Checklist — Sécuriser l’IoT / équipements connectés

Bureautique & Industriel — Déploiement, exploitation et préparation aux incidents

Généré automatiquement — sections actionnables pour responsable IT / RSSI

Déploiement initial (avant 1ère mise en service)

- ☐ Fournisseur validé (patch policy, EOL, SBOM) — oui/non.
- ☐ VLAN dédié créé + ACL par défaut deny-all.
- ☐ Authentification admin protégée (changement mot de passe, certificats, RADIUS si possible).
- ☐ Télémetrie & logs configurés vers un collector central.
- ☐ Update / rollback testés en laboratoire.

Exploitation (quotidien / hebdo)

- ☐ Découverte : tout device inconnu est signalé et vérifié.
- ☐ Scan de vulnérabilité programmé (non-intrusif si OT).
- ☐ Vérifier intégrité firmware (hashes) pour devices sensibles.
- ☐ Suivi des mises à jour et planning de patch.
- ☐ Vérification régulière des logs et alertes réseau (NetFlow / IDS).

Incident readiness (préparation incident)

- ☐ Playbooks de triage & containment disponibles et accessibles.
- ☐ Contacts vendor / support avec SLA documentés.
- ☐ Backups des configurations & procédure de restauration testée.
- ☐ VLAN/quarantaine prête à l'emploi pour isoler devices compromis.
- ☐ Enregistrement des actions et du temps (journaux d'incident).

Priorités immédiates (0–30 jours)

- ☐ Inventaire complet (découverte passive + active) et enregistrement dans CMDB.
- ☐ Segmenter tous les IoT dans VLANs isolés avec ACL deny-all par défaut.
- ☐ Activer logs & monitoring (NetFlow, règles Zeek/Suricata basiques).
- ☐ Exiger du fournisseur preuves de patching / plan d’EOL pour équipements critiques.

Sources recommandées: ENISA, NISTIR 8259, CISA, OWASP IoT Project, ISA/IEC 62443, NIST SP 800-82.