Atos' OT Vulnerability Management Proactive Checklist

1. Asset Discovery and Inventory

- [ ] Maintain a real-time, continuously updated OT asset inventory that captures the make, model, firmware, and software versions.
- [ ] Classify assets by criticality and business impact.
- [ ] Map all connections between OT, IT, and external environments.

2. Risk-based Vulnerability Prioritization

- [ ] Continuously assess OT assets using threat intelligence, exploitability data, and business impact.
- [ ] Apply a risk-based scoring model to prioritize remediation.
- [ ] Address critical vulnerabilities proactively, even before vendor patches.

3. Secure Configuration and Hardening

- [ ] Enforce baseline security configurations — disable unused services, close unnecessary ports, and remove default credentials.
- [ ] Regularly audit configurations against IEC 62443 and industry best practices.
- [ ] Implement application allow listing and network segmentation to shrink the attack surface.

4. Patch and Firmware Management

- [ ] Define a structured, minimally disruptive OT patch management process.
- [ ] Test patches in controlled environments prior to deployment.
- [ ] Collaborate with vendors to access security updates pre-disclosure.

Atos

5. Network and Access Controls

- [x] Enforce zero-trust access — only authorized users and devices allowed.
- [x] Apply strict remote access policies with MFA.
- [x] Continuously monitor network traffic for unauthorized or abnormal activity.

6. Threat Intelligence and Anomaly Detection

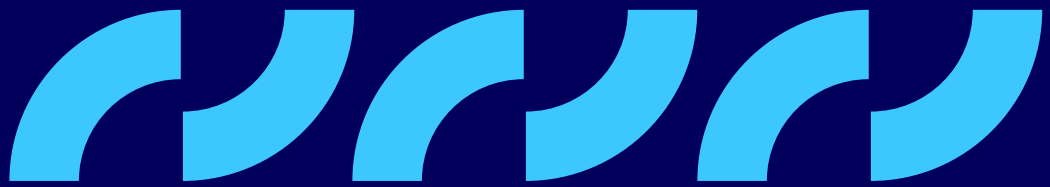
- [x] Integrate OT-specific threat intelligence to track emerging risks.
- [x] Deploy OT-aware IDS to detect anomalies.
- [x] Automate correlation of network activity with known threats and vulnerabilities..

7. Incident Preparedness and Response Simulation

- [x] Regularly conduct tabletop exercises and OT-specific red team drills.
- [x] Define clear roles for operations, IT, security, and compliance teams.
- [x] Maintain a rapid containment and mitigation plan for potential exploits.

8. Compliance and Continuous Improvement

- [x] Align processes with IEC 62443, NIST CSF, and NERC CIP standards..
- [x] Continuously review and refine vulnerability management policies.
- [x] Deliver ongoing security awareness training for OT operators and engineers.



Atos