Procédures de gestion des vulnérabilités et des correctifs

Neo Financia

RÉFÉRENCE	PROC-VULN-2025-V1.0
CLASSIFICATION	INTERNE
VERSION	1.0
DATE D'APPROBATION	À définir
APPROBATION	Direction Sécurité & COMEX
PROPRIÉTAIRE	RSSI
PÉRIODICITÉ DE RÉVISION	Annuelle

Table des matières

1. Introduction et objectifs

1.1 Contexte

En tant que néobanque opérant exclusivement via des canaux digitaux, Neo Financia dépend entièrement de la fiabilité et de la sécurité de ses systèmes d'information. La gestion efficace des vulnérabilités et le déploiement des correctifs constituent des éléments fondamentaux de notre stratégie de cybersécurité et de notre engagement à protéger les données sensibles de nos 2 millions de clients.

Notre modèle d'activité, basé sur une architecture multi-cloud (Azure 70%, OVHcloud 20%, AWS 10%) et incluant la prise en charge du BYOD et du télétravail, exige une approche structurée et rigoureuse pour identifier, évaluer et remédier aux vulnérabilités techniques sur l'ensemble de notre périmètre.

1.2 Objectifs des procédures

Ces procédures visent à :

- Établir un cadre méthodologique pour la gestion systématique des vulnérabilités
- Définir les rôles et responsabilités dans le processus de gestion des vulnérabilités

- Garantir l'identification proactive des failles de sécurité
- Assurer une évaluation cohérente et une priorisation efficace des vulnérabilités
- Définir les délais de remédiation en fonction de la criticité
- Formaliser les processus de déploiement des correctifs
- Garantir la traçabilité et le suivi des actions de remédiation
- Assurer la conformité aux exigences réglementaires (DORA, NIS2, RGPD)

1.3 Portée et applicabilité

Ces procédures s'appliquent à :

- L'ensemble des infrastructures techniques de Neo Financia (sur site et cloud)
- Tous les systèmes d'exploitation, middlewares et applications
- Les bases de données et systèmes de stockage
- Les équipements réseau et de sécurité
- Les terminaux professionnels et personnels utilisés dans le cadre du BYOD
- Les environnements de développement, test, préproduction et production
- Les services fournis par des tiers et intégrés à notre SI

1.4 Principes directeurs

La gestion des vulnérabilités chez Neo Financia repose sur les principes suivants :

- **Approche proactive** : Identification et traitement des vulnérabilités avant qu'elles ne soient exploitées
- **Défense en profondeur** : Application de multiples contrôles complémentaires
- **Évaluation basée sur les risques** : Priorisation selon l'impact potentiel sur l'activité
- **Remédiations adaptées au contexte** : Mesures correctives ou compensatoires selon les contraintes
- **Automatisation** : Utilisation de processus automatisés pour améliorer l'efficacité
- **Amélioration continue** : Révision et optimisation régulières des procédures
- **Traçabilité complète** : Documentation de l'ensemble du cycle de vie des vulnérabilités

2. Gouvernance et responsabilités

2.1 Organisation et rôles

Fonction	Responsabilités
RSSI	- Définition de la stratégie de gestion des vulnérabilités - Validation des processus et procédures - Arbitrage des exceptions - Reporting au COMEX et au Comité des Risques
Équipe Sécurité Opérationnelle	- Coordination du processus global - Évaluation et qualification des vulnérabilités - Validation des plans de remédiation - Suivi de l'avancement - Surveillance des nouvelles menaces
SOC SaaS	- Surveillance continue et détection

	- Alertes sur les vulnérabilités critiques - Corrélation des vulnérabilités avec les événements de sécurité - Assistance à l'analyse d'impact
Équipes Infrastructure & Cloud	- Déploiement des correctifs sur les infrastructures - Application des mesures de remédiation - Test des correctifs - Documentation des actions
Équipes Application	- Correction des vulnérabilités applicatives - Tests de non-régression - Mise en production des correctifs
Responsables Produits	- Validation de l'impact métier - Autorisation des déploiements en production - Définition des fenêtres de maintenance
Propriétaires des actifs	- Validation finale des actions de remédiation - Acceptation formelle des risques résiduels éventuels

2.2 Instances de gouvernance

Instance	Fréquence	Participants	Missions
Comité de Sécurité (COSEC)	Mensuelle	RSSI, DSI, Responsables Sécurité et Infrastructure	- Revue des vulnérabilités critiques - Validation des exceptions - Suivi des indicateurs - Arbitrage des ressources
Comité Opérationnel Vulnérabilités	Hebdomadaire	Équipe Sécurité, Responsables Infrastructure et Applications	- Suivi opérationnel des vulnérabilités - Coordination des actions - Résolution des blocages
Réunion Patch Management	Bi-mensuelle	Équipes Infrastructure, Cloud, Applications	- Planification des déploiements - Revue des correctifs disponibles - Préparation des plans de tests
Comité de Crise	Ad hoc	RSSI, DSI, COMEX	- Traitement des vulnérabilités critiques

			- Gestion des situations d'urgence (0-day)

2.3 Processus d'escalade

Le processus d'escalade définit les modalités de remontée des situations nécessitant une attention particulière :

1. **Niveau 1** - Gestion opérationnelle courante
    - Acteurs : Équipes Sécurité Opérationnelle et techniques
    - Déclenchement : Traitement standard des vulnérabilités
2. **Niveau 2** - Escalade managériale
    - Acteurs : RSSI, Responsables techniques
    - Déclenchement :
        - Vulnérabilités critiques (CVSS ≥ 9.0)
        - Retard significatif dans la remédiation (>25% du SLA)
        - Désaccord sur la priorisation
3. **Niveau 3** - Escalade direction
    - Acteurs : COMEX, Comité de Sécurité
    - Déclenchement :
        - Vulnérabilités avec risque systémique
        - Exploitation active dans la nature
        - Impact potentiel majeur sur l'activité
        - Arbitrages stratégiques nécessaires

3. Identification des vulnérabilités

3.1 Sources d'identification

Neo Financia utilise plusieurs sources complémentaires pour identifier les vulnérabilités :

Source	Description	Fréquence	Responsable
Scans automatisés	Scans de vulnérabilités réalisés avec des outils automatisés	Hebdomadaire (infrastructures critiques) Mensuelle (autres)	Équipe Sécurité Opérationnelle
Scans d'applications	Analyse statique et dynamique du code (SAST/DAST)	À chaque cycle de développement Trimestrielle (applications en production)	Équipes Développement & Sécurité
Audit de sécurité	Tests d'intrusion réalisés par des prestataires externes	Semestrielle (systèmes critiques)	RSSI

		Annuelle (autres systèmes)	
Veille sécurité	Suivi des bulletins de sécurité des éditeurs et CERT	Continue	Équipe Sécurité Opérationnelle
Bug Bounty	Programme de récompense pour la découverte de vulnérabilités	Continue	Équipe Sécurité Opérationnelle
Analyses Cloud	Solutions CSPM (Cloud Security Posture Management)	Continue avec rapports hebdomadaires	Équipe Cloud Security
Remontées internes	Signalements par les collaborateurs	Ad hoc	Tous
Analyse SOC	Détection via la solution SOC SaaS	Continue	SOC SaaS & Équipe Sécurité

3.2 Couverture des scans

Les scans de vulnérabilités doivent couvrir l'ensemble du périmètre de Neo Financia :

Type d'actif	Outils utilisés	Périmètre	Fréquence
Infrastructures internes	Nessus Professional, Qualys VM	100% des actifs	Mensuelle
Infrastructures critiques	Nessus Professional, Qualys VM	100% des actifs critiques	Hebdomadaire
Cloud Azure	Azure Security Center, Defender for Cloud	100% des ressources	Continue
Cloud OVHcloud	Nessus Cloud, solutions CSPM	100% des ressources	Hebdomadaire
Cloud AWS	AWS Inspector, solutions CSPM	100% des ressources	Hebdomadaire
Applications web	OWASP ZAP, Burp Suite	Applications exposées	Mensuelle
Applications mobiles	MobSF, solutions spécifiques	Toutes les versions	À chaque version
Infrastructures DevOps	SonarQube, GitLab Security	Chaînes CI/CD, repositories	Continue
Postes de travail	EDR, solutions de gestion des correctifs	Échantillon représentatif	Mensuelle
Équipements réseau	Solutions dédiées	Tous les équipements	Mensuelle

3.3 Gestion des faux positifs

La gestion des faux positifs est un élément crucial pour maintenir l'efficacité du processus :

1. **Identification** : Analyse approfondie pour confirmer le caractère de faux positif
2. **Documentation** : Enregistrement détaillé avec justification technique
3. **Validation** : Revue et approbation par un expert sécurité
4. **Ajout au référentiel** : Intégration dans la base des faux positifs connus
5. **Exclusion conditionnelle** : Paramétrage des outils pour exclure le faux positif
6. **Revérification périodique** : Validation périodique du statut de faux positif (semestrielle)

Un faux positif ne peut être validé que sur la base d'une analyse technique approfondie, jamais pour des raisons opérationnelles ou de commodité.

3.4 Veille sur les vulnérabilités

Neo Financia maintient un processus de veille structuré :

1. **Sources surveillées** :
    - Bulletins de sécurité des éditeurs (Microsoft, Red Hat, Oracle, etc.)
    - Alertes des CERT (CERT-FR, CERT-EU, US-CERT)
    - Bases de vulnérabilités (NVD, CVE, MITRE)
    - Fournisseurs de Threat Intelligence
    - Communautés spécialisées (secteur financier)
2. **Processus de traitement** :
    - Collecte et centralisation des informations
    - Analyse de pertinence pour le SI de Neo Financia
    - Qualification préliminaire (criticité, exploitabilité)
    - Diffusion ciblée aux équipes concernées
    - Suivi des actions entreprises
    - Consolidation dans l'outil de gestion des vulnérabilités
3. **Alertes d'urgence** :
    - Processus accéléré pour les vulnérabilités critiques
    - Notification immédiate aux responsables concernés
    - Activation des procédures d'urgence si nécessaire

4. Évaluation et priorisation

4.1 Méthodologie d'évaluation

Neo Financia utilise une approche structurée pour évaluer les vulnérabilités :

1. **Évaluation technique** :
    - Utilisation du score CVSS (Common Vulnerability Scoring System) v3.1
    - Analyse des vecteurs d'attaque et de l'exploitabilité
    - Confirmation de l'applicabilité dans l'environnement Neo Financia
    - Validation de l'existence d'un exploit public
2. **Évaluation contextuelle** :

- Criticité de l'actif concerné (selon la classification des actifs)
- Exposition de l'actif (internet, intranet, isolé)
- Données traitées (transactions financières, données clients)
- Mesures de protection existantes (compensatoires)

3. **Évaluation business** :

- Impact potentiel sur les services bancaires
- Conséquences réglementaires (DORA, NIS2, RGPD)
- Risque réputationnel
- Impact financier potentiel

4.2 Matrice de criticité

La criticité finale d'une vulnérabilité est déterminée par la combinaison de la sévérité technique et du contexte business :

Score CVSS	Actifs critiques	Actifs importants	Actifs standards	Actifs mineurs
9.0 - 10.0	Critique	Critique	Haute	Haute
7.0 - 8.9	Critique	Haute	Haute	Moyenne
4.0 - 6.9	Haute	Moyenne	Moyenne	Basse
0.1 - 3.9	Moyenne	Basse	Basse	Basse

Les catégories d'actifs sont définies selon le niveau de classification de Neo Financia :

- **Actifs critiques** : Systèmes de transactions financières, authentification, données clients (P3)
- **Actifs importants** : Applications client, systèmes internes sensibles (P2)
- **Actifs standards** : Systèmes de support, outils internes (P1)
- **Actifs mineurs** : Systèmes non connectés aux services critiques (P0)

4.3 Délais de remédiation (SLA)

Neo Financia définit des délais maximums de remédiation selon la criticité de la vulnérabilité :

Niveau de criticité	Délai de remédiation	Environnements de production	Autres environnements
Critique	24-72 heures	24 heures	72 heures
Haute	7 jours	7 jours	14 jours
Moyenne	30 jours	30 jours	60 jours
Basse	90 jours	90 jours	Selon planification

Pour les vulnérabilités faisant l'objet d'une exploitation active ou largement médiatisées, les délais peuvent être réduits sur décision du RSSI.

4.4 Processus de priorisation

La priorisation des vulnérabilités suit un processus structuré :

1. **Analyse quotidienne** des nouvelles vulnérabilités détectées
2. **Qualification initiale** par l'équipe Sécurité Opérationnelle
3. **Validation de la criticité** avec les propriétaires d'actifs pour les cas complexes
4. **Consolidation** dans un tableau de bord unique
5. **Revue hebdomadaire** lors du Comité Opérationnel Vulnérabilités
6. **Arbitrage** des cas particuliers ou conflits de priorité
7. **Communication** des priorités aux équipes techniques

Les facteurs additionnels pouvant influencer la priorisation incluent :

- Existence d'exploits publics
- Campagnes d'attaques actives
- Dépendances entre vulnérabilités
- Fenêtres de maintenance planifiées
- Ressources disponibles

5. Traitement des vulnérabilités

5.1 Stratégies de remédiation

Neo Financia applique différentes stratégies de traitement selon le contexte :

Stratégie	Description	Cas d'usage
Correction	Application d'un correctif ou mise à jour	Solution privilégiée quand disponible
Reconfiguration	Modification des paramètres de configuration	Désactivation de fonctionnalités vulnérables
Isolation	Limitation de l'exposition de l'actif	Segmentation réseau renforcée
Mesures compensatoires	Mise en place de contrôles alternatifs	WAF, IPS, monitoring renforcé
Suppression	Retrait de la composante vulnérable	Désinstallation de modules non essentiels
Remplacement	Substitution par une alternative sécurisée	Migration vers une solution alternative
Acceptation du risque	Documentation et acceptation formelle	Uniquement pour les risques résiduels faibles

La stratégie privilégiée reste l'application des correctifs, les autres approches étant généralement temporaires dans l'attente d'une solution définitive.

5.2 Processus de remédiation

Le processus de remédiation comprend les étapes suivantes :

1. **Planification** :
    - Identification de la solution technique
    - Évaluation de l'impact opérationnel
    - Définition du plan de déploiement
    - Allocation des ressources nécessaires
2. **Validation préalable** :
    - Tests en environnement hors production
    - Vérification de la compatibilité
    - Tests de non-régression
    - Validation des procédures de rollback
3. **Implémentation** :
    - Déploiement selon le processus de gestion des changements
    - Supervision renforcée pendant le déploiement
    - Documentation des actions réalisées
    - Validation technique post-déploiement
4. **Vérification** :
    - Scan de confirmation
    - Tests fonctionnels
    - Validation de l'efficacité de la correction
    - Clôture de la vulnérabilité

5.3 Mesures d'urgence

Pour les vulnérabilités critiques nécessitant une action immédiate :

1. **Procédure accélérée** :
    - Circuit d'approbation simplifié
    - Mobilisation prioritaire des équipes
    - Communication renforcée
2. **Mesures temporaires** :
    - Désactivation temporaire du service si nécessaire
    - Blocage des vecteurs d'attaque au niveau réseau/applicatif
    - Surveillance renforcée
    - Communication aux utilisateurs si impact
3. **Comité de crise** :
    - Activation pour les vulnérabilités critiques systémiques
    - Suivi continu jusqu'à résolution
    - Reporting direct au COMEX

5.4 Gestion des exceptions

Lorsqu'une vulnérabilité ne peut être corrigée dans les délais définis :

1. **Demande d'exception formelle** :
    - Description détaillée de la vulnérabilité
    - Justification technique ou business

- Évaluation des risques
- Mesures compensatoires proposées
- Durée demandée

2. **Processus d'approbation** :
   - Analyse par l'équipe Sécurité
   - Validation selon le niveau de risque :
     - Risque Moyen : Approbation RSSI
     - Risque Élevé : Approbation COSEC
     - Risque Critique : Approbation Comité des Risques

3. **Documentation et suivi** :
   - Enregistrement dans le registre des exceptions
   - Mise en place et vérification des mesures compensatoires
   - Revue périodique (mensuelle pour Critique, trimestrielle pour autres)
   - Plan d'action défini pour résolution permanente

Une exception ne peut excéder 6 mois sans renouvellement formel, et aucune exception n'est reconductible plus de deux fois.

6. Gestion des correctifs

6.1 Surveillance des correctifs disponibles

Neo Financia maintient une surveillance active des correctifs publiés :

1. **Sources surveillées** :
   - Sites des éditeurs (Microsoft, Oracle, Red Hat, etc.)
   - Portails cloud (Azure, AWS, OVHcloud)
   - Bulletins de sécurité spécifiques
   - Alertes CERT

2. **Classification des correctifs** :
   - Critique : Correction de vulnérabilités majeures
   - Sécurité : Correction de vulnérabilités standards
   - Fonctionnel : Amélioration des fonctionnalités
   - Maintenance : Optimisation et stabilité

3. **Analyse préliminaire** :
   - Applicabilité dans l'environnement Neo Financia
   - Évaluation de l'impact potentiel
   - Identification des systèmes concernés
   - Priorisation initiale

6.2 Cycles de déploiement

Neo Financia a défini des cycles standardisés de déploiement des correctifs :

Type de correctif	Systèmes critiques	Systèmes standards	Cycle de déploiement
Critique	Infrastructures financières,	Production	Hors cycle -

	authentification		Immédiat (48h max)
Sécurité	Production	Tous	Cycle mensuel
Fonctionnel	Production	Production	Cycle trimestriel
Maintenance	Tous	Tous	Cycle trimestriel

Cycles spécifiques par environnement :

- **Environnements cloud** : Correctifs de sécurité automatisés hebdomadaires (sous réserve de tests)
- **Serveurs internes** : Patching mensuel selon calendrier défini
- **Postes de travail** : Déploiement progressif sur 2 semaines
- **Équipements réseau** : Fenêtres de maintenance trimestrielles
- **Systèmes BYOD** : Vérification de conformité à la connexion

6.3 Processus de déploiement

Le déploiement des correctifs suit un processus formalisé :

1. **Préparation** :
    - Inventaire des systèmes concernés
    - Création des packages de déploiement
    - Définition du plan de rollback
    - Communication aux parties prenantes
2. **Tests préalables** :
    - Déploiement en environnement de test
    - Validation technique du correctif
    - Tests de non-régression
    - Ajustements éventuels de la méthode de déploiement
3. **Approbation** :
    - Validation technique
    - Autorisation métier (pour les systèmes critiques)
    - Planification définitive
4. **Déploiement** :
    - Application selon la méthode définie
    - Déploiement progressif si possible
    - Surveillance en temps réel
    - Points de contrôle intermédiaires
5. **Validation** :
    - Vérification de l'application effective
    - Tests fonctionnels post-déploiement
    - Confirmation de la résolution des vulnérabilités
    - Documentation des actions réalisées

6.4 Gestion des correctifs dans les environnements cloud

Neo Financia applique une approche spécifique pour ses environnements cloud :

1. **Azure (70% de l'infrastructure)** :
    - Utilisation d'Azure Update Management
    - Surveillance via Azure Security Center
    - Orchestration des mises à jour avec maintenance windows
    - Tests automatisés pré et post-déploiement
    - Validation progressive des correctifs critiques
    - Utilisation des groupes de mise à jour pour le déploiement séquentiel
2. **OVHcloud (20% de l'infrastructure)** :
    - Utilisation des outils de gestion de configuration
    - Planification avec les équipes OVH pour les composants managés
    - Approche Infrastructure as Code pour les déploiements
    - Validation des mises à jour des images de base
3. **AWS (10% de l'infrastructure)** :
    - Utilisation d'AWS Systems Manager Patch Manager
    - Définition de baseline de correctifs par type d'instance
    - Intégration avec AWS Inspector pour la vérification
    - Automatisation via AWS Lambda

Pour l'ensemble des environnements cloud, priorité est donnée à l'automatisation et à l'approche immutable (redéploiement plutôt que mise à jour in-place).

6.5 Gestion des correctifs pour les terminaux

Pour les postes de travail et équipements mobiles, y compris dans le cadre du BYOD :

1. **Terminaux gérés par Neo Financia** :
    - Outil centralisé de gestion des correctifs
    - Déploiement automatisé selon les groupes de risque
    - Vérification de conformité quotidienne
    - Remédiation automatique quand possible
    - Approche progressive pour limiter l'impact
2. **Terminaux personnels (BYOD)** :
    - Vérification de conformité à la connexion
    - Niveau minimum de correctifs requis
    - Mise en quarantaine des équipements non conformes
    - Accès restreint jusqu'à mise à jour
    - Support à la mise à jour si nécessaire
3. **Appareils mobiles** :
    - Solution MDM pour la gestion des mises à jour
    - Vérification de la version du système d'exploitation
    - Contrôle des applications installées
    - Mise à jour des applications d'entreprise

7. Situations exceptionnelles

7.1 Vulnérabilités Zero-Day

En cas de découverte d'une vulnérabilité sans correctif disponible (zero-day) :

1. **Évaluation immédiate** :
    - Analyse technique approfondie
    - Détermination du périmètre concerné
    - Évaluation du risque d'exploitation
    - Identification des scénarios d'attaque potentiels
2. **Mesures d'atténuation d'urgence** :
    - Mise en place de règles IPS/WAF spécifiques
    - Renforcement du monitoring
    - Restriction d'accès temporaire si nécessaire
    - Déploiement de contrôles compensatoires
3. **Communication et escalade** :
    - Notification au RSSI et à la DSI
    - Activation du comité de crise si nécessaire
    - Information aux parties prenantes concernées
    - Coordination avec le SOC SaaS
4. **Suivi continu** :
    - Veille renforcée sur l'évolution de la menace
    - Recherche active de solutions alternatives
    - Préparation au déploiement urgent du correctif dès disponibilité
    - Documentation détaillée des actions entreprises

7.2 Vulnérabilités critiques largement médiatisées

Pour les vulnérabilités ayant un impact médiatique important (type Log4Shell, Heartbleed) :

1. **Cellule de crise dédiée** :
    - Activation immédiate
    - Points de situation fréquents
    - Coordination centralisée des actions
2. **Communication proactive** :
    - Information du COMEX et du Conseil d'Administration
    - Préparation des éléments de langage
    - Communication externe si nécessaire
3. **Mobilisation exceptionnelle** :
    - Équipes dédiées 24/7 si nécessaire
    - Priorisation absolue des ressources
    - Collaboration renforcée avec les fournisseurs
4. **Reporting spécifique** :
    - Tableaux de bord en temps réel
    - Communication régulière sur l'avancement
    - Bilan post-crise

7.3 Indisponibilité des correctifs

Lorsqu'un correctif n'est pas disponible ou ne peut être déployé :

1. **Analyse des alternatives** :
    - Solutions de contournement documentées
    - Technologies alternatives
    - Isolation renforcée
2. **Implémentation de contrôles compensatoires** :
    - Virtual Patching au niveau WAF/IPS
    - Monitoring spécifique
    - Restriction des accès
    - Modification des configurations
3. **Engagement avec les fournisseurs** :
    - Escalade auprès de l'éditeur/fournisseur
    - Recherche de solutions communautaires
    - Partage d'information avec les pairs du secteur
4. **Réévaluation périodique** :
    - Revue hebdomadaire de la situation
    - Ajustement des contrôles compensatoires
    - Recherche continue de solutions permanentes

8. Reporting et métriques

8.1 Tableaux de bord

Neo Financia maintient plusieurs niveaux de tableaux de bord pour le suivi des vulnérabilités :

1. **Tableau de bord opérationnel** :
    - Mise à jour quotidienne
    - Détail des vulnérabilités par système
    - Statut des actions en cours
    - Alertes sur dépassement des SLA
2. **Tableau de bord tactique** :
    - Mise à jour hebdomadaire
    - Tendances par système et environnement
    - Taux de conformité aux SLA
    - Âge moyen des vulnérabilités
3. **Tableau de bord exécutif** :
    - Mise à jour mensuelle
    - Vue consolidée par niveau de risque
    - Indicateurs clés de performance
    - Comparaison avec les benchmarks du secteur

8.2 Indicateurs clés de performance (KPI)

Neo Financia suit plusieurs indicateurs pour mesurer l'efficacité du processus :

Catégorie	KPI	Objectif	Fréquence de mesure
Exposition	Nombre de vulnérabilités critiques ouvertes	0	Hebdomadaire
Exposition	Nombre de vulnérabilités non corrigées dans les délais	< 5%	Mensuelle
Efficacité	Temps moyen de remédiation - Vulnérabilités critiques	< 3 jours	Mensuelle
Efficacité	Temps moyen de remédiation - Toutes vulnérabilités	< 15 jours	Mensuelle
Couverture	Taux de couverture des scans	> 95%	Trimestrielle
Conformité	Taux de serveurs à jour des correctifs critiques	> 98%	Hebdomadaire
Conformité	Taux de postes de travail à jour des correctifs critiques	> 95%	Hebdomadaire
Performance	Taux de réintroduction de vulnérabilités corrigées	< 2%	Trimestrielle
Processus	Délai d'analyse et qualification des nouvelles vulnérabilités	< 2 jours	Mensuelle

8.3 Reporting réglementaire

Neo Financia produit des rapports spécifiques pour répondre aux exigences réglementaires :

1. **Conformité DORA** :
    - Évaluation de la résilience opérationnelle numérique
    - Rapport sur les vulnérabilités critiques
    - Mesures d'atténuation mises en œuvre
    - Tests de résilience
2. **Conformité NIS2** :
    - Mesures de gestion des risques
    - Vulnérabilités significatives et leur traitement
    - Incidents liés à des vulnérabilités non corrigées
3. **Conformité RGPD** :
    - Vulnérabilités impactant les systèmes traitant des données personnelles
    - Actions entreprises pour assurer la sécurité des traitements
    - Incidents potentiels et leurs conséquences

Ces rapports sont préparés selon la périodicité requise par chaque réglementation et validés par le RSSI avant transmission.

8.4 Communication interne

Neo Financia assure une communication régulière sur l'état des vulnérabilités :

1. **Parties prenantes** :
    - Direction Générale (mensuelle)
    - Comité des Risques (trimestrielle)
    - Propriétaires d'actifs (bi-mensuelle)
    - Équipes techniques (hebdomadaire)
2. **Contenu adapté** :
    - Synthèse exécutive pour la direction
    - Analyse détaillée pour les comités
    - Plans d'action pour les équipes opérationnelles
    - Bulletins de sensibilisation pour l'ensemble des collaborateurs

9. Amélioration continue

9.1 Revue périodique des procédures

Neo Financia évalue régulièrement l'efficacité de ses procédures de gestion des vulnérabilités :

1. **Revue semestrielle** :
    - Évaluation globale du processus
    - Analyse des indicateurs de performance
    - Identification des points faibles
    - Benchmark avec les meilleures pratiques du secteur
2. **Facteurs déclenchant une revue exceptionnelle** :
    - Incident majeur lié à une vulnérabilité
    - Évolution significative du SI
    - Changement réglementaire
    - Nouvelles menaces ou techniques d'attaque

9.2 Retours d'expérience

Les retours d'expérience sont systématiquement organisés :

1. **Après chaque incident significatif** :
    - Analyse des vulnérabilités exploitées
    - Évaluation du délai de détection et de correction
    - Identification des facteurs aggravants
    - Leçons apprises
2. **Après les exercices ou tests** :
    - Évaluation des procédures de détection
    - Efficacité des processus de remédiation
    - Performance des équipes
    - Pertinence des outils

9.3 Plan d'amélioration

Un plan d'amélioration continue est maintenu et mis à jour régulièrement :

1. **Domaines d'amélioration** :

- Automatisation des processus
- Optimisation des outils
- Formation des équipes
- Collaboration entre départements
- Intégration avec les autres processus de sécurité

2. **Méthodologie** :

- Identification des actions prioritaires
- Définition des objectifs mesurables
- Attribution des responsabilités
- Suivi régulier de l'avancement
- Évaluation des résultats

9.4 Veille technologique

Neo Financia maintient une veille active sur les évolutions des pratiques et technologies de gestion des vulnérabilités :

1. **Domaines surveillés** :

- Nouvelles méthodes de détection
- Évolution des référentiels (NIST, CIS)
- Technologies d'automatisation
- Solutions de sécurité cloud natives
- Approches Zero Trust

2. **Modalités** :

- Participation à des groupes sectoriels
- Suivi des publications spécialisées
- Échanges avec les pairs
- Formations spécialisées

10. Annexes

10.1 Matrice RACI détaillée

La matrice RACI ci-dessous définit clairement les responsabilités pour chaque étape du processus de gestion des vulnérabilités :

Activité	RSSI	Équipe Sécurité Opérationnelle	SOC SaaS	Équipes Infrastructure & Cloud	Équipes Application	R
Identification des vulnérabilités						
Configuration des outils de scan	I	A/R	C	C	I	I
Exécution des scans réguliers	I	R	C	C	I	I
Veille sur les	I	R	A	C	C	I

bulletins de sécurité						
Tests d'intrusion	A	R	I	C	C	I
Évaluation et priorisation						
Analyse technique des vulnérabilités	I	A/R	C	C	C	I
Évaluation de l'impact business	C	C	I	I	I	C
Détermination de la criticité finale	A	R	C	C	C	I
Définition des priorités de traitement	A	R	C	C	C	C
Traitement						
Planification des actions	I	A	I	R	R	C
Définition des mesures de remédiation	C	A	C	R	R	C
Déploiement des correctifs - Infrastructure	I	A	I	R	I	C
Déploiement des correctifs - Applications	I	A	I	C	R	C
Validation des corrections	I	A/R	C	C	C	I
Gestion des exceptions						
Demande d'exception	I	C	I	R	R	C
Évaluation des risques	C	A/R	C	C	C	I
Approbation des exceptions - Risque Moyen	A/R	C	C	I	I	I

Approbation des exceptions - Risque Élevé	A	C	C	I	I	I
Approbation des exceptions - Risque Critique	R	C	C	I	I	I
Situations d'urgence						
Détection des vulnérabilités critiques	I	R	A	C	C	I
Activation du comité de crise	A	R	I	I	I	I
Définition du plan d'action d'urgence	A	R	C	C	C	C
Communication interne/externe crise	A	C	I	I	I	C
Reporting et suivi						
Préparation des indicateurs opérationnels	I	A/R	C	C	C	I
Rapport mensuel au COSEC	A	R	C	I	I	I
Rapport trimestriel au Comité des Risques	A/R	C	I	I	I	I
Amélioration continue						
Revue périodique du processus	A	R	C	C	C	C
Définition des plans d'amélioration	A	R	C	C	C	C
Validation des évolutions majeures	A	R	C	C	C	C

Légende :

- R : Responsable (exécute l'action)
- A : Autorité (approuve et est responsable de l'action)
- C : Consulté (doit être consulté avant l'action)
- I : Informé (doit être informé du résultat)

10.2 Workflow de gestion des vulnérabilités

Le processus de gestion des vulnérabilités suit les étapes séquentielles décrites ci-dessous :

Phase 1 : Identification

1. **Collecte des vulnérabilités**
    - Sources automatisées : scans programmés, outils SAST/DAST, CSPM
    - Sources manuelles : tests d'intrusion, bug bounty, signalements internes
    - Veille externe : bulletins de sécurité, alertes CERT, threat intelligence
2. **Centralisation**
    - Consolidation dans l'outil de gestion des vulnérabilités
    - Dédoublonnage et rationalisation des alertes
    - Enrichissement avec les informations contextuelles
3. **Vérification initiale**
    - Analyse préliminaire de la véracité (élimination des faux positifs évidents)
    - Confirmation de l'applicabilité dans l'environnement
    - Association aux actifs concernés dans la CMDB

Phase 2 : Évaluation

4. **Analyse technique**
    - Évaluation technique selon CVSS v3.1
    - Vérification de l'exploitabilité
    - Confirmation des impacts techniques potentiels
    - Identification des actifs concernés
5. **Évaluation contextuelle**
    - Détermination de la criticité des actifs affectés
    - Analyse de l'exposition (interne/externe)
    - Prise en compte des contrôles existants
    - Identification des données impactées (particulièrement les transactions financières et documents clients)
6. **Détermination de la criticité finale**
    - Application de la matrice de criticité (section 4.2)
    - Validation par l'équipe Sécurité Opérationnelle
    - Escalade aux propriétaires d'actifs pour les cas complexes
    - Définition du SLA de remédiation applicable

Phase 3 : Traitement

7. **Planification**

- Attribution aux équipes responsables
- Définition de la stratégie de remédiation optimale
- Élaboration du plan d'action détaillé
- Validation du planning de déploiement

8. **Remédiation**

   - Développement ou préparation des correctifs
   - Tests préalables en environnement non-productif
   - Demande de changement selon le processus standard
   - Déploiement selon la méthode appropriée
   - Surveillance renforcée durant l'application

9. **Vérification**

   - Scan post-remédiation
   - Validation technique de la correction
   - Tests fonctionnels de non-régression
   - Documentation des actions réalisées

Phase 4 : Clôture et capitalisation

10. **Clôture**

    - Mise à jour du statut dans l'outil de suivi
    - Notification aux parties prenantes
    - Archivage de la documentation
    - Mise à jour des indicateurs

11. **Capitalisation**

    - Analyse des causes profondes pour les vulnérabilités significatives
    - Identification des améliorations potentielles
    - Partage des enseignements avec les équipes
    - Mise à jour des procédures si nécessaire

Flux parallèles

- **Gestion des exceptions** : Processus parallèle déclenché lorsqu'une vulnérabilité ne peut être corrigée dans les délais
- **Procédure d'urgence** : Circuit accéléré pour les vulnérabilités critiques nécessitant une action immédiate
- **Reporting continu** : Production des indicateurs et tableaux de bord tout au long du processus

10.3 Formulaire de demande d'exception

FORMULAIRE DE DEMANDE D'EXCEPTION - GESTION DES VULNÉRABILITÉS

1. Informations générales

Champ	Contenu
Référence	EXC-[ANNÉE]-[NUMÉRO SÉQUENTIEL]
Date de soumission	JJ/MM/AAAA
Demandeur	[Nom, Fonction, Direction]

Systèmes concernés	[Liste des systèmes, applications, infrastructures]

2. Description de la vulnérabilité

Champ	Contenu
Identifiant(s)	[CVE, ID interne, etc.]
Titre	[Titre descriptif de la vulnérabilité]
Description	[Description détaillée]
Score CVSS	[Score numérique] [Vecteur CVSS complet]
Classification Neo Financia	☐ Critique ☐ Haute ☐ Moyenne ☐ Basse
Date de détection	JJ/MM/AAAA
Date limite de remédiation	JJ/MM/AAAA

3. Justification de l'exception

Champ	Contenu
Raison principale	☐ Contrainte technique ☐ Impact business ☐ Dépendance fournisseur ☐ Ressources indisponibles ☐ Autre (préciser)
Justification détaillée	[Explication détaillée et documentée des raisons rendant impossible la correction dans les délais]
Impact en cas de remédiation immédiate	[Description des conséquences négatives d'une remédiation dans les délais standards]
Alternatives envisagées	[Solutions alternatives étudiées et raisons de leur non-adoption]

4. Analyse de risque

Champ	Contenu
Probabilité d'exploitation	☐ Très probable ☐ Probable ☐ Possible ☐ Peu probable ☐ Improbable
Impact en cas d'exploitation	☐ Critique ☐ Majeur ☐ Modéré ☐ Mineur ☐ Négligeable
Risque résiduel évalué	☐ Critique ☐ Élevé ☐ Moyen ☐ Faible
Données potentiellement impactées	☐ Transactions financières ☐ Documents clients ☐ Données personnelles ☐ Données d'authentification ☐ Données internes ☐ Autres
Exposition	☐ Internet ☐ Partenaires ☐ Interne ☐ Isolé
Existence d'exploit public	☐ Oui ☐ Non ☐ Inconnu

Exploitation active connue	□ Oui □ Non □ Inconnu

5. Mesures compensatoires

Champ	Contenu
Mesures techniques	[Description détaillée des contrôles techniques mis en place]
Mesures organisationnelles	[Description des contrôles organisationnels]
Surveillance spécifique	[Mécanismes de détection spécifiques mis en place]
Efficacité estimée	□ Complète □ Significative □ Partielle □ Limitée

6. Plan de remédiation

Champ	Contenu
Date prévue de correction	JJ/MM/AAAA
Étapes intermédiaires	[Jalons et dates prévues]
Dépendances	[Facteurs externes nécessaires à la résolution]
Ressources requises	[Équipes et ressources nécessaires]

7. Durée d'exception demandée

Champ	Contenu
Durée	□ 1 mois □ 3 mois □ 6 mois
Renouvellement	□ Premier □ Second (dernier possible)
Date d'expiration	JJ/MM/AAAA

8. Validation

Niveau	Nom et fonction	Décision	Date	Commentaires
Équipe Sécurité Opérationnelle		□ Recommandée □ Non recommandée		
RSSI		□ Approuvée □ Rejetée □ Escaladée		
COSEC		□ Approuvée □ Rejetée □ Escaladée		
Comité des Risques		□ Approuvée □ Rejetée		

9. Suivi de l'exception

Champ	Contenu

Référence registre exceptions	[ID dans le registre central]
Dates de revue	[JJ/MM/AAAA, JJ/MM/AAAA...]
Statut des contrôles compensatoires	[Résultats des vérifications]
Évolution du contexte	[Changements notables depuis l'approbation]

10. Clôture de l'exception

Champ	Contenu
Date effective de résolution	JJ/MM/AAAA
Méthode de résolution	[Description de la solution mise en œuvre]
Validation de la résolution	[Résultat des tests de vérification]
Date de clôture formelle	JJ/MM/AAAA
Signataire de clôture	[Nom, Fonction]

10.4 Critères d'évaluation des vulnérabilités

A. Méthodologie CVSS v3.1

Neo Financia utilise le Common Vulnerability Scoring System (CVSS) version 3.1 comme base d'évaluation technique des vulnérabilités. Cette méthodologie standardisée comprend trois groupes de métriques :

1. **Métriques de base** (impact technique intrinsèque)
    - Vecteur d'attaque (AV) : Network, Adjacent, Local, Physical
    - Complexité d'attaque (AC) : Low, High
    - Privilèges requis (PR) : None, Low, High
    - Interaction utilisateur (UI) : None, Required
    - Portée (S) : Unchanged, Changed
    - Confidentialité (C) : None, Low, High
    - Intégrité (I) : None, Low, High
    - Disponibilité (A) : None, Low, High
2. **Métriques temporelles** (évolution dans le temps)
    - Maturité du code d'exploitation (E) : Not Defined, Unproven, Proof-of-Concept, Functional, High
    - Niveau de remédiation (RL) : Not Defined, Official Fix, Temporary Fix, Workaround, Unavailable
    - Confiance dans l'évaluation (RC) : Not Defined, Unknown, Reasonable, Confirmed
3. **Métriques environnementales** (contexte spécifique à Neo Financia)
    - Exigences de sécurité modifiées : Confidentiality, Integrity, Availability (Low, Medium, High)
    - Valeurs modifiées des métriques de base adaptées au contexte

Le calcul génère un score entre 0.0 et 10.0, classé comme suit :

- 0.0 : Aucun
- 0.1 - 3.9 : Faible
- 4.0 - 6.9 : Moyen
- 7.0 - 8.9 : Élevé
- 9.0 - 10.0 : Critique

B. Évaluation contextuelle Neo Financia

En complément du score CVSS, Neo Financia enrichit l'évaluation avec des critères contextuels spécifiques à son environnement :

1. **Classification des actifs**

Catégorie	Description	Exemples	Coefficient multiplicateur
Critique (P3)	Actifs essentiels à l'activité, traitant des données sensibles	Systèmes de transaction, authentification, stockage des documents clients	×1.5
Important (P2)	Actifs supportant des fonctions significatives	Applications client, API partenaires, systèmes internes sensibles	×1.2
Standard (P1)	Actifs supportant des fonctions courantes	Systèmes de support, outils internes	×1.0
Mineur (P0)	Actifs non critiques	Systèmes auxiliaires, environnements de test	×0.8

2. **Exposition**

Niveau	Description	Coefficient
Publique	Accessible depuis Internet	×1.4
Partenaire	Accessible aux partenaires via API	×1.2
Interne	Accessible au réseau interne	×1.0
Isolée	Accès très restreint	×0.7

3. **Données traitées**

Type	Description	Coefficient
Transactions financières	Données de paiement, virements	×1.5
Documents clients	KYC, contrats, justificatifs	×1.4
Authentification	Identifiants, jetons	×1.3
Données personnelles	Informations clients hors	×1.2

	documents	
Configurations	Paramètres système	×1.0
Données publiques	Informations non sensibles	×0.7

4. **Facteurs aggravants**

Facteur	Description	Modificateur
Exploit public	Existence d'un exploit fonctionnel	+1.0 point
Exploitation active	Attaques en cours observées	+1.5 points
Médiatisation	Couverture médiatique importante	+0.5 point
Sans correctif	Absence de correctif officiel	+0.8 point

5. **Facteurs atténuants**

Facteur	Description	Modificateur
Contrôles compensatoires	Mesures de protection spécifiques	-0.5 à -1.5 point
Isolation renforcée	Segmentation spécifique	-0.7 point
Monitoring dédié	Surveillance spécifique	-0.3 point
Non-exposition des composants	Composant vulnérable non exposé	-1.0 point

C. Calcul du score final Neo Financia

Le score final de criticité Neo Financia (NFScore) est déterminé comme suit :

1. **Calcul du score de base ajusté (SBA)**

```
SBA = Score CVSS × Coefficient Classification × Coefficient Exposition × Coefficient Données
```

2. **Application des modificateurs**

```
Score Intermédiaire = SBA + Somme(Facteurs aggravants) - Somme(Facteurs atténuants)
```

3. **Normalisation**

   - Si Score Intermédiaire > 10.0, alors NFScore = 10.0
   - Si Score Intermédiaire < 0.1, alors NFScore = 0.1
   - Sinon, NFScore = Score Intermédiaire (arrondi à 0.1 près)

4. **Classification finale**

   - 0.0 - 3.9 : Basse
   - 4.0 - 6.9 : Moyenne
   - 7.0 - 8.9 : Haute
   - 9.0 - 10.0 : Critique

D. Processus d'évaluation

1. **Évaluation initiale automatisée**
    - Calcul du score CVSS par les outils d'analyse
    - Application des coefficients basée sur les métadonnées de l'actif
2. **Ajustement manuel**
    - Revue de l'équipe Sécurité Opérationnelle
    - Ajustement des facteurs contextuels
    - Documentation des décisions d'ajustement
3. **Validation**
    - Revue par le responsable Sécurité Opérationnelle
    - Validation du RSSI pour les vulnérabilités critiques
    - Consultation des propriétaires d'actifs si nécessaire
4. **Détermination du SLA**
    - Application automatique du SLA correspondant au niveau de criticité final

10.5 Calendrier des déploiements de correctifs

A. Cycles standards de déploiement

Neo Financia suit un calendrier structuré pour le déploiement des correctifs de sécurité :

1. Serveurs et infrastructures sur site

Semaine du mois	Environnement	Type de correctifs	Fenêtre de maintenance
Semaine 1	Développement	Tous types	Mercredi, 20h00-22h00
Semaine 1	Test	Tous types	Jeudi, 20h00-22h00
Semaine 2	Pré-production	Critique et sécurité	Mardi, 22h00-00h00
Semaine 2	Pré-production	Fonctionnel et maintenance	Jeudi, 22h00-00h00
Semaine 3	Production non critique	Critique et sécurité	Mardi, 00h00-04h00
Semaine 3	Production non critique	Fonctionnel et maintenance	Jeudi, 00h00-04h00
Semaine 4	Production critique	Critique et sécurité	Samedi, 22h00-04h00
Semaine 4	Production critique	Fonctionnel et maintenance	Dimanche, 22h00-04h00

2. Environnements cloud

Environnement	Azure (70%)	OVHcloud (20%)	AWS (10%)	Type de correctif
Développement	Lundi, automatisé	Lundi, automatisé	Lundi, automatisé	Tous type
Test	Mardi, automatisé	Mardi, automatisé	Mardi, automatisé	Tous type
Pré-production	Mercredi, semi-automatisé	Mercredi, semi-automatisé	Mercredi, semi-automatisé	Tous type
Production non critique	Jeudi, validé par vague	Jeudi, validé par vague	Jeudi, validé par vague	Critique et sécurité
Production critique	Samedi, validé individuellement	Samedi, validé individuellement	Samedi, validé individuellement	Critique et sécurité uniquemen

3. Postes de travail et BYOD

Semaine	Type de poste	Méthode	Catégorie d'utilisateurs
Semaine 1	Postes internes	Automatisé	Groupe pilote (10%)
Semaine 2	Postes internes	Automatisé	Groupe 1 (30%)
Semaine 2	BYOD	Notification et vérification	Groupe pilote (10%)
Semaine 3	Postes internes	Automatisé	Groupe 2 (30%)
Semaine 3	BYOD	Notification et vérification	Groupe 1 (30%)
Semaine 4	Postes internes	Automatisé	Groupe 3 (30%)
Semaine 4	BYOD	Notification et vérification	Groupe 2 et 3 (60%)

4. Équipements réseau et sécurité

Mois	Équipements	Fenêtre de maintenance
Janvier, Avril, Juillet, Octobre	Pare-feu et équipements périmètre	1er samedi, 23h00-05h00
Février, Mai, Août, Novembre	Équipements LAN et Wi-Fi	1er samedi, 23h00-05h00

Mars, Juin, Septembre, Décembre	Équipements WAN et routeurs	1er samedi, 23h00-05h00

B. Ajustements saisonniers et périodes de gel

1. Périodes de gel

Période	Dates (indicatives)	Restrictions
Clôture mensuelle	28 au 3 de chaque mois	Gel des systèmes financiers et comptables
Clôture trimestrielle	Dernier jour du trimestre +/- 5 jours	Gel de tous les systèmes de production
Périodes de fêtes	15 décembre au 5 janvier	Gel des systèmes critiques et client
Lancement produit majeur	2 semaines avant/1 semaine après	Gel des systèmes concernés

Durant ces périodes, seuls les correctifs critiques (0-day, exploitation active) peuvent être déployés, après validation explicite par le COSEC.

2. Planification annuelle

Mois	Activités spécifiques
Janvier	Revue annuelle de la stratégie de patching
Février	Audit de conformité des environnements
Mars	Tests majeurs de résilience (basculement)
Juin	Revue semestrielle du processus
Septembre	Préparation du plan pour l'année suivante
Novembre	Optimisation des outils et processus

C. Processus de planification

1. **Planification à long terme**
    - Établissement du calendrier annuel (T4 année précédente)
    - Validation par le COSEC et les directions métiers
    - Communication générale
2. **Planification trimestrielle**
    - Ajustement du calendrier selon les contraintes identifiées
    - Allocation des ressources
    - Communication détaillée aux équipes concernées
3. **Planification mensuelle**
    - Revue des correctifs disponibles
    - Préparation des packages
    - Validation technique et fonctionnelle

- Création des demandes de changement

4. **Planification hebdomadaire**
    - Confirmation des déploiements prévus
    - Briefing des équipes d'intervention
    - Préparation des communications spécifiques
    - Vérification des prérequis

10.6 Plan d'intervention d'urgence

A. Critères d'activation

Le plan d'intervention d'urgence est activé dans les situations suivantes :

1. **Vulnérabilités critiques immédiates**
    - Score CVSS ≥ 9.0 affectant des systèmes critiques
    - Existence d'un exploit public ou exploitation active confirmée
    - Recommandation d'urgence d'un organisme officiel (ANSSI, CERT)
2. **Vulnérabilités à forte exposition médiatique**
    - Vulnérabilités faisant l'objet d'une couverture médiatique importante
    - Vulnérabilités ayant un nom marketing (ex: Heartbleed, Log4Shell)
    - Impact significatif sur le secteur financier
3. **Autres déclencheurs**
    - Alerte spécifique du SOC SaaS indiquant une menace imminente
    - Demande expresse du RSSI ou de la Direction Générale
    - Incident de sécurité en cours lié à une vulnérabilité

B. Organisation de crise

1. Cellule de crise

Rôle	Responsabilité	Titulaire	Suppléant
Directeur de crise	Pilotage global, décisions stratégiques	RSSI	DSI
Coordinateur technique	Coordination des actions techniques	Responsable Sécurité Opérationnelle	Architecte Sécurité
Responsable analyse	Évaluation technique, analyse d'impact	Expert Sécurité	Analyste SOC
Responsable remédiation	Supervision des actions correctives	Responsable Infrastructure	Responsable Cloud
Responsable communication	Communication interne et externe	Responsable Communication	RSSI Adjoint
Support métier	Évaluation impact business	Directeur Production	Directeur des Risques

2. Moyens dédiés

- Salle de crise physique (siège Paris) et virtuelle (Teams dédié)

- Ligne d'audioconférence dédiée avec numéro d'urgence
- Outils collaboratifs sécurisés (documentation, suivi)
- Annuaire des contacts d'urgence à jour
- Accès privilégiés d'urgence (comptes "break glass")

C. Procédure d'intervention

1. Phase d'alerte (T+0 à T+1h)

- Détection et qualification initiale par l'équipe sécurité/SOC
- Information immédiate du RSSI et du Responsable Sécurité Opérationnelle
- Évaluation rapide de l'impact potentiel sur les systèmes Neo Financia
- Décision d'activation du plan d'urgence
- Convocation de la cellule de crise (physique ou virtuelle)

2. Phase d'analyse (T+1h à T+3h)

- Réunion initiale de la cellule de crise
- Analyse technique approfondie de la vulnérabilité
- Cartographie précise des systèmes impactés
- Évaluation des risques d'exploitation
- Identification des mesures immédiates possibles
- Définition de la stratégie d'intervention

3. Phase de mise en œuvre (T+3h à T+8h)

- Déploiement des mesures de protection temporaires
  - Configuration des pare-feu/WAF/IPS
  - Isolation préventive des systèmes critiques si nécessaire
  - Renforcement de la surveillance
- Information des parties prenantes
- Préparation des correctifs et test accéléré
- Validation technique et fonctionnelle

4. Phase de déploiement (T+8h à T+24h)

- Déploiement progressif des correctifs
  - Approche par vagues selon criticité
  - Surveillance renforcée des systèmes corrigés
  - Tests de validation post-correction
- Suivi continu de l'efficacité des mesures
- Points de situation réguliers (toutes les 2-4h)
- Ajustement de la stratégie si nécessaire

5. Phase de stabilisation (T+24h à T+48h)

- Finalisation du déploiement sur l'ensemble du périmètre
- Vérification complète de l'efficacité des mesures
- Retour à la normale des systèmes temporairement modifiés
- Maintien d'une surveillance renforcée

6. Phase de clôture et retour d'expérience (T+48h à T+1 semaine)

- Réunion de clôture de la cellule de crise
- Documentation complète des actions réalisées
- Analyse des points forts et axes d'amélioration
- Élaboration du rapport final

- Présentation au COSEC et au Comité des Risques
- Mise à jour des procédures si nécessaire

D. Modèles de communication

1. Communication interne

Modèle d'alerte initiale

```
ALERTE SÉCURITÉ PRIORITAIRE - VULNÉRABILITÉ CRITIQUE

Date et heure : [DATETIME]
Niveau d'alerte : [ROUGE/ORANGE/JAUNE]

Systèmes concernés :
[LISTE DES SYSTÈMES]

Description de la vulnérabilité :
[DESCRIPTION CONCISE]

Impact potentiel :
[DESCRIPTION DE L'IMPACT]

Actions immédiates requises :
[LISTE DES ACTIONS]

Point de situation prévu à [HEURE] via [CANAL].

Contact en cas d'urgence : [CONTACT]
```

Modèle de point de situation

```
POINT DE SITUATION - VULNÉRABILITÉ [RÉFÉRENCE]
Date et heure : [DATETIME]
Situation actuelle :
- [ÉTAT D'AVANCEMENT]
- [SYSTÈMES CORRIGÉS/RESTANTS]
- [INCIDENTS ÉVENTUELS]

Prochaines étapes :
- [ACTIONS PLANIFIÉES]
- [DÉLAIS PRÉVUS]

Consignes pour les équipes :
- [CONSIGNES SPÉCIFIQUES]

Prochain point de situation : [DATETIME]
```

2. Communication externe (clients)

Modèle d'information préventive

```
Information importante concernant la sécurité de nos services
```

```
Chers clients,

Nous avons identifié une vulnérabilité de sécurité affectant certains de nos services.
Nos équipes sont mobilisées pour appliquer les correctifs nécessaires.

Impact potentiel pour vous : [DESCRIPTION]

Mesures que nous mettons en place : [DESCRIPTION]

Actions recommandées : [ÉVENTUELLES ACTIONS UTILISATEUR]

Nous vous tiendrons informés via [CANAUX] et vous prions de nous excuser pour la gêne
occasionnée.

L'équipe Neo Financia
```

E. Contacts d'urgence

[Liste des contacts internes et externes à utiliser en cas d'urgence - à maintenir séparément pour des raisons de confidentialité]

10.7 Liste des outils utilisés

Neo Financia utilise un ensemble d'outils complémentaires pour assurer la gestion efficace des vulnérabilités :

A. Outils de découverte et d'analyse

Catégorie	Outil	Version	Usage principal	Périmètre
Scan de vulnérabilités	Tenable Nessus	Enterprise	Scan infrastructure	Serveurs, réseau
Scan de vulnérabilités	Qualys VM	Cloud	Scan infrastructure secondaire	Cloud, systèmes critiques
Analyse applications	OWASP ZAP	Latest	Test dynamique applications	Applications web
Analyse applications	SonarQube	Enterprise	Analyse statique de code	Développement, CI/CD
Analyse applications	Checkmarx	Enterprise	Analyse statique avancée	Applications critiques
Test d'intrusion	Burp Suite	Professional	Tests manuels approfondis	Applications sensibles
Scan mobiles	MobSF	Latest	Analyse applications mobiles	Apps iOS/Android
Analyse	OWASP	Latest	Vérification	Toutes

dépendances	Dependency Check		composants	applications
Analyse containers	Trivy	Latest	Scan images containers	Kubernetes, Docker
Cloud Security	Azure Defender for Cloud	SaaS	Sécurité Azure	Infrastructure Azure (70%)
Cloud Security	AWS Inspector	SaaS	Sécurité AWS	Infrastructure AWS (10%)
Cloud Security	Prisma Cloud	SaaS	CSPM multi-cloud	Tous environnements cloud

B. Gestion du cycle de vie des vulnérabilités

Catégorie	Outil	Version	Usage principal	Périmètre
Gestion centralisée	Threadfix	Enterprise	Consolidation, suivi, workflows	Toutes vulnérabilités
Gestion des correctifs	Microsoft WSUS	Latest	Correctifs Windows	Serveurs et postes Windows
Gestion des correctifs	Red Hat Satellite	Latest	Correctifs Linux	Serveurs Linux
Gestion des correctifs	Azure Update Management	Cloud	Correctifs VM Azure	VMs Azure
Gestion des correctifs	AWS Systems Manager	Cloud	Correctifs AWS	EC2, containers AWS
Gestion des correctifs	Ivanti Security Controls	Enterprise	Correctifs tiers	Applications tierces
Gestion des terminaux	Microsoft Intune	Cloud	MDM, gestion correctifs mobiles	Terminaux mobiles, BYOD
Bug Bounty	HackerOne	SaaS	Programme de bug bounty	Applications exposées

C. Surveillance et détection

Catégorie	Outil	Version	Usage principal	Périmètre
SIEM	Splunk	Enterprise	Collection et analyse de logs	Infrastructure globale
EDR	CrowdStrike Falcon	Cloud	Protection endpoints	Serveurs et postes
NDR	Darktrace	Enterprise	Détection	Infrastructure

			anomalies réseau	réseau
SOC SaaS	Arctic Wolf	Managed	Surveillance sécurité 24/7	Infrastructure globale
Threat Intelligence	Recorded Future	Enterprise	Veille menaces	Vulnérabilités, menaces
SOAR	Palo Alto Cortex XSOAR	Enterprise	Automatisation réponse	Incidents sécurité
Suivi exploits	Exploit Database	N/A	Veille exploits	Recherche vulnérabilités
WAF	F5 Advanced WAF	Latest	Protection applications web	Applications exposées

D. Intégration et automatisation

Catégorie	Outil	Version	Usage principal	Périmètre
CI/CD Security	GitLab Security	Enterprise	Intégration sécurité CI/CD	Pipeline développement
Infrastructure as Code	Terraform	Enterprise	Déploiement infrastructure	Environnements cloud
Configuration Management	Ansible	Enterprise	Automatisation configuration	Serveurs
Conteneurisation	Kubernetes	Latest	Orchestration containers	Applications containerisées
Automatisation	Azure Logic Apps	Cloud	Workflows cloud	Environnement Azure
Automatisation	PowerShell	Latest	Scripts automatisés	Windows
Automatisation	Python	Latest	Scripts automatisés	Multi-plateforme

E. Gouvernance et reporting

Catégorie	Outil	Version	Usage principal	Périmètre
GRC	MetricStream	Enterprise	Gestion des risques	Gouvernance globale
CMDB	ServiceNow CMDB	Enterprise	Inventaire des actifs	Infrastructure globale
Reporting	Microsoft Power BI	Enterprise	Tableaux de bord	Reporting exécutif
Gestion documentaire	SharePoint	Online	Documentation	Procédures, politiques

Gestion de projet	Jira	Cloud	Suivi des actions	Projets de remédiation
Gestion des incidents	ServiceNow	Enterprise	Suivi des incidents	Incidents sécurité

10.8 Glossaire

Terme	Définition
API (Application Programming Interface)	Interface permettant à des applications de communiquer entre elles selon des règles prédéfinies. Neo Financia utilise des API sécurisées pour les interconnexions avec ses partenaires fintech (Mangopay, Lemonway).
BYOD (Bring Your Own Device)	Politique permettant aux employés d'utiliser leurs appareils personnels dans un cadre professionnel. Neo Financia autorise le BYOD sous certaines conditions de sécurité.
CERT (Computer Emergency Response Team)	Équipe dédiée à la réponse aux incidents de sécurité informatique. Neo Financia surveille les alertes des CERT nationaux et sectoriels.
CI/CD (Continuous Integration/Continuous Deployment)	Pratique de développement consistant à intégrer et déployer fréquemment les modifications de code, avec des tests automatisés.
CNIL	Commission Nationale de l'Informatique et des Libertés, autorité française de protection des données personnelles.
CSPM (Cloud Security Posture Management)	Solutions qui identifient et remédient aux problèmes de configuration dans les environnements cloud.
CVE (Common Vulnerabilities and Exposures)	Système de référencement standardisé des vulnérabilités de sécurité connues.
CVSS (Common Vulnerability Scoring System)	Système standardisé pour évaluer la gravité des vulnérabilités de sécurité informatique. Neo Financia utilise la version 3.1.
DAST (Dynamic Application Security Testing)	Test de sécurité réalisé sur une application en cours d'exécution pour identifier les vulnérabilités exploitables.
DORA (Digital Operational Resilience Act)	Règlement européen visant à renforcer la résilience opérationnelle numérique du secteur financier.
EDR (Endpoint Detection and Response)	Solution de sécurité qui surveille en continu les terminaux pour détecter et répondre aux menaces.
ICO (Information Commissioner's Office)	Autorité britannique de protection des données personnelles.

IPS (Intrusion Prevention System)	Système de prévention d'intrusion qui surveille le réseau pour détecter et bloquer les activités malveillantes.
KPI (Key Performance Indicator)	Indicateur clé de performance utilisé pour mesurer l'efficacité d'un processus.
MDM (Mobile Device Management)	Solution permettant de gérer et sécuriser les appareils mobiles au sein de l'entreprise.
NFScore	Score de criticité propre à Neo Financia, calculé en enrichissant le CVSS avec des critères contextuels.
NIS2	Directive européenne renforçant la cybersécurité dans les secteurs critiques, dont la finance.
PCI-DSS (Payment Card Industry Data Security Standard)	Norme de sécurité pour la protection des données de cartes de paiement.
RACI (Responsible, Accountable, Consulted, Informed)	Matrice définissant les rôles et responsabilités dans un processus.
RGPD (Règlement Général sur la Protection des Données)	Réglementation européenne encadrant le traitement des données personnelles.
RTO/RPO (Recovery Time Objective/Recovery Point Objective)	Objectifs définissant respectivement le temps de reprise et la perte de données maximale acceptable lors d'un incident.
SaaS (Software as a Service)	Modèle de distribution logicielle où les applications sont hébergées par un fournisseur et accessibles via internet.
SAST (Static Application Security Testing)	Analyse de code source pour identifier les vulnérabilités sans exécuter l'application.
SIEM (Security Information and Event Management)	Solution centralisant la collecte, l'analyse et la corrélation des événements de sécurité.
SLA (Service Level Agreement)	Accord définissant le niveau de service attendu, notamment les délais de remédiation des vulnérabilités.
SOC (Security Operations Center)	Centre opérationnel dédié à la surveillance et à la gestion des incidents de sécurité. Neo Financia utilise un SOC SaaS externalisé.
SOAR (Security Orchestration, Automation and Response)	Solutions permettant d'automatiser la réponse aux incidents de sécurité.

Virtual Patching	Technique permettant de protéger contre une vulnérabilité sans appliquer directement un correctif sur le système concerné.
WAF (Web Application Firewall)	Pare-feu applicatif web protégeant contre les attaques visant les applications web.
Zero-Day	Vulnérabilité non corrigée et non publiquement connue, mais activement exploitée. Ces vulnérabilités nécessitent une réponse d'urgence.