



Plan de réponse aux incidents

Responsable de la politique : Responsable informatique

Date d'entrée en vigueur : 8 janvier 2024

Visée

Le présent document décrit le plan de gestion des incidents et des événements en lien avec la sécurité de l'information et fournit des conseils aux employés ou aux intervenants sur un incident qui pensent avoir découvert un incident de sécurité ou y répondent.

Champ d'application

La présente politique couvre l'ensemble des événements ou incidents liés à la sécurité de l'information ou à la confidentialité des données.

Définition d'un incident et d'un événement

Un événement de sécurité est un événement observable concernant la confidentialité, la disponibilité ou l'intégrité de données, systèmes ou réseaux contrôlés par l'entreprise.

Un incident de sécurité est un événement de sécurité qui entraîne une perte ou un dommage en lien avec la confidentialité, la disponibilité ou l'intégrité de données, systèmes ou réseaux contrôlés par l'entreprise.

Signalement et documentation des incidents

Signalement des incidents

Si un employé, un sous-traitant, un utilisateur ou un client de Evalandgo Software prend connaissance d'un événement ou d'un incident de sécurité de l'information, d'un incident potentiel ou imminent, d'un accès non autorisé, d'une violation de politique, d'une faille de sécurité ou d'une activité suspecte, il remontera immédiatement les informations correspondantes en utilisant l'un des canaux de communication suivants :

- Envoyer par e-mail à l'adresse help@evalandgo.com ou support@evalandgo.com des informations ou des rapports sur l'événement ou l'incident.
- Contacter le support client par téléphone au numéro suivant : +33 (0)4 67 17 96 77

Les personnes signalant un événement ou un incident doivent agir en bons témoins et se comporter comme s'ils dénonçaient un crime. Les rapports doivent inclure des détails spécifiques sur ce qui a été observé ou découvert.

Gravité

L'équipe d'assistance de Evalandgo Software, responsable de la gestion des rapports d'incidents ou d'événements de sécurité, doit gérer les tickets d'incidents et d'événements et leur attribuer une gravité selon les catégories suivantes.

S3/S4 - Gravité faible ou moyenne

Les problèmes relevant de ce niveau de gravité sont simplement des soupçons ou des comportements bizarres. Ils n'ont pas été vérifiés et nécessitent une enquête plus approfondie. Rien n'indique clairement que les systèmes sont soumis à des risques tangibles et ne nécessitent pas d'intervention d'urgence. Cette catégorie couvre la perte ou le vol d'un ordinateur portable avec chiffrement de disque, les e-mails suspects, les pannes, une activité étrange sur un ordinateur portable, etc.

S2 - Gravité élevée

Les problèmes relevant du niveau de gravité élevée correspondent à des problèmes pour lesquels l'existence d'une exploitation active ou malveillante n'a pas encore été prouvée, et peut ne pas s'être produite, mais est susceptible de se produire. Il peut s'agir d'un ordinateur portable perdu ou volé sans chiffrement de disque, de vulnérabilités présentant un risque direct d'exploitation, de menaces présentant un risque ou d'une présence malveillante continue sur nos systèmes (p. ex. : portes dérobées, logiciels malveillants), d'un accès malveillant à des données métier (par exemple : mots de passe, données sur les vulnérabilités, informations de paiement).

S1 - Gravité critique

Les problèmes critiques concernent des risques activement exploités qui impliquent un acteur malveillant ou des menaces qui font courir un risque de dommage physique à une personne. L'identification de l'exploitation active est requise pour un classement dans cette catégorie de gravité.

Remontée des incidents et signalement interne

Les contacts à utiliser pour la remontée des incidents sont indiqués ci-dessous dans l'Annexe A.

S1 - Gravité critique : les problèmes de niveau S1 nécessitent une notification immédiate au responsable du service informatique. De plus, une issue dans Github sur le repository de l'application doit être créée et l'évènement doit être noté et daté.

S2 - Gravité élevée : une issue dans Github sur le repository de l'application doit être créée et le gestionnaire approprié (voir le paragraphe S1 ci-dessus) doit également être informé via Google chat en mentionnant le numéro de l'issue.

S3/S4 - Gravité faible ou moyenne : une issue dans Github sur le repository de l'application doit être créée et affectée au service approprié pour résolution.

Documentation des incidents et événements

Tous les événements de sécurité, incidents et activités de résolution signalés doivent être documentés et protégés de manière adéquate dans le système d'issue de Github.

Une analyse des causes racines peut être effectuée sur tous les incidents de sécurité vérifiés de niveau S1. Un rapport d'analyse des causes racines doit être documenté et mentionné dans le ticket d'incident. L'analyse des causes racines doit être validée par le VP support informatique et/ou le responsable informatique qui déterminera si une réunion d'analyse post-mortem sera organisée.

Processus de réponse aux incidents

Pour les problèmes critiques, l'équipe de réponse aux incidents agira selon un processus de réponse itératif conçu pour enquêter sur l'exploitation et la contenir, éradiquer la menace, restaurer le

système et les services, corriger les vulnérabilités et documenter une analyse post-mortem avec les leçons tirées de l'incident.

Résumé

- Événement signalé
- Catégorisation et analyse
- Enquête
- Contrôle et neutralisation (court terme/catégorisation)
- Récupération et correction des vulnérabilités
- Amélioration du renforcement et de la détection (leçons apprises, réponse à long terme)

Version détaillée

- Le responsable informatique ou le VP support informatique gère les actions de réponse aux incidents.
- Si nécessaire, un « centre de crise » centralisé sera désigné, et peut correspondre à un emplacement physique ou virtuel sur Google Chat.
- Une réunion récurrente de réponse aux incidents se déroulera à intervalles réguliers jusqu'à la résolution de l'incident.
- L'équipe juridique et les membres de la direction seront informés selon les besoins.

Ordre du jour de la réunion de réponse aux incidents

- Mise à jour du ticket d'incident et des échéanciers.
- Documentation de nouveaux indicateurs de compromission (IOC).
- Conduite d'une enquête par questions-réponses.
- Application de mesures d'atténuation d'urgence.
- Signalement externe/signalement des violations
- Planification de mesures d'atténuation à long terme.
- Documentation de l'analyse des causes racines (RCA).
- Éléments supplémentaires selon les besoins.

Considérations particulières

Problèmes internes

Les problèmes dans lesquels l'acteur malveillant est un employé interne, un sous-traitant, un fournisseur ou un partenaire nécessitent d'être traités avec sensibilité. Le responsable des incidents doit contacter les RH ou le PDG et ne discutera pas avec d'autres employés. Cela est valable pour des problèmes critiques nécessitant un suivi.

Compromission des communications

Les intervenants sur un incident doivent disposer de Google Chat avant d'associer leur nom à un incident. Si des risques de fuite informatique existent, une solution hors bande sera choisie et communiquée aux intervenants sur un incident par téléphone portable.

Compromission du compte racine

Si une compromission du compte racine AWS est connue ou prévue, reportez-vous au manuel stratégique à l'Annexe D.

Exigences supplémentaires

- Les événements et incidents présumés et signalés doivent être documentés.
- Les incidents présumés doivent être évalués et classés comme un événement ou un incident.

- La réponse aux incidents doit être effectuée conformément à ce plan et à toutes les procédures associées.
- Tous les incidents doivent être documentés de manière formelle et une analyse documentée des causes racines doit être effectuée.
- Les intervenants sur un incident doivent recueillir, stocker et préserver les preuves liées à l'incident, conformément aux directives et aux meilleures pratiques de l'industrie telles que NIST SP 800-86, « guide d'intégration des techniques d'analyse d'informatique légale dans la réponse aux incidents ».
- Les événements présumés et confirmés impliquant un accès non autorisé doivent être examinés par l'équipe de réponse aux incidents. La classification comme une violation ne doit être effectuée que par le PDG et le conseiller juridique en coordination avec la direction générale.
- Evalandgo Software informera rapidement et correctement les clients, partenaires, utilisateurs, parties touchées et organismes réglementaires des incidents ou violations pertinents conformément aux politiques, engagements contractuels et exigences réglementaires de Evalandgo Software, comme déterminé par le PDG, le service juridique.
- Ce plan de réponse aux incidents doit être examiné et officiellement testé au moins une fois par an. Les résultats des activités de test du plan de réponse aux incidents, y compris les conclusions et les leçons apprises, seront documentés de façon officielle et conservés pour soutenir les exigences en matière de sécurité, de conformité et d'audit.

Communications externes et signalement des violations

Le personnel juridique et exécutif doit s'entretenir avec les équipes techniques en cas d'accès non autorisé aux systèmes, réseaux et/ou données de l'entreprise ou du client. Le personnel juridique et le directeur général déterminent s'il est nécessaire de signaler une violation ou de communiquer avec l'extérieur. Les violations doivent être signalées aux clients, aux consommateurs, aux personnes concernées et aux régulateurs dans les meilleurs délais et conformément à tous les engagements contractuels et à la législation applicable.

Aucun membre du personnel ne peut divulguer des informations concernant un incident ou une violation potentielle à un tiers ou à une personne non autorisée sans l'approbation du service juridique et/ou de la direction générale.

Atténuation et correction

Le personnel juridique et exécutif détermine les mesures d'atténuation ou de correction immédiates ou à long terme à prendre à la suite d'un incident ou d'une violation. Dans le cas où des mesures d'atténuation ou des actions correctives sont nécessaires, le personnel exécutif doit orienter le personnel en ce qui concerne la planification, la communication et l'exécution de ces activités.

Coopération avec les clients, le responsable du traitement des données et les autorités

Selon les besoins et les décisions du personnel juridique et exécutif, l'entreprise doit coopérer avec les clients, les responsables du traitement des données et les régulateurs pour remplir toutes ses obligations en cas d'incident ou de violation des données.

Rôles et responsabilités

Tout employé et tout utilisateur de toute ressource d'information de Evalandgo Software a la responsabilité de protéger ces actifs informationnels. Le tableau ci-dessous établit les responsabilités spécifiques associées aux rôles des intervenants en cas d'incident.

Membres de l'équipe de réponse aux incidents

Rôle	Responsabilité
------	----------------

Responsable informatique	Le responsable des incidents est le décideur principal et ultime pendant la période de réponse à un incident. Il endosse la responsabilité finale de la résolution de l'incident et de la fermeture formelle des actions de réponse à l'incident. Voir l'Annexe A pour obtenir les coordonnées du responsable des incidents. Ces responsabilités couvrent les points suivants : • Veiller à ce que les personnes adaptées, issues de toutes les fonctions, soient activement impliquées au besoin. • Communiquer des mises à jour sur le statut de l'incident aux personnes ou équipes concernées à intervalles réguliers. • Résoudre les incidents dans l'immédiat. • Déterminer les actions de suivi nécessaires. • Affecter les activités de suivi aux personnes appropriées. • Remonter rapidement les détails de l'incident susceptibles de déclencher le signalement d'une violation, par écrit, au Directeur des systèmes d'information.
Équipe support	Les personnes qui ont été sollicitées et travaillent activement sur l'incident. Tous les membres de l'ERI restent sollicités pour répondre à l'incident jusqu'à ce que l'incident soit formellement résolu ou qu'il soit formellement clos par le responsable des incidents.
Équipe développeur	Des ingénieurs qualifiés seront planifiés dans une astreinte tournante et peuvent agir en tant que responsables des incidents (si les ressources principales ne sont pas disponibles) ou en tant que membre de l'ERI lorsqu'ils sont appelés pour répondre à un incident. Il incombe aux ingénieurs de comprendre les technologies et les composants des systèmes d'information, les dispositifs de contrôle de sécurité en place, y compris les outils de journalisation, de surveillance et d'alerte, les canaux de communication appropriés, les protocoles de réponse aux incidents, les procédures de remontée des incidents et les exigences en matière de documentation. Lorsque des ingénieurs sont appelés pour répondre à un incident, ils deviennent membres de l'ERI.
Utilisateurs	Ce sont les employés et sous-traitants de Evalandgo Software. Les utilisateurs ont la responsabilité de respecter les politiques et de signaler les problèmes, les problèmes présumés, les faiblesses, les activités suspectes, ainsi que les incidents et événements de sécurité.
Clients	Il incombe aux clients de signaler les problèmes liés à leur utilisation des services de Evalandgo Software. Il incombe aux clients de vérifier que les problèmes signalés sont résolus.
Conseiller juridique	En collaboration avec le PDG et la direction générale, il a la responsabilité de déterminer si un incident présente une exposition légale ou réglementaire et s'il doit être considéré comme une violation à signaler. Le conseiller doit examiner et approuver par écrit tous les avis de violation externes avant que ceux-ci ne soient envoyés à une partie externe.
Direction générale	En collaboration avec le PDG et le conseiller juridique, elle a la responsabilité de déterminer si un incident doit être considéré comme une violation à signaler. Un responsable approprié de l'entreprise doit examiner et approuver par écrit tous les avis de violation externes avant que ceux-ci ne soient envoyés à une partie externe. Evalandgo Software doit rechercher le consensus des parties prenantes lorsqu'il s'agit de déterminer si une violation a eu lieu. Dans le cas où un consensus ne peut être atteint, le PDG de Evalandgo Software doit prendre la décision finale concernant la violation.

Engagement de la direction

La direction de Evalandgo Software a approuvé la présente politique et s'engage à fournir les ressources, outils et formations nécessaires pour répondre de manière raisonnable aux événements et incidents de sécurité identifiés pouvant avoir une influence négative pour l'entreprise ou ses clients.

Exceptions

Les demandes d'exception à la présente politique doivent être soumises et autorisées par le responsable informatique pour approbation. Les exceptions doivent être documentées.

Violations et application

Toute violation connue de la présente politique doit être signalée au responsable informatique ou au PDG. Toute violation de cette politique peut entraîner le retrait ou la suspension immédiate des privilèges système et réseau, et/ou une sanction disciplinaire conformément aux procédures de l'entreprise, pouvant aller jusqu'au licenciement.

Version	Date	Description	Auteur	Approuvé par
1.0	8-janv-2024	Première version	Valentin Boschatel	Aurélie Gaspar

Annexe A - Coordonnées

Les coordonnées de la direction du service informatique et ingénierie ainsi que des membres de la direction peuvent être trouvées dans le Document des Contacts et des Astreintes sur le trust center de Evalandgo Software à l'adresse suivante :
<https://app.vanta.com/evalandgo/trust/vl9odudhw94jvv4qj71zu>.

Annexe B - Formulaire de recueil d'incident

Informations générales				
Informations sur la personne détectant l'incident				
Nom :			Date et heure de la détection :	
Poste :				
Téléphone :			Emplacement depuis lequel l'incident a été détecté :	
E-mail :				
			Informations complémentaires :	

Résumé de l'incident				
Type d'incident détecté :				
Déni de service	Utilisation non autorisée	Espionnage	Investigation	Canular
Code malveillant	Accès non autorisé	Autre :		
Emplacement de l'incident :				
Site :				
Point de contact sur site :				
Téléphone :				
E-mail :				

Comment l'incident a-t-il été détecté ?				
Informations complémentaires :				

Emplacement(s) des systèmes concernés(s) :				
Date et heure d'arrivée des gestionnaires d'incidents sur le site :				
Décrivez les systèmes d'information concernés (il est recommandé de remplir un formulaire par système) :				
Fabricant du matériel :				
Numéro de série :				
Numéro de propriété de l'entreprise (le cas échéant) :				
Le système concerné est-il connecté à un réseau ?	Oui	Non		
Décrire la sécurité physique de l'emplacement des systèmes d'information concernés (verrouillages, alarmes de sécurité, accès au bâtiment, etc.) :				
Isoler les systèmes concernés :				
Approbation du retrait du réseau ?	Oui	Non		
Si OUI, nom de l'approbateur :				
Date et heure du retrait :				
Si NON, indiquez la raison :				
Sauvegarde du ou des systèmes concernés :				
Dernière sauvegarde du système réussie ?	Oui	Non		
Nom des personnes ayant effectué la sauvegarde :				
Date et heure de début des dernières sauvegardes :				
Date et heure de fin des dernières sauvegardes :				
Emplacement du stockage de sauvegarde :				
Éradication de l'incident :				
Nom des personnes effectuant des analyses d'informatique légale :				
La vulnérabilité (cause racine) a-t-elle été identifiée :	Oui	Non		
Décrire :				
Comment l'éradication a-t-elle été validée ?				

Annexe C - Procédures de violation HIPAA pour les informations de santé protégées (ISP)

Procédures

Si Evalandgo Software identifie une violation potentielle des ISP, les procédures suivantes doivent être suivies.

Étape 1 : identification (découverte)

Une violation des ISP sera considérée comme « découverte » à partir du premier jour où Evalandgo Software a connaissance de la violation ou, en exerçant une diligence raisonnable, aurait ou devrait avoir connaissance de la violation.

Si une violation potentielle est découverte, c'est un événement urgent qui doit être signalé immédiatement.

Ce qui suit est une description complète de la notion d'une ISP :

- Une ISP est toute information sanitaire qui peut être liée à une personne, notamment :
 1. Les noms (nom complet ou nom de famille et initiales) ;
 2. Tous les identifiants géographiques plus petits qu'un État, à l'exception des trois premiers chiffres d'un code postal si, selon les données actuelles accessibles au public de l'agence du recensement : l'unité géographique constituée en regroupant tous les codes postaux ayant les mêmes trois premiers chiffres a une population supérieure à 20 000 personnes ; et les trois premiers chiffres d'un code postal pour toutes ces unités géographiques ayant une population inférieure ou égale à 20 000 personnes sont remplacés par 000 ;
 3. Les dates (autres que l'année) directement liées à une personne, y compris la date de naissance, la date d'admission, la date de sortie, la date de décès ; et tous les âges supérieurs à 89 ans et tous les éléments de dates (y compris l'année) indicatifs de cet âge, à l'exception du fait que ces âges et éléments peuvent être regroupés en une seule catégorie d'âge de 90 ans ou plus ;
 4. Les numéros de téléphone ;
 5. Les numéros de fax ;
 6. Les adresses e-mail ;
 7. Les numéros de sécurité sociale ;
 8. Les numéros de dossier médical ;
 9. Les numéros de bénéficiaire de l'assurance maladie ;
 10. Les numéros de compte ;
 11. Les numéros de permis ;
 12. Les identifiants de véhicule (y compris les numéros de série et les numéros de plaque d'immatriculation) ;
 13. Les identifiants d'appareil et les numéros de série ;
 14. Les localisateurs de ressources uniformes Web (URL) ;
 15. Les numéros d'adresse IP (Internet Protocol) ;
 16. Les identifiants biométriques, y compris les empreintes digitales, rétinienne et vocales ;
 17. Les images photographiques du visage entier et toute image comparable ;
 18. Tout autre numéro d'identification, caractéristique ou code unique, à l'exception du code unique attribué par l'enquêteur pour coder les données.

Il existe également des normes et des critères supplémentaires pour protéger la confidentialité de la personne contre la réidentification. Tout code utilisé pour remplacer les identifiants dans les

ensembles de données ne peut être dérivé d'aucune information liée à la personne et aux codes maîtres, et la méthode pour dériver les codes ne peut être divulguée. Par exemple, les initiales d'un sujet ne peuvent pas être utilisées pour coder ses données parce que les initiales sont dérivées de son nom. En outre, le chercheur ne doit pas avoir la connaissance réelle que le sujet de recherche pourrait être ré-identifié à partir des identifiants restants dans les ISP utilisées lors de l'étude de recherche. En d'autres termes, les informations seraient toujours considérées comme identifiables s'il existe un moyen d'identifier la personne, même si les 18 identifiants ont été supprimés.

Étape 2 : signalement initial/remontée

Si vous pensez qu'une violation potentielle des ISP s'est produite, le responsable de la sécurité et/ou de la protection de vie privée désigné, ou son représentant désigné, doit être immédiatement informé.

Veuillez fournir toutes les informations disponibles au moment de la découverte initiale de la violation potentielle, notamment :

- Les noms
- Les dates
- La nature des ISP potentiellement violées
- Le mode de divulgation (fax, e-mail, courrier, orale)
- Tous les employés impliqués
- Le destinataire
- Toutes les autres personnes en ayant connaissance
- Toute documentation écrite ou électronique associée qui pourrait exister

La notification et la documentation associée peuvent elles-mêmes contenir des ISP et ne doivent être remises qu'au responsable de la sécurité et/ou de la protection de vie privée désigné, ou à son représentant désigné.

Ne discutez pas de la violation potentielle avec qui que ce soit et n'essayez pas de mener une enquête, ces tâches étant effectuées par le responsable de la sécurité et/ou de la protection de vie privée désigné, ou son représentant désigné.

Étape 3 : enquête

Dès réception de la notification d'une violation potentielle, le responsable de la sécurité et/ou de la protection de vie privée désigné, ou son représentant désigné, doit mener une enquête dans les meilleurs délais.

L'enquête doit inclure les activités suivantes :

- Entretiens avec les employés impliqués
- Collecte des documents écrits
- Tous les documents nécessaires dûment remplis
- Enquête légale (facultative en fonction de l'incident)

Le responsable de la sécurité et/ou de la protection de vie privée désigné, ou son représentant désigné, doit conserver tous les documents relatifs aux enquêtes sur les violations potentielles, conformément aux exigences établies en matière de conservation des documents, ou pendant au moins six ans, selon la période la plus longue.

Étape 4 : évaluation des risques et recommandations

Une fois l'enquête terminée, le responsable de la sécurité et/ou de la protection de vie privée désigné, ou son représentant désigné, doit effectuer une évaluation des risques afin de déterminer si

l'utilisation ou la divulgation des ISP constitue une violation et requiert une notification supplémentaire à l'entité visée.

Le responsable de la sécurité et/ou de la protection de vie privée désigné, ou son représentant désigné, doit documenter de manière appropriée l'évaluation des risques et formuler une recommandation à l'intention de la direction générale et/ou du conseiller juridique quant à la nécessité de notifier l'entité visée de la violation potentielle.

Lors de la conduite de l'évaluation des risques, une norme de « jugement raisonné » sera appliquée à l'incident en fonction des faits et des facteurs suivants :

- La divulgation a-t-elle impliqué des ISP non sécurisées en premier lieu ?
- Qui a utilisé ou divulgué de manière illicite les ISP non sécurisées ?
- À qui les informations ont-elles été divulguées de manière illicite ?
- Ont-elles été renvoyées avant qu'il soit possible d'y accéder à des fins inappropriées ?
- Quel type d'ISP non sécurisées est concerné et en quelle quantité ?
- La divulgation a-t-elle été faite à des fins inappropriées ?
- Existe-t-il un risque important de préjudice financier, d'atteinte à la réputation ou autre pour la personne dont les ISP ont été divulguées ?
- Des mesures immédiates ont-elles été prises pour atténuer tout dommage potentiel ?
- L'une des exceptions spécifiques à la violation s'applique-t-elle ?

Étape 5 : décision finale

En collaboration avec le conseiller juridique, la direction générale de Evalandgo Software a l'autorité finale, après l'analyse des preuves et de l'évaluation des risques, d'établir si une violation des ISP s'est produite et, le cas échéant, de décider des mesures à prendre.

Étape 6 : notification

Dans le cas où la direction exécutive et/ou le conseiller juridique de Evalandgo Software détermine qu'une notification auprès de l'entité couverte est justifiée, la direction exécutive et/ou le conseiller juridique de Evalandgo Software ou le représentant désigné doit préparer et transmettre dans les plus brefs délais un avis à l'entité prise en charge.

1. Délai de notification

Evalandgo Software doit notifier l'entité visée « dans les meilleurs délais », mais au plus tard 60 jours après la découverte et/ou la notification de la violation, comme l'exige la loi.

Les accords de service et de partenariat de l'entreprise Evalandgo Software établissent que Evalandgo Software est un entrepreneur indépendant ; par conséquent, le délai accordé à l'entité visée pour fournir l'avis requis prend effet à la date à laquelle Evalandgo Software notifie l'entité visée de la violation.

2. Report de notification

2.1. Report injustifié

S'il apparaît au responsable de la sécurité et/ou de la protection de vie privée désigné, ou à son représentant désigné, que l'enquête ne sera pas terminée dans un délai raisonnable, la direction générale et/ou le conseiller juridique doivent en être informés afin de garantir que l'entité visée sera notifiée avant la fin de l'enquête.

2.2. Retard dans l'application de la loi

Un report dans la notification est autorisé si un agent de l'application de la loi déclare que la notification de la violation entraverait une enquête criminelle ou porterait atteinte à la sécurité nationale

1. Si une demande d'application de la loi est reçue, la déclaration d'application de la loi doit être faite par écrit et doit préciser la durée du report requis.
2. Si la demande de report de notification est orale, Evalandgo Software doit documenter la déclaration et demander une confirmation écrite dans les 30 jours. Si aucune demande écrite de report n'est reçue dans ce délai, Evalandgo Software doit envoyer la notification de la violation à l'entité visée.

2.3. Contenu de la notification

Toute notification à l'entité visée (EV) fournie par Evalandgo Software doit inclure toutes les informations requises par la loi, mais à minima les informations suivantes :

- L'identité de chaque personne dont les ISP sont présumées avoir été violées
- La date de la découverte de l'incident
- La date de la divulgation
- Les faits et circonstances entourant la divulgation
- Tous les documents associés
- Toutes les autres informations disponibles connues de Evalandgo Software que l'entité visée doit inclure dans son propre avis à la (ou au) personne(s) concernée(s).

Toute information supplémentaire concernant la violation que Evalandgo Software découvre après l'avis initial à l'entité visée doit immédiatement être communiquée à l'entité visée, comme l'exige la loi.

Tout avis à l'entité visée doit être envoyé par courrier de première classe avec accusé de réception, et l'accusé de réception ainsi qu'une copie de l'avis à l'entité visée doivent être conservés avec la documentation connexe et conformément aux exigences établies en matière de conservation des dossiers ou pendant un minimum de six ans, selon la période la plus longue.

Étape 7 : documentation

Toutes les étapes du processus doivent être documentées en détail, au cas par cas, d'une manière suffisante pour démontrer que toutes les étapes pertinentes ont été suivies. Tous les documents justificatifs associés à la violation potentielle sont conservés conformément aux exigences établies en matière de conservation des dossiers ou pendant au moins six ans, selon la période la plus longue.

Liste de contrôle des violations HIPAA

- En cas de violation réelle ou présumée d'informations de santé électroniques protégées (ePHI) non sécurisées, Evalandgo Software doit en informer l'entité visée concernée (EV).
- Le responsable de la sécurité et/ou de la protection de la vie privée et le service juridique doivent être informés d'une violation présumée des eISP dans les quatre (4) heures.
- L'équipe de réponse aux incidents enquête sur la violation présumée et effectue une évaluation des risques pour vérifier si les données eISP ont été compromises.
- L'équipe de réponse aux incidents doit remplir un rapport de notification de violation.
- L'équipe de réponse aux incidents transmet le rapport de notification de violation dûment rempli au responsable de la sécurité et/ou de la protection de la vie privée pour examen et approbation.
- Le responsable de la sécurité et/ou de la protection de la vie privée examine et approuve le rapport de notification de violation envoyé.

- Le responsable de la sécurité et/ou de la protection de la vie privée fournit une copie du dernier rapport de notification de violation au service juridique de Evalandgo Software dans un délai d'un (1) jour ouvrable suivant l'approbation.
- Le service juridique examine le rapport de notification de violation et envoie le rapport à l'entité visée par le biais des canaux de communication approuvés.
- Le service juridique veille à ce que la notification à l'entité visée ait lieu au plus tard soixante (60) jours civils après la découverte initiale d'une violation ou d'une violation présumée, sauf si elle est reportée par un organisme d'application de la loi compétent.

Contenu et modèle de notification de violation HIPAA

Le rapport de notification de violation à l'entité visée (EV) doit inclure les informations suivantes :

- L'identité de chaque personne associée à l'entité visée (EV) concernée dont on soupçonne l'accès, l'acquisition, l'utilisation ou la divulgation des eISP (dans la mesure du possible).
- Toute autre information que l'entité visée est tenue d'inclure dans la notification à la personne concernée en vertu de la partie 164.404(c) du Code des règlements fédéraux, notamment :
 - Une brève description de ce qui s'est passé, y compris la date de la violation et la date de sa découverte, si elle est connue.
 - Une description des types d'informations de santé protégées non sécurisées concernées par la violation (par exemple, si le nom complet, le numéro de sécurité sociale, la date de naissance, l'adresse du domicile, le numéro de compte, le diagnostic, le code de handicap ou d'autres types d'informations sont concernés).
 - Toutes les mesures que les personnes doivent prendre pour se protéger des dommages potentiels résultant de la violation.

Modèle de notification de violation HIPAA

Sécurité de l'information : rapport de notification de violation HIPAA/eISP	
Numéro d'incident : (numéro de ticket)	
Autres incidents liés à cet incident :	
Statut de l'incident de violation	(p. ex. nouveau, en cours, transféré pour enquête, résolu)
Résumé de l'incident	Description de ce qui s'est passé et de ce qui est connu à ce jour
Description de l'incident	Date et heure de découverte de l'incident :
Date et heure de signalement de l'incident :	
Date et heure de l'incident :	
Lieu de l'incident :	
Personnel impliqué dans l'incident :	
Type et volume d'informations impliquées :	
Accessibilité/vulnérabilité des eISP/mesures de protection en place : (p. ex. chiffrement, etc.) :	
Indicateurs de compromission liés à l'incident :	
Cause racine de l'incident :	
Sensibilisation à l'incident (qui est au courant maintenant) :	
Évaluation initiale des risques	Nombre de personnes potentiellement concernées :

Violation potentielle de la confidentialité (Oui/Non) :	
Risque pour les personnes (types et étendues) :	
Risque financier pour l'organisation :	
Risque juridique/contractuel pour l'organisation :	
Risque réglementaire pour l'organisation :	
Risque de relations publiques pour l'organisation :	
eISP accédées ou modifiées de façon non autorisée (Oui/Non) :	
Mesures prises	Actions en cours :
Preuves recueillies/chaîne de possession :	
Personnes contactées : (p. ex. propriétaires du système, administrateurs du système, organisme d'application de la loi, conseillers externes, enquêteurs judiciaires) :	
Fournisseur de services en cas de violation des données contacté :	
Organismes notifiés :	
Fermer ou passer à la phase d'enquête et pourquoi :	
Notification	Entité(s) visée(s) (EV) concernée(s) :
Date de notification des entités visées (EV) :	
Méthode(s) utilisée(s) pour notifier les entités visées (EV) :	
Enregistrement de notification (n° de ticket documentant la notification) :	
Liste générée par le système des personnes concernées jointe (obligatoire) :	
Détails justificatifs :	
Recommandations	Exigences de notification immédiate : les entités visées concernées DOIVENT être informées dans les soixante (60) jours d'une violation présumée.
Priorités et considérations pour une enquête plus approfondie :	
Prochaines étapes à suivre (p. ex. reconstruire l'hôte, mettre à niveau une application, mettre en œuvre des contrôles supplémentaires, etc.) :	
Recommandations pour les personnes concernées :	

Annexe D - Manuel sur la compromission des comptes racine AWS

Runbook de réponse aux incidents - utilisation racine

Objectif

L'objectif de ce runbook est de fournir des conseils spécifiques sur la gestion de l'utilisation des comptes racine AWS. Ce runbook ne remplace pas une stratégie détaillée de réponse aux incidents. Ce runbook porte sur le cycle de vie des réponses aux incidents :

- Établir le contrôle ;
- Déterminer l'impact ;
- Récupérer selon les besoins ;

- Enquêter sur la cause racine ;
- Améliorer.

Les indicateurs de compromission (IOC), les étapes initiales (arrêter les pertes) et les commandes CLI détaillées nécessaires pour exécuter ces étapes sont répertoriés ci-dessous.

Suppositions

- La CLI est configurée et installée.
- Le processus de signalement est déjà en place.
- Trusted Advisor est actif.
- Security Hub est actif.

Indicateurs de compromission

- Activité anormale pour le compte :
 - Création d'utilisateurs IAM ;
 - CloudTrail est désactivé ;
 - Cloudwatch est désactivé ;
 - SNS est suspendu ;
 - Step Functions est suspendu.
- Lancement d'AMI nouvelles ou inattendues ;
- Modifications apportées aux coordonnées du compte.

Étapes à suivre pour corriger la situation : établir le contrôle

La documentation d'AWS relative à un éventuel compte compromis indique les tâches spécifiques répertoriées ci-dessous. La documentation relative à un éventuel compte compromis peut être consultée à la page suivante : [Que faire si je remarque une activité non autorisée dans mon compte AWS ?](#)

1. Contactez l'assistance AWS et le responsable de compte technique dès que possible.
2. Modifiez et faites tourner le mot de passe racine et ajoutez un appareil MFA associé à ce mot de passe.
3. Faites tourner les mots de passe, les clés d'accès/secrètes et les commandes CLI en fonction des étapes de correction.
4. Examinez les actions entreprises par l'utilisateur racine.
5. Ouvrez les runbooks pour ces actions.
6. Fermez l'incident.
7. Examinez l'incident et comprenez ce qui s'est passé.
8. Corrigez les problèmes sous-jacents, mettez en œuvre les améliorations et mettez à jour le runbook selon les besoins.

Actions supplémentaires - Déterminer l'impact

Examinez les éléments créés et les appels mutants. Certains éléments peuvent avoir été créés pour permettre l'accès à l'avenir. Voici quelques éléments à prendre en compte :

- Les rôles inter-comptes IAM
- Les utilisateurs IAM
- Les compartiments S3
- Les instances EC2
- Les rôles administrateur sur l'application Eval&GO
- Les utilisateurs pour l'interface de base de données (PMA) et les permissions