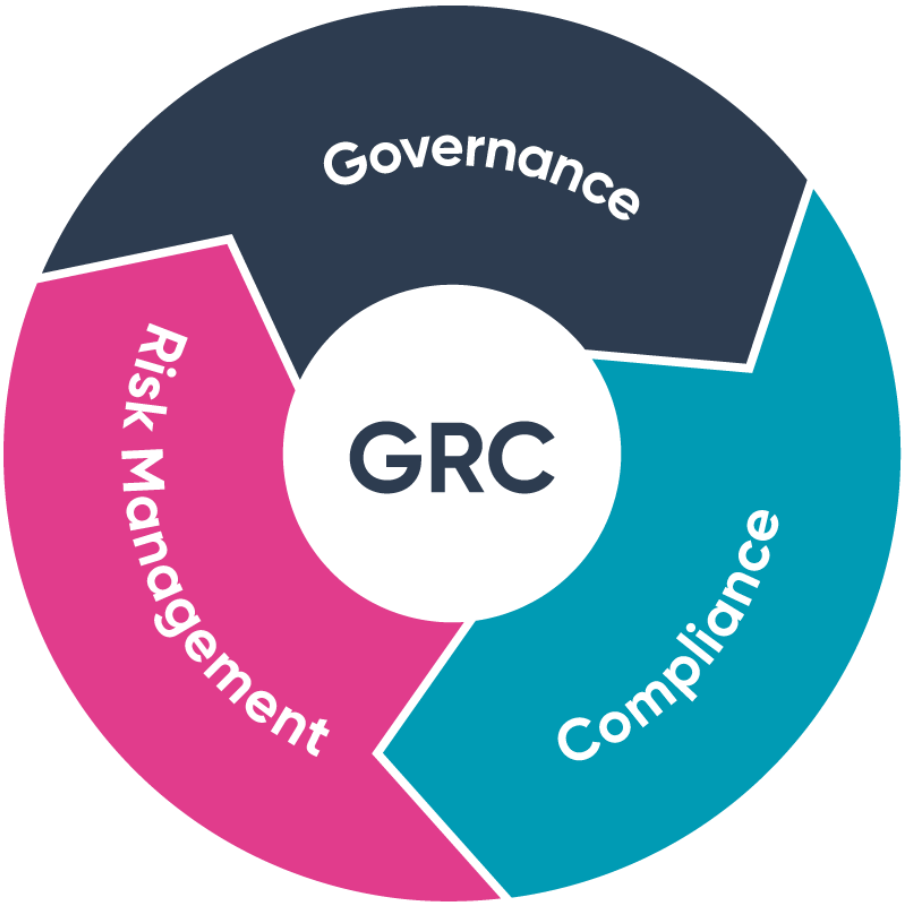
DEL-Cyber

Gouvernance Risque Conformité



1. Compréhension de l'organisation....6
1.1 Compréhension de l'organisation et de son contexte.... 6
1.1.1. Mission, valeurs, objectifs, stratégie....6
1.1.2. Enjeux internes et externes....6
1.1.3. Analyse SWOT (forces, faiblesses, opportunités, menaces).... 6
1.2 Compréhension des besoins et attentes des parties intéressées....8
1.2.1 Parties internes.... 8
1.2.2 Parties externes.... 8
1.2.3 Attentes et exigences principales....9
1.3 Détermination du périmètre du SMSI....9
1.3.1 Activités couvertes par le SMSI....9
1.3.2 Systèmes, sites et processus inclus....9
1.3.3 Exclusions et justification.... 10
1.3.4 Enoncé du domaine d'application du SMSI....10
1.4 Système de management de la sécurité de l'information....10
2. Leadership.... 10
2.1 Engagement de la direction....10
2.2 Politique de sécurité de l'information....11
2.3 Rôles, responsabilités et autorités....11
3. Inventaire des actifs.... 12
3.1 Liste des actifs primordiaux....12
3.2 Liste des actifs supports....13
3.3 Cartographie....14
4. Analyse de risque....15
4.1. Atelier 1 : Cadrage et socle de sécurité.... 16
4.1.1 Identification des valeurs métiers.... 16
4.1.2.Les événements redoutés associés aux valeurs métiers....17
4.1.3 Détermination du socle de sécurité.... 19
4.2 Atelier 2 : Sources de risques / Objectifs visés.... 20
4.3 Atelier 3 : Scénarios stratégiques....21
4.3.1. Les parties prenantes....22
4.3.2. Tableau d'évaluation du niveau de menace de chaque partie prenante..... 22
4.3.3. Représentation de la cartographie des menaces....23
4.3.4 Scénario stratégiques avec chemins d'attaques....24
4.4. Atelier 4 : Scénarios opérationnels....24
4.4.1. Echelle de probabilité de succès et de difficulté....25
4.4.2 Mode opératoire des Scénarios opérationnels....26
4.4.3. Tableau de vraisemblance des différents modes opératoires.... 30
4.5. Atelier 5 : Traitements des risques....31
4.5.1. Echelle d'évaluation des risques.... 31
4.5.2. Liste des risques.... 31
4.5.2. Le niveau des risques initiaux.... 32

4.5.3. Plan de traitement du risque (anciennement PACS)..... 32
4.5.4. Calcul des risques résiduels après application du PACS..... 34
4.5.6. Le niveau des risques résiduels :..... 38
5. Checklist de conformité ISO 27001..... 39
6. Propositions d'amélioration : PSSI, chartes, journalisation centralisée..... 41
6.1. Résumé du PTR..... 41
6.2. Proposition d'amélioration de la Politique de sécurité du système d'information..... 41
6.3. Mise en place d'une charte informatique..... 42
7. Plan de sauvegarde quotidien chiffré local + cloud..... 43
7.1. Portée de la Sauvegarde..... 43
7.2. La fréquence des sauvegardes..... 43
7.3. Le lieu de stockage et les supports de sauvegarde..... 44
7.4. Convention de Nommage..... 45
7.5. Politique de Rétention..... 45
7.6. Gestion des Accès..... 46
7.7. Vérification et Contrôle..... 46
8. PRA : restauration AD + serveur web..... 47
8.1. Analyse d'impact..... 47
8.2. Les stratégies de reprise..... 48
8.3. Les plans d'urgence..... 49
8.3.1. Responsabilités avec leurs actions..... 49
8.3.2. Timeline..... 50
8.4. Formation et sensibilisation..... 51
8.4.1. Formation..... 51
8.4.2 Sensibilisation..... 51
9. Tests de restauration à programmer mensuellement..... 52
9.1 Les rôles et responsabilités des participants..... 52
9.2. Les objectifs et la fréquence des exercices..... 53
9.3. Périmètre du plan..... 53
9.4. L'ensemble des risques à gérer..... 53
9.5. Ressources requises pour être efficace..... 54
9.6. Compétence des personnes qui participent à la campagne d'exercices..... 54
9.7. Rapports sur la réalisation des exercices et tests..... 54
9.8 Validation par la hiérarchie..... 54
10. Estimation des coûts (logiciels, stockage, personnel)..... 55
11. Plan de réponse aux incidents..... 57
11.1. Schéma de plan de gestion d'incident..... 57
11.2. Schéma de plan de réponse à incident..... 58
11.3. Préparation..... 58
11.4. Identification..... 61
11.5. Confinement..... 62
11.6. Remédiation..... 63
11.7. Récupération..... 64
11.8. Capitalisation et apprentissage..... 64

12. Rapport d’analyse post-incident....65
12.1. Description de l’incident....65
12.2. Déroulement des faits :....65
12.3. Origine du problème....66
12.4. Indicateurs de compromissions....66
12.5. Actifs supports impactés....66
12.6. Impacts sur l’entreprise....67
12.7. Identification des Vulnérabilités....67
12.8. Catégorisation et timeline de l’incident....67
12.9. Composants/actifs concernés....67
12.10. Auteur impliqué....68
12.10.1. Description de l'auteur....68
12.10.2. Motivation réelle ou perçue....68
12.11. Résolution de l'incident : Actions menées....68
12.11.1. Confinement....68
12.11.2. Protection des preuves....68
12.11.3. Éradication....68
12.11.4. Récupération....69
12.11.5. Personnes/entités notifiées....69
12.12.Conclusion....69
13. Plan de communication de crise....69
13.1 Objectif....69
13.2 Déclenchement du plan....70
13.3 Chaîne de notification interne....70
13.3.1 Priorisation des notifications....70
13.3.2 Processus de notification....70
13.4 Canal de communication....71
13.5 Responsabilités clés....71
13.6 Modèle de notification interne....71
13.7 Modèle de notification externe (partenaires, clients, fournisseurs)....72
13.8. Notification des Autorités....72

Introduction

Iron4Software est une TPE spécialisée dans le développement de logiciels innovants. L’entreprise dispose d’une infrastructure informatique composée de serveurs Linux et Windows, d’un accès VPN permettant aux employés de travailler à distance et d’un serveur web exposé à Internet. Consciente des risques croissants liés à la cybersécurité et souhaitant répondre aux exigences de la norme ISO 27001, Iron4Software a engagé une démarche visant à renforcer la sécurité de son système d’information.

Cette initiative poursuit plusieurs objectifs : identifier les vulnérabilités existantes au sein de l'infrastructure, mettre en œuvre des mesures de sécurisation adaptées, instaurer un système de surveillance des incidents et garantir la confidentialité, l'intégrité et la disponibilité des informations. Elle doit également permettre à l'entreprise de se conformer aux bonnes pratiques de gestion de la sécurité de l'information et de renforcer la confiance de ses clients et partenaires.

Pour mener à bien ce projet, Iron4Software s'appuie sur l'expertise de Del-Cyber. Le rôle de Del-Cyber consiste à réaliser un audit de sécurité complet, à analyser les risques liés aux actifs critiques, à proposer et mettre en place des mesures correctives et préventives, ainsi qu'à accompagner l'entreprise dans le déploiement d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO 27001.

1. Compréhension de l’organisation

1.1 Compréhension de l’organisation et de son contexte

Exigence de la norme : Conformément à l’ISO/IEC 27001:2022 (§4.1), l’organisation doit déterminer les enjeux internes et externes pertinents qui influencent sa capacité à atteindre les résultats attendus de son SMSI.

1.1.1. Mission, valeurs, objectifs, stratégie

La mission d’Iron4Software est de concevoir et de développer des solutions logicielles innovantes et évolutives, adaptées aux besoins spécifiques de ses clients.

L’entreprise valorise sa capacité à s’adapter rapidement aux besoins des clients ainsi qu’aux évolutions technologiques.

Iron4Software vise à accroître la valeur perçue par ses clients en leur offrant des solutions logicielles performantes et sécurisées. L’entreprise ambitionne également de devenir le numéro un du développement et du conseil logiciel à Montpellier.

La stratégie repose sur la mise en place d’un Système de Management de la Sécurité de l’Information (SMSI), qui constitue un socle de gouvernance. Elle inclut également l’industrialisation des bonnes pratiques de développement sécurisé, telles que le DevSecOps, les tests automatisés et l’intégration continue (CI/CD).

1.1.2. Enjeux internes et externes

Les enjeux internes concernent le développement de logiciels innovants et évolutifs avec des équipes réactives, tout en accompagnant la forte croissance de l’entreprise et la montée en compétence en sécurité informatique. Ces défis doivent être relevés malgré l’existence de bugs et un manque de structuration générale.

Les enjeux externes portent sur l’adaptation aux évolutions réglementaires et légales, sur la concurrence vieillissante et sur l’opportunité offerte par la norme ISO 27001 pour renforcer la confiance des clients et accéder à de nouveaux marchés. Ils incluent également la nécessité d’anticiper la réaction de concurrents comme Calamar5Software, de pallier le manque de veille sur les changements imprévus, ainsi que de répondre aux exigences réglementaires concernant le traitement des données.

1.1.3. Analyse SWOT (forces, faiblesses, opportunités, menaces)

Dans le cadre de son accompagnement, Del-Cyber a assisté Iron4Software afin de procéder à une analyse SWOT approfondie. Cette analyse a pour objectif d’évaluer

la posture actuelle de l'entreprise en matière de sécurité de l'information et d'identifier les principaux axes d'amélioration.

Les résultats mettent en évidence les forces et faiblesses internes, ainsi que les opportunités et menaces externes pouvant influencer la capacité d'Iron4Software à atteindre et à maintenir la conformité avec la norme ISO 27001.

Cette démarche stratégique fournit une vision globale du contexte de l'organisation et constitue un élément essentiel pour définir, déployer et améliorer en continu le Système de Management de la Sécurité de l'Information (SMSI).

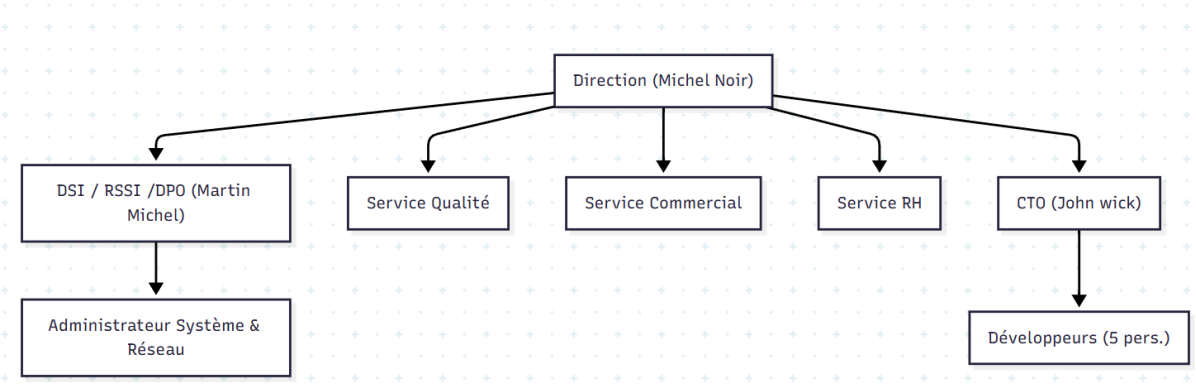
Forces	Faiblesses
Logiciels jeunes et innovants Concurrence vieillissante Réactivité des équipes Logiciels très scalables L'entreprise est en forte croissance	Culture sécurité de l'information faible Logiciel en construction, bugs présents Manque de structure générale Manque de veille sur les changements
Opportunités	**Menaces**
Évolutions réglementaires et légales L'ISO 27001 est gage de confiance pour les clients (sécurité et fiabilité). Possibilité de **répondre à de nouveaux appels d'offres** exigeant ISO 27001.	Réaction de la concurrence (Calamar5Software) Évolutions subies et non anticipées Exigences réglementaires sur les données traitées, évolutions de la réglementation

1.2 Compréhension des besoins et attentes des parties intéressées

Exigence de la norme : Conformément à l'ISO/IEC 27001:2022 (§4.2), l'organisation doit identifier les parties intéressées pertinentes ainsi que leurs besoins et exigences en matière de sécurité de l'information.

1.2.1 Parties internes

- **La direction (Michel Noir)** attend du SMSI qu'il soutienne la stratégie globale et assure l'engagement de l'entreprise vers la conformité ISO 27001.
- **Le DSI / RSSI / DPO (Martin Michel)** est responsable de la gestion du SMSI, de l'appréciation des risques et du reporting.
- **Le CTO (John Wick)** est responsable des développeurs.
- **Les développeurs (5 personnes)** doivent appliquer les bonnes pratiques de développement sécurisé (DevSecOps, tests, CI/CD).
- **L'administrateur système & réseau** est chargé de sécuriser les serveurs Linux/Windows, le VPN et le réseau interne.
- **Le service qualité** gère les demandes d'amélioration et de correction des clients.
- **Le service commercial** exige la confidentialité des informations contractuelles et CRM.
- **Le service ressource humaine** doit veiller à la conformité RGPD concernant les données personnelles des employés.



1.2.2 Parties externes

- **Les clients** (Cabinet Roux, Boulangerie Leroy, Vignobles Rousseau, Hôtel du Languedoc, Tech Montpellier) attendent des solutions fiables et sécurisées, respectant le RGPD et les engagements contractuels.

- Les **prestataires** (Vendame (comptabilité), Molo (ménage), salesforceOne (CRM) ,DELCYBER (consultant cyber et gouvernance) doivent respecter des

exigences spécifiques, notamment la confidentialité des données et le respect des règles de sécurité internes.

- **Les autorités et organismes réglementaires** imposent le respect du RGPD, de la LCEN et du Code de la consommation.

1.2.3 Attentes et exigences principales

De façon générale, les parties intéressées attendent la protection de la confidentialité, de l'intégrité et de la disponibilité des informations, le respect des exigences légales, réglementaires et contractuelles, ainsi qu'une communication claire et transparente en cas d'incident.

1.3 Détermination du périmètre du SMSI

Exigence de la norme : Conformément à l'ISO/IEC 27001:2022 (§4.3), l'organisation doit définir les limites et l'applicabilité de son SMSI, en précisant les activités couvertes, les systèmes, sites et processus inclus, ainsi que les exclusions dûment justifiées.

1.3.1 Activités couvertes par le SMSI

Le SMSI d'Iron4Software couvre les activités suivantes :

- conception et développement de logiciels innovants et évolutifs (applications web et mobiles) ;
- infogérance et maintenance applicative ;
- gestion et protection des données clients dans le cadre des projets logiciels.

1.3.2 Systèmes, sites et processus inclus

Sont inclus dans le périmètre du SMSI :

- les serveurs **Linux** et **Windows**, dont le serveur Active Directory Windows 2019 et le serveur Ubuntu exposé à Internet
- l'infrastructure réseau (firewall PFSense, switchs, borne Wi-Fi)
- les **postes de travail** : 15 postes fixes Windows 10 et 5 laptops commerciaux
- les applications critiques :
    - CRM en mode SaaS,
    - messagerie **Office 365**,
    - logiciel interne de gestion de projet
- le **site de Montpellier**, incluant les locaux, bureaux et salles serveurs
- les processus organisationnels : développement (DevSecOps, CI/CD), administration système, support client, gestion RH et commerciale.

1.3.3 Exclusions et justification

Sont exclus du périmètre du SMSI :

- les services externes de ménage (prestataire Molo)

Ces exclusions sont justifiées car elles n'ont pas d'impact direct sur la sécurité de l'information ni sur la protection des actifs critiques de l'entreprise.

1.3.4 Enoncé du domaine d'application du SMSI

Le SMSI d'Iron4Software couvre la conception, le développement, le déploiement, la maintenance de solutions logicielles, la gestion et la protection des données clients, l'infogérance, le support client, ainsi que l'infrastructure informatique et le site de Montpellier. Ce périmètre assure la confidentialité, l'intégrité et la disponibilité des informations selon la norme ISO/IEC 27001:2022.

1.4 Système de management de la sécurité de l'information

Iron4Software a décidé de mettre en place un **Système de Management de la Sécurité de l'Information (SMSI)** afin de protéger ses actifs informationnels et d'intégrer la sécurité au cœur de sa gouvernance.

L'**objectif global du SMSI** est d'instaurer un gage de confiance pour les clients et partenaires, de permettre à l'entreprise de répondre à des appels d'offres exigeant la certification ISO 27001 et d'aligner la sécurité sur sa stratégie d'innovation et de performance logicielle.

Le SMSI est déployé conformément aux **exigences de la norme ISO 27001**, ainsi qu'aux obligations légales et réglementaires applicables, notamment le RGPD.

Enfin, Iron4Software s'engage à une démarche d'**amélioration continue** de son SMSI, fondée sur le cycle PDCA (Planifier – Déployer – Contrôler – Améliorer), intégrant les résultats des audits internes, des revues de direction, des retours d'expérience et des évolutions du contexte interne et externe.

2. Leadership

2.1 Engagement de la direction

Exigence de la norme : Conformément à l'ISO/IEC 27001:2022 (§5.1), la direction doit démontrer son leadership et son engagement envers le SMSI en intégrant la sécurité

de l’information dans les processus de l’organisation et en fournissant les ressources nécessaires.

La direction d’Iron4Software reconnaît l’importance stratégique de la sécurité de l’information dans la continuité et le développement de ses activités. Elle s’engage à fournir les ressources nécessaires, à soutenir la mise en place du SMSI et à veiller à son efficacité. Cet engagement se traduit par :

- l’intégration des exigences de sécurité de l’information dans les processus métier ;
- la communication régulière de l’importance de la sécurité auprès des collaborateurs et partenaires ;
- la participation active aux revues de direction ;
- la promotion de l’amélioration continue du SMSI.

2.2 Politique de sécurité de l’information

Exigence de la norme : Conformément à l’ISO/IEC 27001:2022 (§5.2), la direction doit établir une politique de sécurité de l’information adaptée, communiquée, comprise et appliquée.

Iron4Software s’engage à établir, documenter, mettre en œuvre et communiquer une **Politique de Sécurité de l’Information (PSI)**. Cette politique définit les orientations et objectifs généraux en matière de sécurité, notamment :

- garantir la confidentialité, l’intégrité et la disponibilité de l’information
- respecter les exigences légales, réglementaires et contractuelles
- protéger les actifs critiques de l’entreprise
- sensibiliser et responsabiliser l’ensemble des collaborateurs

La politique sera approuvée par la direction et communiquée à toutes les parties concernées. Elle sera revue périodiquement pour rester adaptée au contexte de l’entreprise.

2.3 Rôles, responsabilités et autorités

Exigence de la norme : Conformément à l’ISO/IEC 27001:2022 (§5.3), l’organisation doit attribuer et communiquer clairement les rôles et responsabilités relatifs au SMSI.

La direction d'Iron4Software désigne un **Responsable de la Sécurité de l'Information (RSI / Lead SMSI)**, chargé de coordonner la mise en œuvre et le suivi du SMSI.
Les responsabilités sont réparties comme suit :

- **La direction générale Michel Noir** : pilotage stratégique et validation des décisions majeures

- **Le lead SMSI et RSSI Martin Michel**: mise en œuvre opérationnelle, suivi des mesures de sécurité, reporting à la direction.

- **Les managers** (CTO, administration systèmes, commercial, RH) : application des mesures dans leur périmètre respectif.

- **Tous les employés** : respect des règles de sécurité et signalement des incidents.

Ces rôles et responsabilités seront formalisés dans la documentation du SMSI et communiqués à l'ensemble du personnel.

3. Inventaire des actifs

3.1 Liste des actifs primordiaux

L'organisation propose plusieurs biens et services essentiels à ses activités, notamment :

- le développement de sites web ;
- la conception et le déploiement d'applications mobiles (iOS et Android) ;
- la vente de solutions web personnalisées ;
- les services d'infogérance destinés aux clients.

Pour soutenir ces prestations, plusieurs actifs informationnels primordiaux sont mobilisés :

- les bases de données contenant la liste des clients ;
- les bases de données associées aux sites web hébergés ;
- le code source des sites web hébergés ;
- le code source des applications mobiles ;
- les processus métiers relatifs à la conception et à la livraison des programmes.

Ces actifs constituent le cœur de l'activité et doivent faire l'objet d'une protection particulière dans le cadre du SMSI.

3.2 Liste des actifs supports

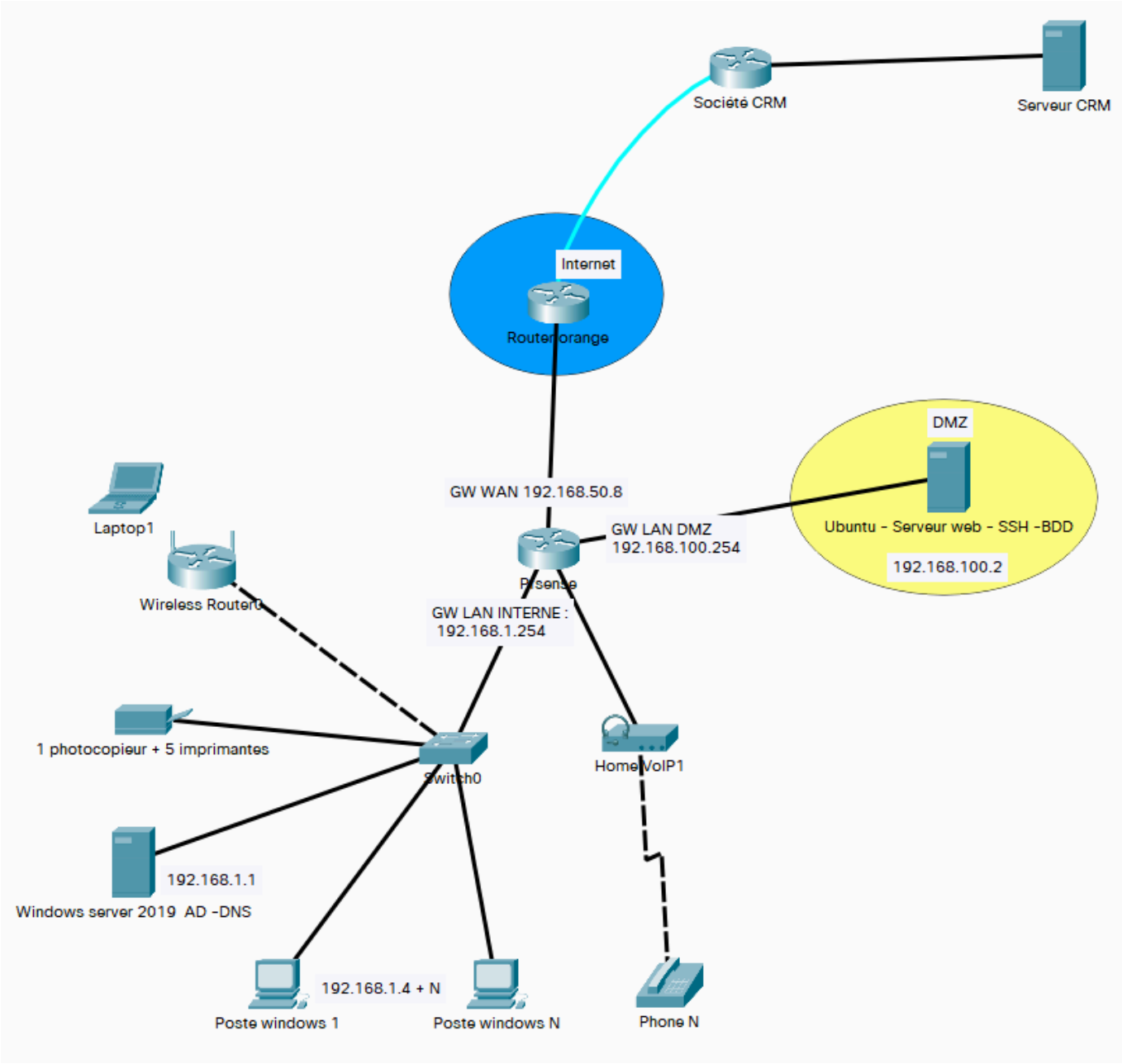
Afin d'assurer la continuité et la réalisation des services proposés, l'organisation s'appuie sur plusieurs actifs supports :

- **Ressources humaines** : l'ensemble du personnel.
- **Infrastructures physiques** : le local de bureau situé au centre-ville de Montpellier.
- **Infrastructures techniques** :
    - un serveur de bases de données mutualisé hébergeant l'ensemble des données des sites web
    - un serveur **Active Directory** sous Windows Server 2019
    - quinze postes de travail fixes sous Windows 10
    - cinq ordinateurs portables mis à disposition des commerciaux
    - une borne Wi-Fi
    - un pare-feu **pfSense**
    - un switch 48 ports et le câblage réseau associé
    - un photocopieur et cinq imprimantes
    - un système téléphonique PABX + les téléphones associés.
    - un NAS

- **Logiciels et applications** :
    - un logiciel CRM en mode SaaS pour la gestion de la relation client Iron4Software)
    - un logiciel interne de gestion de projet développé par Iron4Software
    - une solution de messagerie électronique en mode SaaS (Microsoft Office 365).
    - Teams pour la communication interne directe.

Ces actifs supports constituent l'environnement nécessaire au bon fonctionnement et à la sécurisation des actifs primordiaux identifiés précédemment.

3.3 Cartographie

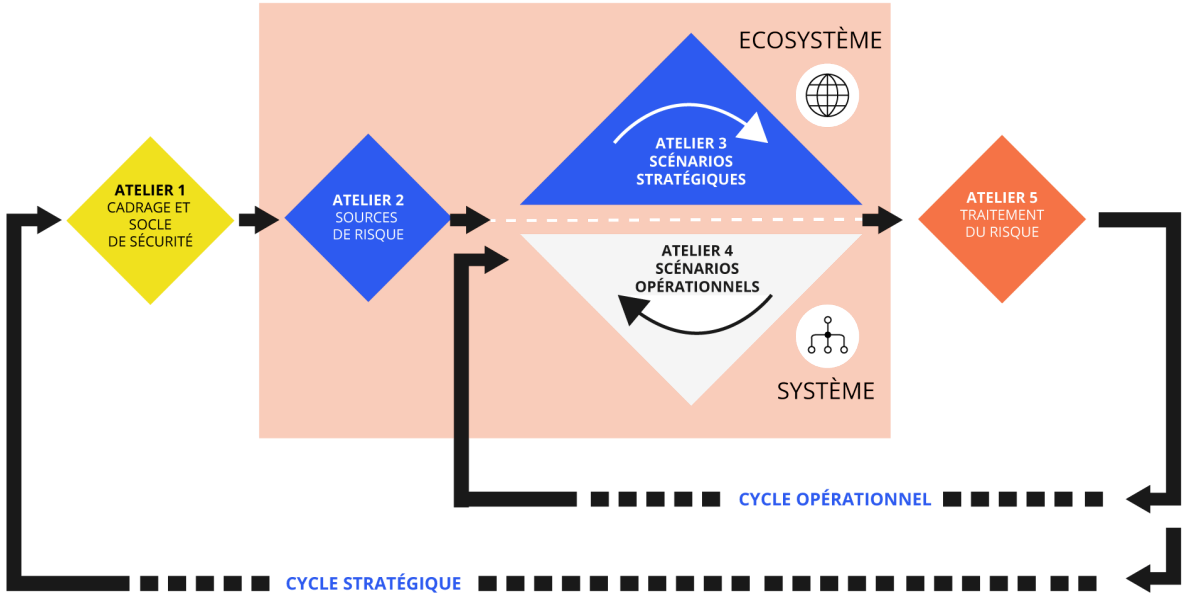


Liste des réseaux :

192.168.1.0/24	LAN
192.168.100.0/24	DMZ
192168.50.0/24	WAN

4. Analyse de risque

Pour évaluer et traiter les menaces sur les actifs numériques d'Iron4Software, nous utilisons la méthode EBIOS RM. Cette approche permet d'identifier les valeurs métiers, les sources de risques et les scénarios d'attaque, afin de définir des mesures de sécurité adaptées et de gérer efficacement les risques.



4.1. Atelier 1 : Cadrage et socle de sécurité

4.1.1 Identification des valeurs métiers

Mission : Développer des sites web et des applications mobiles

Dénomination de la valeur métier	Description	Entité / responsable	Biens supports associés
Développement des sites web et applications	-Conception, développement et tests des sites web et applications mobiles pour les clients. Gestion du cycle de vie des projets (planification, versioning, déploiement). -Maintenance corrective et évolutive des solutions livrées. -Documentation technique et gestion des dépendances logicielles.	CTO	- Développeurs (CTO Chief Technology Officer) - Infrastructure essentielle au développement située à Montpellier (DSI) - Logiciel interne de gestion de projet développé par Iron4Software (DSI)
Maintien opérationnel et sécurité des services web	- Supervision et réponse aux incidents de sécurité. -Hébergement sécurisé des applications et sites web sur serveurs Linux/Windows. -Surveillance de la disponibilité, des performances et des sauvegardes. Mise en œuvre de la protection des données des clients.	DSI	- Infrastructure IT liée à l'infogérance située à Montpellier (DSI) - Pare-feu (Administrateur système & réseau) - Outils de supervision SPLUNK (Administrateur système & réseau) - Outils de sauvegarde (Administrateur système & réseau)
Code source de nos applications et sites web	-Ensemble des fichiers, scripts et bibliothèques composant les produits développés. Contient la logique métier, les algorithmes et la propriété intellectuelle de l'entreprise.	CTO	-Serveur de production et dépôt Git sécurisé (CTO, DSI) -Logiciel de développement permettant l'accès, la lecture et la modification du code source (DSI)
Données clients	-Regroupement des données personnelles et commerciales des clients (coordonnées, projets, contrats, factures). Sert à la gestion de la relation client, au suivi des projets et à la facturation. -Contient des données sensibles relevant de la confidentialité (RGPD).	DPO	- Logiciel SAAS CRM (Responsable du service commercial, DPO) - Serveur hébergeant les données clients en SAAS (Sous-traitant)

4.1.2.Les événements redoutés associés aux valeurs métiers

Nous utiliserons l'échelle de gravité suivante pour mesurer le niveau des impacts.

ÉCHELLE	CONSÉQUENCES
G4 Critique	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 Grave	Fortes dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G2 Significative	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 Mineure	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

Valeur métier	Événement redouté	Impacts principaux	Gravité
Développement des sites web et applications	Indisponibilité du dépôt Git	Interruption du service de déploiement, pénalité de retard, financier.	3
	Départ ou indisponibilité d'un développeur clé sans transfert de connaissance	Qualité des livrables en danger,risque réputationnel, retard du développement	2

Valeur métier	Événement redouté	Impacts principaux	Gravité
Maintien opérationnel et sécurité des services web	Indisponibilité des services web (ex. panne serveur, attaque par déni de service - DDoS)	Financier, perte de temps, Juridique, risque réputationnel	2
	Altération ou compromission des configurations serveur et des mécanismes de sécurité (suite à un ransomware)	Opérationnel (chômage technique), perte de temps, financier	4

Valeur métier	Événement redouté	Impacts principaux	Gravité
Code source des applications et sites web	Vol ou fuite du code source vers des tiers non autorisés	Perte de propriété intellectuelle, risque de copies frauduleuses, perte d'avantage concurrentiel	3

Valeur métier	Événement redouté	Impacts principaux	Gravité
Données clients	Divulgation non autorisée des données clients (vol, fuite, accès illégal)	Juridique CNIL, image, réputation	3
	Perte complète des données clients	Réputation, opérationnel	3

4.1.3 Détermination du socle de sécurité

Type de référentiel	Nom du référentiel	État d'application
Règles d'hygiène informatique et bonnes pratiques	Guide d'hygiène informatique de l'ANSSI	Appliqué avec restrictions
Norme de sécurité des systèmes d'information	ISO 27001	En cours de déploiement
Légal et contractuel	Loi française, clauses contractuelles sécurité	Appliqué
Finance	Loi de finance	Appliqué
Légal	LCEN Loi pour la Confiance dans l'Économie Numérique	Appliqué
Guide de bonnes pratiques	Guide Nomadisme Numérique ANSSI	Absente
Politique interne	Politique interne de sécurité du SI (PSSI)	Absente
	Politique de continuité d'activité (PCA/PRA)	En cours
	Politique de gestion des mises à jour (Patch Management)	Absente
	Politique de gestion des postes de travail	Absente
	Politique de sauvegarde et de restauration	En cours
	Politique de gestion des incidents	Absente
	Politique de journalisation et supervision	En cours
	Politique de gestion des accès et des identités	Absente
Juridique et réglementaire	Code de la consommation	Appliqué
Protection des données personnelles	Règlement Général sur la Protection des Données	En cours
Bonnes pratiques de développement sécurisé	OWASP Top 10 + pratiques internes	Appliqué
Bonnes pratiques de développement mobile	OWASP Mobile Security Testing Guide	Appliqué

4.2 Atelier 2 : Sources de risques / Objectifs visés

Nous utiliserons l'échelle de pertinence suivante pour prioriser nos couples SR/OV.

Matrice de pertinence		RESSOURCES				
		Incluant les ressources financières, le niveau de compétences cyber, l'outillage, le temps dont l'attaquant dispose pour réaliser l'attaque, etc.				
			1. Ressources limitées	2. Ressources significatives	3. Ressources importantes	4. Ressources illimitées
MOTIVATION	Intérêts, éléments qui poussent la source de risque à atteindre son objectif	4. Fortement motivée	Moyennement pertinent	Plutôt pertinent	Très pertinent	Très pertinent
		3. Assez motivée	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent	Très pertinent
		2. Peu motivée	Peu pertinent	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent
		1. Très peu motivée	Peu pertinent	Peu pertinent	Moyennement pertinent	Moyennement pertinent

Nous avons identifié **6 sources de risques principales** menaçant la sécurité de l'information de l'entreprise :

ID	Source de risque	Objectif visé	Motivation	Ressources	Pertinence
SR1	Concurrents déloyaux (Calamar5Software)	Espionnage industriel pour voler le code source des applications	3	3	Plutôt pertinent
SR2		Voler le portefeuille client	3	3	Plutôt pertinent
SR3	Script kiddies (hacker néophyte)	S'amuser en essayant de rendre les sites webs inaccessibles	2	1	Peu pertinent
SR4	Employé malveillant	Lucratif : Revente des données personnelles clients	2	4	Plutôt pertinent
SR5	Vengeur (salarié licencié)	Se venger via le sabotage des sites webs et applications	3	3	Plutôt pertinent
SR6	Cybercriminels organisés	Lucratif : Récupérer une rançon via ransomware	3	3	Plutôt pertinent

Toutes les sources de risques seront traitées pour la suite de l'étude.

4.3 Atelier 3 : Scénarios stratégiques

Nous utiliserons la métrique de cotation des parties prenantes suivantes pour évaluer leur niveau de menace.

Dépendance stratégique	**Pénétration**	**Maturité cyber**	**Confiance**
1 : Relation non nécessaire aux fonctions stratégiques.	Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, téléphone mobile, etc.).	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées.
2 : Relation utile aux fonctions stratégiques.	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
3 : Relation indispensable mais non exclusive.	Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation certains risques.	Les intentions de la partie prenante sont connues et probablement positives.
4 : Relation indispensable et unique (pas de substitution possible à court terme).	Accès avec privilèges de type administrateur à des équipements d'infrastructure (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles sécurisées de l'organisation.	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et assurée de manière proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.

4.3.1. Les parties prenantes

Les parties prenantes que nous avons sélectionnées sont les suivantes :

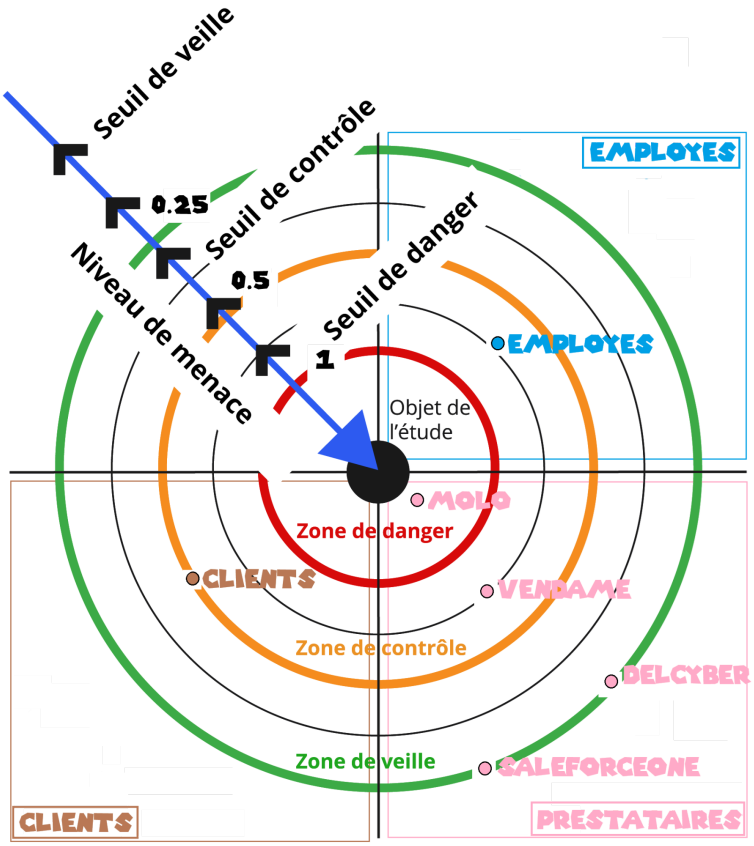
- ➢ Employés
- ➢ Les clients (Cabinet Roux, Boulangerie Leroy, Vignobles Rousseau, Hôtel du Languedoc, Tech Montpellier).
- ➢ Prestataire Vendame (comptabilité)
- ➢ Prestataire Molo (ménage)
- ➢ Prestataire salesforceOne (CRM)
- ➢ Prestataire DEL-CYBER
- ➢ Les autorités et organismes réglementaires

4.3.2. Tableau d'évaluation du niveau de menace de chaque partie prenante

Niveau de menace = (Dépendance stratégique * Pénétration) / (Maturité Cyber * Confiance)

Catégorie	Partie prenante	Dépendance	Pénétration	Maturité cyber	Confiance	Niv.
Société Iron4Software	E1 - Employés	1	4	2	3	0.667
Clients	C1 - Cabinet Roux, Boulangerie Leroy, Vignobles Rousseau, Hôtel du Languedoc, Tech Montpellier ...	1	1	1	2	0.5
Prestataires	P1 - SalesforceOne	3	1	4	3	0.25
	P2 - DEL-CYBER	1	4	4	4	0.25
	P3 - Vendame	3	1	1	4	0.75
	P4 - Molo	1	4	1	2	2

4.3.3. Représentation de la cartographie des menaces



Zone de danger	Niveau de menace très élevé et inacceptable !
Zone de contrôle	Niveau de menace élevé mais tolérable sous contrôle
Zone de veille	Niveau de menace faible et acceptable en l'état

4.3.4 Scénario stratégiques avec chemins d'attaques

Source de risque	Objectif visé	Gravité	Ecosystème (Chemin d'attaque)	Iron4software
SR1 : Concurrent (Calamar5Software)	Espionnage industriel pour voler le code source des applications	3	INDIRECT : Corruption d'un employé de **MOLO** DIRECT : Intrusion sur le dépôt GIT via exploitation d'une faille de vulnérabilité	Code source des applications et sites webs
SR2 : Concurrent (Calamar5Software)	Voler le portefeuille client	3	INDIRECT : Ingénierie sociale sur un des employés afin d'obtenir un accès au CRM DIRECT : Intrusion dans le CRM via brute-force	Liste des clients
SR3 : Script kiddies (hacker néophyte)	S'amuser en essayant de rendre les sites webs inaccessibles	2	INDIRECT : Aucun DIRECT : Attaque DDOS pour rendre indisponible les sites web	Maintien opérationnel et sécurité des services web
SR4 : Employé malveillant	Lucratif : Revente des données personnelles clients	3	DIRECT : Connexion au CRM non autorisé et exfiltration des données INDIRECT : Exfiltration des données grâce à une complicité avec un autre employé	Liste des clients
SR5 : Vengeur (salarié licencié)	Se venger via le sabotage des sites webs et applications	4	DIRECT : Altération du dépôt du code source INDIRECT : Compromission d'un client	Développement des sites web et applications
SR6 : Cybercriminels organisés	Lucratif : Récupérer une rançon via ransomware	4	DIRECT : Exploitation d'une faille de vulnérabilité sur le site web INDIRECT : Introduction par phishing sur un des employés	Maintien opérationnel et sécurité des services web

4.4. Atelier 4 : Scénarios opérationnels

4.4.1. Echelle de probabilité de succès et de difficulté

Nous utiliserons l'échelle de probabilité de succès et l'échelle de difficulté technique suivante afin d'évaluer le niveau de vraisemblance.

ÉCHELLE DE PROBABILITÉ DE SUCCÈS D'UNE ACTION ÉLÉMENTAIRE	
NIVEAU DE L'ÉCHELLE	**DESCRIPTION**
4 - QUASI-CERTAIN	Probabilité de succès quasi-certaine > 90%
3 - TRÈS VRAISEMBLABLE	Probabilité de succès très élevée > 60%
2 - VRAISEMBLABLE	Probabilité de succès significative > 20%
1 - PEU VRAISEMBLABLE	Probabilité de succès faible < 20%

ÉCHELLE DE DIFFICULTÉ TECHNIQUE D'UNE ACTION ÉLÉMENTAIRE	
NIVEAU DE L'ÉCHELLE	**DESCRIPTION**
4 - TRÈS ÉLEVÉE	**Difficulté très élevée :** l'attaquant engagera des ressources très importantes pour mener à bien son action
3 - ÉLEVÉE	**Difficulté élevée :** l'attaquant engagera des ressources importantes pour mener à bien son action
2 - MODÉRÉE	**Difficulté modérée :** l'attaquant engagera des ressources significatives pour mener à bien son action
1 - FAIBLE	**Difficulté faible :** les ressources engagées par l'attaquant seront faibles

4.4.2 Mode opératoire des Scénarios opérationnels

Soit **Pr** : probabilité de succès , Soit **Diff** : difficulté technique

Scénario stratégique 1 : Calamar5Software souhaite voler le code source des applications **Gravité : 3**					
Connaître	**Rentrer**	**Trouver**	**Exploiter**	**Pr**	**Diff**
INDIRECT **MO1 :** Reconnaissance externe sources ouvertes **Pr :** 3(3) **Diff :** 2(2)	Corruption du prestataire Molo, fourniture d'un Rubber Ducky **Pr :** 2(2) **Diff :** 2(2)	——————▶	-Plug de la clé sur le réseau **Pr :** 4(2) **Diff :** 1(2) ▼ -Récupération du code source du serveur de production et dépôt Git sécurisé. **Pr :** 3(2) **Diff :** 2(2)	2	2
DIRECT **MO2 :** Reconnaissance externe sources ouvertes **Pr:** 3(3) **Diff :** 2(2)	Exploitation d'une faille sur un des sites webs **Pr :** 2(2) **Diff :** 3(3)	-Recherche sur le réseau -Latéralisation et connexion à distance le serveur GIT local **Pr :** 3(2) **Diff :** 3(3)	-Exfiltration du code source **Pr :** 3(2) **Diff :** 2(3)	2	3

Scénario stratégique 2 : Calamar5Software souhaite voler le portefeuille client d'Iron4Software.
Gravité : 3

Connaître	Rentrer	Trouver	Exploiter	Pr	Diff
DIRECT **MO3 :** Reconnaissance externe sources ouvertes **Pr :** 3(3) **Diff :** 2(2)	Intrusion dans le CRM via brute-force **Pr :** 2(2)**Diff :** 3(3)	——————▶	-Exfiltration des données d'accès (compte et mot de passe) **Pr :** 4(2) **Diff :** 1(3) ▼ -Exploitation à distance en utilisant les accès utilisateurs (CRM en saas) **Pr :** 4(2) **Diff :** 1(3)	2	3
INDIRECT **MO4** : Reconnaissance externe sources ouvertes **Pr :** 3(3)**Diff :** 2(2)	Appel téléphonique en se faisant passer pour le prestataire du CRM auprès d'un employé et demande des identifiants CRM **Pr :** 2(2) **Diff :** 2(2)	——————▶	-Exploitation à distance en utilisant les accès utilisateurs (CRM en saas) **Pr :** 4(2)**Diff :** 1(2)	2	2

Scénario stratégique 3 : Un hacker néophyte essaye de rendre les sites webs inaccessibles
Gravité : 2

Connaître	Rentrer	Trouver	Exploiter	Pr	Diff
DIRECT **MO5** : Reconnaissance basique de l'adresse IP publique et du nom de domaine des sites Iron4Software **Pr :** 4(4) **Diff :** 1(1)	Utilisation d'outils DDoS gratuits **Pr :** 3(3) **Diff :** 1(1)	——————▶	- Lancement de l'attaque DDoS HTTP **Pr :** 3(3) **Diff :** 2(2) ▼ - Saturation de la bande passante du serveur web **Pr :** 3(3) **Diff :** 2(2) ▼ - Indisponibilité temporaire des sites web clients **Pr :** 3(3) **Diff :** 2(2)	3	2

Scénario stratégique 4 : Un employé malveillant souhaite revendre les données personnelles des clients.
Gravité : 3

Connaître	Rentrer	Trouver	Exploiter	Pr	Diff
DIRECT **MO6** : fait partie intégrante de l'organisation (connaissance interne) **Pr :** 4(4) **Diff :** 1(1)	Identification avec ses propres identifiants sur le CRM **Pr :** 4(4) **Diff :**1(1)	——————▶	-Exfiltration des données personnelles via messagerie en ligne **Pr :** 4(4)**Diff :** 2(2)	4	2
INDIRECT **MO7** : fait partie intégrante de l'organisation (connaissance interne) **Pr :** 4(4) **Diff :** 1(1)	Complicité d'un commercial **Pr :** 3(3)**Diff :** 1(1)	——————▶	-Exfiltration des données personnelles via messagerie en ligne **Pr :** 4(3)**Diff :** 2(2)	3	2

Scénario stratégique 5 : Un ex employé qui a été licencié veut saboter les sites webs et applications.
Gravité : 4

Connaître	Rentrer	Trouver	Exploiter	Pr	Diff
DIRECT MO8 : faisait partie de l'organisation - **Pr :** 4(4) **Diff :** 1(1)	Dispose d'ancien accès VPN toujours valide **Pr :** 2(2) **Diff :** 2(2)	-Recherche sur le réseau -Latéralisation et connexion à distance le serveur GIT local **Pr :** 3(2) **Diff :** 2(2)	Suppression massive du serveur GIT local via la commande : git push -force - - delete **Pr :** 4(2) **Diff :** 2(2)	2	2
INDIRECT MO9 : faisait partie de l'organisation - **Pr :** 4(4) **Diff :** 1(1)	-Compromission d'un client **Pr :** 2(2) **Diff :** 3(3) ▼ - Transmission du fichier vérolé à Iron4Software **Pr :** 3(2) **Diff :** 1(3)	——————▶	-Propagation automatique du virus sur le réseau **Pr :** 3(2) **Diff :** 2(3) ▼ Suppression et altération de l'ensemble du réseau dont le code source **Pr :** 4(2) **Diff :** 2(3)	2	3

DIRECT **MO10** : faisait partie de l'organisation **Pr :** 4(4) **Diff :** 1(1)	Soirée d'ancien collègue **Pr :** 3(3) **Diff :** 1(1)	Trouver un poste de travail disponible **Pr :** 4(3)**Diff :** 1(1)	Il supprime la branche main du GIT. **Pr :** 3(3) **Diff :** 2(2)	3	2

Scénario stratégique 6 : Un cybercriminel souhaite obtenir de l'argent via l'introduction d'un ransomware. **Gravité : 4**					
Connaître	**Rentrer**	**Trouver**	**Exploiter**	**Pr**	**Diff**
INDIRECT **MO11 :** Reconnaissance externe sources ouvertes **Pr :** 3(3) **Diff :** 2(2)	Intrusion via phishing sur un des employés **Pr :** 2(2) **Diff :** 2(2)	-Latéralisation vers un poste d'administrateur **Pr :** 3(2) **Diff :** 2(2) ↓ -Elévation de privilège **Pr :** 2(2) **Diff :** 3(3)	- Installation d'une Backdoor sur le poste de l'administrateur **Pr :** 4(2) **Diff :** 2(3) ↓ -Exécution du ransomware et cryptage de l'ensemble de serveur de production pour demander une rançon. **Pr :** 4(2) **Diff :** 1(3)	2	3
DIRECT **MO12** : Reconnaissance externe sources ouvertes **Pr :** 3(3) **Diff :** 2(2)	Exploitation d'une faille sur un des sites webs **Pr :** 2(2) **Diff :** 3(3)	-Elévation de privilège **Pr :** 2(2) **Diff :** 3(3)	- Installation d'une Backdoor sur le serveur de production **Pr :** 4(2) **Diff :** 2(3) ↓ -Exécution du ransomware et cryptage de l'ensemble de serveur de production pour demander une rançon. **Pr :** 4(2) **Diff :** 1(3)	2	3

4.4.3. Tableau de vraisemblance des différents modes opératoires

		Difficulté technique			
		4	3	2	1
Probabilité de succès	4			MO6	
	3			MO5 MO7 MO10	
	2		MO2 MO3 MO9 MO11 MO12	MO1 MO4 MO8	
	1				

Légende de vraisemblance des différents modes opératoires

4- Quasi-certain
3- Très vraisemblable
2- Vraisemblable
1- Peu vraisemblable

4.5. Atelier 5 : Traitements des risques

4.5.1. Echelle d'évaluation des risques

Nous utiliserons l'échelle d'évaluation des risques suivante pour évaluer l'acceptabilité du risque.

Niveau de risque	Acceptabilité du risque	Intitulé des décisions et des actions
Faible	Acceptable en l'état	Aucune action n'est à entreprendre.
Moyen	Tolérable sous contrôle	Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d'une amélioration continue sur le moyen et long terme.
Élévé	Inacceptable	Des mesures de réduction du risque doivent être impérativement prises à court terme. Dans le cas contraire, tout ou partie de l'activité sera refusé.

4.5.2. Liste des risques

	Gravité	Vraisemblance	Niveau de risque
R1 : Calamar5Software souhaite voler le code source des applications en corrompant un employé de chez Molo.	**3**	**3**	**9 (Elevé)**
R2 : Calamar5Software souhaite voler le portefeuille client d'Iron4Software grâce à l'ingénierie sociale sur un des employés.	**3**	**3**	**9 (Elevé)**
R3 : Un hacker néophyte essaye de rendre les sites webs inaccessibles via attaque DDOS.	**2**	**3**	**6 (Moyen)**
R4 : Un employé malveillant souhaite revendre les données personnelles des clients exfiltrées du CRM.	**3**	**4**	**12 (Elevé)**
R5 : Un ancien employé qui a été licencié veut saboter les sites webs et applications en altérant le code source.	**4**	**3**	**12 (Elevé)**
R6 : Un cybercriminel souhaite obtenir une rançon via l'introduction d'un ransomware.	**4**	**2**	**8 (Moyen)**

4.5.2. Le niveau des risques initiaux

	Vraisemblance				
Gravité		**1**	**2**	**3**	**4**
	4		**R6**	**R4 R5**	
	3			**R1 R2**	
	2			**R3**	
	1				

4.5.3. Plan de traitement du risque (anciennement PACS)

Mesure de sécurité	Scénarios de risques associés	Responsable	Freins et difficultés de mise en œuvre	Coût/ Complexité	Échéance	Statut
Gouvernance						
Établir et maintenir une politique de sécurité du SI clairement documentée et validée par la direction	TOUS	RSSI		++	6 mois	En cours
Sensibilisation du personnel sur le phishing	R2,R6	RSSI		+	3 mois	À lancer
Engagement de confidentialité et de non divulgation	R1,R4	Direction	Nouveaux contrats à faire ou ajuster	+	2 mois	À lancer

Protection						
Protection des branches Git(main/production) Signature commit Lead dev	R5	CTO, RSSI	Ralenti le temps de développement	+	1 mois	À lancer
Restreindre l'utilisation des supports amovibles	R1	RSSI	Impact utilisateurs, gestion whitelist pour périphériques légitimes	+	3 mois	À lancer
Renforcement du contrôle d'accès physique au bureau	R1,R4,R5	Direction		++	3 mois	À lancer
Défense						
Webhooks surveillance traçage Git (alertes temps réel sur actions critiques ⇒suppression, ⇒force push)	R5	DSI	Développement scripts alertes, intégration avec monitoring	+	1 mois	À lancer
Surveillance renforcée des flux entrants/sortants et journalisation des événements	TOUS	DSI, RSSI		+	2 semaines	A vérifier et renforcer
Mis en place d'un WAF	R3	DSI	Achat d'un web application firewall	+++	6 mois	À lancer
Mise à jour de sécurité régulière de serveurs	R6	Admin sys		+	1 mois	En cours

Résilience						
Mettre en place un PCA/PRA et le tester	R5,R6	DSI, RSSI		+++	2 mois	En cours
Mettre en place un plan de sauvegarde de l'ensemble des données du SI intégrant des tests de restauration	R5,R6	DSI, RSSI	Prévoir des tests de restauration réguliers	+	1 mois	En cours
Souscription cyber-assurance avec couverture ransomware (rançon + reconstruction)	R6	DSI, RSSI	Audit probablement demandé par l'assureur	+++	3 mois	À lancer

4.5.4. Calcul des risques résiduels après application du PACS

R1 : Calamar5Software souhaite voler le code source des applications en corrompant un employé de chez Molo.		
Événements redoutés concernés Vol ou fuite du code source vers des tiers non autorisés		
Mesures de traitement existantes et complémentaires: -Engagement de confidentialité et de non divulgation -Restreindre l'utilisation des supports amovibles -Établir et maintenir une politique de sécurité du SI clairement documentée et validée par la direction -Surveillance renforcée des flux entrants/sortants et journalisation des événements		
Évaluation du risque résiduel		
Gravité initiale : 3	Vraisemblance initiale : 3	Niveau de risque initial : Elevé
Gravité résiduelle : 3	Vraisemblance résiduelle : 2	Niveau de risque résiduel: Moyen

R2 : Calamar5Software souhaite voler le portefeuille client d'Iron4Software grâce à l'ingénierie sociale sur un des employés.		
Événements redoutés concernés Divulgation non autorisée des données clients (vol, fuite, accès illégal)		
Mesures de traitement existantes et complémentaires: -Sensibilisation du personnel sur le phishing -Établir et maintenir une politique de sécurité du SI clairement documentée et validée par la direction -Surveillance renforcée des flux entrants/sortants et journalisation des événements		
Évaluation du risque résiduel		
Gravité initiale : 3	Vraisemblance initiale : 3	Niveau de risque initial : Elevé
Gravité résiduelle : 3	Vraisemblance résiduelle : 2	Niveau de risque résiduel: Moyen

R3 : Un hacker néophyte essaye de rendre les sites webs inaccessibles via attaque DDOS.		
Événements redoutés concernés: - Indisponibilité des services web (ex. panne serveur, attaque par déni de service - DDoS)		
Mesures de traitement existantes et complémentaires: - Mis en place d'un WAF - Établir et maintenir une politique de sécurité du SI clairement documentée et validée par la direction - Surveillance renforcée des flux entrants/sortants et journalisation des événements		
Évaluation du risque résiduel		
Gravité initiale : 2	Vraisemblance initiale : 3	Niveau de risque initial : Moyen
Gravité résiduelle : 2	Vraisemblance résiduelle : 2	Niveau de risque résiduel: Faible

R4 : Un employé malveillant souhaite revendre les données personnelles des clients exfiltrer du CRM.		
Événements redoutés concernés -Divulgation non autorisée des données clients (vol, fuite, accès illégal)		
Mesures de traitement existantes et complémentaires: -Engagement de confidentialité et de non divulgation -Renforcement du contrôle d'accès physique au bureau -Établir et maintenir une politique de sécurité du SI clairement documentée et validée par la direction -Surveillance renforcée des flux entrants/sortants et journalisation des événements		
Évaluation du risque résiduel		
Gravité initiale : 3	Vraisemblance initiale : 4	Niveau de risque initial : Elevé
Gravité résiduelle : 3	Vraisemblance résiduelle : 2	Niveau de risque résiduel: Moyen

R5 : Un ancien employé qui a été licencié veut saboter les sites webs et applications en altérant le dépôt du code source.		
Événements redoutés concernés Indisponibilité du dépôt Git		
Mesures de traitement existantes et complémentaires: -Protection des branches Git(main/production) Signature commit Lead dev -Renforcement du contrôle d'accès physique au bureau -Webhooks surveillance traçage Git (alertes temps réel sur actions critiques⇒suppression,⇒force push) -Mettre en place un PCA/PRA et le tester -Mettre en place un plan de sauvegarde de l'ensemble des données du SI intégrant des tests de restauration -Établir et maintenir une politique de sécurité du SI clairement documentée et validée par la direction -Surveillance renforcée des flux entrants/sortants et journalisation des événements		
Évaluation du risque résiduel		
Gravité initiale : 4	Vraisemblance initiale : 3	Niveau de risque initial : Elevé
Gravité résiduelle 2	Vraisemblance résiduelle : 2	Niveau de risque résiduel: Faible

R6 : Un cybercriminel souhaite obtenir une rançon via l'introduction d'un ransomware.		
Événements redoutés concernés -Altération ou compromission des configurations serveur et des mécanismes de sécurité (suite à un ransomware)		
Mesures de traitement existantes et complémentaires: -Sensibilisation du personnel sur le phishing -Mise à jour de sécurité régulière de serveurs -Mettre en place un PCA/PRA et le tester -Mettre en place un plan de sauvegarde de l'ensemble des données du SI intégrant des tests de restauration -Souscription cyber-assurance avec couverture ransomware (rançon + reconstruction) -Établir et maintenir une politique de sécurité du SI clairement documentée et validée par la direction -Surveillance renforcée des flux entrants/sortants et journalisation des événements		
Évaluation du risque résiduel		
Gravité initiale : 4	Vraisemblance initiale : 2	Niveau de risque initial : Moyen
Gravité résiduelle : 2	Vraisemblance résiduelle : 1	Niveau de risque résiduel: Faible

4.5.6. Le niveau des risques résiduels :

	Vraisemblance initiale				
Gravité initiale		1	2	3	4
	4		R6	R4 R5	
	3			R1 R2	
	2			R3	
	1				

	Vraisemblance résiduelle				
Gravité résiduelle		1	2	3	4
	4				
	3		R1 R2 R4		
	2	R6	R3 R5		
	1				

5. Checklist de conformité ISO 27001

- **EL** : Exigences légales
- **OC** : Obligation contractuelle
- **EOMPA** : Exigence Opérationnelle / Meilleure Pratique
- **RAR** : Résultat de l'appréciation des risques

Article	Objectif de sécurité / Mesure	Mesures actuelles	Remarques (avec justification des exclusions)	EL	OC	EOMPA	RAR	Etat actuel
Mesures de sécurité organisationnelles								
Annexe A.5.1	Une politique de sécurité de l'information et des politiques spécifiques à une thématique doivent être définies, approuvées par la direction, publiées, communiquées et demandées en confirmation au personnel et aux parties intéressées concernés, ainsi que révisées à intervalles planifiés et si des changements significatifs ont lieu.	La PSI n'est pas rédigée.	N/A				X	Non-conforme
Mesures de sécurité physique								
Annexe A.7.2	Les entrées physiques Les zones sécurisées doivent être protégées par des mesures de sécurité des accès et des points d'accès appropriés.	Une mesure de sécurité est planifiée sous 3 mois. *Renforcement du contrôle d'accès physique au bureau*	N/A				X	Non-conforme
Mesures de sécurité applicables aux personnes								
Annexe A.6.1	Sélection des candidats Les vérifications des références de tous les candidats à l'embauche	Contrôle des candidats avant signature officiel Obtenir systématiquement le	N/A			X		Conforme

	doivent être réalisées avant qu'ils n'intègrent l'organisation puis de façon continue en tenant compte des lois, des réglementations et de l'éthique applicables, et doivent être proportionnelles aux exigences métier, à la classification des informations auxquelles ils auront accès et aux risques identifiés.	consentement écrit du candidat avant toute vérification de références, en l'informant sur le but, la portée et la procédure envisagée. Vérifier l'identité du candidat et son droit de travailler, dès l'embauche et pendant toute la durée du contrat, notamment avec les documents officiels requis par la législation. Recueillir les références auprès des anciens employeurs ou responsables directs						
Mesures de sécurité technologiques								
Annexe A.8.16	Activités de surveillance Les réseaux, systèmes et applications doivent être surveillés pour détecter les comportements anormaux et des mesures appropriées doivent être prises pour évaluer les éventuels incidents de sécurité de l'information.	Un SIEM splunk est installé et centralise l'ensemble des logs des actifs de l'entreprise	N/A			X		Conforme

6. Propositions d’amélioration : PSSI, chartes, journalisation centralisée.

6.1. Résumé du PTR

Afin de renforcer la sécurité, on propose des mesures supplémentaires :

- des engagements de confidentialité rigoureux.
- des politiques de sécurité robustes.
- une surveillance continue.
- des formations du personnel.
- des contrôles d'accès stricts.
- et des plans de reprise et de continuité d'activité.

Après examen des contrôles existants et l’application du plan de traitement, les risques résiduels sont considérés comme faibles à moyens, ce qui est jugé satisfaisant.

6.2. Proposition d'amélioration de la Politique de sécurité du système d’information.

Iron4Software ne dispose actuellement pas de PSSI, sa rédaction et son implémentation est nécessaire. Elle doit être un document directeur qui établit les principes et les règles de sécurité que l'organisation s'engage à respecter.

Objectifs:

- Définir les responsabilités et les rôles de chacun en matière de sécurité.
- Établir les objectifs de sécurité et les mesures à mettre en œuvre.
- Assurer la conformité avec les réglementations en vigueur (RGPD, ISO 27001, etc.).

Pour rappel, le contenu de la PSSI devraient disposer des éléments suivants :

- Introduction et objectifs : Présentation de la politique, de son périmètre et de ses finalités.
- Organisation de la sécurité : Rôles et responsabilités, comité de pilotage sécurité.
- Gestion des risques : Méthodologie d'identification, d'évaluation et de traitement des risques.
- Politiques spécifiques :
    - Politique de contrôle d'accès : Gestion des identités, authentification, autorisation, séparation des privilèges.
    - Politique de gestion des actifs : Inventaire, classification, protection des informations.

    - Politique de sécurité physique : Protection des locaux et des équipements.
    - Politique de gestion des incidents de sécurité : Détection, réponse, récupération.
    - Politique de continuité des activités : Plans de reprise après sinistre (PRA) et de continuité d'activité (PCA).
    - Politique de sauvegarde et de restauration.
    - Politique de gestion des mises à jour.
    - Politique de sensibilisation et de formation : Programme de formation pour le personnel.
- Conformité : Références aux lois, réglementations et normes applicables.
- Révision et mise à jour : Processus de revue régulière de la PSSI.

Mise en œuvre :

- La PSSI doit être approuvée par la direction générale.
- Elle doit être communiquée à l'ensemble du personnel et aux parties prenantes concernées.
- Des revues régulières doivent être planifiées pour s'assurer de son adéquation et de son efficacité.

6.3. Mise en place d'une charte informatique

Il serait intéressant pour Iron4Software de créer une charte informatique qui est un document essentiel qui définit les règles et les bonnes pratiques d'utilisation des ressources informatiques de l'entreprise. Elle vise à protéger le système d'information, à assurer la conformité légale et à sensibiliser les employés aux risques liés à leur utilisation des outils numériques.

Exemple des bonnes pratiques informatiques à présenter dans la charte

- ➢ Je verrouille mon ordinateur dès que je quitte mon poste et je pense à l'éteindre en fin de journée.
- ➢ Je télécharge des fichiers uniquement sur des sites officiels et sûrs.
- ➢ Je ne divulgue jamais de données sur l'entreprise, sauf accord préalable.
- ➢ Par défaut, j'évite de connecter tout appareil de stockage externe, et surtout pas une clé USB dont je ne maîtrise pas l'origine.
- ➢ Par défaut, je ne clique pas sur un lien et je n'ouvre aucune pièce jointe provenant d'un expéditeur inconnu.
- ➢ Je ne dois jamais utiliser mon adresse e-mail @Iron4Sofware.fr dans un contexte hors professionnel, notamment sur des sites internet (chats, forums, blogs, etc.).
- ➢ J'ai la possibilité d'utiliser mon ordinateur ou tout équipement informatique à des fins personnelles, dès lors que j'applique les règles d'usage et de sécurité établies par l'entreprise.
- ➢ En cas de doute ou de suspicion d'activité anormale, je préviens sans délai les équipes informatiques

7. Plan de sauvegarde quotidien chiffré local + cloud.

Ce plan vise à garantir la **Confidentialité, l'Intégrité** et la **Disponibilité** (CID) des données d'Iron4Software, en ligne avec les objectifs de sécurité mentionnés dans le **Rapport GRC**. L'utilisation de **Veritas Backup Exec** permet de gérer à la fois les sauvegardes sur disque dur, sur bande magnétique et dans le cloud.

7.1. Portée de la Sauvegarde

La sauvegarde doit être basée sur l'identification des **actifs critiques**.

- **Données Primordiales (Criticité Élevée)** :
    - Bases de données de l'application web (MySQL).
    - Code source de l'application (dépôts Git, fichiers de production).
    - Fichiers de configuration critiques des serveurs (OS et applications).
    - Serveurs d'identité (Active Directory/LDAP).
- **Données Supports (Criticité Moyenne)** :
    - Systèmes d'exploitation.
    - Journaux (logs) essentiels à la traçabilité et à l'audit (SIEM Splunk)

Nous allons utiliser **Veritas Backup Exec** pour la sauvegarde applicative (bases de données) et de l'annuaire Active Directory. Une sauvegarde complète du serveur web, ainsi que du serveur DNS et Active Directory (AD), sera effectuée, complétée par des sauvegardes incrémentielles régulières.

7.2. La fréquence des sauvegardes

Pour la sauvegarde sur bande / cloud azure / disque dur :

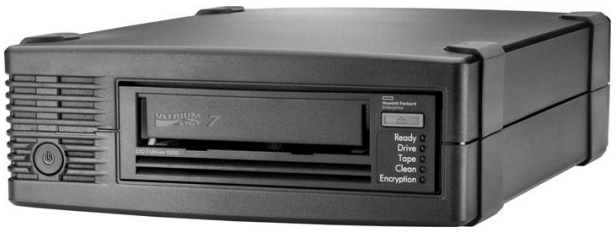
- **Complète** : une fois par semaine le dimanche. Elle enregistre l'ensemble de toutes les données du serveur web, ainsi que du serveur DNS et Active Directory (AD).

- **Incrémentielle** : Du lundi au samedi. Ne sauvegarde que les blocs de données modifiés depuis la dernière sauvegarde.
    - Avantage : Très rapide et faible consommation de bande passante et de stockage.
- **Fréquence Quotidienne** : La sauvegarde incrémentielle doit être lancée toutes les nuits entre 23h00 et 05h00 pour minimiser l'impact sur les opérations en journée.

Pour la sauvegarde sur disque dur :

- **Toutes les heures** : La sauvegarde des BinLogs (journaux de transaction UPDATE, INSERT) doit être lancée toutes les heures pour respecter le RPO de 1H.

7.3. Le lieu de stockage et les supports de sauvegarde



Microsoft Azure

Localisation	Support	Objectif	Rôle de Veritas Backup Exec
Hors-site	Cloud (Azure)	Désastre majeur (incendie, vol, ransomware) et rétention à long terme	Utilisation du connecteur Cloud de Backup Exec pour la copie de données dédupliquées.
Local	Bande	Rétention longue	Gestion des bibliothèques de bandes.
Local	NAS	Rétention courte	Sauvegarde sur disque

7.4. Convention de Nommage

Une étiquette claire facilite la gestion du catalogue et la restauration.

- **Format standard :** [ENVIRONNEMENT]_[TYPE_SAUVEGARDE]_[SOURCE]_[DATE_HEURE]_[DESTINATION]
- **Exemples** :
  - PROD_INC_AppWebIron4_20251111-2300_LOCAL_NAS
  - DEV_FULL_ServeurBDDIron4_20251109-0200_CLOUD
- **Règles** :
  - Environnement : PROD, DEV, PRE-PROD.
  - Type : FULL, INC (Incrémentielle)
  - Destination : LOCAL_BANDE ,LOCAL_NAS, CLOUD
  - Chiffrement : une clé de chiffrement AES256 unique pour l'ensemble des sauvegardes sera défini.

7.5. Politique de Rétention

La politique doit être dictée par la criticité des données, les exigences légales (RGPD, etc.) et l'analyse de risque.

Rétention	Période	Type de Sauvegarde	Lieu de Stockage	Objectif
Toutes les heures	24H	Partielle	-Local NAS	Récupération des modifications bdd
Quotidienne	7 jours	Complète (La dernière de la semaine) + Incrémentielle	-Cloud -Local Bande -Local NAS	Récupération d'erreurs rapides.
Mensuelle	12 mois	Complète (La dernière du mois)	-Hors site bande -Local NAS	Rétention d'audit et conformité.

Annuelle	7 ans	Complète (La dernière de l'année)	-Hors site bande -Local NAS	Conformité légale et historique.

7.6. Gestion des Accès

Appliquer le **Principe du Moindre Privilège** :

- **Groupe dédié** : Utilisation du groupe dans l'AD "Opérateurs de Sauvegarde et Restauration".
- **Accès limité** : Seuls les membres de ce groupe ont les privilèges d'accès au serveur Backup Exec (**Server 2019 AD**), à la clé de chiffrement, et aux supports de stockage.
- **Audits** : Chaque sauvegarde, extraction ou restauration doit être tracée (audit trail). Ce journal d'audit fournit une trace chronologique complète de toutes les opérations, incluant qui a effectué l'action, quand, et quelles données ont été concernées.

7.7. Vérification et Contrôle

La sauvegarde sera vérifié selon les méthodes suivantes :

- **Vérification Quotidienne** : Configurer Backup Exec pour effectuer un test de vérification à la fin de chaque tâche (vérification des sommes de contrôle). Contrôle humain en complément.
- **Test de restauration partiel mensuel** : Tester la restauration de fichiers uniques et de bases de données pour valider l'intégrité à un niveau approfondi.
- **Test de restauration complète trimestriel** : Effectuer des tests de restauration complets de l'application web et de l'Active Directory dans un environnement isolé.

8. PRA : restauration AD + serveur web

8.1. Analyse d’impact

L’analyse de l'impact sur l'activité (BIA) évalue les dommages potentiels d’une interruption des opérations, et le classement des processus business par importance. L’analyse portera sur les activités de **développement web** et d'**hébergement** qui dépendent des systèmes d’AD et du serveur web.

Echelle d’impact		
5	**Catastrophique**	**Perte de valeur qui peut entraîner la fin des activités de l’organisme**
4	**Intolérable**	**Perte de valeur qui n’est pas tolérée par l'organisme, mais qui peut éventuellement être récupérée**
3	**Majeure**	**Perte importante de valeur d’affaires**
2	**Considérable**	**Perte considérable de valeur d'affaires**
1	**Mineure**	**Perte mineure de valeur d’affaires**

Liste des activités avec leur RTO / RPO

Processus métier	**Impacts en cas d’interruption**	**Impact après**			**RTO**	**RPO**	**Dépendances**
		1H	**4H**	**24H**			
Développement web Toutes activités de conception, développement, test, intégration continue, maintenance applicative.	- Retards importants sur les projets - Pénalités contractuelles - Blocage des équipes techniques - Dégradation de la satisfaction client - Possible perte de contrats stratégiques	1	2	3	24 h	1H	- Active Directory -Réseau - Serveur web interne (CI/CD, documentation, dépôt) - Git local - Postes de développement
Hébergement	- Non-respect des SLA d’engagement - Atteinte à la réputation et risque contractuel fort	2	3	4	4H	1H	- Serveur web - Réseau

Élément	RTO	RPO
Serveur Active Directory (AD)	**24H**	**1H**
Serveur Web	**4H**	**1H**

RTO – Recovery Time Objective : temps maximum acceptable d'interruption d'un service, avant que l'impact sur l'entreprise devienne critique.

RPO – Recovery Point Objective : quantité maximale de données que l'entreprise peut se permettre de perdre, mesurée en temps.

8.2. Les stratégies de reprise

Ci-dessous,une description détaillée des méthodes et technologies utilisées pour la reprise des opérations après un sinistre.

Méthode de reprise du serveur web

- Application de la restauration via les Binlogs (journaux de transaction UPDATE, INSERT) de la base de données mysql afin de respecter le RPO de 1H.

  Support de stockage utilisé : NAS en priorité

- Restauration des applicatifs des clients déployés sur le serveur via la sauvegarde journalière de **Veritas Backup Exec**.

  Support de stockage utilisé :
  Priorité 1 : NAS
  Priorité 2 : cloud
  Priorité 3 : bande magnétique

- Une vérification et un contrôle de la restauration doivent être effectués par l'administrateur système et le RSSI.
- Contrôler que le serveur est opérationnel : que les services web et mysql sont correctement rétablis. Contrôle fonctionnel aléatoire de certains sites webs clients.

- Un contrôle fonctionnel plus poussé sera fait aussi par les développeurs.

Méthode de reprise du serveur AD

- ➢ Récupération de la sauvegarde journalière de la veille de Veritas Backup Exec.
- ➢ Report des modifications de la journée faites par l'administrateur

  Support de stockage utilisé :
  Priorité 1 : NAS
  Priorité 2 : cloud
  Priorité 3 : bande magnétique

- ➢ Une vérification et un contrôle de la restauration doivent être effectués par l'administrateur système et le RSSI.
- ➢ Contrôler que le serveur AD est fonctionnel en redémarrant quelques postes et vérifier par exemple que les GPO s'appliquent correctement.

8.3. Les plans d'urgence

8.3.1. Responsabilités avec leurs actions

Ci-dessous sur les actions à entreprendre immédiatement après l'incident. On y trouve également les postes concernés et la distribution des rôles et des responsabilités. Les responsabilités sont alignées sur le Principe du Moindre Privilège et les rôles clés identifiés dans les documents de méthode de reprise.

Phase	**Rôle Responsable**	**Actions Spécifiques pendant la Restauration**
Identification/Déclenchement	DSI (Martin Michel)	-Déclaration de l'incident, décision d'activer le PRA
Restauration	Admin Systèmes	- Restauration AD - Restauration du Serveur Web à partir de sauvegarde c hiffrée (Cloud/Local). - Restauration granulaire de fichier ou de la base de données.
Vérification Post-Restauration	Admin Systèmes / Equipe Dev	- Tests de connectivité. - Remise en service progressive du Web et de l'AD.

Capitalisation	RSSI/DSI	- Rédaction du rapport d'analyse post-incident. - Mise à jour des procédures si nécessaire.

8.3.2. Timeline

Plan d'actions immédiates (0–30 minutes)

Objectif : préparation et activation du PRA

1. Notification de la direction et des équipes concernées.
2. Analyse rapide du périmètre impacté (AD ? Réseau ? Serveur web ?).
3. Déclenchement du PRA par le **DSI.**

Procédures de reprise (30 minutes – RTO cible)

Objectif : corriger l'incident pour atteindre le RTO de 4H initialement prévu.

Étape 1 – Restauration des services prioritaires

Ordre défini par le BIA :

1. **Serveur web**
2. **Active Directory**

Étape 2 – Vérification des services restaurés

Serveur web

➢ Contrôler que le serveur web est opérationnel : que les services web et mysql sont correctement rétablis. Contrôle fonctionnel aléatoire de certains sites webs clients.

➢ Un contrôle fonctionnel plus poussé sera fait aussi par les développeurs.

Active Directory

➢ Contrôler que le serveur AD est fonctionnel en redémarrant quelques postes et vérifier par exemple que les GPO s'appliquent correctement.

8.4. Formation et sensibilisation

Les personnes concernées par les formations et sensibilisations seront l’administrateur système et réseau, le RSSI et pourront être ouvertes à d’autres parties prenantes du PRA.

8.4.1. Formation

Des formations spécialisées permettent d'apprendre à concevoir, planifier et exécuter la restauration d'Active Directory, notamment sous Windows Server. Ces formations abordent la sauvegarde, la restauration au niveau objet ou global, la gestion de la réplication AD.

Les formations abordent aussi la priorisation des services critiques, le respect des objectifs RTO (Recovery Time Objective) et RPO (Recovery Point Objective), et les tests réguliers des procédures pour assurer leur fiabilité.

8.4.2 Sensibilisation

La sensibilisation doit couvrir les scénarios courants de sinistre affectant les serveurs web (panne matérielle, attaque, perte de données), les procédures de sauvegarde automatisées (cloud / NAS / bande), et les étapes précises de restauration pour minimiser les interruptions.

9. Tests de restauration à programmer mensuellement.

Un calendrier des tests et des mises à jour du PRA est mis en place pour assurer son efficacité et sa pertinence sur la durée, et refléter les éventuels changements dans l'environnement opérationnel et technologique de l'entreprise.

9.1 Les rôles et responsabilités des participants.

Phase	Rôle Responsable	Actions Spécifiques pendant les exercices
Exercice Bureau		
Reunion	DSI, CTO , Admin , système, Directeur	-Discussion de leurs rôles et responsabilités dans un scénario potentiel
Exercice Simulation		
Restauration	Admin Systèmes	- Restauration AD - Restauration du serveur web à partir de sauvegarde chiffrée (Cloud/Local). - Restauration granulaire de fichier ou de la base de données.
Vérification Post-Restauration	Admin Systèmes / Equipe Dev	Tests de connectivité. Remise en service progressive du Web et de l'AD.
Capitalisation	RSSI/DSI	- Rédaction du rapport d'analyse post-incident. - Mise à jour des procédures si nécessaire.

9.2. Les objectifs et la fréquence des exercices.

Des exercices de bureau seront planifiés tous les 6 mois pour définir les rôles et responsabilités de chacun pour les différents PRA.

Des exercices de simulation seront aussi planifiés tous les 3 mois. avec pour objectifs principaux :

- ➢ Valider le PRA : Confirmer que la documentation et les procédures du Plan de Reprise d'Activité sont complètes, à jour et opérationnelles.
- ➢ Mesurer les indicateurs clés : S'assurer que les temps de restauration réels (RTO) et les pertes de données (RPO) sont conformes aux objectifs métiers définis.
- ➢ Tester la compétence : Évaluer l'efficacité de l'entreprise face à un scénario de crise et renforcer la coordination.

9.3. Périmètre du plan

Le périmètre des tests se concentre sur les actifs critiques identifiés, conformément au PRA et au SMSI.

- ➢ Systèmes critiques :
  - Restauration des services d'annuaire : Contrôleur de Domaine Active Directory (DC-IRON).
  - Restauration du service web : Serveur Web Ubuntu (192.168.100.2) et applications.
- ➢ Périmètre Réseau : Les procédures de restauration doivent couvrir les réseaux interne (192.168.1.0/24) et DMZ (192.168.100.0/24).
- ➢ Domaine d'activité : L'accent est mis sur la reprise des activités de développement et d'hébergement.

9.4. L'ensemble des risques à gérer

Les tests de restauration doivent permettre de gérer les risques suivants :

- ➢ Risque de non-fonctionnement de la sauvegarde : Les données de sauvegarde sont corrompues, incomplètes ou illisibles.
- ➢ Risque de dépassement des RTO/RPO : Le temps de reprise des services critiques est supérieur à ce qui est toléré par l'activité métier.
- ➢ Risque de défaillance humaine : Erreurs de procédure dues à un manque de formation ou de clarté de la documentation.

9.5. Ressources requises pour être efficace

- ➢ Infrastructure de test : Un environnement isolé (bac à sable) et sécurisé pour effectuer la restauration sans impacter la production.
- ➢ Outils de gestion de crise : Outils de communication(outlook) et de suivi des tâches (Jira).
- ➢ Personnel : Le DSI, l'administrateur système dédiée à la restauration et l'équipe de développement.
- ➢ Documentation : Procédures de restauration détaillées et configurations de sécurité (GPO, pare-feu).

9.6. Compétence des personnes qui participent à la campagne d'exercices

Les participants doivent posséder les compétences suivantes :

- ➢ Administrateur Système et réseau : Maîtrise des procédures de restauration de l'Active Directory et du serveur web Ubuntu, des bases de données associées et de l'application Iron4Software.
- ➢ DSI : Connaissance approfondie du PRA et du processus de gestion de crise pour coordonner l'exercice.
- ➢ Développeur : Connaissance des structures des applications. Tests de fonctionnalités.

9.7. Rapports sur la réalisation des exercices et tests

Un rapport formel doit être produit après chaque exercice de restauration, incluant :

- ➢ Déroulement de l'exercice : Chronologie détaillée des actions menées, y compris les tentatives échouées et les étapes critiques.
- ➢ Résultats vs. Objectifs : Mesures précises des RTO/RPO réels comparées aux objectifs fixés.
- ➢ Écarts et Problèmes : Liste des problèmes rencontrés (erreurs de procédure, défauts techniques, manque de compétence, etc.).
- ➢ Recommandations : Propositions d'améliorations pour le PRA, la documentation et les systèmes.

9.8 Validation par la hiérarchie

Le processus de validation assure l'engagement de la direction et la prise en compte des résultats :

- ➢ Relecture Technique : Le rapport est validé par le DSI (Martin Michel) pour s'assurer de l'exactitude des données et de la pertinence technique des recommandations.

➢ Approbation Stratégique : Le rapport est soumis à la Direction Générale pour validation des résultats

10. Estimation des coûts (logiciels, stockage, personnel).

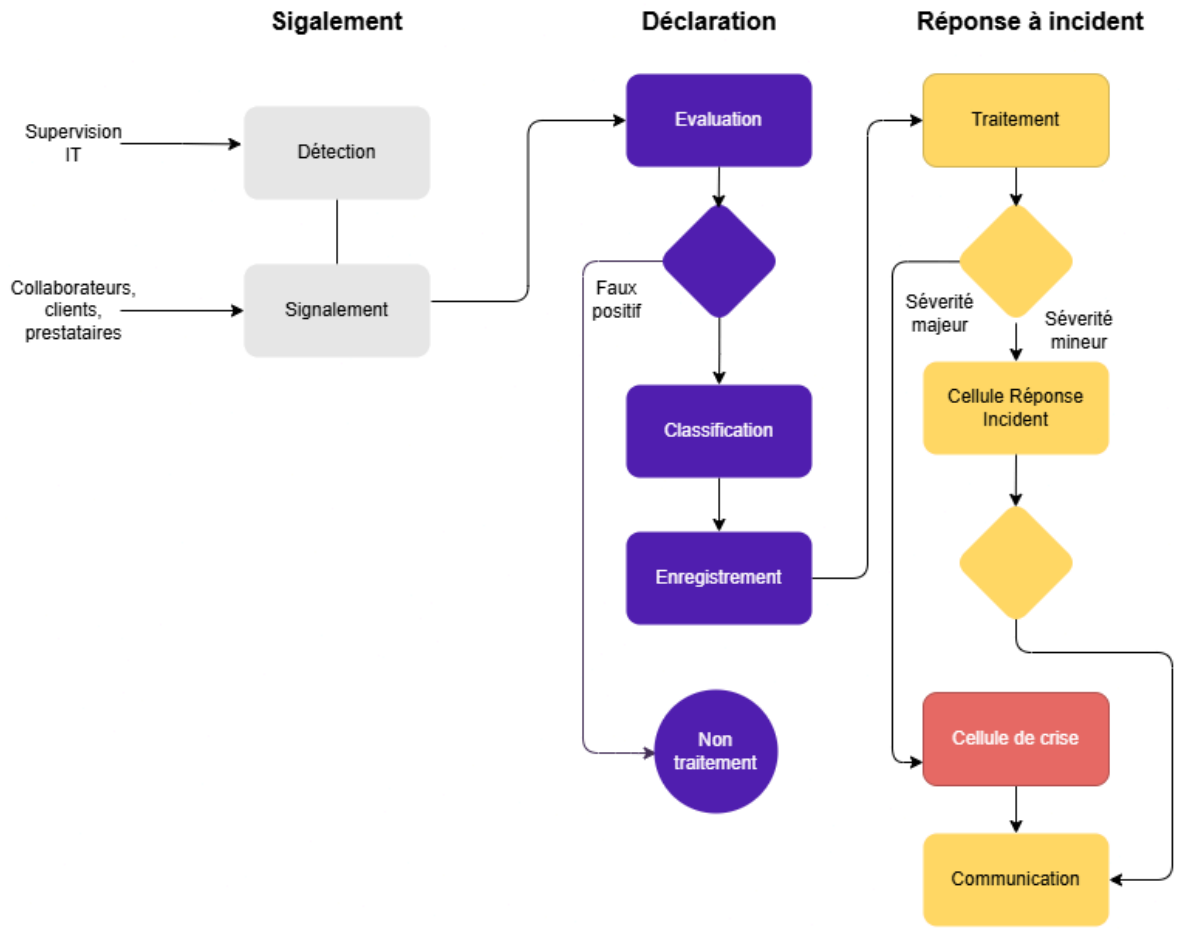
Ressources			
	Tarif journaliers	**Nombre de jours**	**Total**
Consultant GRC	1000	20	15000
Pentester DEL CYBER	800	30	16000
Juriste	1200	5	6000
Formation et sensibilisation			
E-learning Phishing			1500
E-learning Cybersécurité			1500
E-learning Sensibilisation RGPD			1500
Logiciels			
Jira			2500
Avant de cliquer			1500
Proxy Sophos			3000
EDR TEHTRIS			3000

Veritas Backup Exec		2400
Matériel		
WAF		4000
NAS		500
Backup HP LTO-8 externe		4000
Mise en place d’un système de badge CASTEL		4500
Autres		
Cloud Azure	Pour 35 To par mois (Sauvegarde journalière 5 to x 7)	9000
Assurance		1500
Threat Intelligence (service de veille)		600
Coût Total Annuel		91 000

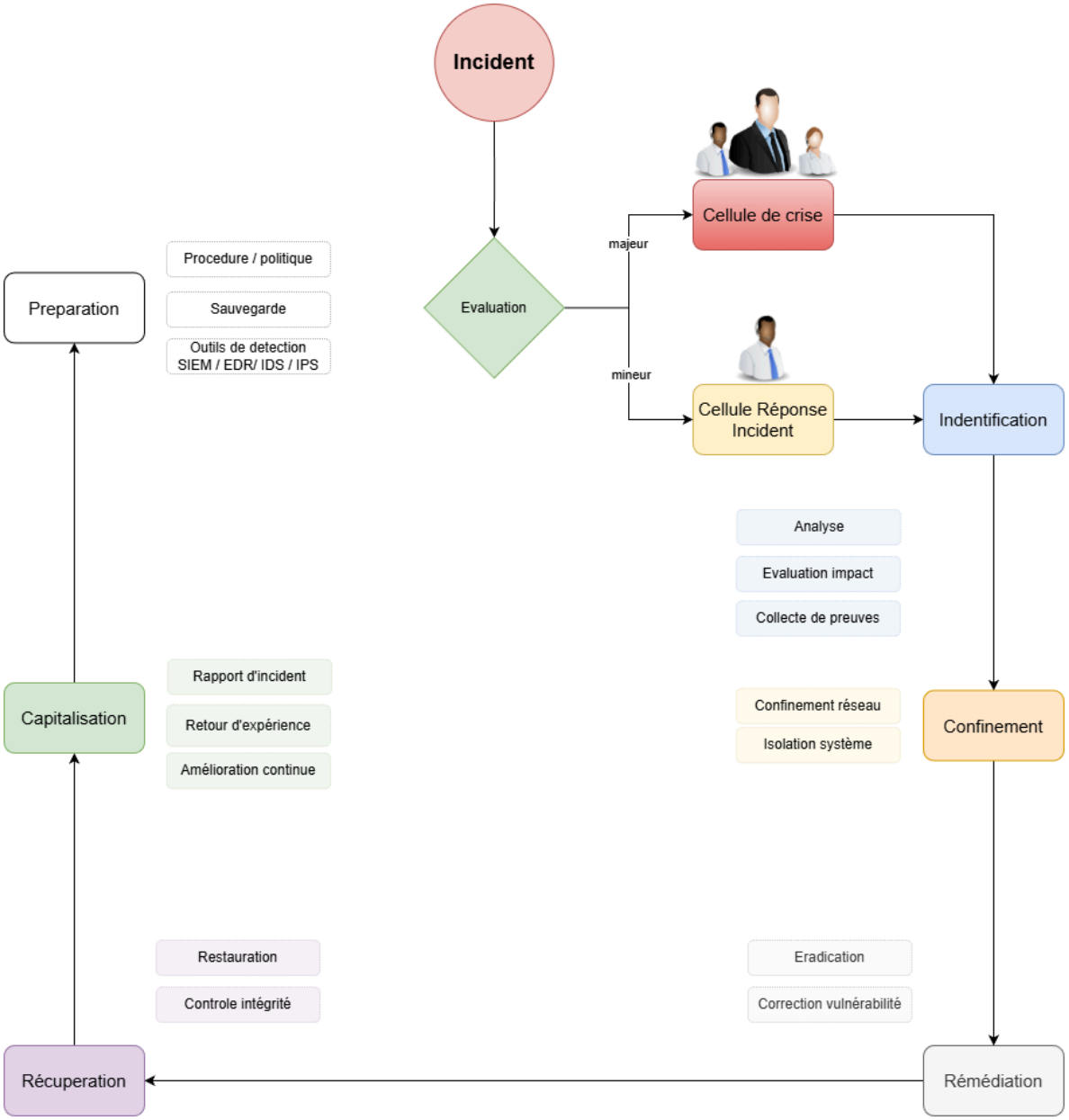
11. Plan de réponse aux incidents

Ce plan de réponse aux incidents de cybersécurité fournit un cadre d'actions en six étapes clés (inspiré du référentiel ISO/IEC 27035). Il est conçu pour être intégré dans un rapport technique post-pentest, en tenant compte de diverses failles potentielles.

11.1. Schéma de plan de gestion d'incident



11.2. Schéma de plan de réponse à incident



11.3. Préparation

Objectif :

Se préparer à gérer efficacement un incident avant qu'il ne survienne. Cette phase consiste à mettre en place l'organisation, les outils et les procédures nécessaires pour être prêt à réagir sans perdre de temps en cas d'attaque.

Organisation et contacts :

Afin d'assurer une gestion des incidents fluide et efficace, il est primordial de définir avec clarté les rôles et responsabilités de chaque acteur impliqué.

Interlocuteurs internes :

Martin MICHEL (RSSI/DSI) : Responsable de l'évaluation de la gravité, de l'activation du plan, de la coordination de la communication sécurité. Supervise l'impact sur les systèmes et infrastructures.

Michel NOIR (Direction Générale) : Valide les messages clés et les décisions publiques. Déclenchement du plan en cas d'impact majeur.

DPO (Délégué à la Protection des Données) : Gère la communication vers les autorités (CNIL) si des données personnelles sont affectées.

Équipe Technique : Fournit les mises à jour techniques et le statut de résolution. Assure la remédiation et la récupération.

Équipe Sécurité (CERT/RSSI) : Constitution, gestion et maintien à jour des procédures de réponse.

Juriste (à recruter) : Gestion des aspects légaux, dépôt de plainte, conformité.

Ressources Humaines (RH) : Gestion des incidents impliquant le personnel (ex. employé malveillant).

Relations Publiques / Communication : Prépare et diffuse la stratégie de communication interne et externe.

Interlocuteurs externes :

ANSSI / CERT-FR : Notification en cas d'incident majeur (NIS2) – services critiques ou essentiels.

CNIL : Notification obligatoire en cas de violation de données personnelles avec risques.

Forces de l'ordre : Dépôt de plainte en cas de cyberattaque avérée (ransomware, sabotage, extorsion, etc.).

Assureur cybersécurité : Notification en cas d'incident couvert contractuellement.

Clients / Partenaires / Fournisseurs : Notification en cas d'impact sur leurs données ou services.

Organismes régulateurs : Notifications selon les lois applicables (en plus de la CNIL).

Politiques, procédures et modèles de documents :

On doit :

- ➢ S’assurer que l’entreprise dispose d’une politique de sécurité claire et de procédures d’escalade bien définies.
- ➢ Définir à l’avance les critères de gravité d’un incident et les conditions d’activation d’une cellule de crise.
- ➢ Préparer des modèles de documents (Formulaire de déclaration d’incident, rapport d’incident ...)

Outillage de détection et d’intervention :

On doit :

- ➢ Déployer et maintenir les outils de supervision de sécurité (EDR: TETRHIS, IDS/IPS : Pfsense) sur tous les postes, serveurs et points d'accès réseau.
- ➢ Vérifier leur bon fonctionnement et s'assurer de la capacité à isoler rapidement un hôte compromis pour limiter la propagation des attaques.

Journalisation :

On doit :

- ➢ Centraliser et sécuriser les journaux système, applicatifs, réseau via le SIEM splunk.
- ➢ Protéger contre la modification ou suppression non autorisée (intégrité).
- ➢ Configurer pour capturer les événements critiques (accès, erreurs, tentatives d’intrusion) , par exemple : des alertes temps réels configurées dans le SIEM splunk.
- ➢ Revues régulières des journaux (tableaux de bord) par le RSSI.

Sauvegardes :

On doit :

- ➢ Sauvegarder régulièrement les données et systèmes critiques via le logiciel Backup Exec.
- ➢ Conserver les logs avec archivage protégé.

➢ Documenter et automatiser des procédures de sauvegarde/restauration.

Exercices et sensibilisation :

On doit :

➢ Réaliser périodiquement des exercices de simulation d'incident pour entraîner les équipes techniques et managériales à suivre le plan de réponse. Chaque membre de l'équipe doit être familier avec ses rôles et responsabilités en cas de crise.
➢ Mener des actions de sensibilisation sécurité auprès des employés pour réduire le risque humain (phishing, utilisation de mots de passe faibles, etc.).

11.4. Identification

Objectif :

Détecter l'incident dès que possible, en évaluer l'ampleur et mobiliser les acteurs appropriés. Cette phase consiste à reconnaître qu'une attaque ou anomalie de sécurité est en cours, à confirmer qu'il s'agit bien d'un incident et non d'une fausse alerte, puis à rassembler un maximum d'informations factuelles sur ce qui se passe.

Détection initiale :

On doit :
➢ Surveillez en permanence les alertes techniques (SIEM splunk, IDS/IPS, EDR, antivirus) ainsi que les journaux systèmes et applicatifs à la recherche d'anomalies (pics de trafic, messages d'erreur, tentatives de connexions suspectes, etc.).
➢ Prendre en compte les retours des utilisateurs ou de l'équipe technique qui peuvent signaler des comportements étranges.
➢ Rester attentifs aux notifications d'entités extérieures (veille, renseignement, partenaires, autorités) qui informent parfois qu'une attaque a été détectée ou que des données de la société circulent publiquement.

Analyse et confirmation de l'incident :

On doit :
➢ Valider qu'il s'agit bien d'un incident avéré en corroborant les éléments lors de la détection initiale.
➢ Rassembler les premières preuves techniques : extraire les journaux pertinents.
➢ Observez les symptômes sur les systèmes touchés (processus inconnus en mémoire, modifications de fichiers, élévation de privilège réussie, etc.).

- ➢ Capturer l'activité réseau suspecte si possible afin de pouvoir l'analyser hors-ligne.

Évaluation de l'ampleur et impact :

On doit :

- ➢ Identifier les systèmes compromis, les comptes utilisateurs impactés et le chemin d'attaque emprunté par l'adversaire.
- ➢ Comprendre l'objectif de l'attaquant et la portée de l'attaque en cours (ex. vol de données, sabotage, ransomware...).
- ➢ Corréler les indices et constituer la timeline de l'attaque : IP source de l'attaque, ports et protocoles utilisés, horaires des événements, vecteur d'intrusion exploité (faille applicative, phishing, RDP ouvert, etc.).

Collecte des preuves numériques :

On doit avant toute action de confinement :

- ➢ Initier la collecte de preuves pour alimenter l'enquête. Sur les hôtes compromis, réaliser si possible un dump mémoire vive via l'outil volatility.
- ➢ Utiliser des outils forensiques pour faire des copies des disques (Autopsy) ou extraire des artefacts système pertinents (journaux d'événements Windows, fichiers de configuration, etc.), de sorte à pouvoir les analyser plus tard.
- ➢ Veiller à préserver l'intégrité des preuves (hash des fichiers collectés) pour une éventuelle analyse forensique approfondie ou une exploitation juridique ultérieure.
- ➢ Documenter tout ce qui est recueilli (heures, sources, type de données) dans le but de faire un rapport forensique plus tard.

11.5. Confinement

Objectif :

Limiter l'impact de l'incident en cours, empêcher sa propagation et maîtriser l'attaque et tout en protégeant les preuves (par exemple pour les futures analyses forensiques ou des poursuites judiciaires).

Isolation des systèmes compromis :

Selon la criticité de la ressource touchée, deux approches sont possibles :

On doit si le **système est critique pour l'activité (haute dispo requise) :**

- ➢ Maintenir le système en ligne si son arrêt impactera gravement le métier, mais l'isoler du réseau pour limiter la propagation.

On doit si le **système est non critique (peut être coupé sans grand impact) :**

- ➢ Déconnecter physiquement la machine du réseau ou du courant dès que possible
- ➢ Stopper les processus malveillants identifiés.
- ➢ Mettre en quarantaine les fichiers malveillants

Confinement réseau et segmentation :

On doit :

- ➢ Appliquer en urgence une segmentation (filtrage renforcé du pfsense, blocage VPN, restriction Internet) pour protéger les actifs critiques non encore touchés.
- ➢ Vérifier les droits et couper l'accès aux bases de données ou partages de fichiers contenant des informations critiques pour tout système ou compte suspect.
- ➢ Bloquer ou neutraliser les points de sortie en cas de fuite de données: dépôt GIT, serveurs de partage 192.168.1.1 ou destinataires identifiés.

11.6. Remédiation

Objectif :

Une fois l'incident contenu, la remédiation consiste à supprimer la cause de l'incident (malware, accès illégitime, vulnérabilité exploitée) et à prendre des mesures pour éviter une nouvelle intrusion par le même vecteur.

Éradication de la menace :

On doit :

- ➢ Supprimer les logiciels malveillants (fichiers infectés, webshells, scripts d'attaque) et leurs mécanismes de persistance (tâches planifiées, services ajoutés, clés de registre de démarrage, backdoors, comptes clandestins, etc.).
- ➢ Purger les entrées de registre ou les fichiers temporaires créés par le malware.).
- ➢ Réinitialiser ou supprimer les comptes utilisateurs ayant été utilisés par l'attaquant.
- ➢ Utiliser si nécessaire des outils de suppression des médias pour effacer complètement le disque dur.
- ➢ Procéder en dernier ressort à la destruction physique.

Corrections des vulnérabilités et faiblesses :

On doit :

- ➢ Corriger la faille initiale exploitée par l'attaquant pour éviter toute récidive (installer le(s) correctif(s) de sécurité(s), corriger le(s) code(s) applicatif(s) vulnérable(s)).

11.7. Récupération

Objectif :

Restaurer le fonctionnement normal du système d'information et vérifier que l'incident est bien éradiqué. La récupération vise à remettre en production les systèmes touchés en toute sécurité, une fois la menace éliminée, et à s'assurer de l'intégrité de l'environnement avant de reprendre une exploitation normale.

Réinstallation ou nettoyage complet des systèmes :
On doit :

- ➢ Procéder à une réinstallation complète du système à partir de sources saines
- ➢ Changer tous les mots de passe des comptes du système (comptes locaux, comptes AD, comptes de service)
- ➢ Forcer les utilisateurs à changer leurs mots de passe personnels lors de leur prochaine connexion.

Vérifier l'intégrité des fichiers et données :
On doit :

- ➢ Comparer les sommes de contrôle (hash SHA-256, etc.) des exécutables critiques et fichiers sensibles avec des valeurs de référence pour détecter toute altération par l'attaquant et remplacer systématiquement tout binaire système modifié par une version saine d'origine .
- ➢ Inspecter les bases de données et fichiers de configuration pour détecter des backdoors (utilisateur caché, trigger malveillant) et restaurer des copies saines si nécessaire.

Restaurer les données perdues/corrigées :
On doit :

- ➢ Si altération des données restaurer celles-ci à partir des sauvegardes intactes.
- ➢ Reconstruire les systèmes clés.

Appliquer les mises à jour et correctifs système :
On doit :

- ➢ Mettre à jour tous les systèmes restaurés avec les derniers patchs de sécurité (si cela n'a pas été fait dans la phase remédiation).
- ➢ Appliquer les bonnes pratiques qui auraient pu manquer.

11.8. Capitalisation et apprentissage

Objectif :
Tirer les leçons de l'incident, améliorer en continu le dispositif de sécurité et les procédures de réponse. Une fois l'incident résolu, il est indispensable de réaliser un retour d'expérience afin de bénéficier de l'enseignement de cette crise.

Le retour d'expérience :
On doit :

- ➢ Déterminer les causes initiales de l'infection.
- ➢ Déterminer la chronologie de chaque événement important.
- ➢ Déterminer ce qui s'est bien passé et ce qui ne s'est pas bien passé.
- ➢ Chiffrer le coût de l'incident.
- ➢ Rechercher et enregistrer les indicateurs de compromission qui seront utiles pour prévenir une future attaque.

La capitalisation :
On doit :

- ➢ Identifier et apporter des améliorations à la mise en œuvre des contrôles de sécurité de l'information.
- ➢ Identifier et améliorer les résultats de l'évaluation des risques liés à la sécurité de l'information et de la revue de direction.
- ➢ Identifier et améliorer le plan de gestion des incidents de sécurité de l'information.

12. Rapport d'analyse post-incident

12.1. Description de l'incident

Plusieurs systèmes du réseau interne ont été compromis. Un attaquant est parvenu à obtenir un accès utilisateur sur un serveur Linux (192.168.1.2) et un accès administrateur sur un poste Windows (192.168.1.4). Des données sensibles (identifiants, adresses e-mail, salaires) ont été exfiltrées depuis la base de données du serveur web.

12.2. Déroulement des faits :

L'investigation initiale montre que l'intrus a exploité plusieurs vulnérabilités en chaîne :

- ➢ attaque par force brute sur le service SSH d'un serveur web public (192.168.1.2).
- ➢ injection SQL sur les pages de connexion et d'administration.
- ➢ upload d'un fichier PHP malveillant permettant l'exécution de commandes (RCE).

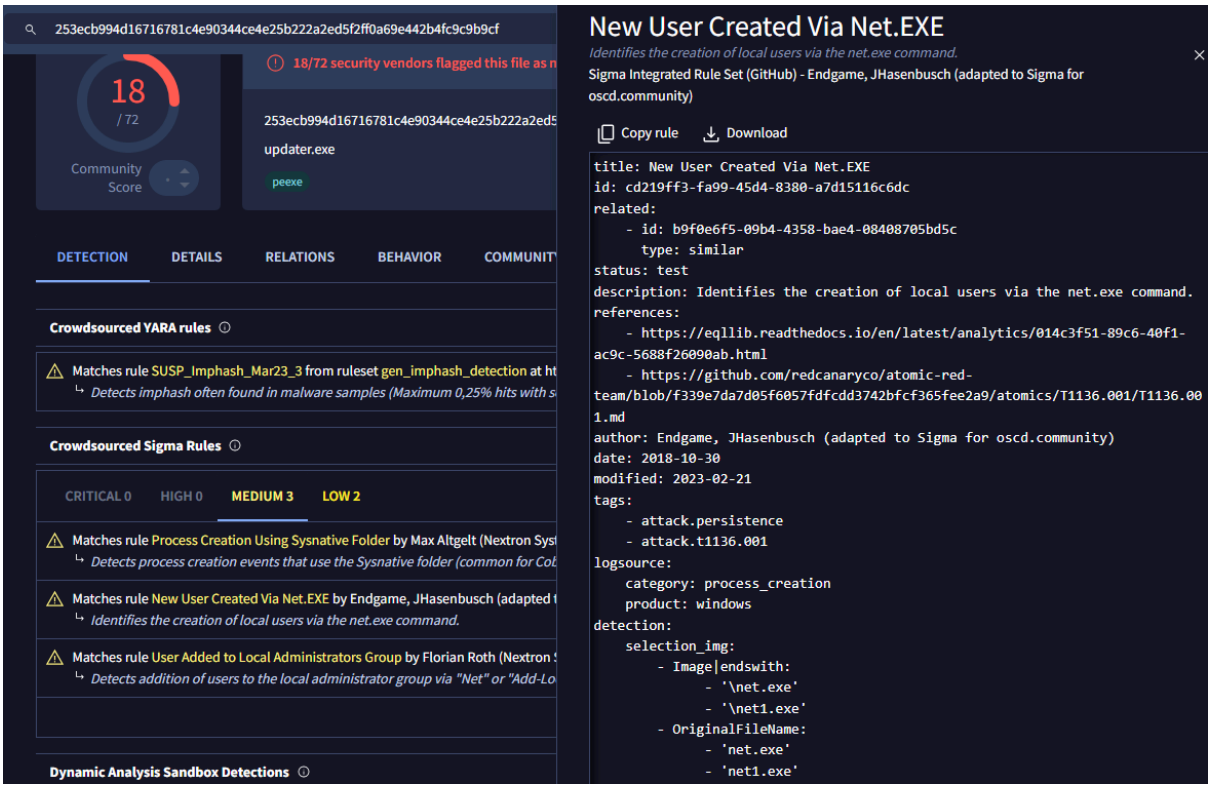
- exploitation d'une faille LFI pour accéder aux fichiers de configuration et aux identifiants de base de données.
- utilisation de ces identifiants pour accéder à distance à le poste Windows 10 (RDP).
- élévation de privilèges locale sur la machine Windows par modification d'un binaire système (updater.exe), menant à la création d'un compte administrateur non autorisé (cyberu).

12.3. Origine du problème

- Le service SSH du serveur web est mal sécurisé.
- Une absence de filtrage des entrées dans l'application web.
- Un accès RDP activé alors que non autorisé.
- Une gestion défaillante des droits sur les fichiers exécutables Windows.

12.4. Indicateurs de compromissions

- **Analyse de virus total du fichier malware :** update.exe



- **Adresse IP :** 192.168.50.9
- **Compte inconnu local :** cyberU

12.5. Actifs supports impactés

- Serveur web Ubuntu 192.168.1.2 hébergeant l'application interne (ports SSH et HTTP ouverts).

- Poste utilisateur Windows 10 (192.168.1.4) membre du domaine IRON4SOFTWARE.LAB.
- Contrôleur de domaine Windows Server 2019 (192.168.1.1).
- Routeur/pare-feu pfSense (192.168.1.254).

12.6. Impacts sur l'entreprise

- **Opérationnel** :
  Arrêt des activités de développement pour remettre en état de fonctionnement les différents serveurs.

- **Financier** :
  Les coûts liés à l'investigation, à la remédiation et à la restauration seront importants.
  Une fuite de données personnelles expose également l'entreprise à des amendes RGPD et à des pertes de confiance clients.

- **Réputationnel** :
  L'exposition de données sensibles et la compromission de comptes administrateurs nuisent gravement à la crédibilité et à la confiance envers IRON4SOFTWARE.

- **Réglementaire** :
  Des données personnelles (identifiants, e-mails, salaires) ayant été exfiltrées, une notification à la CNIL est obligatoire sous 72 heures.

12.7. Identification des Vulnérabilités

- Service SSH vulnérable à attaque bruteforce.
- Injection SQL sur /auth/login.php et /secure/admin.php.
- Upload de fichier PHP non filtré (RCE).
- Accès RDP exposé sans restriction du poste windows 10 192.168.1.4.
- Mauvaise permission de droits sur les dossiers locaux du poste windows 10 192.168.1.4.

12.8. Catégorisation et timeline de l'incident

- **Date et heure de l'incident** :
  04/09/2025, 14:54 (début des activités malveillantes détectées).
- **Date et heure ouverture du ticket d'incident** :
  05/09/2025, 09:00 (Signalement au POC (RSSI) par le développeur Georges DeLaJungle de IRON4SOFTWARE)
- **Catégorie d'incident :** Intrusion / compromission de systèmes internes.

12.9. Composants/actifs concernés

- ➢ Serveur Ubuntu (192.168.1.2)
- ➢ Poste Windows 10 (192.168.1.4)
- ➢ Contrôleur de domaine Windows Server 2019 (192.168.1.1)

12.10. Auteur impliqué

12.10.1. Description de l'auteur

Acteur malveillant inconnu. Les TTP observés (brute-force SSH, injection SQL, RCE, mouvement latéral, élévation de privilèges) sont cohérents avec ceux d'un groupe cybercriminel expérimenté ciblant des environnements Windows/Linux mixtes.

12.10.2. Motivation réelle ou perçue

Financière (vol d'informations et possible revente ou extorsion).

12.11. Résolution de l'incident : Actions menées

12.11.1. Confinement

- ➢ Isolement immédiat des machines compromises (192.168.1.2 et 192.168.1.4) du réseau.
- ➢ Désactivation du compte utilisateur info et du compte local cyberu.
- ➢ Blocage des connexions RDP et SSH non autorisées.

12.11.2. Protection des preuves

- ➢ Sauvegarde des journaux système, réseau et applicatifs des machines compromises (192.168.1.2 et 192.168.1.4).
- ➢ Réalisation d'images disque des machines compromises et de captures mémoire des systèmes compromis pour analyse forensique, et récupération des captures réseau du pfsense.
- ➢ Archivage des fichiers malveillants (shell.php, updater.exe altéré) sur un espace sécurisé hors réseau.

12.11.3. Éradication

- ➢ Corriger les vulnérabilités exploitées (injection SQL, LFI, RCE, binaire modifiable) du serveur web (192.168.1.2).
- ➢ Appliquer les correctifs de sécurité et mettre à jour tous les systèmes concernés.
- ➢ Renforcer la politique d'authentification (MFA, rotation des mots de passe, suppression des comptes obsolètes).

- ➢ Vérifier l’intégrité du contrôleur de domaine et des comptes Active Directory.
- ➢ Surveiller les données divulguées sur internet.

12.11.4. Récupération

- ➢ Restaurer le serveurs web (192.168.1.2) affecté à partir de sauvegardes saines au 03/09/2025 via le logiciel backup Exec.
- ➢ Effacer et réinstaller la machine client windows 10 compromise.

12.11.5. Personnes/entités notifiées

- ➢ **En internes :**Michel noir (DG), Martin Michel (RSSI/DSI).
- ➢ **Extérieures :** CNIL (notification en cours de préparation, délai de 72h), Autorités judiciaires (plainte en cours de dépôt).

12.12.Conclusion

L’incident survenu au sein du réseau IRON4SOFTWARE a mis en évidence plusieurs faiblesses techniques et organisationnelles dans la gestion de la sécurité des systèmes d’information. L’exploitation en chaîne de vulnérabilités (SSH, SQLi, RCE, LFI, élévation de privilèges) a démontré l’importance d’une approche de sécurité globale intégrant à la fois la protection, la détection et la réponse aux incidents.

Dans une logique **d’amélioration continue**, plusieurs axes prioritaires sont identifiés :

- **Renforcement des contrôles préventifs** : mise en place d’un durcissement des systèmes (SSH, RDP, services web), application rigoureuse des correctifs et revue régulière des configurations de sécurité.

- **Amélioration du développement sécurisé** : adoption de pratiques OWASP Top 10 et en incluant aussi des tests de sécurité automatisés (analyse de code, tests d’intrusion applicatifs, validation des entrées utilisateur).

- **Renforcement de la sensibilisation et des processus** : formation continue des équipes IT et métiers à la sécurité, mise à jour des procédures de gestion d’incident et intégration du retour d’expérience dans le plan de sécurité global.

13. Plan de communication de crise

13.1 Objectif

L'objectif est de maintenir une communication rapide, claire et coordonnée entre les parties prenantes internes d'Iron4Software en cas d'incident ou de crise de sécurité impactant la confidentialité, l'intégrité ou la disponibilité des informations.

13.2 Déclenchement du plan

Le plan est activé par :

- Le responsable sécurité **Martin MICHEL** (RSSI/DSI) suite à une remontée d'incident d'un membre de la société (source alerte SIEM ou humaine).
- La direction **Michel NOIR** en cas d'impact opérationnel ou réputationnel majeur.

Critères de déclenchement :

- ➢ Brèche de données clients ou internes
- ➢ Interruption majeure de service ou d'infrastructure
- ➢ Intrusion avérée ou suspicion forte
- ➢ Non-conformité réglementaire grave (RGPD, ISO 27001, contrat client)

13.3 Chaîne de notification interne

13.3.1 Priorisation des notifications

Niveau	Situation typique	Notification obligatoire à
Niveau 1- Incident mineur	Anomalie limitée, sans impact client	Équipe technique, RSSI
Niveau 2- Incident majeur	Dysfonctionnement avec impact client ou risque de fuite de données	RSSI, DSI, DPO
Niveau 3- Crise	Perte de service critique, violation de données massive, communication publique nécessaire	Direction générale, RSSI, DSI, DPO, Équipes concernées

13.3.2 Processus de notification

- Détection : L'incident est identifié par une alerte ou un employé.

Signalement par l'employé : Message interne (Teams, email d'urgence, Téléphone) à : incident@iron4software.com / 0380702430

Selon le niveau d’incident, une notification sera faite dans les 2H au grand maximum suivant la détection :

- Information des équipes par le responsable de notification (RSSI / DSI / Direction) :

Message interne concis via Teams ou messagerie expliquant la situation, les consignes (ex. désactivation de comptes, arrêt de services).

13.4 Canal de communication

Le téléphone sera la canal de communication privilégié en cas de crise importante : ligne directe RSSI / DSI

Les canaux numériques autorisés pour les incidents majeur et mineur :

- ➢ Teams.
- ➢ Emails internes.

Aucun échange d’information critique autre que cité ci-dessus n’est autorisé.

13.5 Responsabilités clés

Rôle	**Responsabilités principales**
RSSI	Évalue la gravité, active le plan, coordonne la communication sécurité
DSI	Supervise l’impact sur les systèmes et infrastructures
Direction Générale	Valide les messages clés et décisions publiques
DPO	Gère la communication vers autorités (CNIL) si données personnelles affectées
Équipes techniques	Fournissent les mises à jour techniques et le statut de résolution

13.6 Modèle de notification interne

Objet : [URGENT] Incident de sécurité – [Type] – [Date/Heure]

Bonjour à tous,

Un incident de sécurité a été détecté sur [système/équipe].
Type d'incident : [ex. compromission de compte, panne critique, fuite de données suspectée]
Impact : [ex. service interrompu, données clients potentiellement affectées]
Actions en cours : [mesures immédiates, équipe en intervention]
Consignes : [ce que les employés doivent/ne doivent pas faire]

Le RSSI et la direction vous tiendront informés de l'évolution.

Iron4Software – Cellule de crise

13.7 Modèle de notification externe (partenaires, clients, fournisseurs)

Chers Clients,

Notre hébergement a fait l'objet d'une cyber attaque dans la nuit du DD/MM/YYYY. Les premières décisions ont été d'isoler les clients potentiellement impactés par cet incident.

Malheureusement, vos environnements de production et ceux d'autres clients ont été mis à l'isolement par prudence. Nous sommes sincèrement désolés de cet incident, nous vous tiendrons informés de l'avancement de la résolution de cet incident.

A ce jour, DD/MM/YYYY nous avons constaté de fuites d'informations et de corruption de données (les back-up J-1 ne semblent pas impactés, des vérifications sont en cours). Une cellule de crise est ouverte afin d'avancer au plus vite sur la résolution de l'incident.

Nous étudions les options de redémarrage possible sur nos hébergements. Nous vous tiendrons informé dès que possible.

Nous restons à votre disposition et vous tiendrons informés de la résolution de l'incident.

Nous vous enverrons une prochaine communication le DD/MM/YYYY à 16h00.

L'Equipe Iron4Software

13.8. Notification des Autorités

Autorité / Entité	Quand notifier ?	Délai	Responsable	Moyen de notification
ANSSI / CERT-FR	Incident majeur (NIS2) – services critiques ou essentiels	Initiale : 24h, Rapport final : 30j	RSSI / DSI	https://club.ssi.gouv.fr/#/declarations
CNIL	Violation de données personnelles avec risques	72h après détection	DPO	https://notifications.cnil.fr/notifications/index
Forces de l'ordre	Cyberattaque avérée (ransomware, sabotage, extorsion, etc.)	Dès confirmation	La direction + RSSI	Dépôt de plainte en commissariat / contact cybercrime (local)
Clients Partenaires Fournisseurs	Impact sur données ou services tiers	Dès décision de la cellule de crise	La direction	Canaux contractuels, mail, téléphone
Assureur cybersécurité	Incident couvert contractuellement	Immédiatement ou selon clause	La direction	Par canal contractuel (mail / plateforme)