# Case Study: 24x7 Cybersecurity Operations & Incident Response for the Defense Logistics Agency (DLA)

**Client:** Defense Logistics Agency (DLA)
**Industry:** Federal Government / Cybersecurity
**Services Provided:** Cybersecurity Operations, Incident Response, Threat Intelligence, Malware Analysis, Training & Awareness

---

## Project Overview

Horizon serves as a key cybersecurity partner to **DLA Cybersecurity**, supporting its role as the **Cybersecurity Service Provider (CSSP)** for all of DLA. Our work focuses on **incident response, continuous monitoring, threat intelligence, and cybersecurity content development**, particularly for **externally hosted applications**.

We provide **24x7 Computer Network Defense (CND)** and incident handling through DLA's CERT, supporting all devices and environments — including cloud-based assets. Our team fully staffs the Incident Response mission, ensuring compliance, timeliness, and readiness across all operations.

---

## Solutions & Capabilities Delivered

### 24x7 Incident Response & Monitoring

- Staffed DLA CERT with qualified personnel for full-time coverage
- Monitored and analyzed security events via SIEM, HBSS, NetScout, Wireshark, and custom tools

### Threat Detection & Countermeasures

- Developed and deployed custom SNORT signatures, IPS rules, and IP blacklisting
- Provided tailored responses to minimize impact across all DLA CERT subscribers

### Malware Analysis & Threat Hunting

- Created and maintained a dedicated CERT Malware Lab
- Delivered one-day Malware Boot Camps attended by DLA government personnel
- Authored key SOPs for malware handling, threat hunting, and CERT incident processes**Training & Knowledge Sharing**

- Trained both contractor and government staff on emerging cyber threats
- Shared real-time intelligence with CYBERCOM, DIA, and other DoD agencies

**Advanced Frameworks & Best Practices**

- Leveraged **MITRE ATT&CK**, **Cyber Kill Chain**, and **OODA Loop** for analysis and proactive defense
- Maintained compliance with all DoD/DLA escalation and reporting protocols

---

**Challenges Overcome**

**Talent Retention in a High-Clearance Environment**
Maintaining a qualified, cleared workforce in a competitive cybersecurity landscape was a constant challenge. Horizon addressed this by investing in training, professional development, and mentorship.

**Evolving Threat Landscape**
Cyber threats are constantly changing. Horizon remained proactive by fostering a learning culture, incorporating new tools, and staying engaged with federal cybersecurity communities.

---

**Results & Impact**

- **100% success rate** meeting incident response timelines and reporting requirements
- **No missed coverage** during 24x7 operations for DLA CERT
- **Improved cybersecurity posture** of critical external applications, including EPOS
- **Enhanced SOP documentation** used agency-wide by DLA CERT
- **Positive government feedback** with no corrective actions required

---

## About Horizon

Horizon is a trusted cybersecurity partner to federal agencies, offering scalable threat detection, incident response, and training services. Our proven ability to secure complex environments ensures mission continuity in a dynamic threat landscape.

**Contact us at** bd@hil.us to learn how Horizon can help you defend your most critical systems.