Operational Technology(OT) Cybersecurity @ HDR

HDR OT Cybersecurity Services

Brandon Erndt, PE
Brandon.erndt@hdrinc.com

State of the Cybersecurity Workforce

Just one example of the situation:

- There are approximately 100K holders of an active CISSP Certification in the U.S.
- There are currently over 600K job postings that list the CISSP as a “core requirement”
- Most of these CISSPs work in IT and have no OT/ICS experience

The same rough numbers apply across other senior level certifications as well. One defense contractor discovered there was a key certification with only 400 U.S. holders of the credential. They sent emails to every one of those people offering a 35% salary bump to “all takers”. They quickly cornered the market on that certification with over 300 making the jump.

Market Trend

Transition from Unregulated/Unaware to Regulated/Aware

- **Cyber is becoming uninsurable…**
- Some firms have a Policy cap at $300M
- Insurance enforced minimum protections to obtain policies

US Regulated Markets

All US Federal Projects & Systems
Power Generation
Oil and Gas Pipelines
Passenger & Freight Rail
All utilities in NJ, NY, TN, FL, MD

MILCON UFCs Triggering Cyber Requirements

UFC-1-200-01
UFC-4-010-06
DoDi 8510.01
DoDi 8570 – Staff Certification Requirements

HDR OT Cyber Services

At HDR, cybersecurity is not an afterthought or something that is “bolted on” to a design after the fact. Instead, it is something that is integral to each design and unique to each client and their organizational structures and risk tolerance. Cybersecurity of OT systems requires balancing stakeholder requirements for security, operability, and maintainability.

Our cybersecurity and control systems team is comprised of over 100 staff across our US based offices.   Our control system and cybersecurity teams offer full lifecycle services including assessments, planning, design, integration & testing; and cybersecurity specialty services including asset inventory, risk & vulnerability assessment, test bed design and penetration testing, training, RMF design services, governance documents (policies, procedures and standards), validation and authorization support.

We are design experts for Department of Defense with over 300 UFC-4-010-06 compliant design projects including Army, Navy, Air Force, National Guard and Army Reserve Installations.

HDR OT Cyber Services (cont.)

Consulting

- Studies
- Executive Briefing
- Develop policies, procedures, & standards
- Master Planning / Develop Goals & Objectives
- Develop RFPs for Cyber Services

Planning & Assessment

- Scalable assessments
- Current state asset inventory and network documentation
- Architecture Review
- Vulnerability Assessment
- Test Bed Penetration Testing

HDR OT Cyber Services (cont.)

Design

- Risk Management Framework to scale solutions to owner’s risk tolerance and level of investment (capital & operating)
- Design to a listed Cybersecurity Standard
- Insurance Mandated Controls
- Regulatory Mandated Controls / Processes

Construction Validation

- Configuration Validation
- Factory Test Support

Training

- Develop owner’s training program

State of the Practice

The Operational Technology (OT) cybersecurity market was impacted by several significant events in 2023 including:

- US Department of Defense: UFC-4-010-06 Update and Reissuance. The update significantly increases the complexity of the design effort, interaction with related disciplines and represents a significant increase in the mitigations required for critical and essential systems.
- Ukraine – OT Attack by Russia as part of modern warfare Russian Hackers Used OT Attack to Disrupt Power in Ukraine Amid Mass Missile Strikes - SecurityWeek).
- Proposed Federal Acquisition Regulation (FAR) rules including requirements for all government OT systems to comply with NIST 800-82, and additional requirements which will impact our IT security teams.
- New CISA "Shields Ready" campaign released in November Shields Ready | CISA for US Critical Infrastructure

State of the Practice (cont.)

The Operational Technology (OT) cybersecurity market was impacted by several significant events in 2023 including:

- Accountability for incidents challenged: SEC Lawsuit Against SolarWinds (Cybersecurity Leaders Spooked by SEC Lawsuit Against SolarWinds CISO - SecurityWeek)