



Rock Secure

RockSec

OT CYBER RESILIENCE PLAYBOOK

Key OT Case Studies & Lessons Learned

- **NotPetya Attack:** Highlighted the necessity of Vulnerability Management and timely patching.
- **Colonial Pipeline Attack:** Emphasized Secure Remote Access and access controls.
- **Ukraine Power Grid Attack:** Demonstrated the importance of Network Segmentation and Disaster Recovery.
- **Other Critical Incidents:** Illustrated the need for robust Incident Response in OT environments.

Core RockSec Service Offerings:

Empowering Industrial Cyber Security Excellence

We provide tailored security services designed to enhance OT cybersecurity maturity, detect vulnerabilities, validate controls, and reduce industrial cyber risk.

- **Asset Inventory:** Automated discovery and context of all OT devices across networks.
- **Vulnerability Management:** Assess and remediate vulnerabilities to minimize attack surface.
- **Risk Management:** Validate compliance with OT standards and manage cyber risk.
- **Threat Detection & Response:** Detect and respond to threats with real-time monitoring and incident response.

Our mission is to strengthen your Industrial Cyber Security Posture, reduce risk and enhance operational