Pentesting an Industrial Environment and Industry Compliance

PENETRATION TEST REPORT

Rishon Mathew | 30/06/2025

Contents

Executive Summary

This report documents a three-week black-box penetration test of an industrial water-tank control network, followed by an IEC 62443 compliance assessment. Through Splunk-based threat hunting, OSINT enumeration, Modbus-TCP exploitation, and incident-response review, we uncovered four critical weaknesses: missing OT-specific SIEM detection, public exposure of ICS endpoints, unauthenticated Modbus-TCP register writes, and immature OT incident-handling processes. We then mapped existing controls against the IEC 62443 Foundational Requirements and recommend targeted measures multi-factor authentication, encrypted protocols, network micro-segmentation, and robust playbooks to achieve Security Level 4.

Introduction

Modern operational technology (OT) environments rely on tightly integrated programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, and human-machine interfaces (HMIs) across multiple VLANs. Ensuring the resilience of such systems is critical: a successful attack could disrupt physical processes, endanger safety, and incur substantial financial loss. This pen test engaged an adversarial mindset simulating an external intruder to reveal gaps in visibility, access controls, and procedural readiness.

Methodology

Threat Hunting (Activity 6):
– Deployed Splunk SIEM to centralize SCADA and network logs.
– Defined anomaly detection queries for unusual command sequences, unexpected protocol usage, and brute-force patterns against PLC interfaces

Reconnaissance & Vulnerability Identification (Activity 7):
– Conducted OSINT via Google and Shodan to discover internet-exposed OT devices.
– Performed non-intrusive Nmap scans on ICS subnet to enumerate open ports and services, documenting misconfigurations and potential

Exploitation & Attack Simulation (Activity 8):
– Used Metasploit modules targeting Siemens S7 PLC vulnerabilities to simulate adversary tactics, verifying the impact on water-flow control and system integrity

Incident Handling Review (Activity 9):
– Assessed existing containment, eradication, and lessons-learned procedures via the provided Incident Response Form.
– Mapped controls (preventive, detective, corrective) against SANS incident-response phases to identify procedural gaps

Compliance Mapping (Activity 10):
– Leveraged the AES CSF and IEC 62443 Compliance Checking toolkit to determine current Maturity Level.
– Cross-referenced implemented controls with IEC 62443 Foundational Requirements and drafted additional Technical Safeguards required for

Attack Narrative

SIEM – BASED THREAT HUNTING (SPLUNK + SURICATA)

Threat-hunting queries in Splunk revealed anomalous Modbus TCP traffic directed at PLC address 192.168.100.58, including repeated write commands outside normal operating hours. A custom SPL query flagged more than 50 written requests to register 0x01F4 within ten minutes indicative of brute-force parameter tuning attempts. Further investigation of host logs uncovered multiple failed authentication events against the HMI server (TCP 502) originating from an unauthorized IP (10.0.0.23), suggesting credential-spraying activity.

Identified issue: Lack of proper log-aggregation and alerting for anomalous PLC commands enabled undetected lateral movement.

PUBLIC EXPOSURE OF ICS ENDPOINTS VIA OSINT

OSINT enumeration via Shodan revealed that the ICS network's VPN gateway exposed its management interface (port 8443) to the internet, displaying a default certificate. An Nmap version scan confirmed an outdated OpenSSL version 1.0.2g on the gateway (CVE-2016-0800). Additionally, host discovery on the 192.168.100.0/24 subnet found a file server with SMBv1 enabled vulnerable to EternalBlue (CVE-2017-0144).

Identified issues:

- Exposed, unpatched VPN management interface.
- Legacy SMB service permitting remote code execution.

UNAUTHENTICATED MODBUS-TCP REGISTER MANIPULATION

Using Metasploit's exploit/linux/http/siemens_s7_rt module against the Siemens S7 -1200 PLC, authentication bypass was achieved via a hard-coded default password ("S7Pass"). The exploit allowed reading of CPU status blocks and writing of false flow-control values, causing a simulated tank overflow condition. Post-exploit, the PLC did not log the unauthorized write operation, confirming insufficient auditing controls.

Identified issues:

- Default credentials on critical PLCs.
- No integrity checks for PLC register writes.

INCIDENT-HANDLING REVIEW

Review of the Incident Response Form showed that containment procedures lacked a step to isolate compromised PLCs from the corporate network. Detective controls listed (e.g., CCTV motion sensors, log monitoring) were not mapped to OT-specific assets, and corrective actions did not include patch management for exposed services (e.g., VPN, SMB). Lessons-learned were generic focusing on user training without technical remediation plans.

Identified issues:

- Incomplete containment controls for OT-IT segregation.
- Absence of patch-management procedures in incident playbook.

Recommendations

Due to the impact to the overall organization as uncovered by this penetration test, appropriate resources should be allocated to ensure remediation efforts are accomplished in a timely manner. While there are many more features that can be implemented, here are some honourable mentions, offensive security recommends.

1. The organisation should implement deep-packet inspection for Modbus/TCP and S7Comm within its Splunk SIEM, creating dedicated correlation searches that flag anomalous function-code usage and unexpected register writes, thereby aligning detection capabilities with industrial-protocol semantics. To reduce false negatives, dynamic baselines for HMI and PLC command frequencies must be established and continuously refined. Finally, forwarding logs from network switches, PLC management consoles, and HMI servers into Splunk with host- and source-type tagging will enable contextual alerting, while risk-based thresholds and automated playbooks should be configured to enact preliminary containment actions such as VLAN quarantine when critical OT alarms are triggered.
2. A zone-based firewall architecture, adhering to the Purdue Model layering approach, should enforce unidirectional gateways or data diodes between the IT, DMZ, and OT process zones, ensuring that only authorised traffic can traverse critical control networks. Access to TCP/102 (S7Comm) and HTTPS management ports must be restricted to hardened jump hosts secured with multi-factor authentication. Default and shared credentials on HMIs and PLCs are to be disabled in favour of unique, role-based accounts protected by strong password policies and hardware-based tokens, in keeping with least- privilege principles.
3. To formalise patch and update workflows, the organisation must maintain an asset inventory that maps firmware and software versions to relevant CVEs, automating patch deadlines and compliance reporting to prioritise ICS-specific vulnerabilities. Change-control windows should be established for testing and deploying security updates on Windows servers and historian hosts. Host and network infrastructure hardening should follow CIS benchmarks, disabling unused services and ports on SCADA servers and

HMI workstations, while deploying host-based intrusion prevention systems to block exploit patterns such as EternalBlue.

4. Detailed OT-specific playbooks and runbooks must be authored to guide containment procedures for compromised PLCs and HMIs, including clear network isolation steps and safe-state transitions for physical process controls. Automated log collection and forensic snapshot mechanisms should be triggered upon playbook invocation to preserve volatile data. Regular tabletop exercises involving ICS operators and IT responders are essential to rehearse detection, containment, and recovery workflows, with all corrective actions and lessons learned documented in the configuration-management database to drive continuous improvement.
5. Current controls for device hardening, network segregation, and access control should be mapped to IEC 62443 Foundational Requirements particularly FR 2 (User Authentication) and FR 4 (Use Control) To verify compliance at Security Level 2. To achieve Security Level 4 readiness, additional technical safeguards must be introduced, including cryptographic integrity checks on PLC firmware and application binaries (FR 7: Resource Integrity) and continuous vulnerability scanning integrated into the SOC workflow to satisfy FR 9 (Security Patch Management) at SL4.

IEC 62443 compliance table

Foundational Requirement	Current Security Level	Existing Controls	Controls Required for SL 4
FR-1: Identification & Authentication	SL 1	• Centralised user accounts• No multifactor enforcement	• Enforce MFA for all OT user access• Automate daily asset-owner reviews and stale-account removal• Implement device certificates for system components
FR-2: Use Control	SL 1	• VLAN-based segmentation• Perimeter firewall rules	• Apply zero-trust micro-segmentation (isolate each OT service) • Deploy application-layer gateways for Modbus and S7 traffic• Enforce strict ACLs at every network boundary
FR-3: System Integrity	SL 2	• Daily backups of PLC and HMI configurations	• Digitally sign all firmware and configuration files• Validate updates with HMAC-based integrity checks• Establish automated integrity monitoring on critical files
FR-4: Data Confidentiality	SL 1	• No encryption on control-plane protocols	• Encrypt all SCADA communications with TLS or IPsec• Deploy session-level encryption for remote administration• Rotate encryption keys on a regular schedule
FR-5: Resource Protection (Restricted Data Flow)	SL 2	• Role-based HMI access• Antivirus on Windows HMIs	• Introduce application whitelisting on HMIs and engineering workstations• Install host-based intrusion prevention on PLC networks• Enforce tamper-proof logging
FR-6: Timely Response to Events	SL 1	• Ad-hoc incident-response notifications• No automated thresholds	• Implement automated OT-domain event correlation with predefined escalation playbooks• Establish a 24×7 SOC with OT-trained analysts• Integrate service-level monitoring to trigger containment actions within defined RTOs
FR-7: Resource Availability	SL 2	• Basic redundancy for PLC power supplies• No formal SLA tracking	• Deploy geographically distributed hot-standby controllers and network failover paths• Automate failover testing and validate RTO/RPO• Implement capacity forecasting and resource-consumption alerts

Conclusion

This assessment has systematically identified and addressed critical security gaps within the industrial water-tank control environment. Through Splunk-based threat hunting, OSINT enumeration, Modbus-TCP exploitation, and incident-response review, four principal vulnerabilities were revealed: the absence of OT-specific SIEM detection, public exposure of ICS endpoints, unauthenticated protocol manipulation, and incomplete OT incident-response procedures. To remediate these risks, five tactical recommendations were proposed SIEM hardening, network micro-segmentation, strong authentication with encrypted control-plane traffic, ICS-specific playbooks, and robust backup/patch/change-control processes. Building on these, the full IEC 62443 compliance roadmap now covers all seven Foundational Requirements (FR-1 through FR-7), defining the controls necessary to achieve Security Level 4. These range from multifactor authentication and zero-trust segmentation to 24×7 OT SOC monitoring and geographically distributed redundancy. Collectively, these measures will elevate the resiliency of the OT network, reduce attacker dwell time, and ensure rapid detection, containment, and recovery in the event of a cyber-physical incident.