OT Security Remediation Strategy (TO-BE)

Date: 2025-11-29 **Reference:** Based on Assessment Report dated 2025-11-29

1. Strategic Executive Summary

Following the vulnerability assessment, this report outlines the strategic roadmap for remediation. The focus is on prioritizing high-impact mitigations that align with business objectives and compliance mandates.

2. Prioritized Remediation Plan

■ Mitigation: Exploit Success

Risk Driver: CRITICAL Risk identified in assessment.

Recommended Actions: - **Patch Management**: Urgent patching of web services. - **Network Isolation**: Restrict access to HMI/PLC web interfaces.

Cost & Effort Analysis: - **Estimated Cost:** $1,000 - $5,000 (Labor) - **Implementation Effort:** Low

---

■ Mitigation: ICS Impact

Risk Driver: CRITICAL Risk identified in assessment.

Recommended Actions: - Implement **Zone-based Segmentation** (IEC 62443). - Deploy **Industrial IPS** with deep packet inspection. - Enable **PLC Protection Levels** and password authentication.

Cost & Effort Analysis: - **Estimated Cost:** $15,000 - $50,000 (Hardware + Labor) - **Implementation Effort:** High (Downtime Required)

■ Mitigation: Web Vulnerability

Risk Driver: HIGH Risk identified in assessment.

Recommended Actions: - Standard hardening and monitoring.

Cost & Effort Analysis: - **Estimated Cost:** $1,000 - $5,000 (Labor) - **Implementation Effort:** Low

---

■ Mitigation: Default SNMP Community String

Risk Driver: MEDIUM Risk identified in assessment.

Recommended Actions: - **Identity Management**: Enforce strong password policies. - **MFA**: Implement multi-factor authentication for critical access.

Cost & Effort Analysis: - **Estimated Cost:** $15,000 - $50,000 (Hardware + Labor) - **Implementation Effort:** High (Downtime Required)

■ Mitigation: NSE Info: s7-info

Risk Driver: INFO Risk identified in assessment.

Recommended Actions: - Standard hardening and monitoring.

Cost & Effort Analysis: - **Estimated Cost:** $15,000 - $50,000 (Hardware + Labor) - **Implementation Effort:** High (Downtime Required)

■ Mitigation: NSE Info: modbus-discover

Risk Driver: INFO Risk identified in assessment.

Recommended Actions: - Standard hardening and monitoring.

Cost & Effort Analysis: - **Estimated Cost:** $10,000 - $30,000 - **Implementation Effort:** Medium

---

■ Mitigation: NSE Info: ssh-auth-methods

Risk Driver: INFO Risk identified in assessment.

Recommended Actions: - Standard hardening and monitoring.

Cost & Effort Analysis: - **Estimated Cost:** $5,000 - $10,000/yr - **Implementation Effort:** Medium

---