IUT DE LA RÉUNION
BUT Réseaux & Télécommunications

ANALYSE DE RISQUES

Méthode EBIOS

GROUPE NATIONALE+

Stock Fast • Cheesy-Milk • Numéra Support

Réalisé par :

Angélique GRONDIN
Kylian HONORINE

Année Universitaire 2025-2026

Table des matières

1. Introduction

1.1 Contexte

Le Groupe Nationale+ est une entreprise diversifiée opérant dans trois secteurs d'activité distincts : le stockage de données (Stock Fast), l'agroalimentaire (Cheesy-Milk), et les services informatiques (Numéra Support). Fondé en 1950 avec Stock Fast, le groupe s'est progressivement développé sous la direction d'Olivier Mortin, qui a diversifié les activités en rachetant Cheesy-Milk en 2001 et en créant Numéra Support en 2015.

Cette analyse de risque, menée selon la méthodologie EBIOS Risk Manager, vise à identifier et évaluer les risques cybersécurité auxquels le groupe est confronté. L'objectif est de proposer un plan de traitement des risques adapté aux enjeux métiers et à la criticité des systèmes d'information.

1.2 Périmètre de l'analyse

L'analyse couvre l'ensemble du groupe Nationale+ et ses trois entités :

- Stock Fast : Entreprise de stockage de données avec la solution StockaMax (800 employés)
- Cheesy-Milk : Entreprise agroalimentaire spécialisée dans la production de fromage en Asie du Sud-Est
- Numéra Support : Entreprise de gestion des systèmes d'information du groupe

L'analyse intègre également l'écosystème complet de partenaires et prestataires externes, qui constituent à la fois des actifs critiques pour le fonctionnement du groupe et des vecteurs potentiels de compromission (attaques par la chaîne d'approvisionnement) :

Partenaire	Type / Rôle	Accès au SI	Criticité / Risque
STOCK+	Hébergeur BDD	Accès physique serveurs SRVBDD01-02PRD	CRITIQUE - Refuse audits sécurité
SUPPORT WORD	Support N1	Accès comptes utilisateurs clients	ÉLEVÉ - Controverses éthiques
HelpDEV	Développement	Accès Azure DevOps, code source	MODÉRÉ - 30% équipe dev externe
FunMoney	Comptabilité	Accès données financières/comptables	MODÉRÉ - Société récente 2021
TOP_PUB	Publicité	FTP dépôt fichiers MP4	ÉLEVÉ - Historique piratage
WorkplaceCloud	Infogérance cloud	Administration serveurs Azure	CRITIQUE - Accès admin cloud
WEB Support	Hébergement web	Gestion SRVWEB01-03PRD	ÉLEVÉ - Accès serveurs web

P2P	Éditeur ERP/MES	Mises à jour logiciels production	CRITIQUE - Code systèmes industriels
SALES-I	Éditeur Sales4All	Mises à jour application ventes	MODÉRÉ - Audits sécurité OK
FormAll	Formation e-learning	SSO Active Directory (SAML 2.0)	MODÉRÉ - Intégration AD sensible

1.3 Méthodologie EBIOS Risk Manager

EBIOS Risk Manager est une méthode d'analyse de risque développée par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Elle se décompose en 5 ateliers complémentaires qui permettent une évaluation progressive et approfondie des risques :

1. **Atelier 1 :** Cadrage et socle de sécurité - Identification des valeurs métiers et événements redoutés
2. **Atelier 2 :** Sources de risque - Identification des acteurs malveillants et leurs objectifs
3. **Atelier 3 :** Scénarios stratégiques - Chemins d'attaque de haut niveau
4. **Atelier 4 :** Scénarios opérationnels - Modes opératoires techniques détaillés
5. **Atelier 5 :** Traitement du risque - Mesures de sécurité et plan d'action

2. Atelier 1 : Cadrage et socle de sécurité

2.1 Objectifs de l'atelier

L'atelier 1 vise à définir le périmètre de l'étude, identifier les valeurs métiers essentielles de l'organisation et déterminer les événements redoutés qui pourraient impacter ces valeurs. Cette étape fondamentale permet d'établir le cadre de référence pour l'ensemble de l'analyse.

2.2 Valeurs métiers

Les valeurs métiers représentent les éléments essentiels qui contribuent aux missions et objectifs de l'organisation. Pour le Groupe Nationale+, nous avons identifié les valeurs métiers suivantes :

Valeur métier	Description	Entité concernée
Disponibilité des services	Continuité d'accès à la solution StockaMax pour les clients et aux systèmes de production pour Cheesy-Milk	Stock Fast, Cheesy-Milk
Confidentialité des données	Protection des données clients, des informations RH, financières et propriété intellectuelle (recettes)	Toutes les entités
Intégrité des données	Garantie de l'exactitude et de la fiabilité des données stockées et des processus de production	Stock Fast, Cheesy-Milk
Réputation de l'entreprise	Image de marque du groupe, notamment face aux controverses (SUPPORT WORD)	Toutes les entités
Conformité réglementaire	Respect du RGPD pour les données personnelles et des normes agroalimentaires (traçabilité 10 ans)	Toutes les entités
Continuité de production	Maintien du flux tendu de production agroalimentaire	Cheesy-Milk

2.3 Biens supports

Les biens supports sont les éléments techniques et organisationnels qui portent les valeurs métiers :

Type de bien	Exemples	Criticité
Infrastructure réseau	• Datacenter France, Allemagne, Alibaba • Firewalls (Fortinet, Stormshield, pfSense) • Switches (Cisco, Huawei)	Critique
Serveurs applicatifs	• SRVWEB01-03PRD (StockaMax) • SRVBDD01-02PRD (bases de données) • Serveurs MES, ERP (Cheesy-Milk)	Critique
Applications métiers	• StockaMax (stockage cloud) • M-MES (gestion production) • PeopleManage, PeoplePay (RH)	Élevée
Données	• Données clients StockaMax • Données RH et financières • Recettes et formules (R&D)	Critique
Active Directory	• Forêt NATIONALP.Local • Forêt StockFast.NationalP.local • Forêt Cheesy.local	Critique
Solutions SaaS	• PeopleFind, PeoplePay (RH) • Azure DevOps (développement) • TrendMe, SoC NETW (marketing)	Modérée

2.4 Événements redoutés

Les événements redoutés sont les scénarios que l'organisation souhaite éviter. Ils sont évalués selon leur gravité potentielle sur les valeurs métiers :

ID	Événement redouté	Valeur métier impactée	Impact	Gravité
ER1	Indisponibilité prolongée de la solution StockaMax	Disponibilité des services	• Perte de clients • Perte financière • Image dégradée	4/4
ER2	Fuite de données clients (fichiers stockés)	Confidentialité, Conformité RGPD	• Sanctions RGPD • Perte de confiance • Poursuites judiciaires	4/4
ER3	Corruption des données de production (Cheesy-Milk)	Intégrité des données, Continuité production	• Arrêt de production • Défauts qualité • Perte traçabilité	4/4
ER4	Vol de propriété intellectuelle (recettes Cheesy-Milk)	Confidentialité	• Avantage concurrentiel perdu • Perte de parts de marché	3/4
ER5	Compromission des données RH et financières	Confidentialité, Conformité	• Sanctions RGPD • Chantage • Atteinte réputation	4/4
ER6	Attaque par ransomware sur le SI	Disponibilité, Intégrité	• Arrêt activité • Perte de données • Coûts de récupération	4/4
ER7	Manipulation des systèmes de contrôle qualité	Intégrité, Conformité	• Produits défectueux • Risques sanitaires • Rappels produits	4/4
ER8	Défiguration du site web / atteinte à l'image	Réputation	• Perte de confiance • Impact médiatique négatif	3/4

ER9	Espionnage industriel via partenaires compromis	Confidentialité	• Fuite stratégie • Désavantage compétitif	3/4
ER10	Sabotage des équipements de production	Continuité production, Intégrité	• Arrêt production • Coûts de réparation • Retards livraison	3/4

Les événements redoutés représentent les scénarios de sécurité que l'organisation cherche absolument à éviter en raison de leur impact potentiellement catastrophique sur une ou plusieurs valeurs métiers. Chaque événement redouté est évalué selon une échelle de gravité de 1 à 4 définie précédemment, permettant de prioriser les efforts de sécurisation.

Pour le Groupe Nationale+, l'analyse a permis d'identifier 10 événements redoutés majeurs dont 7 sont classés en gravité maximale (4/4), témoignant de la forte exposition aux risques cyber et de la criticité des actifs à protéger.

2.5 Échelle de gravité

Niveau	Description
1 - Négligeable	Impact limité, récupération rapide, pas d'impact financier significatif
2 - Limitée	Impact modéré, récupération en quelques jours, impact financier limité (<100k€)
3 - Importante	Impact significatif, récupération en semaines, impact financier notable (100k-1M€)
4 - Critique	Impact majeur, récupération longue, menace existentielle, impact financier >1M€

3. Atelier 2 : Sources de risque

3.1 Objectifs de l'atelier

L'atelier 2 vise à identifier les sources de risque potentielles, c'est-à-dire les acteurs malveillants susceptibles de chercher à nuire à l'organisation. Il s'agit de caractériser ces acteurs selon leurs motivations, leurs ressources et leurs objectifs stratégiques.

3.2 Cartographie des sources de risque

Nous avons identifié les principales sources de risque suivantes :

Source de risque	Motivation	Ressources	Objectifs
Cybercriminels opportunistes	Gain financier rapide	• Compétences moyennes • Outils automatisés • Budget limité	• Ransomware • Vol de données • Cryptominage
Groupes APT (Advanced Persistent Threat)	Espionnage, sabotage	• Compétences élevées • Ressources importantes • Temps illimité	• Vol de propriété intellectuelle • Sabotage long terme • Maintien d'accès
Concurrents	Avantage compétitif	• Budget moyen à élevé • Prestataires spécialisés • Connaissance métier	• Vol de recettes (Cheesy-Milk) • Vol de données clients • Sabotage réputation
Employés malveillants / mécontents	Vengeance, gain	• Accès légitime • Connaissance interne • Compétences variables	• Vol de données • Sabotage • Revente d'informations
Hacktivistes	Idéologie (anti-SUPPORT WORD)	• Compétences moyennes • Coordination groupe • Visibilité médiatique	• Défiguration site • DDoS • Fuite de documents
Partenaires compromis	Vecteur d'attaque involontaire	• Accès privilégié • Confiance établie • Maturité variable	• Supply chain attack • Accès au SI • Pivot interne
États-nations	Géopolitique, espionnage industriel	• Ressources illimitées	• Espionnage longue durée

		• Compétences maximales • o-days	• Sabotage infrastructures critiques

3.3 Analyse des objectifs visés

Pour chaque source de risque, nous avons identifié les objectifs stratégiques (OV) qu'elle pourrait chercher à atteindre :

ID	Objectif visé	Sources de risque concernées	Criticité
OV1	Compromettre les infrastructures cloud (Alibaba, Azure)	APT, États-nations, Cybercriminels	Élevée
OV2	Exfiltrer les données clients de StockaMax	Cybercriminels, APT, Concurrents	Critique
OV3	Voler les recettes et formules de Cheesy-Milk	Concurrents, APT, Employés malveillants	Élevée
OV4	Déployer un ransomware sur le SI	Cybercriminels, Hacktivistes	Critique
OV5	Compromettre la chaîne d'approvisionnement via les partenaires	APT, États-nations	Élevée
OV6	Saboter la production de Cheesy-Milk	Concurrents, Employés malveillants, Hacktivistes	Élevée
OV7	Nuire à la réputation du groupe (controverse SUPPORT WORD)	Hacktivistes, Concurrents	Modérée
OV8	Établir une persistance long terme dans le SI	APT, États-nations	Critique
OV9	Compromettre les systèmes RH et financiers	Cybercriminels, Employés malveillants	Élevée
OV10	Manipuler les contrôles qualité de production	Concurrents, États-nations, Employés malveillants	Critique

3.4 Matrice sources de risque x objectifs visés

Cette matrice croise les sources de risque avec les objectifs visés pour identifier les couples SR/OV les plus critiques :

Source de risque / OV	OV1	OV2	OV3	OV4	OV5	OV8	OV10
Cybercriminels	●	●●	-	●●	-	-	-
Groupes APT	●●	●●	●●	-	●●	●●	●●
Concurrents	-	●	●●	-	-	-	●
Employés malveillants	-	●	●	-	-	-	●
Hacktivistes	-	●	-	●	-	-	-
États-nations	●●	●●	●	-	●●	●●	●●

Légende : - = Non pertinent | ● = Probabilité modérée | ●● = Probabilité élevée

4. Atelier 3 : Scénarios stratégiques

4.1 Objectifs de l'atelier

L'atelier 3 vise à construire des scénarios stratégiques de haut niveau qui décrivent comment les sources de risque pourraient atteindre leurs objectifs. Ces scénarios tiennent compte de l'écosystème de l'organisation et identifient les chemins d'attaque potentiels.

4.2 Cartographie de l'écosystème

L'écosystème du Groupe Nationale+ comprend de nombreux partenaires et prestataires qui constituent des points d'entrée potentiels :

Partie prenante	Type	Niveau d'accès au SI	Niveau de confiance
STOCK+ (hébergement BDD)	Partenaire critique	Accès physique aux serveurs BDD	Élevé (lien personnel)
SUPPORT WORD (support N1)	Prestataire	Accès utilisateurs clients	Faible (controverses)
HelpDEV (développement)	Prestataire	Accès Azure DevOps, code source	Modéré
FunMoney (compta/finance)	Prestataire	Accès données financières	Modéré (jeune société)
TOP_PUB (publicité)	Partenaire	FTP, dépose fichiers MP4	Faible (historique piratage)
WorkplaceCloud (infogérance Azure)	Prestataire cloud	Administration serveurs cloud	Élevé
WEB Support (hébergement web)	Prestataire	Gestion SRVWEB01-03PRD	Élevé
P2P (éditeur ERP/MES)	Éditeur	Mise à jour logiciels critiques	Modéré
SALES-I (éditeur Sales4All)	Éditeur	Mise à jour application ventes	Élevé (audits sécurité)
FormAll (plateforme formation)	Éditeur / Hébergeur	SSO AD, connexion internet	Modéré

4.3 Scénarios stratégiques prioritaires

Nous avons identifié les scénarios stratégiques les plus critiques :

ID	Scénario	Chemin d'attaque	Vraisemblance	Gravité
SS1	Compromission via STOCK+	• Attaque de STOCK+ (faible maturité sécurité) • Accès aux SRVBDD01-02PRD • Exfiltration données clients	Élevée	Critique (ER2)
SS2	Supply chain via TOP_PUB	• Compromission de TOP_PUB (historique piratage) • Injection de malware dans fichiers MP4 • Exécution sur SI via FTP	Modérée	Élevée (ER6)
SS3	Attaque via SUPPORT WORD	• Employé SUPPORT WORD malveillant • Accès aux comptes clients/utilisateurs • Pivot vers données sensibles	Modérée	Élevée (ER2, ER5)
SS4	Ransomware via HelpDEV	• Compromission prestataire HelpDEV • Injection code malveillant dans DevOps • Déploiement ransomware via pipeline CI/CD	Faible	Critique (ER6)
SS5	Vol de propriété intellectuelle (Cheesy-Milk)	• Employé R&D malveillant ou concurrence • Accès aux partages réseau R&D • Exfiltration des recettes	Modérée	Élevée (ER4)
SS6	Sabotage production via M-MES	• Compromission système MES (base 1C) • Manipulation paramètres production • Arrêt chaîne ou défauts qualité	Faible	Critique (ER3, ER7)
SS7	APT via FormAll (SSO AD)	• Compromission plateforme FormAll	Modérée	Critique (ER6)

		• Exploitation SSO via compte de service • Mouvement latéral dans l'AD		
SS8	Exfiltration via FunMoney	• Compromission FunMoney (société récente) • Accès aux données financières/comptables • Chantage ou revente de données	Modérée	Élevée (ER5)
SS9	Compromission infrastructure cloud	• Attaque ciblée Alibaba/Azure • Accès aux VM StockaMax • Ransomware ou exfiltration massive	Très faible	Critique (ER1, ER2)
SS10	Hacktivisme anti-SUPPORT WORD	• Activistes exploitant la controverse • Attaque DDoS ou défacement • Publication de documents internes	Modérée	Modérée (ER8)

4.4 Matrice de criticité des scénarios

Cette matrice positionne les scénarios selon leur vraisemblance et leur gravité :

Gravité / Vraisemblance	Très faible	Faible	Modérée	Élevée	Très élevée
Critique	SS9	SS4, SS6	SS3, SS7, SS8	SS1	-
Élevée	-	-	SS2, SS5, SS8, SS10	-	-
Modérée	-	-	-	-	-
Faible	-	-	-	-	-

Légende : Rouge = Risque critique prioritaire | Orange = Risque élevé | Vert = Risque acceptable

5. Atelier 4 : Scénarios opérationnels

5.1 Objectifs de l'atelier

L'atelier 4 détaille les scénarios stratégiques en modes opératoires techniques concrets. Il identifie les chemins d'attaque spécifiques, les techniques utilisées (référence MITRE ATT&CK), et évalue la vraisemblance de réussite en fonction des mesures de sécurité existantes.

5.2 Scénarios opérationnels détaillés

Nous présentons ci-dessous les scénarios opérationnels des 5 scénarios stratégiques les plus critiques :

5.2.1 SO1 : Exfiltration de données via STOCK+ (basé sur SS1)

Phase	Description technique
1. Reconnaissance	• Scan passif du réseau STOCK+ (T1595) • Identification des versions logicielles des SRVBDD • Recherche d'employés sur LinkedIn (OSINT)
2. Accès initial	• Phishing ciblé sur employé STOCK+ (T1566.001) • Exploitation d'une vulnérabilité web (CVE non patchée) • Bruteforce SSH/RDP si exposé (T1110)
3. Élévation de privilèges	• Exploitation de misconfiguration sudo (T1068) • Récupération de credentials en clair dans fichiers config • Accès root sur serveur BDD
4. Persistance	• Création d'un compte backdoor (T1136) • Modification de clés SSH autorisées • Installation d'un webshell
5. Collecte de données	• Dump de la base de données clients (T1005) • Compression et chiffrement des données • Staging des données pour exfiltration
6. Exfiltration	• Transfert via protocole chiffré (HTTPS) vers C2 (T1041) • Fragmentation pour éviter la détection • Suppression des traces (logs)
Mesures existantes	Aucun audit de sécurité accepté par STOCK+, niveau de sécurité inconnu, relation de confiance basée sur lien personnel
Vraisemblance de réussite	ÉLEVÉE - Absence de contrôles de sécurité vérifiés chez STOCK+

5.2.2 SO2 : Ransomware via supply chain TOP_PUB (basé sur SS2)

Phase	Description technique
1. Compromission de TOP_PUB	• Exploitation de l'historique de piratage (sécurité faible) • Accès aux systèmes de production de fichiers MP4 • Injection de payload dans encodeur vidéo
2. Injection de malware	• Ajout de code malveillant dans métadonnées MP4 • Exploitation de vulnérabilité codec vidéo (ex: CVE-2020-1560) • Payload déclenchant l'exécution au décodage
3. Livraison via FTP	• Dépôt du fichier MP4 infecté sur FTP Stock Fast • Attente du téléchargement par le service marketing • Possible exploitation de vulnérabilité FTP (traversal)
4. Exécution initiale	• Ouverture du fichier par un employé (T1204.002) • Exploitation automatique lors de l'aperçu vidéo • Déploiement du dropper de ransomware
5. Mouvement latéral	• Exploitation de SMB pour propagation réseau (T1021.002) • Utilisation de credentials en cache (T1003) • Compromission du domaine Active Directory
6. Impact	• Chiffrement des fichiers sur serveurs et postes (T1486) • Destruction des sauvegardes Veeam si accessibles • Affichage de la demande de rançon
Mesures existantes	FTP avec contrôle d'accès, mais pas de sandbox pour analyse de fichiers, pas d'EDR mentionné
Vraisemblance de réussite	MODÉRÉE - Nécessite compromission TOP_PUB ET exécution fichier

5.2.3 SO3 : Pivot interne via SUPPORT WORD (basé sur SS3)

Phase	Description technique
1. Menace interne	• Employé SUPPORT WORD malveillant ou recruté • Accès légitime aux comptes clients/utilisateurs • Exploitation de la controverse pour motivation
2. Accès aux systèmes	• Utilisation de credentials clients légitimes • Accès à PeopleManage, PeoplePay via SSO • Récupération de tokens d'authentification
3. Escalade de privilèges	• Exploitation d'une misconfiguration RBAC • Social engineering pour obtenir accès admin • Exploitation de vulnérabilité dans PeopleManage (on-prem)
4. Collecte de données sensibles	• Extraction données RH (salaires, informations personnelles) • Accès aux données financières via lien PeoplePay-PeopleManage • Collecte de documents confidentiels
5. Exfiltration discrète	• Exfiltration progressive via connexion légitime • Utilisation de services cloud personnels • Mélange avec trafic normal de support
6. Couverture des traces	• Suppression de logs d'accès suspects • Utilisation de comptes clients différents • Maintien d'une activité légitime en parallèle
Mesures existantes	Logs d'accès, mais contrôle limité sur les prestataires externes, pas de DLP mentionné
Vraisemblance de réussite	MODÉRÉE - Accès légitime mais nécessite insider malveillant

5.2.4 SO7 : APT via FormAll et SSO AD (basé sur SS7)

Phase	Description technique
1. Compromission FormAll	• Exploitation d'une 0-day dans plateforme FormAll • Attaque de la chaîne d'approvisionnement de l'éditeur • Injection de backdoor lors d'une mise à jour
2. Exploitation du SSO	• Récupération du compte de service SSO (délégation Kerberos) • Extraction du keytab ou password du compte • Forge de tickets Kerberos (Golden/Silver ticket)
3. Accès à l'Active Directory	• Authentification légitime via tickets forgés • Énumération de l'AD (utilisateurs, groupes, GPO) • Identification des comptes à privilèges
4. Élévation de privilèges AD	• Pass-the-Hash/Pass-the-Ticket (T1550) • Exploitation de misconfiguration GPO • DCSync pour récupérer tous les hash (T1003.006)
5. Persistance avancée	• Création de comptes admin cachés • Injection dans LSASS (T1055) • Skeleton Key ou modification de krbtgt
6. Mouvement latéral	• Compromission des 3 forêts AD (NATIONALP, StockFast, Cheesy) • Exploitation des relations de fédération • Accès à tous les systèmes du groupe
Mesures existantes	Fédération AD configurée, mais pas de segmentation forte, pas de monitoring avancé AD mentionné
Vraisemblance de réussite	MODÉRÉE - Complexe mais impact critique si réussi

5.2.5 SO6 : Sabotage production via M-MES (basé sur SS6)

Phase	Description technique
1. Reconnaissance OT	• Identification de la plateforme M-MES (1C) • Scan du réseau industriel (MODBUS, PROFINET) • Cartographie des équipements Siemens
2. Accès initial IT/OT	• Compromission d'un poste ingénieur (spear-phishing) • Exploitation de pont IT/OT mal sécurisé • Utilisation de credentials volés
3. Pivot vers M-MES	• Mouvement latéral vers VLAN Usine • Exploitation de vulnérabilités 1C connues • Accès aux serveurs M-MES
4. Manipulation subtile	• Modification discrète des paramètres de fermentation • Altération des temps de cuisson • Injection de défauts qualité progressifs
5. Manipulation des tests qualité	• Accès à BroadValidator (tests qualité) • Falsification des résultats de tests • Validation de produits défectueux
6. Impact production	• Produits défectueux sur le marché • Risque sanitaire potentiel • Rappel produit massif et perte de réputation
Mesures existantes	Segmentation réseau (PFsense), mais convergence IT/OT, pas de monitoring ICS spécifique
Vraisemblance de réussite	FAIBLE À MODÉRÉE - Nécessite expertise OT et accès persistant

5.3 Synthèse des vulnérabilités identifiées

Catégorie	Vulnérabilités identifiées	Impact	Priorité
Tiers de confiance	• STOCK+ refuse les audits de sécurité • TOP_PUB historique de piratage • FunMoney société récente (2021)	Critique	P1
Segmentation réseau	• Convergence IT/OT insuffisante • Fédération AD entre toutes les forêts • Accès FTP externe	Élevée	P1
Authentification	• SSO via compte de service (FormAll) • Pas de MFA généralisée • PeopleManage sans SSO (auth locale)	Élevée	P2
Monitoring & détection	• Absence de SIEM/SOC mentionné • Pas d'EDR sur endpoints • Pas de monitoring ICS/OT	Critique	P1
Gestion des données	• Pas de DLP mentionné • Pas de sandbox pour analyse fichiers • Sauvegarde accessible depuis production	Élevée	P2
Prestataires	• SUPPORT WORD (controverses éthiques) • 30% de prestataires dev externes • Support délocalisé Inde/Mexique	Modérée	P3

6. Atelier 5 : Traitement du risque

6.1 Objectifs de l'atelier

L'atelier 5 définit les mesures de sécurité à mettre en œuvre pour traiter les risques identifiés. Il propose un plan d'action priorisé selon l'urgence et l'impact des mesures.

6.2 Stratégies de traitement

Pour chaque risque critique identifié, nous proposons une stratégie de traitement :

Risque	Stratégie	Justification	Actions
SS1 - STOCK+	RÉDUIRE + TRANSFÉRER	• Critique pour business • Partenaire de confiance	• Audit imposé • Assurance cyber • Redondance
SS2 - TOP_PUB	RÉDUIRE + ÉVITER	• Partenaire remplaçable • Historique négatif	• Sandbox fichiers • Changer de fournisseur
SS3 - SUPPORT WORD	RÉDUIRE + ACCEPTER partiellement	• Coût changement élevé • Controverses connues	• PAM, monitoring renforcé • Alternative long terme
SS7 - FormAll SSO	RÉDUIRE	• Architecture nécessaire • Risque maîtrisable	• Segmentation AD • Monitoring Kerberos
SS6 - Production OT	RÉDUIRE	• Actif critique • Risque spécifique	• Segmentation IT/OT • IDS industriel

6.3 Plan d'action détaillé

Nous proposons le plan d'action suivant, organisé par priorité :

6.3.1 Priorité 1 (P1) - Mise en œuvre immédiate (0-3 mois)

ID	Mesure	Description	Risques traités	Coût estimé	Délai
M1	Déploiement SIEM/SOC	• Centralisation des logs • Corrélation d'événements • Détection des IoC • SOC 24/7 (interne ou externalisé)	Tous les scénarios	150k-300k€ + 200k€/an	3 mois
M2	Audit de sécurité STOCK+	• Audit externe imposé contractuellement • Remédiation des vulnérabilités critiques • Pentest annuel obligatoire	SS1	30k€ audit + remédiations	1 mois
M3	Déploiement EDR	• EDR sur tous les endpoints (serveurs + postes) • Détection comportementale • Réponse automatisée aux menaces	SS2, SS4, SS7	100k€ + 50k€/an	2 mois
M4	Segmentation réseau renforcée	• Micro-segmentation des environnements critiques • Isolation IT/OT stricte • Firewall nouvelle génération	SS6, SS7	80k€ équipements + config	3 mois
M5	MFA généralisée	• MFA sur tous les accès à distance • MFA sur comptes administrateurs • MFA sur applications critiques (PeoplePay, Azure, etc.)	SS3, SS7	30k€ + 15k€/an	2 mois
M6	Backup isolé (air gap)	• Sauvegarde offline des données critiques • Stockage hors site sécurisé	SS2 (ransomware)	50k€ + 20k€/an	2 mois

		• Tests de restauration trimestriels			

6.3.2 Priorité 2 (P2) - Mise en œuvre à court terme (3-6 mois)

ID	Mesure	Description	Risques traités	Coût estimé	Délai
M7	Solution DLP	• Prévention de fuite de données • Monitoring des transferts sensibles • Chiffrement des données en mouvement	SS1, SS3, SS5	80k€ + 40k€/an	4 mois
M8	Sandbox fichiers	• Analyse automatisée des fichiers • Détection malware avant exécution • Intégration au FTP TOP_PUB	SS2	40k€ + 15k€/an	3 mois
M9	PAM (Privileged Access Management)	• Gestion centralisée des comptes à privilèges • Enregistrement des sessions admin • Rotation automatique des mots de passe	SS3, SS7	100k€ + 30k€/an	5 mois
M10	Durcissement Active Directory	• Tiering model (Tier 0, 1, 2) • Désactivation protocoles faibles (NTLMv1, SMBv1) • Monitoring des événements Kerberos	SS7	50k€ (conseil + mise en œuvre)	6 mois
M11	IDS/IPS industriel (OT)	• Monitoring des protocoles industriels • Détection d'anomalies sur production • Alertes en temps réel	SS6	60k€ + 20k€/an	5 mois
M12	Sensibilisation cybersécurité	• Formation continue des employés • Campagnes de phishing simulé • Procédures de réponse aux incidents	Tous (facteur humain)	20k€/an	6 mois

6.3.3 Priorité 3 (P3) - Mise en œuvre à moyen terme (6-12 mois)

ID	Mesure	Description	Risques traités	Coût estimé	Délai
M13	Réduction dépendance SUPPORT WORD	• Analyse des alternatives • Migration progressive • Diversification des prestataires support	SS3, ER8 (réputation)	Variable selon solution	12 mois
M14	Changement partenaire TOP_PUB	• Sélection nouveau partenaire publicité • Critères de sécurité dans appel d'offres • Due diligence de sécurité	SS2	Coût de migration	9 mois
M15	Programme bug bounty	• Découverte proactive de vulnérabilités • Plateforme publique (HackerOne, YesWeHack) • Récompenses pour chercheurs	Tous	30k€/an budget primes	6 mois
M16	Chiffrement de bout en bout	• Chiffrement des données au repos (BDD) • HSM pour clés sensibles • Gestion centralisée des clés	SS1, SS2, SS5	120k€ + 30k€/an	12 mois
M17	Red Team / Purple Team	• Exercices d'attaque simulée • Tests de réponse aux incidents • Amélioration continue de la détection	Validation des mesures	80k€/exercice (annuel)	12 mois

6.4 Tableau de bord des indicateurs (KPI)

Pour suivre l'efficacité des mesures déployées, nous proposons les indicateurs suivants :

Indicateur	Objectif	Fréquence	Responsable
Nombre d'incidents de sécurité détectés	>80% détectés en <24h	Mensuel	SOC
Temps moyen de réponse aux incidents (MTTR)	<4 heures	Mensuel	SOC / CSIRT
Taux de succès phishing simulé	<5% de clics	Trimestriel	RH / RSSI
Couverture EDR	100% des assets critiques	Mensuel	IT Ops
Taux de patching critique	<30 jours pour CVE critiques	Mensuel	IT Ops
Tests de restauration backup	100% de succès	Trimestriel	IT Storage
Audits de sécurité partenaires	100% partenaires critiques audités/an	Annuel	RSSI
Conformité durcissement AD	>95% recommandations appliquées	Trimestriel	IT Server
Alertes OT/ICS	0 incident production non détecté	Continu	SOC / Production
Exercices de réponse aux incidents	2 exercices/an minimum	Semestriel	RSSI / CSIRT

6.5 Risques résiduels

Malgré la mise en œuvre de toutes les mesures proposées, certains risques résiduels persisteront :

Risque résiduel	Justification	Niveau résiduel	Acceptation
APT État-nation	Ressources quasi-illimitées, 0-days, persistance avancée difficile à détecter	Modéré	À valider COMEX
Menace interne (insider)	Accès légitime difficile à restreindre totalement, confiance nécessaire	Modéré	Accepté avec monitoring
Vulnérabilité 0-day	Par définition inconnue et non patchable avant découverte	Faible	Accepté
Dépendance cloud providers	Risque de compromission Azure/Alibaba (hors contrôle)	Faible	Accepté (transféré)
Social engineering avancé	Sophistication croissante des attaques, facteur humain imprévisible	Modéré	Accepté avec formation continue

6.6 ROI Théorique estimé

Catégorie	Coût initial	Coût récurrent annuel	Coût total sur 3 ans
Priorité 1 (P1)	440 k€	285 k€/an	1 295 k€
Priorité 2 (P2)	350 k€	125 k€/an	725 k€
Priorité 3 (P3)	Variable	140 k€/an	420 k€ + variable
TOTAL	**~800 k€**	**~550 k€/an**	**~2 450 k€**

ROI estimé : Un seul incident de ransomware avec perte de données clients pourrait coûter : amendes RGPD (jusqu'à 4% du CA mondial), coûts de récupération (500k€-2M€), perte de chiffre d'affaires (indisponibilité), et dommages réputationnels irréversibles. L'investissement proposé se rentabilise dès l'évitement d'un incident majeur.

7. Conclusion

7.1 Synthèse de l'analyse

Cette analyse EBIOS a permis d'identifier et d'évaluer les principaux risques de cybersécurité auxquels le Groupe Nationale+ est exposé. Les points clés sont les suivants :

- 10 événements redoutés critiques identifiés, dont 7 de gravité maximale (4/4)
- 7 sources de risque principales, des cybercriminels opportunistes aux groupes APT sophistiqués
- 10 scénarios stratégiques analysés, dont 5 considérés comme critiques
- 5 scénarios opérationnels détaillés avec chemins d'attaque techniques (référence MITRE ATT&CK)
- 17 mesures de sécurité proposées, réparties en 3 priorités avec un budget total de ~2,5M€ sur 3 ans

7.2 Points de vigilance majeurs

L'analyse a révélé plusieurs points de vigilance nécessitant une attention immédiate :

6. **Dépendance critique à STOCK+ :** Le refus d'audit de sécurité et le lien personnel créent un risque majeur pour les données clients
7. **Absence de visibilité :** Pas de SIEM/SOC ni d'EDR déployés, empêchant la détection précoce des menaces
8. **Écosystème à risque :** Plusieurs partenaires présentent des faiblesses (TOP_PUB, FunMoney) ou controverses (SUPPORT WORD)
9. **Convergence IT/OT :** Segmentation insuffisante entre systèmes de gestion et production industrielle chez Cheesy-Milk
10. **Risques réputationnels :** Association avec SUPPORT WORD expose à des campagnes activistes ciblées

7.3 Points potentiels d'amélioration

Pour améliorer durablement la posture de sécurité du groupe, nous recommandons :

- **Nommer un RSSI groupe :** Centraliser la gouvernance sécurité et coordonner les efforts entre les 3 entités
- **Créer un CSIRT :** Équipe dédiée à la réponse aux incidents avec procédures et exercices réguliers
- **Mettre en place une politique de gestion des tiers :** Due diligence sécurité obligatoire, audits réguliers, clauses contractuelles renforcées
- **Adopter un framework de sécurité :** NIST CSF ou ISO 27001 pour structurer et mesurer les efforts de sécurité