Analyse des risques BottleAsec selon la méthode EBIOS

Atelier 1 : Périmètre et Référentiel de Sécurité

1.1 Contexte et Périmètre

Le système BottleAsec est un système d'embouteillage de liquide chimique corrosif, basé sur une architecture ICSSIM étendue. Il comprend une zone industrielle (automates PLC1 pour le réservoir et PLC2 pour le tapis roulant), une zone de supervision avec trois HMI (HMI1, HMI2 en production, HMI3 de secours), et une zone bureaux connectée à Internet via un pare-feu. Les HMI sont des PC portables à grand écran dotés d'interfaces RJ45 vers le réseau de contrôle et Wi-Fi (habituellement désactivé). La zone bureaux repose sur une infrastructure filaire et Wi-Fi autorisant uniquement des équipements gérés (Règle ANSSI 7).

1.2 Missions et Actifs Métier

- Assurer l'approvisionnement en liquide corrosif sans fuite (tolérance zéro), garantir l'automatisation pour limiter l'intervention humaine et éviter la cristallisation en cas d'arrêt abrupt.

Actifs métier :

- Stockage du liquide corrosif (réservoir, capteurs de niveau, vannes) – Disponibilité critique.
- Ligne d'embouteillage (capteurs niveau bouteille, moteur de tapis) – Intégrité des opérations.
- Supervision (HMI1, HMI2, HMI3) – Confidentialité et intégrité des commandes.
- Réseau de contrôle Modbus/TCP non sécurisé (Risque critique, intégrer Règle 21, utiliser TLS pour les flux Modbus).
- Infrastructure bureaux (postes utilisateurs, Wi-Fi) – confidentiel relatif.

1.3 Actifs Supports

- Automates PLC1 et PLC2 (non airgap, Modbus/TCP non chiffré).
- Switches WeOS (5.11.X-3) interconnectant supervision et contrôle.
- PC portables HMI (Wi-Fi et RJ45).
- Serveurs de fichiers et bases de données stockant les traces et journaux.
- Infrastructure réseau bureaux et équipements Wi-Fi.

1.4 Événements redoutés et Sévérité

En se basant sur Règle 4 (identifier informations sensibles et schéma réseau), les événements redoutés incluent :

- Fuite ou perte de liquide corrosif (sévérité G4).
- Perturbation de la ligne d'embouteillage (G3/G4 suivant durée >1 semaine en pic épidémique).
- Altération des commandes HMI (G3).

- Exfiltration de données sensibles de production (G2).
- Saturation ou compromission du réseau Modbus/TCP (G4).

1.5 Référentiel de Sécurité (Règles ANSSI et Normes)
Règles ANSSI prises en compte :
- Règle 4 : Disposer d'un schéma réseau à jour et identifier actifs/infos sensibles.
- Règle 7 : Autoriser uniquement des équipements maîtrisés (blocage Wi-Fi non géré).
- Règle 19 : Segmenter le réseau (tiers 1/2/3/4, cloisonnement via VLAN et pare-feu).
- Règle 21 : Utiliser protocoles sécurisés (prévoir TLS pour Modbus, HTTPS pour HMI web).
État actuel :
- Modbus/TCP non chiffré (écart, impératif implémenter Modbus Security TLS).
- Wi-Fi des HMI souvent désactivé (conforme Règle 7, mais risque activation accidentelle).
- Ségrégation bureautique – supervision – contrôle via VLAN, mais pas encore filtrage Modbus.
- Journaux activés sur HMI et switches, mais pas centralisés ni conservés >1 an.

Atelier 2 : Origines du Risque

2.1 Origines et Objectifs Cibles
Risque externes et internes retenus :
- Ancien employé disposant toujours d'accès HMI3 (menace interne, sabotage de la ligne – TO : arrêt de production).
- Intrus externe piratant la zone bureaux via Wi-Fi non maitrisé, propagation vers supervision (TO : altération des commandes HMI).
- Concurrent cherchant à exfiltrer les recettes de production (TO : vol de savoir-faire et données de process).
- Hacktiviste visant à provoquer une fuite de liquide (TO : sabotage environnemental et image publique).
- Attaque via fournisseur TI (R3) compromettant HMI – exfiltration (TO : vol de données et sabotage).

2.2 Évaluation (Motivation, Ressources, Activité)
Les origines retenues nécessitent un focus sur :
- Menace interne (ancien) : accès légitime, haute crédibilité (pertinence élevée).
- Attaque par Wi-Fi (extrême) : risque modéré, mais possible rebond interne (pertinence moyenne).
- Concurrent : motivation financière, ressources crédibles, activité basse (pertinence modérée).
- Hacktiviste : faible probabilité, mais fort impact potentiel (pertinence moyenne).
- Fournisseur TI mal sécurisé : forte exposition (pertinence élevée).

2.3 Paires RO/TO retenues :
• Ancien employé → Arrêt de production (sabotage via HMI3).

• Fournisseur TI → Exfiltration de données (via HMI ou réseau de supervision).
• Intrus Wi-Fi → Altération HMI (via HMI1/HMI2).
• Concurrent → Exfiltration de savoir-faire.
• Hacktiviste → Fuite de liquide (sabotage physique via altération des vannes PLC1).

Atelier 3 : Scénarios Stratégiques

3.1 Cartographie de la menace dans l'écosystème
Écosystème critique :
- Fournisseur TI (service réseaux) : haut niveau de pénétration, maturité faible → Critique.
- Ancien employé (accès résiduel) : accès direct à HMI3 → Critique.
- Réseau bureaux (Wi-Fi potentiellement activable) : exposition modérée, maturité faible → Élevé.
- Concurrent (invisible, dynamiques avancées) : exposition indirecte, maturité élevée → Moyen.
- Hacktiviste (faible maturité, accès incertain) : menace moins prioritaire.

3.2 Scénarios Stratégiques (RO→TO)
• Ancien employé sabotant la production :
 - Intrusion légitime sur HMI3 (utilisation de compte résiduel).
 - Commande fermeture intempestive de la vanne PLC1 → arrêt immédiat → cristallisation → fuite.
 Impact : G4.

• Fournisseur TI exfiltrant les données :
 - Compromis via contrat de maintenance (accès supervisé, injection de backdoor).
 - Lateralisation vers serveur de fichiers HMI → exfiltration.
 Impact : G3/G2 selon échelle.

• Intrus externe utilisant le Wi-Fi :
 - Activation du Wi-Fi sur HMI → bruteforce du compte admin HMI2.
 - Altération des réglages du process (modification de seuils capteurs).
 Impact : G3.

• Concurrent volant le savoir-faire :
 - Scan réseaux, identification du serveur R&D (supervision).
 - Exfiltration via VPN de l'entité.
 Impact : G2.

• Hacktiviste provoquant une fuite :
 - Accès indirect via fournisseur TI (pivot) → ouverture vanne 1 en dehors horloge.
 Impact : G4.

Tous les scénarios s'appuient sur la segmentation réseau (Règle 19), l'utilisation de protocoles sécurisés (Règle 21), et l'assurance que seuls les équipements maîtrisés sont connectés (Règle 7).

Atelier 4 : Scénarios Opérationnels

4.1 Principales Menaces Techniques

Pour chaque scénario stratégique, on détaille ci-dessous la chaîne d'attaque la plus probable.

• Sabotage par ancien employé :
- Connaissance préalable des identifiants HMI3 (compte non désactivé) : creddump.
- Authentification sur le HMI3 → envoi de commande de fermeture de vanne.
- Pas de 2FA. Impact immédiat.
Likelihood V3.

• Exfiltration par fournisseur TI :
- Maintenance régulière → injection d'un module de monitoring sur switch de supervision.
- Exfiltration via canal SSL/TLS sortant (VPN interne).
- Serveur de fichiers non chiffré.
Likelihood V4 (très probable).

• Intrusion via Wi-Fi :
- Activation du Wi-Fi sur HMI1 non patché (vulnérabilité WPA2).
- Brute-force/Rainbow tables pour compte admin.
- Modification des paramètres Modbus via HMI.
Likelihood V2.

• Vol de savoir-faire concurrent :
- Reversing de traffic non chiffré sur réseau supervision interne.
- Récupération de fichiers R&D depuis serveur local.
- Exfiltration via service FTP interne non protégé.
Likelihood V2.

• Fuite orchestrée par hacktiviste :
- Achats d'informations d'accès fournisseur TI (Dark web) → connexion SSH au switch.
- Modification de la logique de contrôle automatique (SCADA) sur PLC1.
- Vanne ouverte sous contrôle direct, provoquant fuite.
Likelihood V1.

Les scénarios opérationnels sont évalués avec leurs Likelihood respectifs, et confirment la nécessité de mesures correctives fortes.

Atelier 5 : Traitement des Risques

5.1 Synthèse des Risques

- R1 (Ancien employé → Fuite/cristallisation) : Sévérité G4, Likelihood V3 → Risque critique.
- R2 (Fournisseur TI → Exfiltration) : Sévérité G3, Likelihood V4 → Risque critique.
- R3 (Intrus Wi-Fi → Altération HMI) : Sévérité G3, Likelihood V2 → Risque élevé.
- R4 (Concurrent → Vol savoir-faire) : Sévérité G2, Likelihood V2 → Risque significatif.
- R5 (Hacktiviste → Fuite liquide) : Sévérité G4, Likelihood V1 → Risque élevé.

5.2 Mesures de Sécurité (Plan d'Amélioration Continu)

- Désactivation strictement forcée du Wi-Fi sur tous les HMI (Règle 7).
- Implémentation de Modbus Security (TLS 1.2) pour chiffrement des échanges entre PLC1↔PLC2 et HMI (Règle 21).
- Renforcement des accès HMI3 : désactivation des comptes inactifs, mise en place d'une authentification forte (2FA) sur HMI.
- Segmentation réseau : isolation stricte réseau administration, supervision, et contrôle (Règle 19).
- Centralisation des journaux sur un SIEM : conservation ≥ 1 an, corrélation et alerting (Règle 4 pour schéma de données).
- Politique de mise à jour automatisée (correctifs OS, applicatifs SCADA) mensuelle (Règle 34 du Guide ANSSI).
- Mise en place d'un réseau VPN IPsec pour accès nomade aux HMI (Règle 32).
- Révocation immédiate des accès et badges des anciens employés ; revue trimestrielle des comptes privilégiés (Règle 6 du Guide ANSSI).
- Audit de sécurité externe annuel, tests de restauration de sauvegarde trimestriels (Règle 37 du Guide ANSSI).

5.3 Risques Résiduels

- R1 (Ancien employé) : Résidual moyen (sévérité G2/V2) après suppression des comptes.
- R2 (Fournisseur TI) : Résidual moyen (G2/V3) après audit et renforcement.
- R3 (Intrus Wi-Fi) : Résidual faible (G1/V1) après blocage Wi-Fi.
- R4 (Concurrent) : Résidual faible (G1/V1) après chiffrement des fichiers sensi-
- R5 (Hacktiviste) : Résidual moyen (G3/V2) après renforcement PLC.

5.4 Suivi des Risques

- Revue semestrielle des scénarios.
- Tableau de bord mensuel des alertes SIEM.
- Mise à jour du schéma réseau et de l'inventaire des actifs (Règle 4).
- Contrôles/WI-Fi scanners trimestriels pour garantir la non-activation.