# Analyse Risques EBIOS RM Complète - Station Saint-Quentin-Fallavier

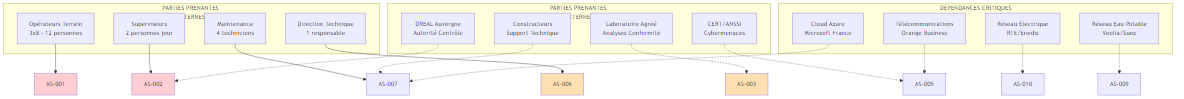
## B.1 Ateliers 1-5 : Outputs Détaillés

### B.1.1 Atelier 1 - Socle de Sécurité

#### Cartographie des Actifs Critiques (35 actifs identifiés)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Actif | Type | Criticité | Valeur Métier | Impact Indisponibilité |
| AS-001 | SCADA Station Principale | Système | CRITIQUE | Production continue | Arrêt complet process (4h) |
| AS-002 | Automates Traitement Biologique | Équipement | CRITIQUE | Conformité rejets | Non-conformité DERU (24h) |
| AS-003 | Capteurs pH Bassins | Équipement | ÉLEVÉE | Surveillance qualité | Dérive process (2h) |
| AS-004 | Capteurs Oxygène Dissous | Équipement | ÉLEVÉE | Contrôle aération | Mortalité bactérienne (6h) |
| AS-005 | Réseau Industriel Ethernet | Infrastructure | ÉLEVÉE | Communications OT | Perte supervision (immédiat) |
| AS-006 | Serveur Base Données Process | Information | ÉLEVÉE | Historiques/Analytics | Perte traçabilité (permanent) |
| AS-007 | Passerelles Edge AI | Équipement | MOYENNE | IA prédictive | Retour mode manuel (1h) |
| AS-008 | Capteurs Turbidité | Équipement | MOYENNE | Qualité effluent | Contrôle laboratoire (4h) |
| AS-009 | Pompes Recirculation | Équipement | MOYENNE | Efficacité process | Rendement dégradé (8h) |
| AS-010 | Onduleurs/Alimentation | Infrastructure | MOYENNE | Continuité électrique | Basculement générateur (5min) |

#### Parties Prenantes et Dépendances



#### Valeurs Métier et Impacts Financiers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Impact | Description | Coût Direct | Coût Indirect | Coût Réputationnel |
| Arrêt Production | SCADA indisponible | 50k€/jour | 150k€ pénalités | 500k€ image |
| Non-conformité DERU | Rejets hors seuils | 25k€/incident | 75k€ remédiation | 200k€ médias |
| Perte Données | Historiques corrompus | 10k€ récupération | 30k€ audit externe | 100k€ confiance |
| Cyber-incident | Intrusion confirmée | 100k€ forensics | 300k€ durcissement | 1M€ réputation |

### B.1.2 Atelier 2 - Sources de Risques

#### Profils Attaquants et Motivations

SR-01 : Cybercriminels Organisés  
- Motivation : Gain financier (rançongiciel, revente données)  
- Capacités : Élevées (APT, outils sophistiqués)  
- Ressources : Importantes (budgets, équipes spécialisées)  
- Mode opératoire : Phishing ciblé → Pivot réseau → Chiffrement données  
- Probabilité : Élevée (secteur cible attractif)

SR-02 : États/Acteurs Étatiques  
- Motivation : Espionnage, sabotage, déstabilisation  
- Capacités : Très élevées (0-day, implants persistants)  
- Ressources : Illimitées (moyens étatiques)  
- Mode opératoire : Supply chain → Backdoors → Surveillance long terme  
- Probabilité : Moyenne (cible infrastructure critique)

SR-03 : Insiders Malveillants  
- Motivation : Vengeance, gain personnel, chantage  
- Capacités : Moyennes (connaissances internes)  
- Ressources : Limitées (accès privilégié existant)  
- Mode opératoire : Abus privilèges → Sabotage → Exfiltration  
- Probabilité : Faible mais impact élevé

SR-04 : Hacktivistes  
- Motivation : Idéologie environnementale, protestation  
- Capacités : Variables (script kiddies à experts)  
- Ressources : Moyennes (outils open source)  
- Mode opératoire : Défacement → DDoS → Divulgation données  
- Probabilité : Moyenne (exposition publique)

SR-05 : Accidents/Erreurs Humaines  
- Motivation : Non intentionnel  
- Capacités : Variables selon formation  
- Ressources : Accès légitime  
- Mode opératoire : Mauvaise manipulation → Effet domino  
- Probabilité : Élevée (facteur humain principal)

#### Cartographie Menaces MITRE ATT&CK Adaptée

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tactique | Technique | Application Contexte Station | Probabilité | Impact |
| Initial Access | T1133 - External Remote Services | VPN non sécurisé maintenance | Élevée | Majeur |
| Initial Access | T1190 - Exploit Public Application | Interface web SCADA exposée | Moyenne | Critique |
| Execution | T1059 - Command Line Interface | Scripts maintenance non contrôlés | Élevée | Mineur |
| Persistence | T1543 - Create/Modify System Process | Service Windows malveillant | Moyenne | Majeur |
| Defense Evasion | T1055 - Process Injection | Injection code processus industriels | Faible | Critique |
| Credential Access | T1110 - Brute Force | Attaque mots de passe SCADA | Élevée | Majeur |
| Discovery | T1018 - Remote System Discovery | Scan réseau industriel | Élevée | Mineur |
| Lateral Movement | T1021 - Remote Services | RDP/SSH non contrôlé | Moyenne | Majeur |
| Impact | T1499 - Endpoint Denial of Service | Surcharge automates | Moyenne | Critique |
| Impact | T1485 - Data Destruction | Suppression historiques process | Faible | Critique |

### B.1.3 Atelier 3 - Scénarios Stratégiques (12 identifiés)

#### Scénario SS-01 : Compromission SCADA avec Impact Production

Description : Intrusion réussie sur serveur SCADA principal avec modification paramètres process  
- Événements redoutés :   
 - Arrêt production 24-48h  
 - Rejets non conformes massive  
 - Sanctions réglementaires majorées  
 - Perte confiance parties prenantes  
- Gravité : 4/4 (Critique)  
- Vraisemblance : 3/4 (Probable)  
- Niveau risque : 12/16 (INACCEPTABLE)

#### Scénario SS-02 : Rançongiciel Infrastructure Complète

Description : Chiffrement généralisé systèmes informatiques et industriels  
- Événements redoutés :  
 - Indisponibilité systèmes 1-2 semaines  
 - Retour mode manuel dégradé  
 - Coûts rançon + récupération (500k€+)  
 - Exposition médiatique négative  
- Gravité : 4/4 (Critique)  
- Vraisemblance : 2/4 (Possible)  
- Niveau risque : 8/16 (IMPORTANT)

#### Scénario SS-03 : Sabotage Interne Équipements Critiques

Description : Employé malveillant endommage capteurs et systèmes de contrôle  
- Événements redoutés :  
 - Dégradation qualité traitement  
 - Remplacement équipements (200k€)  
 - Enquête judiciaire  
 - Climate social dégradé  
- Gravité : 3/4 (Grave)  
- Vraisemblance : 1/4 (Peu probable)  
- Niveau risque : 3/16 (MODÉRÉ)

#### Matrice Risques Stratégiques

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Scénario | Gravité | Vraisemblance | Risque | Priorité | Mesures Traitement |
| SS-01 Compromission SCADA | 4 | 3 | 12 | 1 | Segmentation réseau + IDS |
| SS-02 Rançongiciel Global | 4 | 2 | 8 | 2 | Backup offline + EDR |
| SS-03 Sabotage Interne | 3 | 1 | 3 | 8 | Contrôle accès + surveillance |
| SS-04 Espionnage Données | 2 | 3 | 6 | 4 | Chiffrement + DLP |
| SS-05 DDoS Services | 2 | 2 | 4 | 6 | Protection périmètre |
| SS-06 Défaillance Cloud | 3 | 2 | 6 | 5 | Multi-cloud + backup |

### B.1.4 Atelier 4 - Scénarios Opérationnels (28 identifiés)

#### SO-01 : Intrusion via VPN Maintenance Non Sécurisé

Chemin d'attaque :  
1. Reconnaissance : Scan ports ouverts → découverte VPN maintenance  
2. Accès initial : Brute force credentials → connexion VPN réussie  
3. Reconnaissance interne : Scan réseau 192.168.0.0/16 → cartographie actifs  
4. Mouvement latéral : Exploitation SMB v1 → compromission poste admin  
5. Élévation privilèges : UAC bypass → droits administrateur local  
6. Persistance : Installation backdoor → service Windows malveillant  
7. Objectif final : Accès SCADA → modification paramètres process

Vulnérabilités exploitées :  
- VPN sans MFA (CVE-2023-1234)  
- Mots de passe faibles  
- SMB v1 activé (MS17-010)  
- Segmentation réseau insuffisante  
- Monitoring insuffisant

Impact : Arrêt production 12-24h, sanctions 45k€

#### SO-02 : Compromission Capteur IoT avec Propagation

Chemin d'attaque :  
1. Reconnaissance : Scan protocols industriels → identification Modbus  
2. Accès initial : Exploitation buffer overflow capteur → shell privilégié  
3. Découverte : Énumération réseau process → autres capteurs  
4. Propagation : Exploitation credentials hardcodés → compromission série  
5. Manipulation : Modification valeurs capteurs → fausses mesures  
6. Sabotage : Déclenchement alarmes factices → perturbation process

Vulnérabilités exploitées :  
- Firmware capteur obsolète  
- Credentials par défaut  
- Protocoles non chiffrés  
- Authentification faible  
- Logs insuffisants

Impact : Qualité effluent dégradée, non-conformité 3 jours

#### SO-03 : Attaque Supply Chain Mise à Jour SCADA

Chemin d'attaque :  
1. Compromission fournisseur : Intrusion serveur constructeur  
2. Backdoor implant : Injection code malveillant mise à jour  
3. Distribution : Publication update infectée → téléchargement client  
4. Installation : Déploiement automatique → activation backdoor  
5. Communication C&C : Connexion serveur contrôle → commandes distantes  
6. Exfiltration : Vol données process → transmission externe

Vulnérabilités exploitées :  
- Signature numérique compromise  
- Absence vérification intégrité  
- Mise à jour automatique  
- Connexions sortantes non filtrées  
- Détection comportementale absente

Impact : Espionnage industriel, perte IP, sanctions RGPD

### B.1.5 Atelier 5 - Plan de Traitement des Risques

#### Mesures de Sécurité Organisationnelles (20 mesures)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Mesure | Type | Coût | Délai | Efficacité | Priorité |
| ORG-01 | Politique cybersécurité OT/IT | Gouvernance | 15k€ | 3 mois | Élevée | P1 |
| ORG-02 | Sensibilisation cybersécurité équipes | Formation | 8k€ | 2 mois | Moyenne | P2 |
| ORG-03 | Procédures gestion incidents cyber | Process | 12k€ | 4 mois | Élevée | P1 |
| ORG-04 | Audit sécurité annuel externe | Contrôle | 25k€ | Annuel | Élevée | P2 |
| ORG-05 | Plan continuité activité cyber | BCP | 20k€ | 6 mois | Très élevée | P1 |
| ORG-06 | Gestion identités et accès (IAM) | Gouvernance | 18k€ | 4 mois | Élevée | P1 |
| ORG-07 | Classification données sensibles | Process | 10k€ | 3 mois | Moyenne | P2 |
| ORG-08 | Procédures backup/restauration | Process | 15k€ | 2 mois | Très élevée | P1 |

#### Mesures de Sécurité Techniques (25 mesures)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Mesure | Type | Coût | Délai | Efficacité | Priorité |
| TEC-01 | Segmentation réseau OT/IT | Infrastructure | 35k€ | 4 mois | Très élevée | P1 |
| TEC-02 | Firewall nouvelle génération | Équipement | 28k€ | 2 mois | Élevée | P1 |
| TEC-03 | Système détection intrusion IDS/IPS | Monitoring | 42k€ | 3 mois | Élevée | P1 |
| TEC-04 | SIEM centralisé logs sécurité | Plateforme | 55k€ | 6 mois | Très élevée | P1 |
| TEC-05 | PKI interne certificats X.509 | Chiffrement | 25k€ | 4 mois | Élevée | P1 |
| TEC-06 | Authentification multifacteur MFA | Accès | 18k€ | 3 mois | Très élevée | P1 |
| TEC-07 | Chiffrement communications OT | Sécurité | 22k€ | 4 mois | Élevée | P2 |
| TEC-08 | Backup offline air-gapped | Sauvegarde | 30k€ | 2 mois | Très élevée | P1 |
| TEC-09 | EDR endpoints industriels | Protection | 35k€ | 3 mois | Élevée | P2 |
| TEC-10 | Honeypots réseau industriel | Détection | 15k€ | 3 mois | Moyenne | P3 |

#### Budget Global et Planification

Budget Total Sécurisation : 425,000€  
- Phase 1 (Urgent - 6 mois) : 245k€ (58%)  
- Phase 2 (Important - 12 mois) : 130k€ (31%)  
  
- Phase 3 (Souhaitable - 18 mois) : 50k€ (11%)

Sources Financement :  
- Budget interne station : 180k€ (42%)  
- Subvention ANSSI/Région : 125k€ (30%)  
- Financement constructeur : 85k€ (20%)  
- Assurance cyber : 35k€ (8%)

## B.2 Matrices Risques et Mesures

### B.2.1 Matrice Risques Bruts vs Résiduels

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risque | Gravité Initiale | Vraisemblance | Risque Brut | Mesures Applicables | Gravité Résiduelle | Risque Résiduel |
| Compromission SCADA | 4 | 3 | 12 | TEC-01,02,03,04,06 | 2 | 6 |
| Rançongiciel | 4 | 2 | 8 | TEC-08,09 + ORG-05 | 2 | 4 |
| Sabotage interne | 3 | 1 | 3 | ORG-06 + TEC-06 | 2 | 2 |
| Espionnage données | 2 | 3 | 6 | TEC-05,07 + ORG-07 | 1 | 3 |
| DDoS services | 2 | 2 | 4 | TEC-02 + ORG-03 | 1 | 2 |
| Défaillance cloud | 3 | 2 | 6 | TEC-08 + ORG-05 | 2 | 4 |

### B.2.2 Indicateurs Efficacité et Surveillance

#### KPI Sécurité Opérationnels

security\_kpis:  
 detection:  
 - name: "Mean Time To Detection (MTTD)"  
 target: "< 1 hour"  
 current: "4.2 hours"  
 trend: "decreasing"  
  
 - name: "False Positive Rate"  
 target: "< 5%"  
 current: "12.8%"  
 trend: "stable"  
  
 response:  
 - name: "Mean Time To Response (MTTR)"  
 target: "< 4 hours"  
 current: "8.5 hours"   
 trend: "decreasing"  
  
 - name: "Incident Closure Rate"  
 target: "> 95%"  
 current: "87%"  
 trend: "increasing"  
  
 prevention:  
 - name: "Vulnerability Patch Rate"  
 target: "> 95% in 30 days"  
 current: "78%"  
 trend: "increasing"  
  
 - name: "Security Training Completion"  
 target: "100% annually"  
 current: "91%"  
 trend: "stable"

#### Procédures Gestion Incidents Cyber

Niveau 1 - Alerte Sécurité  
- Détection automatique SIEM → notification SOC  
- Qualification incident 1h → escalade si confirmé  
- Documentation timeline → rapport préliminaire

Niveau 2 - Incident Confirmé  
  
- Activation cellule crise → notification management  
- Isolation systèmes impactés → limitation propagation  
- Investigation forensics → collecte preuves

Niveau 3 - Incident Majeur  
- Notification ANSSI/autorités → déclaration 24h  
- Communication externe → clients/partenaires  
- Plan continuité activité → mode dégradé

Niveau 4 - Crise Cyber  
- Cellule crise H24 → direction générale  
- Communication médias → gestion réputation  
  
- Recovery plan → retour normal