits
- Conducted successful **on-site OT assessments** during multiple field missions

Threat Intelligence & Coordination

- Distributed countermeasures like **custom SNORT signatures**, **IPS rules**, and **IP blacklists**
- Maintained coordination with DoD and Intelligence Community agencies during cyber incidents

Cybersecurity Content Development

- Created SOPs, incident documentation, and threat response procedures
- Used industry frameworks like **MITRE ATT&CK**, **Cyber Kill Chain**, and **OODA Loop**

Vulnerability Management & Awareness

- Supported proactive identification and remediation of OT vulnerabilities
- Promoted cybersecurity awareness across DLA's OT teams and infrastructure

---

Challenges Overcome

Staffing for Cleared OT Roles
Maintaining a qualified, cleared OT cybersecurity workforce required strategic recruitment and continuous professional development. Horizon mitigated this by fostering a strong training culture and supporting certification pathways.

Adapting to Emerging Threats in OT Environments
OT systems present unique cybersecurity challenges. Horizon's fly-away assessments, hands-on engagement, and field-tested SOPs ensured readiness against modern threats without impacting operations.

Results & Impact

- **100% compliance** with DLA and DoD reporting and incident response requirements
- **Successful deployment of fly-away kits**, with proven field effectiveness
- Strengthened OT cybersecurity posture across multiple DLA environments
- Authored and enhanced **CERT SOPs and TTPs**, still in use across the agency
- Improved readiness through **collaborative training and threat awareness programs**

About Horizon

Horizon is a trusted cybersecurity partner for federal agencies, delivering proactive defense, hands-on incident response, and tailored solutions for both IT and OT environments. Our experts help secure critical infrastructure while empowering client teams through knowledge transfer and best practices.

Contact us at bd@hil.us to learn how Horizon can enhance your operational cybersecurity readiness.