**PLAN DE REPONSE AUX INCIDENTS**

**À PROPOS DE CE MODÈLE**

Ce modèle est une liste de contrôle, personnalisable, qui vous aidera à répondre à une cyberattaque, basée sur les meilleures pratiques du secteur de la sécurité et une expérience pratique de la protection des informations et des systèmes sensibles pour les entreprises de toutes tailles. Il est conçu pour établir les bases d’une stratégie d’intervention proactive, pragmatique et simple à adopter.

Les étapes d’action incluses dans le modèle de réponse à l’incident mettent l’accent sur l’importance de protéger les comptes à privilèges afin d’éviter une violation de données critique d’une potentielle cyberattaque. Nous avons défini des actions prioritaires qui vous aident à détecter et à arrêter une attaque rapidement et efficacement tout en maintenant la continuité de l’activité.

**Vous pouvez personnaliser ce modèle pour définir vos critères de risque, vos rôles et responsabilités, ainsi que vos stratégies de communication en cas de crise. Il s’agit d’une ressource clé pour coordonner les efforts de toutes les personnes de votre organisation impliquées dans la réponse aux incidents : responsables de la sécurité, responsables des opérations, équipe du service d’assistance, responsables de l’identité et de l’accès, responsables de l’audit, de la conformité, des communications et des cadres.**

**Personnalisation du modèle**

Pour personnaliser ce modèle, effectuez les opérations suivantes :

1. Supprimez les instructions « À propos de ce modèle » et « Personnalisation du modèle »
2. Remplacez le logo actuel (Your Logo) par le logo de votre entreprise (entête et pied de page)
3. Remplacez les champs en *[italique]* par vos propres informations
4. Une fois les tableaux complétés, vous pouvez supprimer les sections d’instructions en *italique*
5. Mettez à jour toutes les informations de contact spécifiques à la société
6. Mettez à jour les détails d’identification du document
7. Révisez les termes et priorités pour répondre à votre charte/vos besoins
8. Sauvegardez vos modifications
9. Partagez et rassemblez les commentaires de toutes les personnes impliquées dans votre équipe d’intervention en cas d’incident. Assurez-vous que chacun comprend son rôle et les exigences légales à la conformité que votre entreprise doit prendre en compte lors d’un incident.
10. Distribuez le plan conformément à vos directives de gestion

**Clause de non-responsabilité**

Ce document est un modèle et doit être révisé pour respecter les directives de votre organisation en matière de sécurité de l’information. Les entreprises ne doivent pas adopter de politique ou de plan de sécurité sans un examen préalable et sans avoir l’approbation de la direction, des services juridiques et du service informatique (sécurité).

# 

# **Politique de sécurité et approbation**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Créé par | Téléphone | Email | Date | Signature |
| Nom Prénom, Fonction |  |  |  |  |
| Approuvé par |  |  | Date | Signature |
| Direction |  |  |  |  |

# **Suivi des versions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Description | Politique de sécurité # | Date de révision | Date de relecture | Révisé par (Nom + Prénom + Fonction) |
| 1.0 | Version initiale |  |  |  |  |
|  |  |  |  |  |  |

# **Exigences de conformité**

*Inclure ici une liste des exigences de conformité ayant une incidence sur votre organisation. Pour obtenir une liste des mandats de conformité qui peuvent avoir une incidence sur vous, consultez l’annexe A.*

|  |  |
| --- | --- |
| Règle de conformité | Description |
|  |  |
|  |  |

**RESUME**

Pour maintenir la confiance de nos employés, clients et partenaires et répondre aux exigences de conformité, il est essentiel de mettre en place des processus pour protéger le SI et les données de l’entreprise face à une cyberattaque.

L’objectif de ce plan d’intervention en cas d’incident est de préparer *[NOM DE L’ENTREPRISE]* à réagir rapidement et efficacement face à une cyberattaque pendant que nous poursuivons nos activités. Une attention particulière est accordée à la protection des comptes à privilèges qui donnent accès à des systèmes essentiels comme les bases de données, les applications, les réseaux...

Il s’agit notamment des comptes de service, d’application et de compte root, des comptes réseau et d’administrateur ainsi que des comptes de domaine local.

Une réaction efficace en cas de cyber incident concerne tous les services de notre organisation, y compris les équipes informatiques juridiques, les ressources humaines, les communications et les opérations commerciales. Il est important de lire et de comprendre son rôle ainsi que les façons dont votre travail doit être coordonné avec celui des autres collaborateurs de l’entreprise.

Ce plan sera mis à jour *[À DEFINIR (tous les 6 mois, tous les ans…)]* pour refléter l’évolution de notre organisation, les nouvelles technologies et les nouvelles exigences de conformité qui guident notre stratégie de cyber sécurité. Nous pourrons effectuer des tests de ce plan pour nous assurer que tout le monde est bien formé pour participer à une intervention efficace en cas d’incident.

**ACTIONS D’ATTÉNUATIONS IMMÉDIATES**

Indépendamment de la façon dont nous avons pu découvrir un incident ou une violation de sécurité, notre équipe de sécurité informatique doit envisager de prendre en charge plusieurs tâches immédiatement :

* Désactiver les comptes administrateur de domaines existants et les déplacer vers de nouveaux comptes
* Faire la rotation de toutes les informations d’identification locales et de domaine
* Verrouiller l’environnement du système d’exploitation et le mettre à jour avec précaution avec les correctifs de sécurités pertinents face à la violation
* Découvrir les comptes créés après la date de l’incident / obtenir un d’audit des activités
* Vérifier et surveiller les comptes à privilèges afin d’identifier les activités suspectes

**RÔLES, RESPONSABILITES ET COORDONNEES**

Pour répondre correctement à un cyber incident, il est important de prendre en considération toutes les façons dont il peut impacter l’entreprise. Un cyber incident implique tous les collaborateurs de l’entreprise capables de gérer les problèmes systèmes, juridiques et de communications.

*Vous trouverez ci-dessous une liste des rôles requis au sein d'une organisation afin de mener une intervention complète et coordonnée en cas d'incident. Vous pouvez personnaliser cette liste en fonction de la taille, de la structure et des exigences de conformité et sectorielles de votre organisation. Par exemple, une personne peut remplir plusieurs rôles ou plusieurs personnes peuvent se coordonner pour partager la responsabilité d'un seul rôle. Les outils de sécurité peuvent appuyer les efforts des personnes impliquées dans l'équipe d'intervention en cas d'incident, mais ils ne les remplacent pas ; chaque outil doit avoir un propriétaire qui en est responsable. Celui-ci doit l'utiliser pour s'acquitter des responsabilités du rôle qui lui est assigné.*

*Inclure les coordonnées de toutes les personnes – internes et externes - impliquées dans l'intervention en cas d'incident. Notez qu'une cyber attaque peut rendre indisponibles des systèmes critiques tels que la messagerie. Par conséquent, il est judicieux de planifier la mise en place de systèmes de communication alternatifs et d'informations de contact de secours. Vous devez également garder une copie au format papier de votre plan d'intervention en cas d'incident et des coordonnées accessibles.*

|  |  |  |
| --- | --- | --- |
| RÔLE | RESPONSABILITES | COORDONNEES |
| **INFORMATIQUE** | | |
| Chef.fe de la sécurité / Directeur.trice de la sécurité informatique | Responsable stratégique.  Élabore des critères de classement des risques techniques, opérationnels et financiers utilisés pour prioriser le plan d’intervention en cas d’incident.  Autorise quand et de quelle manière les détails de l’incident sont signalés.  Interlocuteur principal pour l’équipe de direction et le conseil d’administration. | *Nom*  *Téléphone*  *Email* |
| Responsable et membres de l’équipe de réponse aux incidents | Équipe qui autorise et coordonne la réponse aux incidents entre les plusieurs équipes et fonctions, à toutes les étapes d’un cyber incident.  Conserve le plan d’intervention en cas d’incident, la documentation et le catalogue des incidents.  Responsable de l’identification, de la confirmation et de l’évaluation de l’ampleur des incidents.  Effectue des vérifications de sécurité aléatoires pour s’assurer de la préparation à une cyberattaque. | *Nom(s)*  *Téléphone(s)*  *Email(s)* |
| Responsable et membres de l’équipe « Identité et accès » | Responsable de la gestion des privilèges, de la protection par mot de passe d’entreprise et du contrôle d’accès basé sur les fonctions.  Découvre, vérifie et génère des rapports sur l’utilisation des comptes à privilèges.  Effectue des vérifications aléatoires pour auditer les comptes à privilèges, vérifie s’ils sont requis et demande une nouvelle authentification à ceux qui le sont.  Surveille les utilisations des comptes à privilèges et vérifie de manière proactive les indicateurs de compromission, tels que les connexions excessives ou tout autre comportement inhabituel.  Prend des mesures pour empêcher la propagation d’une violation en mettant à jour les comptes à privilèges. | *Nom(s)*  *Téléphone(s)*  *Email(s)* |
| Responsable des opérations / du support informatique (interne) | Gère l’accès aux systèmes et aux applications pour le personnel interne et les partenaires.  Gestion centralisée des correctifs, des mises à jour matérielles et logicielles et des autres mises à niveau des systèmes pour prévenir et contenir les attaques informatiques. | *Nom*  *Téléphone*  *Email* |
| Responsable des partenaires techniques (fournisseurs de services Internet, fournisseurs de services, hébergeurs, partenaires, etc.) | Gère les contrôles de sécurité pour limiter la progression d’une cyberattaque sur les systèmes et les organisations tiers. | *Nom*  *Téléphone*  *Email* |
| Équipes externes de réponse aux incidents | Coordination avec l’équipe d’intervention interne pour gérer les risques. Les équipes professionnelles d’intervention en cas d’incident veillent à ce qu’un processus de réponse aux incidents soit suivi. Il est toujours bon d’avoir à votre disposition une équipe d’intervention en cas d’incident composé d’experts externes qui possèdent déjà des connaissances sur votre environnement. | *Nom*  *Téléphone*  *Email* |
| **CONFORMITE** | | |
| Conseiller juridique | Confirme les exigences relatives à l’information des employés, des clients et du public sur les cyber attaques.  Responsable de l’enregistrement auprès de la police locale.  S’assure que l’équipe informatique dispose de l’autorité légale pour la surveillance des comptes à privilèges. | *Nom*  *Téléphone*  *Email* |
| Audit et conformité | Communique avec les organismes de réglementation, conformément aux exigences en matière de rapports d’audit. | *Nom*  *Téléphone*  *Email* |
| Ressources humaines | Coordonne les communications internes des employés concernant les atteintes aux données personnelles et répondent aux questions des employés. | *Nom*  *Téléphone*  *Email* |
| Contact réglementaire | Reçoit des informations sur une violation de données, conformément au calendrier et au format prescrits par les exigences en matière de conformité. | *Nom*  *Téléphone*  *Email* |
| **COMMUNICATION** | | |
| Responsable marketing et des relations publiques | Communication externe avec les clients, les partenaires et les médias.  Coordonne toutes les communications et les demandes d’interview avec les experts internes et l’équipe de sécurité.  Conserve les projets de plans et de déclarations de communication de crise qui peuvent être personnalisés et distribués rapidement en cas de violation. | *Nom*  *Téléphone*  *Email* |
| Responsable webmarketing et médias sociaux | Publie des informations sur le site internet de l’entreprise (intranet), les réseaux sociaux et par email concernant la cyberattaque, y compris le plan de réponse à l’incident et des recommandations pour les utilisateurs.  Configure la surveillance sur les réseaux sociaux pour s’assurer que nous recevons les commentaires ou des questions envoyés par les clients via les réseaux sociaux. | *Nom*  *Téléphone*  *Email* |
| Responsable des opérations / du support informatique (interne) | Fournit des bulletins de sécurité et des conseils techniques aux employés en cas d’infraction, y compris les mises à jour logicielles requises, les changements de mot de passe ou d’autres modifications du système. | *Nom*  *Téléphone*  *Email* |

**CLASSIFICATION DES MENACES**

*Dans votre plan d’intervention en cas d’incident, indiquez comment vous évaluez le risque. Vous pouvez élaborer votre propre classification des menaces ou votre propre système de classement des risques afin de déterminer le niveau d’intervention nécessaire en cas d’incident. Nous avons inclus l’exemple de système ci-dessous comme ligne directrice.*

La triade CID (Confidentialité, Intégrité et Disponibilité) est un cadre de classification des incidents qui permet de hiérarchiser le niveau de réponse aux incidents requis pour une cyberattaque. La CID est la suivante :

1. Confidentialité – Incidents impliquant un accès non autorisé aux systèmes, y compris la compromission des comptes à privilèges. Plus les données sont confidentielles ou plus les systèmes sont importants pour l’entreprise, plus leur impact est important.
2. Intégrité – Incidents impliquant un cryptolocker qui rend les données de l’entreprise inutilisables. Plus les données sont sensibles, plus l’impact est élevé.
3. Disponibilité – Incidents qui affectent la disponibilité ou le fonctionnement des services, tel que le ransomware, y compris l’utilisation de comptes à privilèges pour effectuer des modifications non autorisées. Plus les services sont critiques pour l’entreprise, plus leur impact est important.

*Lors du classement du niveau de risque pour l’organisation et du type de réponse aux incidents requise, vous devez tenir compte de la mesure dans laquelle les comptes à privilèges sont compromis, y compris ceux associés aux utilisateurs, aux administrateurs réseau et aux comptes de service ou d’application. Lorsque des comptes à privilèges sont impliqués dans la violation de données, le niveau de risque augmente de façon exponentielle.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| EXEMPLE DE CYBER INCIDENT | CLASSIFICATION (CID) | VIOLATION D’UN COMPTE A PRIVILEGES | IMPACT POUR L’ENTREPRISE | NIVEAU DE RISQUE |
| Un employé partage des renseignements avec un tiers non autorisé, mais ces renseignements ne sont pas personnels ou protégés par des règles de conformité. | C | Non | Faible | Faible |
| Les programmes malveillants cachés dans un programme utilisent les informations d’identification locales pour s’exécuter et ont accès aux données de l’administrateur réseau. Un logiciel publicitaire apparaît alors sur l’écran du poste utilisateur. | C, I | Oui | Faible | Moyen |
| Un cybercriminel utilise une technique de « pass-the-hash » pour voler des mots de passe et accéder à plusieurs bases de données et comptes « root ». | C | Oui | Elevé | Elevé |
| Le cybercriminel utilise un accès privilégié pour accéder au système de requêtes, ralentir les performances des postes et endommager l’expérience utilisateur. | C, I, D | Oui | Elevé | Elevé |

***[NOM DE L’ENTREPRISE]*** **OBLIGATIONS JURIDIQUES ET DE CONFORMITE**

*Dans le cadre de votre plan d’intervention en cas d’incident, renseignez les exigences légales et les exigences de déclaration de conformité auxquelles votre entreprise doit répondre. De cette façon, vous pouvez réagir immédiatement à un incident, au lieu d’avoir à passer par la récupération sur demande juridique ou vérifier si un rapport est nécessaire alors que vous êtes en pleine crise.*

*Consultez les annexes pour obtenir une liste des règlements qui peuvent avoir une incidence sur votre entreprise. Il est important que vous révisiez votre dossier avec votre conseiller juridique pour vous assurer qu’une liste complète s’applique à vous.*

**MESURES PRISES LORS DE LA REPONSE AUX INCIDENTS**

*Vous trouverez ci-dessous un exemple de modèle de rapport à utiliser pour renseigner les étapes et la documentation nécessaire lors de votre audit et lors de votre réponse à un cyber incident impliquant des comptes à privilèges. Faites des mises à jour qui reflètent votre processus approuvé et les outils que vous utilisez. Ajoutez un responsable pour chaque étape dès maintenant, afin que chacun sache quelles données il doit recueillir et quelles mesures prendre lorsqu’un incident se produit.*

Pour démontrer et améliorer l’efficacité de l’équipe d’intervention en cas d’incident de *[NOM DE L’ENTREPRISE]* et des outils de sécurité, *[NOM DE L’ENTREPRISE]* doit consigner toutes les mesures prises au cours de chaque phase de l’incident. Une documentation à l’appui est nécessaire, y compris toutes les preuves collectées telles que logs d’activité, dump mémoire, audit, trafic réseau et images disques.

Ci-dessous, la liste de contrôle à utiliser pour renseigner les actions menées pour lutter contre une attaque auprès de comptes à privilèges. Chez *[NOM DE L’ENTREPRISE]*, notre objectif est de respecter les exigences en matière conformité et de hiérarchiser la continuité de l’activité afin de minimiser l’impact et les coûts.

|  |  |  |  |
| --- | --- | --- | --- |
| PHASE DU CYBER INCIDENT | ACTION | MEMBRE DE l’EQUIPE/SYSTEME | JOUR/HEURE DES MESURES PRISES |
| **Détection et confirmation des incidents** | Décrire comment l’équipe a été informée de l’attaque (suite à un audit, partenaire, client, alerte de sécurité interne, etc.) |  |  |
| Analyser les logs d’audit pour identifier le comportement inhabituel ou suspect du compte qui indique une attaque probable et confirmer qu’une attaque a eu lieu. |  |  |
| Décrire l’intention du cybercriminel (y compris leurs capacités, les comportements et les motivations connues ou attendues). |  |  |
| Identifier le point d’accès et la source de l’attaque (terminaux, applications, logiciels malveillants téléchargés, etc.) |  |  |
| Préparer un calendrier des incidents afin de tenir un registre permanent du moment où l’attaque s’est produite et des étapes subséquentes de l’analyse et de l’intervention. |  |  |
| Rechercher dans les applications des signatures, des plages d’adresses IP, des fichiers hash, des processus, d’exécutables, d’URLs et des noms de domaine de sites web malveillants connus. |  |  |
| Évaluer l’étendue des dommages lors de la découverte et les risques pour les systèmes et les comptes privilégiés en particulier. Vérifier quels comptes à privilèges ont été utilisés récemment, si des mots de passe ont été modifiés et quelles applications ont été exécutées. |  |  |
| Examiner la liste des biens IT (actifs) pour déterminer quels actifs ont été potentiellement compromis. Noter l’intégralité des biens et des preuves recueillies. |  |  |
| Schématiser l’incident/attaque pour fournir une vue rapide de la violation initiale, puis du comportement au travers du réseau, des fichiers, etc. |  |  |
| Recueillir les notes de réunion dans un référentiel central à utiliser pour préparer les communications avec les intervenants. |  |  |
| Informer les employés de la découverte. |  |  |
| Analyser les indicateurs de compromis avec les outils de renseignement sur les menaces. |  |  |
| **Maîtrise et continuité** | Permettre, temporairement, l’utilisation des comptes à privilèges aux équipes techniques et de sécurité pour accéder rapidement aux systèmes et les surveiller. |  |  |
| Protéger les preuves. Sauvegarder tous les systèmes compromis dès que possible, avant d’effectuer toute action susceptible d’affecter l’intégrité des données sur le support d’origine. |  |  |
| Imposer l’authentification multi facteur ou l’examen par les pairs pour s’assurer que les comptes à privilèges sont utilisés de façon appropriée. |  |  |
| Changer les mots de passe pour tous les utilisateurs, services, applications et comptes réseau. |  |  |
| Augmenter la sensibilité des contrôles de sécurité d’application (autoriser, restreindre et refuser) pour empêcher que des malwares ne soient distribués par le logiciel malveillant. |  |  |
|  | Retirer les systèmes de la production ou les déconnecter si nécessaire. |  |  |
| Informer les employés au sujet de l’endiguement des infractions. |  |  |
| Analyser, enregistrer et confirmer tout cas d’occurrence potentielle d’exfiltration de données sur le réseau. |  |  |
| Communiquer le niveau de maîtrise de la cyberattaque (mises à jour de sites web, emails, publications sur les réseaux sociaux, bulletins d’information support technique, etc.) |  |  |
| **Elimination** | Fermer les ports de pare-feu et les connexions réseau. |  |  |
| Tester les périphériques et les applications pour vous assurer que tout code malveillant est supprimé. |  |  |
| Comparer les données avant et après l’incident pour vous assurer que les systèmes sont correctement réinitialisés. |  |  |
| Informer les employés de la résolution du problème. |  |  |
| Communiquer le niveau de maîtrise de la cyberattaque (mises à jour des sites Web, emails, publications sur les réseaux sociaux, bulletins d’information support technique, etc.) |  |  |
| **Récupération** | Télécharger et appliquer des correctifs de sécurité. |  |  |
| Fermer l’accès au réseau et réinitialiser les mots de passe. |  |  |
| Analyser les vulnérabilités. |  |  |
| Renvoyer tous les systèmes mis hors ligne à la production. |  |  |
| Informer les employés au sujet de la récupération. |  |  |
| Partager des informations concernant la récupération des données (mises à jour des sites Web, emails, publications sur les réseaux sociaux, bulletins d’information support technique, etc.) |  |  |
| **Informations** | Examiner les preuves recueillies. |  |  |
| Évaluer le coût de l’incident. |  |  |
| Rédiger un résumé de l’incident. |  |  |
| Faire rapport à l’équipe de direction et aux auditeurs si nécessaire. |  |  |
| Mettre en place une formation supplémentaire pour toutes les personnes impliquées dans les interventions en cas d’incident et tous les collaborateurs. |  |  |
| Mettre à jour le plan de réponse aux incidents. |  |  |
| Informer les employés des leçons apprises, de la formation supplémentaire, etc. |  |  |
|  | Partager de l’information (mises à jour des sites Web, emails, publications sur les réseaux sociaux, bulletins d’information support technique, etc.) |  |  |

**ANNEXES**

*Cette annexe est facultative et doit être supprimée avant de distribuer cette stratégie de sécurité à votre organisation.*

**ANNEXE A**

**CONFORMITÉ ET OBLIGATIONS JURIDIQUES**

* **RGPD UE**

Toute organisation traitant des informations d’identification personnelle des citoyens de l’UE est tenue de respecter les normes pour une protection efficace des données, des mesures de sécurité adéquates et la vie privée pour se conformer au RGPD de l’Union Européenne.

* **Exigences en matière de rapport –** En vertu du RGPD, la notification des violations est obligatoire dans tous les Etats membres où une violation de données est susceptible de mettre en péril les droits et libertés des personnes. Cela doit être fait dans les 72 heures après avoir pris connaissance de la violation. Les responsables du traitement des données sont tenus d’informer leurs clients, sans retard après avoir été informés d’une violation de données.
* **En savoir plus –** <https://www.eugdpr.org/key-changes.html>

**ANNEXE B**

*Avoir un plan d’intervention en cas d’incident est une première étape importante. Vous devez maintenant vous assurer que vous équipe dispose des bons outils pour soutenir les actions requises dans le plan.*

*Le tableau ci-dessous répertorie les phases de réponse aux incidents de ce plan qui peuvent être mises en œuvre à l’aide de la solution de gestion des privilèges, notamment Secret Server, Privilege Manager et Priviliged Behavior Analytics. Dans le cadre de votre stratégie de défense en profondeur,* ***THYCOTIC*** *vous permet de contenir un cyber incident et de résoudre le problème pendant que vous poursuivez vos activités commerciales normales.*

|  |  |
| --- | --- |
| PHASE DE REPENSE AUX INCIDENTS | ACTIONS DE REPONSE AUX INCIDENTS SOUTENUS PAR THYCOTIC |
| **Détection et confirmation des incidents** | * Détecter automatiquement une activité d’un compte à privilèges hors de l’ordinaire par rapport à une ligne de base. * Déclencher des alertes en temps réel sur les comportements suspects concernant les comptes à privilèges et les envoyer à une équipe d’intervention en cas d’incident pour une enquête et une action plus approfondies. * Déterminer rapidement l’étendue d’un incident en vérifiant quels comptes à privilèges ont été utilisés récemment, si des mots de passe ont été modifiés et quelles applications ont été exécutées. Il est également possible de prendre un instantané des journaux d’audit à des fins de comparaison. * Rechercher dans les applications des signatures, des plages d’adresse IP, des fichiers hash, des processus, des noms d’exécutables, des URL et des noms de domaine de sites web malveillants connus. |
| **Maîtrise et continuité** | * S’assurer que votre équipe d’intervention en cas d’incident dispose des autorisations et des privilèges nécessaires pour mener une enquête. * Permettre, temporairement, l’utilisation des comptes à privilèges aux équipes techniques et de sécurité pour accéder rapidement aux systèmes et les surveiller. * Modifier immédiatement et automatiquement les mots de passe de tous les utilisateurs, services, applications et compte réseau, sans les empêcher d’accéder aux systèmes dont ils ont besoin pour effectuer leur travail. * Augmenter la surveillance des comptes et des systèmes privilégiés en limitant l’accès aux systèmes sensibles, en exigeant des processus d’approbation supplémentaires pour l’accès privilégié ou en forçant l’authentification multi facteur pour les comptes privilégiés. * Augmenter la sensibilité des contrôles de sécurité d’application (autoriser, restreindre et refuser) pour empêcher que des malwares ne soient distribués par l’attaquant. |
| **Elimination** | * Comparer les données avant et après l’incident avec des rapports facilement personnalisés afin de déterminer rapidement quels comptes à privilèges peuvent être malveillants et d’auditer leur cycle de vie. * Surveiller et vérifier toutes les activités des comptes à privilèges afin de déterminer s’ils sont de retour à l’utilisation normale prévue, en accordant une attention particulière à tous les tiers, y compris les travailleurs temporaires, les entrepreneurs et les partenaires. |
| **Récupération** | * Effectuer des contrôles de sécurité moins sensibles pendant un certain temps ou fermer entièrement ces comptes jusqu’à ce que vous soyez certain que les systèmes ont été complètement récupérés. * Afficher toutes les activités en un coup d’œil dans un tableau de bord centralisé afin de pouvoir s’assurer que les systèmes et les données les plus critiques sont protégés et remis à la normale. * Créer facilement des rapports et partagez-les avec les cadres et les auditeurs pour montrer la manière dont les personnes et les outils ont réagi à un incident sans vérifier manuellement vos journaux. |
| **Informations** | * Obtenir une image claire de ce qui a fonctionné et de ce qui doit être amélioré. * Modifier rapidement les paramètres pour tenir compte des nouvelles politiques et exigences. |

**A propos de Thycotic**

Thycotic est le premier fournisseur de solutions de gestions des privilèges dans le cloud. Les outils de sécurité de Thycotic permettent à plus de 12 500 entreprises, des petites entreprises aux entreprises du classement Fortune 100, de limiter les risques liés aux comptes privilégiés, de mettre en œuvre des politiques de moindre privilège, de contrôler les applications et de démontrer la conformité. Thycotic rend la gestion des privilèges au niveau de l’entreprise accessible à tous en éliminant la dépendance envers des outils de sécurité trop complexes et en donnant la priorité à la productivité, à la flexibilité et au contrôleµ. Thycotic, dont le siège social est situé à Washington DC, exerce ses activités dans le monde entier avec des bureaux au Royaume-Uni et en Australie.

Pour plus d’informations : [www.thycotic.com](http://www.thycotic.com)

**DMI, revendeur-intégrateur des solutions Thycotic en Europe**

DMI est un revendeur et intégrateur français des solutions Thycotic. DMI accompagne les directions informatiques sur toutes les phases d’un projet IT : la revente de licences, audit et consulting, expertise et ingénierie, implémentation de solutions, formation, assistance technique…

Plus d’informations sur : [www.dmi-fr.com](http://www.dmi-fr.com)

Contacter l’équipe commerciale : [contact@dmi-fr.com](mailto:contact@dmi-fr.com)

Numéro de téléphone et chat en ligne disponibles depuis le site internet.