tenable OT Security

OPERATIONAL TECHNOLOGY IN THE DEPARTMENT OF DEFENSE

AN OVERVIEW OF SECURITY CHALLENGES AND SOLUTIONS

As attackers become more adept at exploiting vulnerabilities in the Department of Defense's (DoD) Operational Technology (OT) environments, the potential for disruptions and even catastrophic failures in military installations increases. Effectively monitoring and securing OT systems is crucial for safeguarding national security. These systems support critical infrastructure like electricity, water and many other mission-critical operations.

POWER GRID SECURITY

Challenge: Aging infrastructure not originally designed for today's interconnected digital landscape must be secured alongside the latest OT systems.

Solution: The DoD can address vulnerabilities and identify cyber threats while optimizing energy consumption and reliability.

Data Highlight:

- **628,590B BBtus** consumed in 2022
- **$14.5B spent** on DoD operations and training
- The DoD is the **largest single energy consumer** in the U.S.[1]

1. Source: https://www.acq.osd.mil/eie/Downloads/IE/FY22%20AEPRR%20Report.pdf

WATER TREATMENT PLANT SECURITY

Challenge: Water is a critical resource for military operations, and any disruption can have severe consequences.

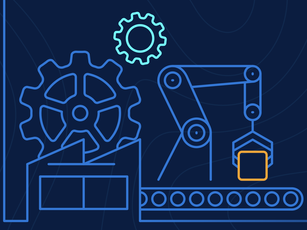
Solution: With a layerd approach that encompasses physical, network and process control security, the DoD can implement robust security measures, balanced with guaranteeing a continuous water supply.

Data Highlight:

- The DoD operates 100 wastewater treatment facilities, supplying water to **3.4 million people**
- According to a joint cybersecurity report, **ransomware gangs** silently hit three U.S. water and wasewater treatment facilities in one year[2]

2. Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a

MANUFACTURING LINE INTEGRITY



Challenge: The complex DIB supporting DoD manufacturing facilities presents a prime target for cyber attackers.

Solution: Supply chain vulnerabilities must be mitigated, while legacy systems are integrated with new, more secure technologies, without compromising production efficiency or workflow.

Data Highlight:

- **73% of OT devices** in manufacturing environments are unmanaged[3]

3. Source: https://www.cit-net.com/cybersecurity-statistics-for-the-manufacturing-industry-protecting-valuable-assets/)

TRANSPORTATION SECURITY AND FLEET MANAGEMENT

Challenge: DoD transportation systems encompass a wide range of vehicles, equipment, and fleet infrastructure, each with unique security requirements.

Solution: Security solutions must include the entire fleet, while managing constantly-evolving cyber threats.

Data Highlight:

- The DoD fleet: **250,000** tactical vehicles **177,000** trucks/ passenger vehicles **280** ships in the Navy **14,000** aircraft
- **400%** in automotive cyberattacks in the transportation sector[4]

4. Source: https://www.brookings.edu/articles/the-department-of-defenses-digital-logistics-are-under-attack/

BUILDING MANAGEMENT AND SECURITY SYSTEMS

Challenge: OT for Building Management Systems (BMS) monitors, supervises, controls and reports on smart building technology systems, each with its own security vulnerabilities.

Solution: Implementing a modern security solution that addresses all aspects of the complex ecosystem of vendors and suppliers is essential.

Data Highlight:

- **500+** installations worldwide and **284,359** buildings, covering **2.31B** square feet[5]
- **42%** of computers in building automation infrastructures faced cyber threats in 2022[6]
- Over **12,000** cyber incidents in the DoD since 2015[7]

5. Source: https://www.acq.osd.mil/eie/Downloads/IE/FY22%20AEPRR%20Report.pdf)
6. Source: https://www.kaspersky.com/about/press-releases/2022_spyware-on-the-rise-restless-building-automation-ot-threats-in-2022
7. Source: https://www.gao.gov/assets/gao-23-105084.pdf

SECURING OT IN THE DOD

Keeping the DoD's OT systems safe is like constantly updating the locks on doors in an ever-changing neighborhood of digital threats. Monitoring and securing OT is vital to the security practices within DoD installations: think uncrackable passwords, keeping an eagle eye on who's coming and going in your systems and always knowing what's connected to what.

OT SECURITY BEST PRACTICES

- Implementing a zero trust framework
- Aligning the correct remote access tools
- Applying robust identity and access management tools
- Rapid identification of suspicious activity and attacks
- Accurate connectivity analysis and network mapping

With Tenable, the DoD can significantly enhance its resilience and operational readiness while protecting OT systems in a shifting landscape of cyber threats.

Learn more about Tenable OT Security

tenable