OT Security Assessment Report (AS-IS)

Date: 2025-11-29 **Compliance Scope:** ISO 27001, PCI DSS, HIPAA

1. Executive Summary

This report details the findings of a security assessment conducted on the Operational Technology (OT) environment. The assessment focused on identifying vulnerabilities that could impact operational continuity, safety, and compliance.

Key Findings: - Critical risks identified in PLC and Modbus communications. - Compliance gaps found regarding Access Control and Network Security.

2. Methodology

The assessment followed a standard penetration testing methodology adapted for OT environments: 1. **Discovery**: Passive and active asset identification. 2. **Enumeration**: Service and version detection. 3. **Vulnerability Analysis**: Identification of known flaws. 4. **Exploitation (Controlled)**: Verification of critical vulnerabilities. 5. **Risk Assessment**: Likelihood and Impact analysis.

3. Asset Inventory

4. Technical Findings & Risk Assessment

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Register written. Setpoint changed to 100.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 3 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Register written. Setpoint changed to 100.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 3 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Register written. Setpoint changed to 100.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 3 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Register written. Setpoint changed to 100.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 3 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Register written. Setpoint changed to 100.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 3 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Exploit Success

Asset: 1 | **Source:** MetasploitAgent **Description:** Exploited with exploit/multi/http/default*cred*sexec. Meterpreter session 1 opened. User: admin (uid=0)

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** Critical (Safety/Operational) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 1 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Register written. Setpoint changed to 100.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ ICS Impact

Asset: 3 | **Source:** IcsAgent **Description:** Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

Risk Assessment: - **Likelihood:** High (Proven) - **Impact:** High (Process Manipulation) - **Risk Level:** CRITICAL

Compliance Impact: - ISO 27001: A.12.1 (Operational Procedures), A.17 (Continuity) - PCI DSS: Req 10 (Monitoring) - HIPAA: 164.308(a)(7) (Contingency Plan)

■ Web Vulnerability

Asset: 1 | **Source:** WebScanner **Description:** Default Credentials (admin/admin)

Risk Assessment: - **Likelihood:** Low - **Impact:** High (Unauthorized Access) - **Risk Level:** HIGH

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Web Vulnerability

Asset: 1 | **Source:** WebScanner **Description:** Default Credentials (admin/admin)

Risk Assessment: - **Likelihood:** Low - **Impact:** High (Unauthorized Access) - **Risk Level:** HIGH

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Web Vulnerability

Asset: 1 | **Source:** WebScanner **Description:** Default Credentials (admin/admin)

Risk Assessment: - **Likelihood:** Low - **Impact:** High (Unauthorized Access) - **Risk Level:** HIGH

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Web Vulnerability

Asset: 1 | **Source:** WebScanner **Description:** Default Credentials (admin/admin)

Risk Assessment: - **Likelihood:** Low - **Impact:** High (Unauthorized Access) - **Risk Level:** HIGH

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Web Vulnerability

Asset: 1 | **Source:** WebScanner **Description:** Default Credentials (admin/admin)

Risk Assessment: - **Likelihood:** Low - **Impact:** High (Unauthorized Access) - **Risk Level:** HIGH

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Web Vulnerability

Asset: 1 | **Source:** WebScanner **Description:** Default Credentials (admin/admin)

Risk Assessment: - **Likelihood:** Low - **Impact:** High (Unauthorized Access) - **Risk Level:** HIGH

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt)

■ Default SNMP Community String

Asset: 1 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Siemens S7-1500 FW:2.1

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 3 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Moxa MGate MB3180

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 1 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Siemens S7-1500 FW:2.1

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 3 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Moxa MGate MB3180

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 1 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Siemens S7-1500 FW:2.1

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 3 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Moxa MGate MB3180

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 1 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Siemens S7-1500 FW:2.1

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 3 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Moxa MGate MB3180

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 1 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Siemens S7-1500 FW:2.1

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 3 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Moxa MGate MB3180

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 1 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Siemens S7-1500 FW:2.1

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ Default SNMP Community String

Asset: 3 | **Source:** SnmpScanner **Description:** Found default community string 'public'. System: Moxa MGate MB3180

Risk Assessment: - **Likelihood:** High - **Impact:** Medium (Info Disclosure) - **Risk Level:** MEDIUM

Compliance Impact: - ISO 27001: A.9.2.1 (User Registration), A.9.4.3 (Password Mgmt) - PCI DSS: Req 2.1 (Default Defaults), Req 8.2 (Auth) - HIPAA: 164.308(a)(5)(ii)(D) (Password Mgmt) - ISO 27001: A.13.1 (Network Security) - PCI DSS: Req 4.1 (Strong Cryptography) - HIPAA: 164.312(e)(1) (Transmission Security)

■ NSE Info: s7-info

Asset: 1 | **Source:** NmapAgent **Description:** Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 1 | **Source:** NmapAgent **Description:** Sid: 1 Device: Simatic Modbus TCP

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: ssh-auth-methods

Asset: 3 | **Source:** NmapAgent **Description:** Supported: publickey, password

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 3 | **Source:** NmapAgent **Description:** Sid: 1 Device: Moxa NPort

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: s7-info

Asset: 1 | **Source:** NmapAgent **Description:** Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 1 | **Source:** NmapAgent **Description:** Sid: 1 Device: Simatic Modbus TCP

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: ssh-auth-methods

Asset: 3 | **Source:** NmapAgent **Description:** Supported: publickey, password

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 3 | **Source:** NmapAgent **Description:** Sid: 1 Device: Moxa NPort

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: s7-info

Asset: 1 | **Source:** NmapAgent **Description:** Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 1 | **Source:** NmapAgent **Description:** Sid: 1 Device: Simatic Modbus TCP

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: ssh-auth-methods

Asset: 3 | **Source:** NmapAgent **Description:** Supported: publickey, password

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 3 | **Source:** NmapAgent **Description:** Sid: 1 Device: Moxa NPort

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: s7-info

Asset: 1 | **Source:** NmapAgent **Description:** Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 1 | **Source:** NmapAgent **Description:** Sid: 1 Device: Simatic Modbus TCP

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: ssh-auth-methods

Asset: 3 | **Source:** NmapAgent **Description:** Supported: publickey, password

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 3 | **Source:** NmapAgent **Description:** Sid: 1 Device: Moxa NPort

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: s7-info

Asset: 1 | **Source:** NmapAgent **Description:** Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 1 | **Source:** NmapAgent **Description:** Sid: 1 Device: Simatic Modbus TCP

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: ssh-auth-methods

Asset: 3 | **Source:** NmapAgent **Description:** Supported: publickey, password

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 3 | **Source:** NmapAgent **Description:** Sid: 1 Device: Moxa NPort

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: s7-info

Asset: 1 | **Source:** NmapAgent **Description:** Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 1 | **Source:** NmapAgent **Description:** Sid: 1 Device: Simatic Modbus TCP

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: ssh-auth-methods

Asset: 3 | **Source:** NmapAgent **Description:** Supported: publickey, password

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO

■ NSE Info: modbus-discover

Asset: 3 | **Source:** NmapAgent **Description:** Sid: 1 Device: Moxa NPort

Risk Assessment: - **Likelihood:** Low - **Impact:** Low - **Risk Level:** INFO
