Société de l'assurance automobile Québec

Déclaration d'un incident de sécurité de l'information numérique (SIN)
(Confidentiel)

32_P-123.2

Section 1. Description de l'événement de SIN à traiter comme un incident de SIN

Numéro de l'événement de SIN : 21	Signalement de l'événement de SIN : 2023-09-07

1.1 Identification de l'événement de SIN

Source de la déclaration :

- ☐ 1- Utilisateur au siège social
- ☐ 2- Utilisateur hors siège social
- ☐ 3- CSTI
- ☐ 4- CERT/AQ
- ☐ 5- Fournisseur externe
- ☐ 6- Mandataire/partenaires
- ☐ 7- Coordonnateur des incidents majeurs
- ☒ 8- Équipe opérationnelle de gestion de la surveillance
- ☐ 9- Équipe opérationnelle de gestion des accès
- ☐ 10- CSIO (ROSI anciennement)
- ☐ 11- ASA d'une ligne d'affaires
- ☐ 12- Autres : _____

Nom: Guia	Prénom : [redacted]	

1.2 Observations du déclarant de l'événement de SIN

Lors d'un test à l'intérieur de notre [redacted] des justificatifs par défaut ont été identifiés sur un [redacted]

1.3 Confirmation ou non que l'événement de sécurité doive être traité comme un incident

Justifications : La présence de justificatifs par défaut sur [redacted] Cisco est facile à exploiter et permettrait à un acteur malveillant d'en prendre facilement le contrôle et de rendre non disponible les [redacted] qui y sont connectés.

Section 2. Description de l'incident de SIN

2.1 Évaluation des impacts de l'événement de SIN (DIC et clientèles)

Numéro de l'incident : 21

Confirmation de l'incident	Début prise en charge	Fin des interventions
2023-09-07 11:45	[redacted]	[redacted]

Impacts DIC	Moyen	Élevé	Très élevé	Commentaires, précisez au besoin le niveau d'impact
Perte de disponibilité :	☐	☐	☒	
Perte d'intégrité :	☐	☐	☐	
Perte de confidentialité :	☐	☐	☐	

Potentiel incident à portée gouvernementale : ☐ oui ☒ non (dans l'affirmative, informer le CSIO)

2.2 Description de l'incident de SIN après investigation approfondie

Catégorie de l'incident de SIN :

- Classe 1 - Accès non autorisé ☐
- Classe 2 - Déni de service ☐
- Classe 3 - Code malveillant ☐
- Classe 4 – Utilisation non appropriée ☐
- Classe 5 – Activité de reconnaissance ☐
- Classe 6 – Analyses approfondies ☐
- Classe 7 - Vulnérabilité ☒
- Classe 8 – Vol de renseignements personnels ☐

Niveau de sévérité :

- Critique ☐
- Élevé ☐
- Moyen ☒
- Faible ☐

Identification des actifs informationnels impliqués et détenteurs des actifs

Actifs informationnels :

☐ 1- Serveurs	☐ 5- Internet	☐ 9- Site transactionnel	☐ 13- Mobile
☐ 2- Postes	☐ 6- Central	☐ 10- Applications/systèmes	☐ 14- Cloud
☒ [redacted]	☐ 7- Base de données	☐ 11- Site transactionnel	☐ 15- CASA :
☐ 4- Messagerie	☐ 8- Site informationnel	☐ 12- Applications/systèmes	☐ 16- Autre :

Détenteur :

Dans le cas de plus d'un actif, compléter les éléments manquants :

Composition de l'équipe de réponse aux incidents de SIN (ERIS)

	Secteurs	Représentants-coordonnées	Secteurs	Représentants-coordonnées	
	COCD – Tiers 3 ou COMSI	[redacted] Schlott			
	COCD – T2	[redacted] Bernard			
	COCD	[redacted] Guia			
	COCD – T2	[redacted] Bisson			
	CASA	[redacted] Goyet			
	PFR	[redacted] Néron			

Responsable de la coordination de la gestion de l'incident de SIN :

COMSI ☒ ou CSIO ☐ Identifier le responsable :

Informations complémentaires : _____

Section 3. Suivi de la déclaration d'un incident de SIN

(**Statut** (VPE : version préliminaire du signalement de l'événement de SIN, EC : Incident de SIN en cours de résolution, R : incident résolu et version finale de déclaration complétée, A : Incident de SIN annulé)

Statut du formulaire	**Responsable de la mise à jour du statut**	**Date**
R	[redacted] Bisson pour [redacted] Schlott	2023-09-12

Informations complémentaires au besoin :

Chronologie évènement :

Société de l'assurance automobile Québec

Événement d'intérêt

Nom de l'EI	**Vulnérabilité** [redacted]
Sévérité	☐ Critique ☒ Élevé ☐ Moyen ☐ Faible
Outil de détection	[redacted] ☒ Autre : [redacted]
Nom événement	Vulnérabilité [redacted]
Source du signalement	☒ COCD ☐ Externe COCD
Dispositif(s) infecté(s)	[redacted]
Code utilisateur	[redacted]
Chemin de la menace	[redacted]
Description	Déficience au niveau de la faiblesse des justificatifs [redacted]
T1 - Compromission	2023-09-07 11:45
T2 – Déclaration d'incident	[redacted]
T3 – Fermeture de l'incident	[redacted]
Niveau de coordination GMVI	2. Centre opérationnel de cyberdéfense (COCD)
COMSI	[redacted] Schlott
Membres de l'ÉRIS	[redacted] Bernard, [redacted] Bisson, [redacted] Schlott, [redacted] Guiad, [redacted] Goyet, [redacted] Néron

INTERVENTIONS TIERS 1	
Date et heure	**Description**
2023-09-07 11:45	Détection de justificatifs faibles sur la [redacted] lors d'un test [redacted]
Cliquez ou appuyez ici pour entrer une date.	[redacted] Goyet (CASA – remplacant de [redacted] Fay) est informé
2023-09-07 15:20	Discussion avec [redacted]. Il n'est pas complètement à l'aise de changer le [redacted] dans vérfication avant du côté CASA. Nous lui demandons aussi de vérifier si le [redacted] est utilisé sur d'autres actifs similaire. Il dit qu'il va tenter de trouver l'info vendredi (demain) en l'absence de [redacted] Fay (qui revient lundi prochain)
2023-09-07 16:15	J'informe [redacted] (coordonnateur COCD) de la vulnérabilité et [redacted] (COMSI) pour un traitement en incident.
2023-09-08 11:45	Suite à un discussion avec le COMSI et le coordonateur du COCD et avec l'appui de la gestion, on demande un ultimatum à [redacted] pour la fin pm
2023-09-08 13:17	[redacted] m'informe que le mot de passe n'a pas été enregistré dans la voûte et aucune de dispo pour Hugo.
2023-09-08 14:58	[redacted] Goyet confirme que ça sera fait aujourd'hui.
2023-09-08 16:20	Hugo : Avec la précieuse aide de [redacted] Néron, nous avons réussi à modifier le mot de passe de l'utilisateur admin avec la bonne encryption et mit dans la voute de casa. De plus, nous avons aussi modifié le mot de passe du mode [redacted] qui est lui aussi dans la voute. La faille devrait être colmaté! L'utilisateur [redacted] n'est plus en mesure de ce connecté ni en [redacted] et n'y en [redacted]. Notes Les backups des config sont envoyés a l'outils de sauvegarde de casa: [redacted] »
2023-09-08 16:21	Valider par [redacted] que la vulnérabilité n'est plus là. Fermeture de l'incident
Cliquez ou appuyez ici pour entrer une date.	

INTERVENTIONS TIERS 2	
Date et heure	**Description**
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	

INTERVENTIONS TIERS 2	
Date et heure	**Description**
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	

INTERVENTIONS TIERS 3	
Date et heure	**Description**
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	
Cliquez ou appuyez ici pour entrer une date.	

Directive sur la gestion des vulnérabilités

DATE DE MISE EN VIGUEUR
2023-11-21

1. RÉSUMÉ

Cette directive découle de la Politique sur la sécurité de l'information de la Société de l'assurance automobile du Québec (Société). Elle complète par ailleurs les dispositions du processus gouvernemental de gestion des menaces, vulnérabilités et incidents (GMVI) en ce qui a trait à la gestion des vulnérabilités, en précisant les exigences en cette matière ainsi que les rôles et responsabilités nécessaires à la mise en œuvre d'un processus de gestion efficace des vulnérabilités à la Société.

2. BUT

La présente directive a pour objectif de renforcer la sécurité de l'information de la Société par un encadrement adéquat de la gestion des vulnérabilités auxquelles elle peut être exposée. Ultimement, elle vise à :

- déterminer les intervenants à qui elle s'applique et définir leurs rôles et leurs responsabilités en matière de gestion des vulnérabilités;
- renforcer les capacités du Centre opérationnel de cyberdéfense (COCD);
- assurer la protection des actifs informationnels de la Société, accélérer la prise en charge de leurs vulnérabilités et ainsi réduire les risques qui leur sont associés.

3. CHAMP D'APPLICATION

Cette directive s'adresse à tout membre du personnel ou prestataire de services, responsable ou impliquée dans la gestion, la mise en place, la surveillance et l'entretien des actifs informationnels de la Société.

La directive s'applique à l'ensemble des actifs informationnels, autant en interne qu'en infonuagique, détenus ou consommés par la Société, que leur gestion soit assurée par elle-même ou confiée à un tiers.

4. PRÉALABLES

La présente directive s'inscrit dans le cadre légal, normatif et réglementaire suivant :

- Politique sur la sécurité de l'information, Société de l'assurance automobile du Québec
- Cadre de gestion de la sécurité de l'information, Société de l'assurance automobile du Québec
- Processus de gestion des menaces, vulnérabilités et incidents, Centre gouvernemental de cyberdéfense

Elle prend également appui sur les documents suivants :

- ISO/CEI 27002 Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information (norme), troisième édition (03-2022)
- NIST SP 800-53 (RA-5 Surveillance et analyse des vulnérabilités, CA-2 Évaluation des contrôles, CA-8 Tests d'intrusion, SA-11 Tests et évaluations des applications, SI-2 Remédiation des failles);
- CIS (N° 03 – Gestion continue des vulnérabilités).

5. DÉFINITIONS

Actif informationnel

Ensemble des ressources informationnelles ayant une valeur pour la personne physique ou morale qui en est détentrice, et dont la protection nécessite la mise en place de mesures de sécurité particulières.

Activité de découverte des vulnérabilités

Toute activité de test ou d'audit permettant de découvrir des vulnérabilités sur les actifs informationnels de la Société. Il peut s'agir de veilles technologiques, de balayages de vulnérabilité, de tests d'intrusion ou d'audits de conformité.

Balayage de vulnérabilités

Balayage consistant à déceler des vulnérabilités sur des cibles préalablement identifiées, dans un contexte précis et selon une portée prédéfinie. Les vulnérabilités détectées sont documentées et ne sont pas exploitées.

Intrusion

Accès non autorisé à un système informatique ou à un réseau, obtenu en contournant ou en désamorçant les dispositifs de sécurité en place ou en exploitant une vulnérabilité.

Test d'intrusion

Test consistant à simuler une attaque en identifiant des vulnérabilités et en exploitant celles-ci, de manière récursive, afin de tester en profondeur les mécanismes de sécurité. Tout comme les tests de vulnérabilités, les vulnérabilités sont documentées, en plus des attaques simulées.

Vulnérabilité

Absence ou faiblesse d'une protection d'actif qui rend une menace potentiellement plus susceptible de se produire ou susceptible de se produire plus fréquemment.

6. PRINCIPES DIRECTEURS

La gestion des vulnérabilités s'appuie sur les principes d'évaluation périodique des risques, de cohérences des mesures, de partage des responsabilités et d'imputabilité.

6.1. **Exigences générales**

- Un processus formel permettant en continu de découvrir, d'analyser, de traiter et de rendre compte des vulnérabilités est mis en œuvre dans les activités du COCD, dans la gestion des infrastructures et dans le cycle de vie du développement et d'acquisition des systèmes et des applications. Le processus est cohérent avec le processus gouvernemental de GMVI.
    - Tout système, équipement ou application est vérifié avant sa mise en production afin d'identifier et de traiter préalablement ses vulnérabilités selon les standards prescrits.
    - Les systèmes, équipements et applications en production font l'objet d'une vérification régulière afin d'identifier et de corriger leurs vulnérabilités.
- Un processus formel d'identification proactive et d'application continue des correctifs de sécurité des actifs informationnels de la Société est mis en œuvre et suivi, afin de réduire les vulnérabilités.

- Un inventaire exhaustif et à jour des actifs informationnels de la Société, incluant leur criticité, est mis en place pour une gestion efficace des vulnérabilités. Les informations contenues dans cet inventaire sont utilisées dans toutes les étapes du processus de gestion des vulnérabilités.
- Des mécanismes de veille en matière de gestion des vulnérabilités sont mis en place pour assurer une meilleure compréhension de l'univers des vulnérabilités et des menaces auxquelles la Société peut être exposée.

6.2. **Exigences liées à la découverte des vulnérabilités**

- Les activités de découverte sont diversifiées pour assurer une meilleure identification des vulnérabilités applicables aux actifs informationnels de la Société. Ces activités sont choisies en fonction des types de vulnérabilités et des systèmes concernés : veille en matière de vulnérabilités publiées par les fournisseurs, balayages de vulnérabilités de l'infrastructure, balayages de vulnérabilités applicatives, revues de codes, audits de conformité, audits de sécurité, tests d'intrusion, revue documentaire, revue des processus.
- Les activités de découverte sont réalisées de façon périodique afin d'identifier, en temps opportun, les vulnérabilités applicables aux actifs informationnels de la Société. La périodicité des activités de découvertes est déterminée en fonction de la sensibilité et de l'exposition des actifs concernés aux menaces et des besoins de la Société.
- Les listes de vulnérabilités découvertes sont documentées et mises à la disposition de chaque responsable de système concerné (plateformes technologiques et applications) pour leur prise en charge.

6.3. **Exigences liées à l'analyse et la priorisation des vulnérabilités**

- Les vulnérabilités découvertes sont évaluées et analysées par les différentes parties prenantes en suivant les standards de la Société et en adéquation avec le processus gouvernemental de GMVI.
- Toutes les vulnérabilités découvertes sont contextualisées pour évaluer le niveau de risque associé, en fonction de leur criticité, de la sensibilité des actifs concernés et de leur exposition à la menace. Les informations de l'inventaire des actifs informationnels sont de ce fait utiles à l'analyse des vulnérabilités et la priorisation des actions de remédiation.
- Les priorités de traitement des vulnérabilités sont établies en fonction du risque évalué, relativement à la concrétisation d'une menace par l'exploitation de celles-ci. Il convient de traiter en priorité les vulnérabilités qui représentent un risque élevé pour l'organisation.

6.4. **Exigences liées au traitement des vulnérabilités**

- Toute vulnérabilité découverte est associée à un responsable afin de faciliter le suivi des correctifs.
- Toutes les vulnérabilités découvertes sont traitées dans les délais prescrits par les standards de la Société, en conformité avec le processus gouvernemental de GMVI et en fonction des niveaux de risques associés aux vulnérabilités, soit en appliquant des actions correctives, soit en mettant en place des mesures d'atténuation.
- Les risques associés à l'installation d'un correctif doivent être comparés aux risques découlant de la vulnérabilité. Le correctif sera appliqué si les risques relatifs à son installation sont inférieurs à ceux liés à la vulnérabilité à corriger.
- Les correctifs sont analysés et testés avant d'être appliqués, afin de vérifier leur efficacité et de s'assurer qu'ils n'entraînent pas d'effets collatéraux.
- Les traitements de vulnérabilités sont effectués dans le respect des processus de gestion des services informatiques, tels que le processus de gestion des demandes de services, le processus de gestion des changements ou celui de la gestion des incidents.

- Les traitements de vulnérabilités sont confirmés par des tests de contrôle tels qu'un second balayage ou une vérification manuelle des configurations.
- Dans les cas où les risques associés à une vulnérabilité doivent faire l'objet d'une acceptation (par exemple lorsqu'un correctif présente plus de risque que la vulnérabilité elle-même ou lorsque des mesures d'atténuation sont déjà en place), la situation est documentée et fait l'objet d'une approbation conjointe du détenteur et du chef délégué de la sécurité de l'information (CDSI), sous recommandation du chef de la sécurité de l'information organisationnelle (CSIO).

6.5. **Exigences liées au suivi du processus**

- Le suivi des vulnérabilités et de leur traitement est documenté dans un registre centralisé.
- Des indicateurs opérationnels alimentent des tableaux de bord qui sont mis à la disposition des équipes responsables des plateformes technologiques et applications afin de leur permettre de suivre l'évolution des vulnérabilités dans leur contexte.
- Des indicateurs de gestion et de performance alimentent un tableau de bord qui est mis à disposition des gestionnaires et responsables concernés comme outil d'aide à la décision en matière de gestion de la sécurité de l'information.
- Les vulnérabilités non corrigées dans les délais prescrits par les standards de la Société et dont le niveau de risque dépasse le seuil de tolérance de celle-ci sont prises en charge par le processus de gestion des incidents de sécurité de l'information.
- Des balayages de contrôle et des tests d'intrusion à la demande sont effectués périodiquement pour valider l'efficacité des actions de traitements des vulnérabilités.
- Une vérification régulière du processus de gestion des vulnérabilités est réalisée pour s'assurer de son efficacité et déceler des points d'amélioration.

7. RÔLES ET RESPONSABILITÉS

Le cadre de gestion de la sécurité de l'information établit la structure de gouvernance et de coordination de la sécurité de l'information de la Société. Outre les responsabilités indiquées dans ce cadre de gestion et celles mises en œuvre dans le processus gouvernemental de GMVI, les responsabilités additionnelles en matière de gestion des vulnérabilités à la Société sont indiquées dans la présente directive.

7.1. Le **chef délégué de la sécurité de l'information (CDSI) :**

- approuve la présente directive;
- approuve, conjointement avec le détenteur de l'actif concerné et sous recommandation du CSIO, les risques associés aux vulnérabilités qui doivent faire l'objet d'une acceptation;
- informe sans délai le chef gouvernemental de la sécurité de l'information (CGSI)[1] lorsqu'une vulnérabilité présente un risque qu'un préjudice sérieux soit causé, c'est-à-dire lorsqu'une coordination au niveau gouvernemental est requise.

7.2. Le **comité sur la sécurité de l'information (CSI) :**

- valide la présente directive et en recommande l'approbation.

[1] Le CGSI œuvre au sein du ministère de la Cybersécurité et du Numérique. Ses responsabilités sont notamment définies dans la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement.

7.3. Le **chef de la sécurité de l'information organisationnelle (CSIO) :**

- définit et communique les objectifs et les orientations en matière de gestion des vulnérabilités;
- s'assure de la mise en œuvre de toute action requise pour la prise en charge d'une vulnérabilité;
- recommande au CDSI l'approbation des risques associés aux vulnérabilités qui doivent faire l'objet d'une acceptation;
- avise sans délai le CDSI lorsqu'une vulnérabilité présente un risque qu'un préjudice sérieux soit causé, c'est-à-dire lorsqu'une coordination au niveau gouvernemental est requise.

7.4. Le **responsable opérationnel en cyberdéfense (ROCD) :**

- s'assure du respect des standards de l'industrie et des exigences gouvernementales en matière de gestion des vulnérabilités;
- avise sans délai le CSIO lorsqu'une vulnérabilité présente un risque qu'un préjudice sérieux soit causé, c'est-à-dire lorsqu'une coordination au niveau gouvernemental est requise;
- est responsable de la mise en œuvre du processus de gestion des vulnérabilités et de son amélioration continue.

7.5. Le **responsable de la gouvernance de la sécurité de l'information (RGSI)**:

- effectue une veille relativement aux vulnérabilités liées au facteur humain et aux techniques d'ingénierie sociale, et demeurent à l'affût des moyens de protections;
- réalise des activités de sensibilisation et de formation du personnel en fonction de ces vulnérabilités;
- s'assure que des mesures sont mises en place afin de traiter les vulnérabilités liées au facteur humain ainsi que celles relatives à la sécurité physique;
- rend compte au CSIO des activités de sensibilisation et du suivi des vulnérabilités humaines et physiques.

7.6. Le **coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) :**

- coordonne le processus de gestion des vulnérabilités et est responsable de son exécution.

7.7. Le **centre opérationnel de cyberdéfense** (COCD) :

- met en place des mécanismes de veille de sécurité relativement aux technologies utilisées à la société;
- effectue une veille des menaces informatiques de sécurité;
- s'assure du déploiement et opère les outils nécessaires à la gestion des vulnérabilités;
- effectue des analyses de vulnérabilités sur les infrastructures de la Société avec les outils normalisés pour cette tâche;
- planifie et les tests d'intrusion et les audits techniques;
- coordonne et supervise la table de gestion des vulnérabilités et pilote les ateliers d'analyse et de priorisation des vulnérabilités;
- accompagne les détenteurs et les équipes responsables de plateformes et d'applications pour le traitement des vulnérabilités;
- s'assure que les responsables de plateformes technologiques et d'applications appliquent les mesures correctives ou compensatoires pour éradiquer ou remédier les vulnérabilités dans les délais prescrits;
- maintient l'inventaire des actifs informationnels de la Société;
- maintient le registre centralisé de suivi des vulnérabilités;
- élabore les tableaux de bord nécessaires au suivi de la gestion des vulnérabilités;

- s'assure d'être en conformité, dans toutes ses actions en matière de gestion des vulnérabilités, avec la politique et le cadre de gestion de la sécurité de l'information de la Société.

7.8. La **table de gestion des vulnérabilités :**

Cette table réunit une équipe pluridisciplinaire formée de membres permanents et d'invités ad hoc en fonction des vulnérabilités découvertes. Elle:

- analyse les vulnérabilités en tenant compte des menaces et de la sensibilité des actifs concernés;
- priorise les vulnérabilités en fonction des risques, de la sensibilité des actifs concernés et de leur exposition aux menaces;
- établit et soumet des plans de traitement aux détenteurs concernés.

7.9. Le **responsable de l'architecture de sécurité de l'information :**

- effectue la veille sur les pratiques et tendances en gestion de la sécurité de l'information;
- conçoit la stratégie des tests d'intrusion et audits techniques;
- participe à la table de gestion des vulnérabilités en tant que membre permanent pour l'analyse, la priorisation et la conception de plans de traitement;
- accompagne les détenteurs et les équipes responsables de plateformes et d'applications pour le traitement des vulnérabilités;
- met à jour, au besoin, les architectures de sécurité relativement au traitement des vulnérabilités.

7.10. Le **responsable de l'architecture technologique :**

- effectue la veille sur les produits de l'infrastructure technologique, incluant le suivi de leur cycle de vie;
- participe à la table de gestion des vulnérabilités en tant que membre permanent pour l'analyse, la priorisation et la conception de plans de traitement;
- accompagne les équipes responsables des actifs informationnels pour le traitement des vulnérabilités détectées;
- met à jour, au besoin, les architectures technologiques relativement au traitement des vulnérabilités.

7.11. Le **responsable du cadre de développement :**

- effectue la veille sur les pratiques et tendances en matière de développement sécuritaire et de gestion de vulnérabilités applicatives;
- participe à la table de gestion des vulnérabilités à titre de membre invité, pour l'analyse, la priorisation et la conception des plans de traitement de vulnérabilités applicatives;
- accompagne les détenteurs et les équipes responsables d'applications pour le traitement des vulnérabilités applicatives;
- met à jour, au besoin, le cadre de développement relativement au traitement des vulnérabilités applicatives.

7.12. Les **équipes responsables de plateformes technologiques :**

- alimentent l'inventaire des actifs informationnels en fournissant l'information à jour concernant les plateformes technologiques sous leur responsabilité;
- effectuent la veille de sécurité relativement aux technologies dont ils sont responsables et demeurent à l'affût des correctifs et des mises à jour annoncées par les fournisseurs pour les actifs sous leur responsabilité;
- identifient et appliquent régulièrement les correctifs de sécurité des systèmes qu'ils gèrent;

- participent à la table de gestion des vulnérabilités à titre de membres invités pour l'analyse, la priorisation et la conception de plans de traitement;
- corrigent ou mitigent les vulnérabilités qui leur sont soumises;
- rendent compte au COCD du traitement des vulnérabilités aux plateformes technologiques identifiées.

7.13. Les **équipes responsables d'applications :**

- alimentent l'inventaire des actifs informationnels en fournissant l'information à jour concernant les applications sous leur responsabilité;
- effectuent la veille de sécurité relativement aux technologies utilisées par les applications dont ils sont responsables, et demeurent à l'affût des correctifs et des mises à jour annoncées par les fournisseurs;
- identifient et appliquent régulièrement les correctifs de sécurité des applications qu'ils gèrent;
- participent à la table de gestion des vulnérabilités à titre de membres invités pour l'analyse, la priorisation et la conception de plans de traitement;
- corrigent ou mitigent les vulnérabilités applicatives qui leur sont soumises;
- rendent compte au COCD du traitement des vulnérabilités applicatives identifiées.

7.14. Les **détenteurs:**

- s'assurent que les informations d'inventaire nécessaires à la gestion des vulnérabilités des actifs sous leur responsabilité sont à jour;
- s'assurent que les vulnérabilités identifiées pour leurs actifs sont prises en charge dans les meilleurs délais, analysées, priorisées et traitées en respectant les niveaux de service convenus à la Société;
- approuvent, conjointement avec le CDSI et sous recommandation du CSIO, les risques associés aux vulnérabilités des actifs sous leur responsabilité qui doivent faire l'objet d'une acceptation.

8. DISPOSITIONS FINALES

- **Responsable du document :** Le chef de la sécurité de l'information organisationnelle est responsable de l'élaboration, du suivi et de l'évaluation de cette directive. Toute demande de dérogation lui est adressée.
- **Mise à jour :** Le chef de la sécurité de l'information organisationnelle est responsable de la mise à jour de la directive qui est révisée tous les trois ans ou au besoin.

Société de l'assurance automobile Québec

CADRE NORMATIF DE LA SÉCURITÉ DE L'INFORMATION

Norme sur la gestion des vulnérabilités

Version 1.0

Juin 2023

Table des matières

1. INTRODUCTION 4
1.1. Objectif de la norme 4
1.2. Champ d'application de la norme 4
1.3. Cadre de référence 5
1.4. Définitions 5
Qu'est-ce qu'une vulnérabilité? 5
Quels sont les différents types de vulnérabilités? 6
Qu'est-ce que la gestion des vulnérabilités? 6
Qu'est-ce que la gestion des correctifs de sécurité? 7
2. STANDARDS ET RÈGLES DE LA SOCIÉTÉ 8
2.1. Règles liées aux activités de préparation 8
[redacted]
Tableau 2 - Description des zones de balayage d'infrastructure 10
Tableau 3 - Fréquence des balayages 10
[redacted]
2.2. Règles liées à la découverte des vulnérabilités 11
Veille technologique et de sécurité 11
Balayages de vulnérabilités d'infrastructure 12
Balayage de vulnérabilité applicative 13
Test d'intrusion 14
Revue de code 15
Examen de conformité des configurations 16
Revue d'architecture de sécurité 16
2.3. Règles liées à l'analyse et la priorisation des vulnérabilités 17
[redacted]
2.4. Règles liées au traitement des vulnérabilités 19
2.5. Règles liées à la vérification de la remédiation des vulnérabilités 21
2.6. Règles liées au suivi des vulnérabilités 21
2.7. Règles liées à la reddition des comptes 23
2.8. Règles liées à l'amélioration continue 25
3. [redacted]

4. DISPOSITIONS FINALES 27
4.1. Autorité 27
4.2. Mise en vigueur 27
4.3. Révision 27
4.4. Approbation 27
ANNEXES 28
Références 28
Description du cadre de référence 28

1. INTRODUCTION

1.1. Objectif de la norme

Le présent document a pour objectif d'uniformiser les pratiques en matière de gestion des vulnérabilités à la Société. Il permet au Centre opérationnel de cyberdéfense (COCD) ainsi qu'aux diverses équipes impliquées dans la découverte, l'analyse, la priorisation et le traitement des vulnérabilités de suivre des normes et des standards définis par la Société en cette matière. Tout au long de ce document, il est impératif de comprendre que la gestion des vulnérabilités est un processus en continu.

1.2. Champ d'application de la norme

La norme sur la gestion des vulnérabilités touche autant l'infrastructure matérielle que logicielle de la Société, qu'elle soit gérée à l'interne ou confiée à un tiers. Le processus de gestion des vulnérabilités concerne donc l'ensemble des composants du système d'information de la Société, notamment :

- Tous les environnements de la Société (production, préproduction, développement et laboratoire);
- Tous les serveurs, indépendamment de leur rôle ou de leur emplacement physique ou logique;
- Tous les postes de travail des utilisateurs connectés au réseau de la Société. On entend par poste de travail les postes fixes, les postes virtuels, PC portables, dispositifs mobiles, etc.;
- Tous les logiciels, progiciels et applications développés, acquis ou en mode service;
- Tous les environnements infonuagiques de la Société;
- Tous les équipements de réseautique, c'est-à-dire les aiguilleurs, pare-feu, commutateurs, bornes Wifi, etc.;
- Tous les dispositifs divers possédant une adresse IP connectés au réseau de la Société : imprimantes, numériseurs, caméras IP, téléphones IP, objets connectés, etc.;
- Tout équipement ou service hébergé chez un fournisseur externe (dans le respect des ententes contractuelles conclues).

> En acquérant une certaine maturité, les vulnérabilités liées à des facteurs environnementaux ou humains ainsi que les vulnérabilités des processus d'affaires et des dispositifs de sécurité physique devront être impliquées dans la portée.

1.3. Cadre de référence

La présente norme s'appuie sur la Directive sur la gestion des vulnérabilités de la Société ainsi que sur les meilleures pratiques de l'industrie, notamment celles décrites à l'annexe 1 :

- Les pratiques recommandées du Secrétariat du Conseil du trésor et du Centre gouvernemental de Cyberdéfense (CGCD);
- Les contrôles du CIS (Center for Internet Security);
- Les recommandations de la norme ISO/IEC 27002 : 2022 – Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques;
- Les recommandations du standard NIST SP 800-53;
- Les recommandations du standard NIST CSF (Cybersecurity framework);
- Les recommandations du standard NIST SP 800-171;
- Les recommandations de la norme PCI-DSS 3.2;
- Les rapports d'analystes de Gartner.

1.4. Définitions

Outre les définitions présentes dans la Directive sur la gestion des vulnérabilités, la présente section permet au lecteur de comprendre tous les concepts autour de la gestion des vulnérabilités.

Qu'est-ce qu'une vulnérabilité?

Dans le domaine de la sécurité de l'information, une vulnérabilité ou faille de sécurité est une faiblesse dans un système d'information permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la disponibilité, à la confidentialité ou à l'intégrité des données qu'il contient.

Ces vulnérabilités sont la conséquence de faiblesses dans la conception, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système d'information, mais il s'agit souvent d'anomalies logicielles liées à des erreurs de programmation ou à de mauvaises pratiques de configuration. Ces dysfonctionnements logiciels sont en général corrigés à mesure de leurs découvertes, mais le système reste exposé à une éventuelle exploitation tant que le correctif (temporaire ou définitif) n'est pas publié et installé. C'est pourquoi il est important de maintenir les logiciels à jour avec les correctifs fournis par les éditeurs de logiciels. La procédure d'exploitation d'une vulnérabilité logicielle est appelée exploit.

Il est à noter qu'une vulnérabilité corrigée peut réapparaître à la suite d'une réinstallation, d'un déploiement de nouveaux systèmes avec d'anciennes configurations, d'une restauration de sauvegarde, etc., d'où la nécessité de continuer à la surveiller même après le déploiement d'un correctif.

Pour les vulnérabilités ne pouvant être corrigées pour diverses raisons (ressources humaines ou financières insuffisantes, correctif non disponible, freins organisationnels, contraintes techniques spécifiques, etc.), l'organisation devra s'atteler à mettre en place des mesures de

sécurité palliatives. Ces mesures peuvent être par exemple des mesures de prévention (règle plus stricte sur un pare-feu situé en amont, etc.) ou des mesures de réaction (renforcement du niveau de supervision des traces, etc.).

Quels sont les différents types de vulnérabilités?

Le type de vulnérabilités qui vient spontanément à l'esprit en tout premier lieu est probablement les bogues logiciels, tels que ceux médiatisés sur les systèmes d'exploitation de Microsoft et des applications qui y sont supportées comme Windows 10, Microsoft Word, Adobe Flash, Oracle, Java, etc. Il s'agit dans ce cas de vulnérabilités dites **technologiques ou d'infrastructures**.

Un autre type de vulnérabilité est relatif aux failles de sécurité applicatives. Par exemple, lorsque la saisie de données d'un utilisateur dans un formulaire électronique d'une application n'est pas contrôlée, elle permet l'exécution de commandes non autorisées pouvant aussi mettre en péril la disponibilité, l'intégrité et la confidentialité des données sous-jacentes. Ce type de vulnérabilité est dite **applicative**.

Lorsque le facteur humain est exploité, par exemple lors de campagnes d'hameçonnage menant à un incident de sécurité de l'information numérique, il s'agit d'une vulnérabilité **humaine**. Une erreur de manipulation ou encore un manque de formation ou de sensibilisation des utilisateurs pourraient aussi être à l'origine de ce type de vulnérabilité.

D'autres types de vulnérabilités sont relatives à la gestion de la sécurité **physique.** Celles-ci concernent les faiblesses dans les mécanismes de contrôle d'accès physique et de protection contre les risques environnementaux (incendies, inondation, etc.) et qui peuvent entraîner des incidents de sécurité de l'information numérique.

Enfin, il existe des vulnérabilités au niveau des **processus** de travail qui peuvent engendrer des incidents de sécurité de l'information numérique. Par exemple, l'omission d'une étape de validation ou encore la non-séparation des tâches pouvant entraîner des pertes d'intégrité ou de la fraude.

Qu'est-ce que la gestion des vulnérabilités?

La gestion des vulnérabilités est le processus par lequel les vulnérabilités du système d'information sont identifiées, les risques de ces vulnérabilités sont évalués et les mesures correctives de ces vulnérabilités sont mises en œuvre pour gérer les risques qui y sont associés.
Les vulnérabilités d'une infrastructure informatique constituent un risque opérationnel majeur. L'exploitation d'une seule vulnérabilité informatique peut porter préjudice aux activités opérationnelles d'une organisation, détériorer son image, entraîner une perte de confiance de ses clients, etc.

Ainsi, la mise en place d'un processus de gestion des vulnérabilités formel est essentielle pour obtenir une visibilité de la surface d'attaque contre les infrastructures de la Société, afin d'appliquer des mesures correctives et de là réduire le risque à un niveau acceptable pour la Société, et ainsi prévenir des incidents de sécurité de l'information.

Gartner préconise la mise en place d'un cycle de gestion des vulnérabilités, en amélioration continue, comme l'indique le schéma ci-dessous :

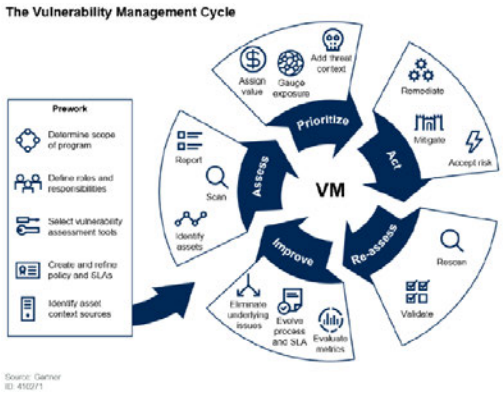


Figure 1 - Cycle de gestion des vulnérabilités

Les facteurs de succès de mise en œuvre d'un tel processus sont :

- Adopter une approche raisonnée et structurée;
- Impliquer la gestion et l'ensemble des parties prenantes concernées;
- Nommer un responsable du programme de gestion des vulnérabilités;
- Identifier et allouer un budget spécifique à la fois d'investissement et de fonctionnement;
- Organiser, automatiser et s'approprier la gestion des vulnérabilités;
- Communiquer de manière transparente et adaptée aux parties prenantes impliquées;
- Créer des éléments de motivation pour les administrateurs informatiques;
- Définir et mettre en œuvre des indicateurs clefs.

Qu'est-ce que la gestion des correctifs de sécurité?

La gestion des correctifs est le processus d'identification, d'acquisition, de test, d'installation et de vérification des correctifs pour les produits et les systèmes. Les correctifs, aussi appelés mises à jour, permettent de remédier à des problèmes de sécurité ou de fonctionnalité des logiciels et des micrologiciels. Ils peuvent servir à d'autres fins que la simple correction de failles logicielles; ils peuvent en effet ajouter ou supprimer des fonctionnalités aux logiciels et micrologiciels, y compris des capacités de sécurité.

Les correctifs de sécurité sont conçus pour colmater des failles de sécurité et ainsi réduire les risques de sécurité d'une organisation.

Lorsque les fournisseurs décident de ne plus prendre en charge les anciennes versions de leurs produits, cela implique de ne plus publier de correctifs pour corriger les nouvelles vulnérabilités. Cela rend les anciennes versions non prises en charge moins sûres au fil du temps. Ainsi, les organisations doivent, dans la mesure du possible, veiller à utiliser des versions de produits prises en charge par les fournisseurs. Dans le cas contraire, des mesures palliatives doivent être mises en place pour atténuer les risques.

En effet, lorsqu'il n'existe pas de correctif, des solutions alternatives existent et peuvent être mises en œuvre, telles que des solutions de contournement temporaires impliquant une reconfiguration de logiciel ou de contrôle de sécurité.

Toute organisation soucieuse de la sécurité de ses systèmes d'information doit porter une attention particulière à la gestion des correctifs de sécurité et en assurer une gestion proactive et effective.

2. STANDARDS ET RÈGLES DE LA SOCIÉTÉ

Les règles ci-dessous s'inspirent [redacted]

2.1. Règles liées aux activités de préparation

2.1.1. Pour une gestion efficace des vulnérabilités, l'inventaire des actifs informationnels doit comporter minimalement les éléments suivants :

- Les équipements connectés au réseau interne (incluant le Wifi);
- Les équipements exposés sur Internet;
- Les autres équipements Bluetooth;
- Les services que ces équipements exposent au réseau;
- Les logiciels et applications exposés au réseau;
- Les sites Web du réseau interne (visibles ou VHost cachés);
- Les sites Web exposés sur Internet (visibles ou VHost cachés).

2.1.2. Le coffre à outils du COCD doit comporter tous les dispositifs nécessaires pour assurer une bonne couverture de la gestion des vulnérabilités. Citons notamment, mais sans s'y limiter :

- Des outils de balayage des vulnérabilités d'infrastructure;
- Des outils d'analyse de code (statique et dynamique);
- Des outils de balayage de ports;
- Des outils d'audit de configuration;
- Des outils de gestion des correctifs;
- Des scanneurs de vulnérabilités ciblés (par exemple : WPScan, RouterSploit, SQLmap, BruteSpray, Burp Suite, Zap, W3af, Nikto, acunnetix, etc.).

2.1.3. Le COCD doit s'assurer de la bonne calibration et de la mise à jour des outils devant servir à la découverte, à l'analyse et à la priorisation des vulnérabilités, en fonction des normes de l'industrie.

Au préalable de chaque activité de découverte des vulnérabilités :

2.1.4. L'équipe responsable de l'activité de découverte doit identifier les actifs concernés et la portée de la découverte, ainsi que les efforts et moyens matériels nécessaires;

2.1.5. Le gestionnaire de l'équipe responsable doit obtenir les autorisations nécessaires pour effectuer la découverte afin d'éviter de la confondre avec une tentative de reconnaissance lancée par un attaquant ou une personne malveillante;

2.1.6. Les détenteurs des actifs impactés par les activités de découvertes doivent être informés;

2.1.7. Les activités de découverte de vulnérabilités doivent faire l'objet d'une demande de changement et doivent être réalisées selon ce qui a été établi dans cette demande. Pour ce faire, un calendrier des balayages doit être établi et approuvé à l'avance au comité des changements;

2.1.8. Toute modification du calendrier des balayages doit faire l'objet d'une nouvelle demande de changement;

2.1.9. En dehors du calendrier de balayages, des balayages ciblés à la demande peuvent être effectués par le COCD, par exemple à la suite d'alertes du CERTAQ, du centre gouvernemental de cyberdéfense (CGCD) ou d'un fournisseur concernant des vulnérabilités critiques actives ou des menaces imminentes sur les produits et services utilisés à la société;

2.1.10. L'équipe responsable de l'activité de découverte doit respecter les plages horaires convenues avec les détenteurs d'actifs concernés pour éviter toute perturbation au fonctionnement normal des systèmes. Pour les infrastructures, les plages et fréquences ci-dessous sont en vigueur à la Société :

Tableau [redacted]

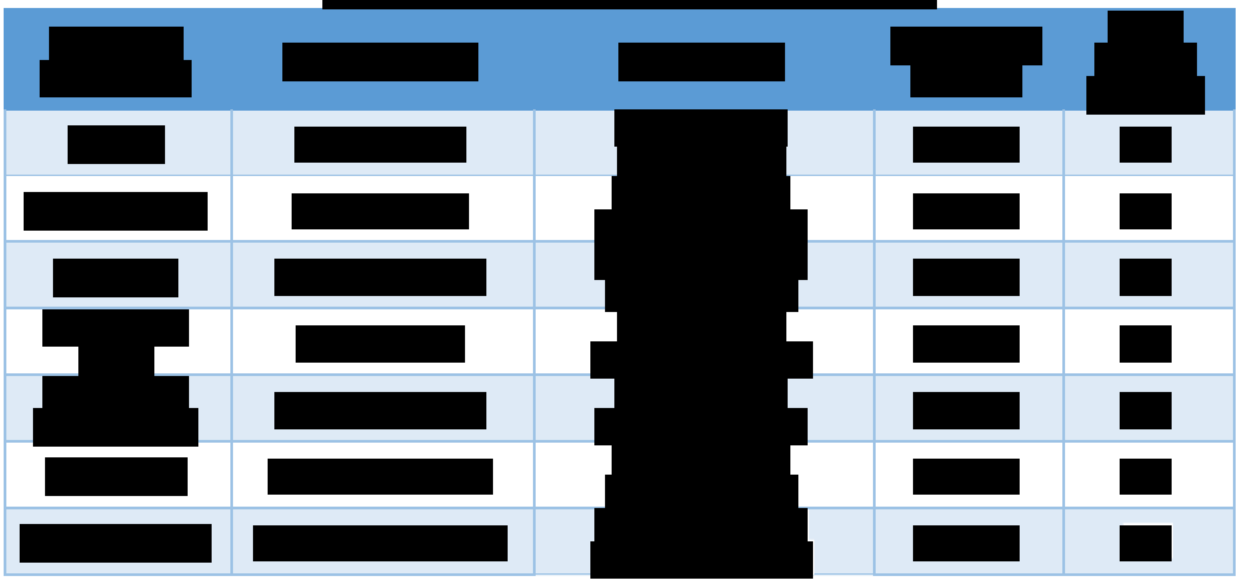


Tableau 2 - Description des zones de balayage d'infrastructure

Zone	Description de la zone
A+ Très confiant	Zone isolée. C'est une zone interne de confiance où nous retrouvons les infrastructures principales de la Société.
A En confiance	Zone interne. C'est une zone où la Société est en confiance avec l'infrastructure qui y réside (surveillance).
B Assez confiant	Zone démilitarisée. C'est une zone où la Société est confiante, mais beaucoup plus surveillée.
C Peu confiant	Zone publique / Internet. C'est une zone où la Société n'a pas de confiance. Zone hypersurveillée.

2.1.11. En fonction des zones de confiance, les balayages de l'infrastructure doivent être réalisés selon les fréquences suivantes :

Tableau 3 - Fréquence des balayages

Balayage	Description	Zone A+	Zone A	Zone B	Zone C
[redacted]	[redacted]				[redacted]
[redacted]	[redacted]			[redacted]	
[redacted]	[redacted]		[redacted]		
[redacted]	[redacted]	[redacted]			

2.1.12. En fonction de sa zone de positionnement, un actif doit être balayé dans les délais maximums ci-dessous. Lorsque ces délais sont dépassés, l'équipe du COCD est alertée et est responsable d'investiguer et de documenter l'écart avec la collaboration de l'équipe responsable. S'il s'avère que l'actif est décommissionné, cela doit être clairement indiqué dans l'inventaire.

[redacted]

L'activité de préparation permet de :

- S'assurer d'avoir un inventaire à jour et complet;
- S'assurer d'avoir un coffre à outils complet et la bonne calibration des outils;
- Déterminer avec précision le périmètre ciblé par la découverte des vulnérabilités;
- Décider du choix du mécanisme d'identification des vulnérabilités à utiliser;
- Définir le calendrier et le plan de travail;
- Obtenir les autorisations nécessaires pour réaliser les opérations;
- Notifier les détenteurs d'information et les autres parties prenantes concernées.

Note : L'équipe réseau doit impérativement connaître tous les réseaux de la Société puisque c'est cette équipe qui crée et gère ces réseaux. De là, des travaux peuvent démarrer facilement avec des plages IP clairement définies, ce qui permet de faire une stratégie efficace.

2.2. Règles liées à la découverte des vulnérabilités

Différents types d'activités permettent à la Société de découvrir les vulnérabilités de ses systèmes d'information. Ces activités sont réalisées soit par le COCD, soit par les équipes responsables d'actifs informationnels, soit par des firmes externes. Pour chaque description d'activité, les responsabilités y sont précisées.

2.2.1. Tout balayage de vulnérabilités doit faire l'objet d'un rapport dont la confidentialité doit être assurée.

2.2.2. Toute vulnérabilité détectée et confirmée doit faire l'objet d'une déclaration auprès du détenteur de la solution ou des données.

2.2.3. Toutes les vulnérabilités découvertes doivent être enregistrées le plus tôt possible dans le registre officiel des vulnérabilités et des correctifs.

2.2.4. Par les activités de découverte, la Société s'attend de recevoir minimalement les informations suivantes sur chacun des actifs analysés :

- Le nom de la vulnérabilité;
- Une brève description de sa nature;
- Sa criticité (score CVSS);
- La cible touchée (incluant leur version);
- Une référence à une base de connaissance type CVE, DSA, etc.;
- Une mention de la simplicité de l'exploitation, le cas échéant;
- Une description de l'impact en cas d'exploitation réussie;
- Une ou plusieurs recommandations pour la résoudre.

Rapports détaillés

Le rapport détaillé des vulnérabilités fournit à l'équipe de gestion des vulnérabilités et aux équipes de remédiation toutes les informations nécessaires sur les vulnérabilités identifiées. Il donne les détails sur le type de menace ou la catégorie des vulnérabilités, les facteurs d'exploit et le niveau de risque associé.

Veille technologique et de sécurité

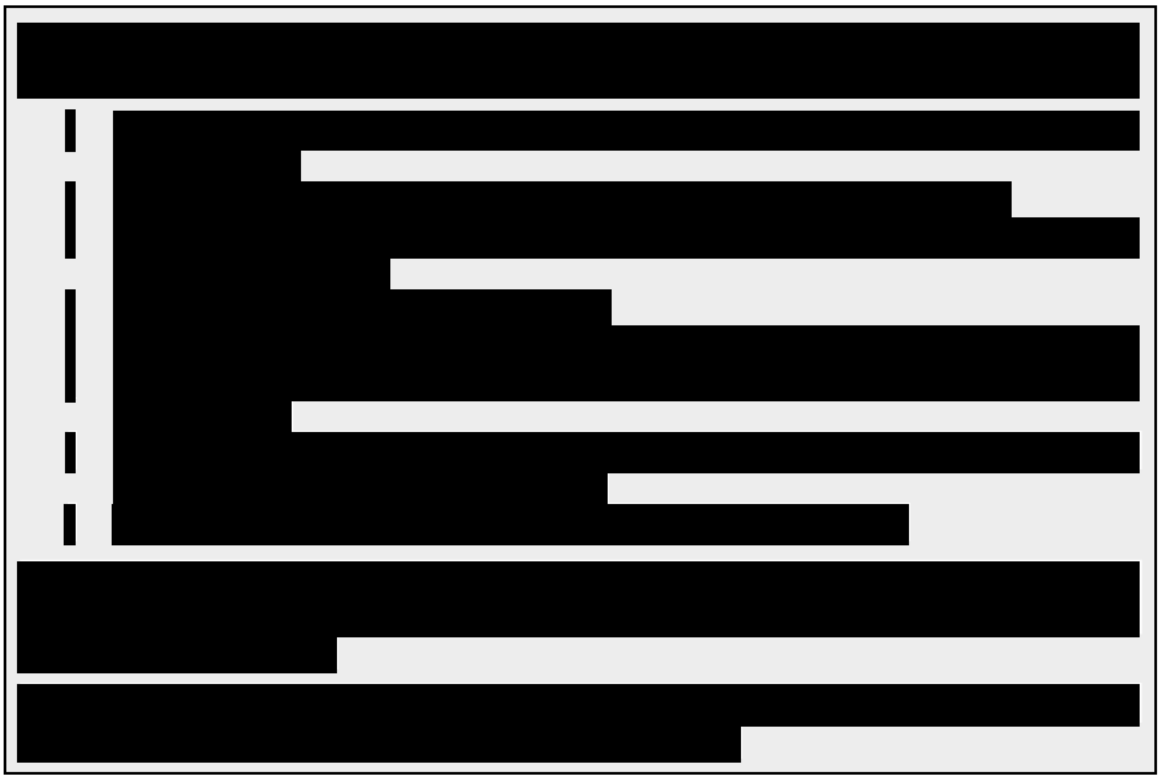
Il est de mise de surveiller et de rester à l'écoute des innovations et des nouveautés dans les technologies et la sécurité au sens large. La veille technologique et de sécurité permet à la Société d'identifier les vulnérabilités et les menaces possibles de ses environnements afin d'en trouver des solutions en amont au lieu d'en subir les conséquences.

2.2.5. Chaque équipe technologique, de développement, ou de sécurité doit mettre en place les moyens nécessaires pour assurer une veille technologique et de sécurité sur l'ensemble des équipements et des diverses technologies dont ils sont responsables, connectés directement ou indirectement à l'infrastructure de la Société.

2.2.6. Chacune des équipes doit procéder à des recherches constantes d'informations en utilisant une multitude de sources fiables qui proposent des informations pertinentes.

2.2.7. Chaque responsable d'actifs doit établir une veille sur les équipements dont il est responsable pour connaître la désuétude associée à chacun d'eux et veiller à leur remplacement ou à la mise en place de mesures de mitigation pour réduire les risques associés à cette désuétude.

2.2.8. Le COCD doit exploiter un engin de veille concernant les menaces et vulnérabilités actives afin d'être toujours à l'avant-garde en matière de gestion de la menace.



Balayages de vulnérabilités d'infrastructure

Les balayages de vulnérabilités d'infrastructure sont des tests de sécurité qui consistent à déceler des failles de sécurité, sur des équipements préalablement identifiés, dans un contexte précis et selon une portée prédéfinie où ces vulnérabilités sont documentées, mais ne sont pas exploitées.

Les balayages de vulnérabilités d'infrastructure servent à identifier les versions de logiciels obsolètes, les correctifs manquants et les erreurs de configuration, et à valider la conformité ou les écarts par rapport à la politique de sécurité de la Société et à des normes applicables.

2.2.9. Tous les actifs connectés ou appelés à se connecter au réseau informatique de la Société doivent faire l'objet de balayage d'infrastructure.

2.2.10. Les dates et fréquences des balayages d'infrastructures sont définies aux points 2.1.10 et 2.1.11.

2.2.11. La stratégie de balayage est déterminée en fonction des besoins de la Société, du type d'actif et de l'envergure des balayages à réaliser. La Société doit toutefois considérer plusieurs méthodologies de balayage afin de recueillir le maximum d'informations sur les vulnérabilités (ex. : anonyme ou authentifié, conformité CIS, conformité PCI-DSS, etc.).

Particularité des balayages sans-fil

Les technologies sans fil, dans leur sens le plus simple, permettent à un ou plusieurs appareils de communiquer sans avoir besoin de connexions physiques telles que des câbles réseau ou périphériques. Ils vont des technologies simples comme les claviers et souris sans fil (Bluetooth), aux réseaux de téléphonie cellulaire complexes (LTE) et aux réseaux locaux sans fil d'entreprise (Wifi).

2.2.12. Un balayage de tous les réseaux sans-fil de la Société doit être effectué d'une façon régulière afin d'identifier des vulnérabilités des systèmes d'exploitation ou micrologiciels, des périphériques sans-fils non autorisés, des portes dérobées potentielles ou autres violations de sécurité.

2.2.13. Un balayage doit être effectué pour découvrir les signaux sans fil non autorisés par la Société afin de détecter des violations potentielles de sécurité.

2.2.14. Une analyse de détection passive des appareils sans fil compatibles Bluetooth doit être effectuée pour déterminer la présence et l'activité potentielles d'appareils malicieux.

2.2.15. Seuls les actifs Bluetooth appartenant à la Société doivent être analysés par des balayages actifs fréquents. Les périphériques Bluetooth non fiables doivent être traités en considérant les risques de sécurité qui y sont associés.

Balayage de vulnérabilité applicative

Une vulnérabilité applicative est une faiblesse dans les processus, outils et pratiques visant à protéger les applications contre les menaces tout au long de leur cycle de vie, qu'il s'agisse d'applications de bureau, Web, mobiles, plug-in, etc., développées à l'interne ou en mode service. Elle peut résulter d'une défaillance dans la conception, la mise en œuvre ou l'utilisation d'un composant logiciel.

2.2.16. Toutes les applications en production, internes ou externes de la Société doivent faire l'objet de balayages périodiques, que celles-ci soient développées à l'interne ou acquises, en mode infonuagique ou non.

2.2.17. La stratégie de balayage est déterminée en fonction des besoins de la Société, du type d'actif et de l'envergure des balayages à réaliser. La Société doit toutefois considérer plusieurs méthodologies de balayage afin de recueillir le maximum d'informations sur les vulnérabilités (anonyme ou authentifié, balayage dynamique ou balayage statique, OWASP, etc.).

2.2.18. Des balayages de vulnérabilités applicatives doivent être intégrés dans les cycles de développement des applications de la Société.

2.2.19. Les vulnérabilités découvertes en phase de développement ou d'implantation de système doivent être corrigées en respectant les règles suivantes :

- **Critiques** – corriger ou mitiger la vulnérabilité avant la mise en production;
- **Élevées** – corriger ou mitiger la vulnérabilité avant la mise en production;
- [redacted]

Test d'intrusion

Les tests d'intrusion servent à valider l'exploitabilité d'une vulnérabilité identifiée par un balayage, une veille technologique ou tout autre mécanisme d'identification. Ils sont aussi utilisés comme un moyen d'identification de certaines vulnérabilités difficilement détectables par les outils de balayage techniques. Des tests d'intrusion peuvent être effectués tant au niveau technologique qu'au niveau applicatif. De tels tests peuvent également servir à vérifier qu'une organisation respecte les règles de sécurité, que ses employés sont sensibilisés à cette problématique et que l'organisation est en mesure d'identifier les incidents et d'y répondre.

2.2.20. Le COCD doit effectuer une planification annuelle des tests d'intrusion autant sur les infrastructures que sur les applications.

2.2.21. Le plan annuel des tests d'intrusions doit inclure au minimum 4 tests externes portant sur l'infrastructure technologique de la Société[1].

Voici une liste de tests d'intrusion qui pourraient être effectués :

- Tests d'intrusions – technologique;
- Tests d'intrusions – applicatif – Site Web informationnel;
- Tests d'intrusions – applicatif PES;
- Revues de code – PES ;
- Tests d'ingénierie sociale;
- Tests de performance;
- Tests d'intrusions – basé sur des objectifs;
- Tests d'intrusions – physique.

[1] À noter que l'exigence gouvernementale est de réaliser un test par année.

2.2.22. Tout nouveau service applicatif de la Société, exposé sur Internet, hébergé en interne ou en externe (projet, modification ou amélioration) doit faire l'objet d'un test d'intrusion avant sa mise en ligne. Pour les systèmes en mode service, une certification de type SOC2 type2, ISO 27002, etc. ou un rapport de test d'intrusion réalisé par une firme indépendante doivent être exigés.

2.2.23. La stratégie de chaque test d'intrusion est déterminée en fonction des besoins de la Société, du type d'actif et des risques. Toutefois la Société doit considérer plusieurs méthodologies de tests d'intrusion afin de recueillir le maximum d'informations sur les vulnérabilités exploitables (test interne, test ciblé, test externe, test à l'aveugle, test en double aveugle).

Différentes stratégies :

Tests d'intrusion ciblés : Ils sont réalisés dans le cadre d'une collaboration entre le service informatique de l'entreprise et l'équipe chargée des tests d'intrusion. Cette méthode est parfois dite « avec lumière allumée » (lights-turned-on), car tout le monde peut voir le test en cours d'exécution.

Tests d'intrusion externes : Ce type de test d'intrusion cible les serveurs ou les appareils d'une entreprise qui sont visibles de l'extérieur, notamment les serveurs de nom de domaine (DNS, Domain Name Server), les serveurs de messagerie, les serveurs Web ou les pare-feu. Le but est de déterminer si un attaquant extérieur peut s'infiltrer dans le système et jusqu'où il peut aller une fois l'accès obtenu.

Tests d'intrusion internes : Ce type de test imite une attaque interne, derrière le pare-feu, par un utilisateur disposant d'autorisations avec droits d'accès standard. Il permet notamment d'estimer les dommages que pourrait causer un employé mécontent.

Tests d'intrusion en aveugle : Une stratégie de test en aveugle consiste à simuler les actions et procédures d'un véritable pirate en limitant strictement les informations communiquées à la personne ou à l'équipe qui effectue les tests. Par exemple, on peut ne leur indiquer que le nom de la Société. Étant donné que ce type de test peut exiger énormément de temps au cours de la phase de reconnaissance, il s'avère souvent onéreux.

Tests d'intrusion en double aveugle : Il s'agit de tests en aveugle poussés à l'extrême. Dans cette approche, seules une ou deux personnes de l'entreprise sont informées qu'un test est en cours. Les tests en double aveugle peuvent servir à mettre à l'épreuve les procédures de contrôle de sécurité et d'identification des incidents d'une entreprise, ainsi que les réponses mises en place.

Revue de code

La revue de code est un examen systématique du code source d'un logiciel. Elle peut être comparée au processus ayant lieu dans un comité de lecture, l'objectif étant de trouver des bogues ou des vulnérabilités potentielles ou de corriger des erreurs de conception afin d'améliorer la qualité, la maintenabilité et la sécurité du logiciel. Une revue de code peut s'appuyer sur la vérification (manuelle ou automatisée) du respect d'un ensemble de règles de programmation.

2.2.24. Le chef de la sécurité de l'information organisationnelle (CSIO) doit effectuer une planification annuelle des revues de code à effectuer sur les applications de la Société.

2.2.25. Les revues de code doivent être réalisées autant sur les applications en développement que celles en exploitation.

2.2.26. Une vérification du code source doit être faite avant toute mise en production et les vulnérabilités doivent être corrigées suivant la règle 2.2.19.

2.2.27. Les revues de code doivent s'appuyer sur la vérification (manuelle ou automatisée) du respect de l'ensemble des règles de programmation du cadre de développement sécuritaire.

Examen de conformité des configurations

L'examen de configuration permet d'évaluer la conformité de la configuration des matériels, logiciels ou services applicatifs par rapport aux guides de bonnes pratiques des éditeurs de logiciels ou de constructeurs de matériel ou par rapport aux guides de sécurité des organismes de sécurité spécialisés comme le NIST, SANS ou autres. L'objectif est d'identifier les failles éventuelles de sécurité présentes sur la configuration des matériels et logiciels, et de mesurer leurs impacts sur le système d'information.

2.2.28. Le CSIO doit effectuer une planification annuelle des examens de conformité.

2.2.29. La conformité de la configuration des matériels, logiciels ou services applicatifs de la Société doit être évaluée périodiquement.

2.2.30. La stratégie d'examen est déterminée en fonction des besoins de la Société, du type d'actif et des risques. La Société doit toutefois considérer les standards de sécurité reconnus (ISO27002, NIST, SANS, etc.) et les recommandations des éditeurs de logiciel et fabricants de matériel.

Revue d'architecture de sécurité

La revue d'architecture a pour objectif de contrôler la résilience de l'architecture de tout ou d'une partie d'un système d'information au regard des menaces de sécurité. Elle vise aussi à vérifier la conformité de l'architecture mise en œuvre par rapport aux principes et directives de sécurité de la Société et aux guides de bonnes pratiques. Elle permet d'identifier les vulnérabilités du système d'information et de proposer des améliorations pour assurer sa résilience et son maintien à un niveau de sécurité acceptable.

2.2.31. La conformité et la résilience de l'architecture de tout ou d'une partie d'un système d'information au regard des menaces de sécurité doivent être vérifiées par rapport aux principes et directives de l'architecture de sécurité de l'entreprise et aux guides de bonnes pratiques établis.

2.2.32. La stratégie de revue est déterminée en fonction des besoins de la Société, du type d'actif et des risques. La Société doit toutefois considérer les standards de sécurité reconnus (ISO27002, NIST, SANS, etc.) et les recommandations des éditeurs de logiciels et constructeurs de matériel.

2.3. Règles liées à l'analyse et la priorisation des vulnérabilités

L'objectif de cette activité est de déterminer le niveau de risque associé aux vulnérabilités identifiées et de procéder à leur priorisation afin de déterminer les actions de mitigation à entreprendre.

2.3.1. **Le COCD doit effectuer une évaluation préliminaire de toutes les vulnérabilités d'infrastructure découvertes.**

2.3.2. **L'évaluation préliminaire doit permettre d'éliminer les faux positifs et déterminer une criticité préalable de la vulnérabilité, afin que soient priorisées uniquement les vulnérabilités applicables au contexte de la Société.**

2.3.3. **L'analyse des faux positifs doit permettre de déterminer le niveau de confiance à accorder à la vulnérabilité en répondant aux questions suivantes :**

- **Est-ce que le produit est bel et bien installé?**
- **Est-ce qu'il existe des mesures de sécurité qui se confondent avec des vulnérabilités?**
- **Est-ce que la détection est suffisamment de bonne qualité?**

2.3.6. [redacted]

2.3.7. La table de gestion des vulnérabilités a pour mission de valider l'évaluation de la criticité des vulnérabilités, de les prioriser et de proposer des plans de traitements. Elle prendra également en charge les activités ci-dessous :

- Faire le suivi de l'état d'avancement des plans de traitement des vulnérabilités;
- Débattre des problématiques techniques pouvant impacter l'éradication des vulnérabilités;
- Apporter des propositions pour bonifier le programme de gestion des vulnérabilités;
- Définir les indicateurs de gestion liés aux processus de gestion des vulnérabilités.

2.3.8. [redacted]

2.3.9. La table de gestion des vulnérabilités doit prioriser le traitement des vulnérabilités en fonction du contexte d'affaires de la Société, des risques de sécurité, des mesures de mitigations déjà en place, des impacts de l'application du correctif et d'une évaluation coût-avantage du traitement de la vulnérabilité, si nécessaire.

Une analyse coûts / avantages peut fournir aux gestionnaires une analyse quantitative des économies accrues à réaliser grâce à la mise en œuvre.

Les autres avantages qui peuvent être communiqués à la haute direction comprennent une exposition réduite, un contrôle accru des actifs, une diminution des vulnérabilités, une approche proactive de la sécurité et le maintien de la conformité.

2.3.10. La table de gestion des vulnérabilités doit établir un plan de traitement qui hiérarchise les vulnérabilités en fonction de leur criticité et le communiquer aux équipes technologiques ou de développement en charge d'apporter les corrections nécessaires pour colmater les vulnérabilités (actions techniques, acteurs, etc.).

2.3.11. Chaque plan de remédiation doit être validé par le ou les détenteurs des actifs concernés qui doivent approuver l'atténuation prévue des actions avant leur mise en œuvre.

2.3.12. Le COCD doit mettre à jour le registre des vulnérabilités au fur et à mesure de l'activité d'analyse et de la priorisation.

Plan de traitement

Le plan de traitement constitue le document de travail des équipes technologiques responsables d'apporter les corrections nécessaires pour colmater les vulnérabilités.

Il décrit les actions techniques : application d'un correctif de sécurité, modification d'un paramétrage de configuration d'un système, installation ou désinstallation d'un produit, etc. Il donne aussi les détails sur les acteurs susceptibles d'intervenir dans le plan de traitement ainsi que les délais de sa réalisation.

2.4. Règles liées au traitement des vulnérabilités

2.4.1. La mise en œuvre des actions permettant d'éradiquer les vulnérabilités ou, le cas échéant, de mettre en place des actions de remédiation, est de la responsabilité des équipes technologiques ou de développement qui élaborent le plan de mise en œuvre et le transmettent au COCD.

2.4.2. [redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

2.4.3. [redacted]

2.4.4. Les correctifs de sécurité ou les solutions de remédiation doivent être testés en laboratoire (dans un environnement similaire à celui dans lequel l'action d'atténuation serait mise en œuvre) ou sur une portée réduite avant d'être déployés sur l'ensemble des actifs concernés.

2.4.5. Les actions de remédiations doivent être réalisées dans le cadre du processus des changements de la Société et approuvées par le détenteur du système concerné.

2.4.6. Les équipes responsables du traitement des vulnérabilités doivent informer le COCD lorsque la vulnérabilité est traitée.

2.4.7. [redacted]

2.4.8. [redacted]

Les mesures palliatives peuvent être par exemple des mesures de prévention (règle plus stricte sur un pare-feu situé en amont, etc.), ou des mesures de réaction (renforcement du niveau de supervision des traces, etc.)

2.4.9. [redacted]

2.4.10. Dans le cadre de l'exécution des plans de mise en œuvre, le COCD doit mettre à jour le registre des vulnérabilités en permanence afin d'identifier les activités qui ont été accomplies, partiellement accomplies ou qui sont en attente.

2.5. Règles liées à la vérification de la remédiation des vulnérabilités

À la suite de la mise en œuvre du plan de traitement, la vérification du succès de la remédiation permet de s'assurer que les correctifs déployés ont permis l'élimination de la vulnérabilité ou que les mesures palliatives permettent de protéger l'organisation contre l'exploitation de la vulnérabilité.

2.5.1. **Le COCD est responsable de la vérification du succès des activités de remédiation des vulnérabilités.**

2.5.2. **La vérification est réalisée par les mêmes méthodes utilisées à l'étape d'identification des vulnérabilités (balayage, test d'intrusion, examen de conformité des configurations, etc.).**

2.5.3. **La vérification de l'application des correctifs doit être réalisée sur les systèmes concernés.**

2.5.4. **Lorsque des vulnérabilités réapparaissent à la suite de la vérification, celles-ci doivent être analysées, notamment au regard des questions suivantes :**

- **Le système a-t-il fait l'objet d'une réinstallation?**
- **De nouveaux systèmes ont-ils été installés avec d'anciennes configurations?**
- **Le système a-t-il fait l'objet d'une restauration de sauvegardes?**
- **Toutes les images existantes avaient-elles été corrigées?**

[redacted]

2.5.5. **Dans le cadre de la vérification du succès de la remédiation, le COCD doit mettre à jour le registre des vulnérabilités afin de consigner les informations concernant les remédiations qui ont réussi ou celles qui ont échoué et qui doivent être traitées à nouveau.**

2.6. Règles liées au suivi des vulnérabilités

Le suivi des vulnérabilités permet de s'assurer qu'elles sont adéquatement prises en charge. Il est principalement réalisé par la mise en place et l'analyse du registre et des tableaux de bord de gestion et de performance. L'alimentation du registre et des tableaux de bord servira :

- **Aux équipes impliquées dans la gestion des vulnérabilités pour le suivi et pour les références éventuelles;**
- **À la gestion pour le suivi, la reddition de comptes et l'aide à la décision;**
- **À titre de banque de connaissance en matière de gestion des vulnérabilités et pour la gestion des incidents.**

2.6.1. **Chaque vulnérabilité découverte doit faire l'objet d'un suivi régulier jusqu'à la confirmation de sa remédiation. Il est requis d'inscrire dans le registre tous les détails relatifs à la vulnérabilité dans chacune des étapes du processus.**

Découverte : - Date de découverte de la vulnérabilité; - CVSS et criticité annoncée par le fournisseur; - Type d'actif vulnérable (réseau, poste, serveur, etc.); - Détails de la vulnérabilité; - Nom ou identification du système touché. **Analyse et priorisation :** - Score environnemental; - DIC du système touché; - Localisation du système; - Facteurs d'atténuation et/ou facteurs aggravants; - Priorité de la remédiation; - Date de la recommandation du correctif ainsi que la nature de celui-ci (mise en place et/ou mesure d'atténuation); - Date de l'approbation d'exécution; - Accord d'exécution (approuvé, refusé, non-statué, en attente ou faux positif); - Date de l'accord d'exécution.	**Remédiation :** - Date du dépôt du plan de mise en œuvre; - Date d'approbation du plan de mise en œuvre; - Numéro de billet (DDC); - Date de la prise en charge de la mise en œuvre; - Statut d'avancement (non débuté, en analyse, en attente, en cours, complétée); - Date complétée de la remédiation; - Détails des actions. **Vérification :** - Vérification de la correction (oui, non, n/a); - Date de l'accord de la vérification; - Confirmation de la correction (oui, non, n/a); - Détails des actions et de la réponse; - Statut final (corrigé, non corrigé); - Date complétée à la suite de la vérification.

2.6.2. Les métriques suivantes doivent être mises en place pour la gestion des vulnérabilités, sans s'y limiter :

✓ **Des indicateurs de gestion qui donnent un portrait de l'état actuel de vulnérabilité de la Société :**

- Nombre de vulnérabilités découvertes par criticité;
- Nombre de vulnérabilités du jour zéro (zero-day);
- Nombre de vulnérabilités par types d'actifs
- Nombre d'actifs vulnérables par catégorie (serveurs, postes, etc.);
- Nombre de vulnérabilités qui impactent des lignes d'affaires;
- Niveau de risque par unité administrative ou groupe d'actifs;
- Nombre de vulnérabilités non corrigées dont le risque a été accepté;
- Nombre de vulnérabilités non corrigées en attente de résolution;
- Nombre de vulnérabilités ouvertes à haut risque dépassant leur délai de traitement;
- Nombre de vulnérabilités ouvertes avec exploitation active.

2.7. Règles liées à la reddition des comptes

La communication est une composante très importante du programme de gestion des vulnérabilités. Elle permet de donner une visibilité sur l'état de santé du système d'information de la Société. De plus, elle permet de fournir aux différentes parties prenantes toute l'information nécessaire pour avoir une appréciation des risques de sécurité auxquels la Société est exposée. L'escalade de l'information aux personnes concernées, conformément à la matrice RACI, leur permet de prendre des décisions éclairées, s'il y a lieu.

Les indicateurs de gestion des vulnérabilités permettent d'alimenter plusieurs tableaux de bord qui serviront à la prise de décision en matière de gestion des risques de sécurité de l'information au sein de la Société, et ce, à différents niveaux.

2.7.1. Les outils de reddition de comptes suivants doivent être mis en place pour la gestion des vulnérabilités, sans s'y limiter :

- ✓ **Des tableaux de bord opérationnels quotidiens**

  Regroupement d'indicateurs de gestion et de performance nécessaires pour la gestion opérationnelle des vulnérabilités par le COCD et les équipes de remédiation. Ils

fournissent une grande variété de modèles de rapports destinés à aider les équipes qui corrigent les vulnérabilités et les équipes de sécurité pour suivre leurs progrès.

- ✓ **Des tableaux de bord mensuels de gestion ou à la demande**

  Regroupement d'indicateurs de gestion et de performance nécessaires à la gestion pour la prise de décisions en matière de gestion des risques. Ils présentent une vue récapitulative de haut niveau ou une vue des tendances des vulnérabilités au sein de la Société ou d'une unité administrative.

Les tableaux de bord doivent être basés sur le temps et être générés périodiquement pour permettre d'identifier et mesurer des tendances et des changements saisonniers.

- ✓ **Tableaux de suivi des traitements**

  Le tableau de suivi donne une vue sur l'état d'avancement des actions correctives adoptées. Il permet de faire le suivi du traitement des vulnérabilités.

- ✓ [redacted]

- ✓ **Sommaire exécutif**

  Tel que son nom l'indique, le sommaire exécutif donne une vue synthétique sur l'état des vulnérabilités de la Société. Il permet de communiquer à la haute gestion les vulnérabilités ayant un intérêt particulier, les risques associés et les actions mises en œuvre pour les corriger.

2.7.2. Ces outils permettent au responsable opérationnel de cyberdéfense (ROCD) et au CSIO d'effectuer les redditions de compte appropriées au sujet de la gestion des vulnérabilités.

- Le ROCD est responsable d'escalader au CSIO les vulnérabilités non corrigées dans les délais de remédiation et qui représentent un risque inacceptable pour la Société.
- Le ROCD présente, à chaque détenteur d'actif, un sommaire exécutif mensuel des vulnérabilités découvertes sur ses actifs.
- Le ROCD présente au CSIO un sommaire exécutif mensuel (ou à la demande).
- Le CSIO présente au chef délégué de la sécurité de l'information (CDSI) un sommaire exécutif trimestriel.

2.8. Règles liées à l'amélioration continue

L'examen régulier des indicateurs et tableaux de bord permet d'identifier des tendances ou des problématiques plus profondes à résoudre de façon permanente.

2.8.1. L'amélioration continue du processus concerne :

- L'identification et la résolution de problèmes liés à des systèmes en particulier;
- L'amélioration de la gestion des actifs, soit l'amélioration de la sécurité des configurations et/ou des noyaux des postes de travail et des serveurs;
- L'amélioration de l'organisation du travail et la performance des équipes.

2.8.2. Le COCD doit tenir à jour un registre des leçons apprises pour passer en revue les activités liées aux processus et de proposer des améliorations le cas échéant.

3. [redacted]

[redacted]											
[redacted]											
[redacted]											
[redacted]											
[redacted]											
[redacted]											
[redacted]											
[redacted]											
[redacted]											
[redacted]											
[redacted]											
[redacted]											
[redacted]											

[redacted]

[redacted]

[redacted] [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted] [redacted]

4. DISPOSITIONS FINALES

4.1. Autorité

Le CSIO est propriétaire de la présente norme.

À noter qu'aucune disposition de la présente norme ne doit être interprétée comme contredisant les normes et les directives gouvernementales. En effet, les règles de la présente norme peuvent être plus contraignantes que les standards gouvernementaux en fonction du contexte de la Société.

4.2. Mise en vigueur

La norme est en vigueur et s'applique à compter de sa date d'approbation.

- Un délai de 6 mois est accordé pour rectifier les situations de non-conformité préexistante au moment de l'entrée en vigueur de la norme.
- Toute demande de dérogation doit être adressée au CSIO.
- Le CSIO et le ROCD peuvent effectuer des vérifications ponctuelles de l'application de la norme.

4.3. Révision

La norme est révisée minimalement aux trois ans ou lorsque des changements majeurs surviennent à la Société.

4.4. Approbation

La présente norme est approuvée par le CSIO.

ANNEXES

Références

Liens Web:

- https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/elaboration_miseenoeuvre_processus_gestion_risques_securite_information.pdf
- https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/tests_intrusions_vulnerabilites.pdf
- https://fr.wikipedia.org/wiki/Scanner_de_vuln%C3%A9rabilit%C3%A9
- https://www.lemagit.fr/definition/Test-dintrusion
- https://www.first.org/cvss/
- https://cyber.gc.ca/en/guidance/security-vulnerabilities-and-patches-explained-it-security-bulletin-government-canada-itsb
- https://www.klipfolio.com/resources/kpi-examples
- https://fr.wikipedia.org/wiki/Nmap
- https://www.indusface.com/blog/what-are-some-good-kpis-for-a-vulnerability-management-program/

Autres documents consultés:

- NITS 800 -40 rev3.pdf
- clusif-2014-gestion-vulnerabilites-tome-1.pdf
- Voir le Guide CVSS (ré : CCD – Guide d'implémentation d'un système de métriques CVSSv3 v1.0.docx)
- Gartner a_guidance_framework_for_dev_410271.pdf

Description du cadre de référence

SCT-CGCD

La pratique recommandée PR-061 du Secrétariat du Conseil du trésor vise à soutenir les organismes publics dans la mise en œuvre des tests d'intrusion et de vulnérabilités, en application du paragraphe g) de l'Article 7 de la Directive sur la sécurité de l'information gouvernementale, présente une vue d'ensemble des tests d'intrusion et de vulnérabilités, ainsi que les étapes à suivre pour la réalisation de ces tests. Ce document servira donc de guide dans l'exécution des activités de découverte des vulnérabilités à la Société, incluant les tests d'intrusion et de vulnérabilité.

Contrôles du CIS (Center for Internet Security)

Le référentiel de contrôles CIS priorise 20 principaux contrôles à mettre en place en matière de sécurité. Les contrôles qui ont un lien direct avec la gestion des vulnérabilités et des tests d'intrusion sont listés ci-dessous :

- CIS-1 : Inventaire et contrôle des actifs matériels;
- CIS-2 : Inventaire et contrôle des actifs logiciels (incluant les applications);
- **CIS-3 : Gestion continue des vulnérabilités (détection + remédiation);**
- CIS-9 : Limitation et contrôle des ports, protocoles et services du réseau;
- **CIS-20 : Tests d'intrusions et exercices Red Teams.**

Les **contrôles 1 et 2 - inventaire et contrôle des actifs matériels et logiciels** sont un prérequis pour une bonne gestion des vulnérabilités et des tests d'intrusion. Ils permettent d'identifier les appareils présents sur le réseau en mode « black box/attaquant » et d'en connaitre les caractéristiques, la sensibilité et ainsi que les entités responsables de leur gestion.

Le **contrôle 3 - Gestion continue des vulnérabilités,** concerne le cœur de cette norme. Il permet d'acquérir, d'évaluer et de prendre des mesures en permanence pour identifier les vulnérabilités, les corriger et ainsi minimiser les opportunités pour les attaquants.

Le **contrôle 9 - Limitation et contrôle des ports, protocoles et services du réseau (pare-feu, IPS)** - permet de gérer (suivre / contrôler / corriger) l'utilisation opérationnelle en cours des ports, des protocoles et des services sur les périphériques en réseau afin de minimiser les fenêtres de vulnérabilité accessibles aux attaquants.

Le **contrôle 20 - Tests d'intrusions et exercices de sécurité (Red Teams)** – permet de tester la force globale de la défense de la Société (la technologie, les processus et les personnes) en simulant les objectifs et les actions d'un attaquant.

ISO/IEC 27002 : 2013 – Technologies de l'information - Techniques de sécurité — Code de bonnes pratiques pour le management de la sécurité de l'information

Le référentiel de bonnes pratiques ISO/IEC 27002 : 2013 est une norme internationale concernant la sécurité de l'information qui est composée de 114 mesures regroupées en 15 familles de contrôles destinées pour la mise en place et le maintien d'un système de gestion de la sécurité de l'information. Ci-dessous sont listées les mesures qui ont un lien direct avec la gestion des vulnérabilités et des tests d'intrusion. Elles sont classées selon les contrôles CIS :

- CIS-1 : Section A8.1.1, A8.1.2, A9.1.2, A11.1.5, A11.2.5, A13.1.1, A13.1.2;
- CIS-2 : Section A8.1.1, A8.1.2, A12.1.2, A12.5.1, A12.6.2, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2;
- **CIS-3 : Section 12.6 Gestion des vulnérabilités techniques;**
- CIS-9 : Section A13.1.1, A13.1.2, A13.1.3.

NIST SP 800-53

Ce standard américain fournit un catalogue de contrôles de sécurité pour les organisations fédérales américaines. Il contient 256 mesures regroupées en 18 familles de contrôles. Ci-dessous sont listés les contrôles qui ont un lien direct avec la gestion des vulnérabilités et des tests d'intrusion. Ils sont classés selon les contrôles CIS :

- CIS-1 : SI-4, CM-1, IA-4;
- CIS-2 : CM-8, CM-11, IA-4;
- **CIS-3 : RA-5 Surveillance et analyse des vulnérabilités, SI-2 Remédiation des failles;**
- CIS 9 : SI-4;
- **CIS 20 : CA-2 Évaluation des contrôles, CA-8-Tests d'intrusion, SA-11 Tests et évaluations des applications.**

NIST CSF (Cybersecurity framework)

Ce standard américain fournit un cadre de référence en matière de sécurité informatique pour les organisations américaines du secteur privé désirant évaluer et améliorer leur capacité à prévenir, détecter et répondre aux cyberattaques. Ci-dessous sont listés les contrôles qui ont un lien direct avec la gestion des vulnérabilités et des tests d'intrusion. Ils sont classés selon les contrôles CIS :

- CIS-1 : DE.CM-7 – ID.AM-1 – PR.DS-3 – PR.AC-1 – PR.AC-6;
- CIS-2 : ID.AM-1 – ID.AM-2 – DE.CM-7 – PR.DS-6;
- **CIS-3 : DE.CM-8 – ID.RA-1 – ID.RA-5 – PR.IP-12 – RS.MI-3;**
- CIS-9 : DE.CM-8 – PR.IP-1;
- **CIS-20 : PR.AC-1.**

NIST SP 800-171

Ce standard américain fournit un catalogue de contrôles de sécurité pour la protection des informations contrôlées non classifiées dans les systèmes et organisations non fédéraux. Il contient 110 mesures regroupées en 14 familles de contrôles. Ci-dessous sont listés les contrôles qui ont un lien direct avec la gestion des vulnérabilités et des tests d'intrusion. Ils sont classés selon les contrôles CIS :

- CIS-1 : 3.4.1 – 3.5.1 – 3.1.2e – 3.1.1 – 3.1.16;
- CIS-2 : 3.1.2e – 3.4.1 - 3.4.7 – 3.4.8 – 3.4.9;
- **CIS-3 : 3.11.2 – 3.11.3 – 3.12.2 – 3.14.1;**
- CIS-9 : 3.4.7 – 3.1.3;
- **CIS-20 : 3.12.1.**

PCI-DSS 3.2

La norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard ou PCI DSS) est un standard de sécurité des données qui s'applique aux différents acteurs de la chaîne monétique. Le PCI DSS spécifie 12 conditions de conformité, regroupées dans 6 groupes appelés « objectifs de contrôle ». Ci-dessous sont listées les conditions qui ont un lien direct avec la gestion des vulnérabilités et des tests d'intrusion. Elles sont classées selon les contrôles CIS :

- CIS-1 : 2.4, 7.1.4, 8.1, 8.2, 8.2.2, 8.5, 8.6, 9.5, 9.6, 9.7, 9.8, 9.9, 10.1, 10.6.1, 11.1, 11.1.1, 11.4, 11.5, 12.10.5, 12.3, 12.3.3;
- CIS-2 : 2.4, 9.9, 10.1, 10.6.1, 11.1, 11.1.1, 11.4, 11.5, 12.10.5, 12.3.3, 12.3.7;
- **CIS-3 : 6.1, 6.2, 6.5, 10.6.3, 11.2, 11.3, 11.5.1, 12.2, 12.5.2, 12.10;**

- CIS-9 : 1.2, 2.2, 11.2;
- **CIS-20 : 2.1, 8.1, 8.2, 8.5, 8.6, 12.3.**

Gartner

Les documents de référence de la firme de conseil et de recherche Gartner serviront également de guide dans la définition et la mise en place du processus, ainsi que dans l'exécution des activités du processus à la Société, incluant l'exécution des tests d'intrusion et de vulnérabilité.