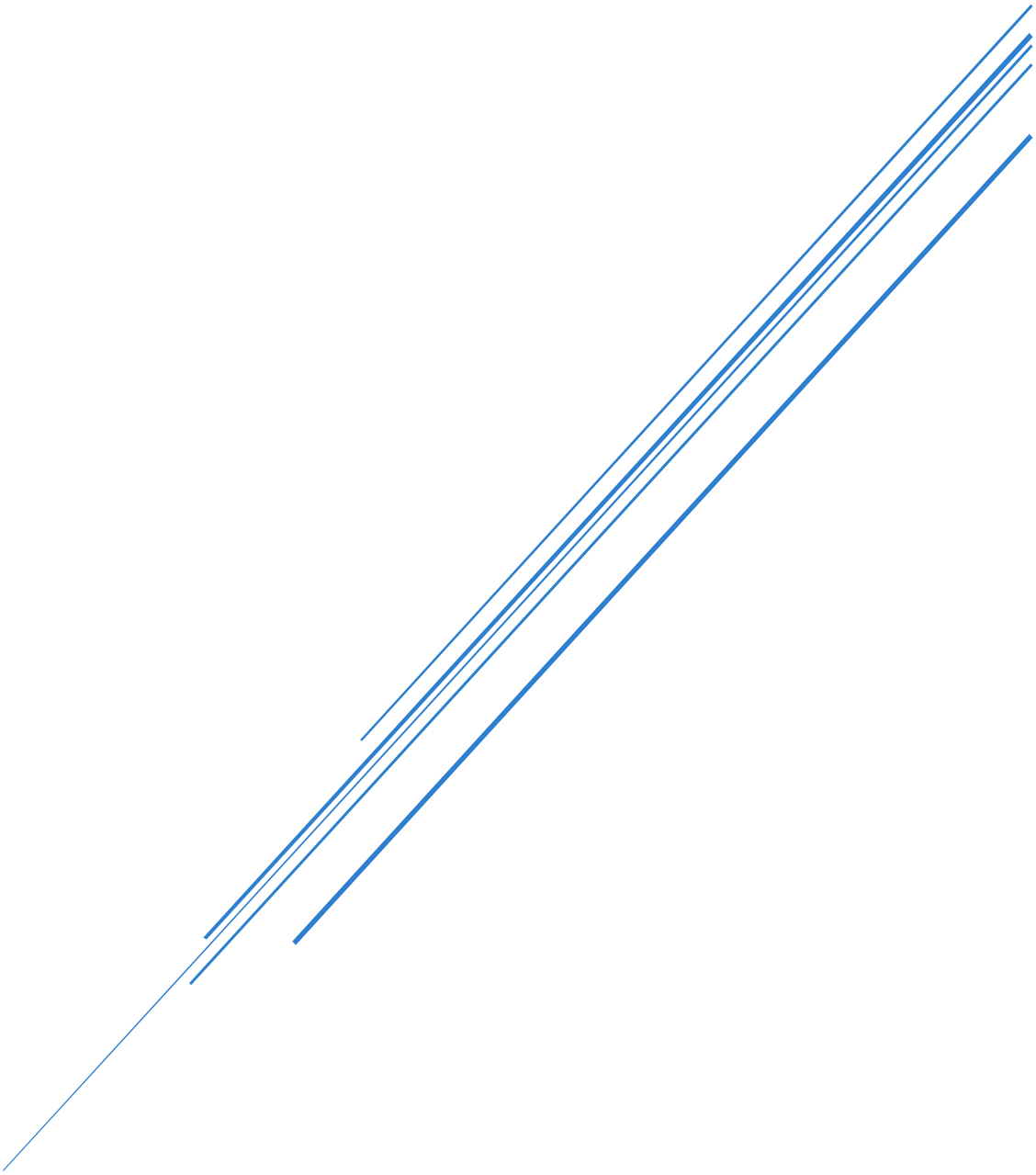
GUIDE DE PREPARATION AUX INCIDENTS DE SECURITE D'ORIGINE CYBER

Spécialisation : menace interne



Julien GARCIA
https://github.com/AugmentedSecurityForce

Table des matières

Objectif

L'objectif est de fournir une liste de points de contrôle et d'exemples de mesures permettant à une organisation d'appréhender et de gérer au mieux risques liés aux menaces internes.

Cet ensemble de contrôles est conçu pour aider les équipes de sécurité de l'information à renforcer leur posture de sécurité et à anticiper les menaces potentielles.

Pourquoi se concentrer sur le menace interne ?

Il est courant pour les organisations de focaliser leurs efforts de sécurité sur les menaces externes, en supposant que les risques internes sont minimes, grâce à des procédures de recrutement « rigoureuses », une culture d'« entreprise familiale » et des solutions de sécurité annoncées comme parfaites telles que les EDR (Endpoint Detection and Response) / XDR (eXtended Detection and Response).

Cependant, cette vision peut s'avérer trompeuse. Les menaces internes, qu'elles soient malveillantes ou non intentionnelles, représentent une menace significative souvent sous-estimée.

Les employés ont un accès direct aux données sensibles et aux systèmes critiques, ce qui leur donne un potentiel unique pour compromettre la sécurité, que ce soit par négligence, erreur ou intention malveillante.

Les mesures de sécurité externe seules ne suffisent pas à protéger une organisation de ces menaces internes. Il est crucial d'adopter une approche équilibrée qui inclut des contrôles internes, une surveillance proactive et une sensibilisation continue pour compléter les défenses contre les attaques provenant de l'extérieur.

En comprenant et en adressant les menaces internes, les organisations peuvent mieux protéger leurs informations sensibles et garantir une sécurité globale plus robuste.

Licence

Sources

Ce document est basé sur les projets « Insider-Threat » disponible ici :

- https://github.com/Insider-Threat/Insider-Threat
    - Limitation : ne semble pas spécialement maintenu.
- https://insiderthreatmatrix.org
    - Limitation : axé technique et certaines sections sont vides.

Je recommande toutefois la consultation de ces deux services pour obtenir une vue plus complète.

Phase initiale

Il s’agit de la première phase permettant d’initier un doute. A ce stade le risque n’est pas encore avéré. Il s’agit souvent des premières actions amenant à penser qu’un personnel est en train de devenir un risque pour l’entreprise.

Navigation sur les sites d’embauches

Description :

La navigation sur des sites d’embauche peut indiquer qu’un employé envisage de quitter l'entreprise. Lorsque les employés consultent régulièrement des plateformes de recherche d'emploi ou de recrutement depuis le réseau de l'entreprise, cela peut signaler une intention de départ. Ce comportement peut également être un indicateur précoce de mécontentement ou de la volonté de se préparer à un changement de carrière. Il est crucial de surveiller cette activité pour comprendre les motivations sous-jacentes et envisager des mesures préventives si nécessaire, tout en respectant la vie privée des employés.

Proposition de processus de protection :

- **Configurer un firewall ou un proxy** pour bloquer l'accès aux sites de recrutement connus à partir du réseau de l'entreprise. Cette mesure vise à prévenir la navigation non autorisée sur ces plateformes.
- **Mettre en place des outils de surveillance** du trafic réseau pour détecter les connexions à des sites d'emploi populaires. Cela permet d’identifier les tendances et comportements suspects, offrant une meilleure visibilité sur les intentions des employés.

Commentaire :

Il est préférable de ne pas bloquer l’accès à ces sites sur le lieu de travail. En effet, ce blocage n’empêcherait pas le salarié de chercher un autre poste en dehors du réseau de l’entreprise, mais il priverait l’organisation de la possibilité de suivre cette activité. Un suivi plus discret et analytique pourrait s’avérer plus pertinent.

Documentation :

N/A

Personnel faisant l'objet d'actions disciplinaires, en attente de licenciement ou fin de mission

Description :

Lorsqu'un employé fait l'objet de mesures disciplinaires, sont en cours de licenciement ou à la fin de leur mission, cela peut représenter une vulnérabilité accrue en matière de sécurité. Ce type de situation peut générer du ressentiment ou une perte de confiance, incitant potentiellement l'employé à adopter des comportements à risque, tels que contourner les contrôles de sécurité ou compromettre les informations de l'entreprise. Par conséquent, une vigilance particulière est nécessaire pour surveiller ses activités et prévenir tout comportement nuisible ou toute tentative de fuite d'informations sensibles.

Proposition de processus de protection :

- **Limiter temporairement l'accès** aux données sensibles et aux systèmes critiques pour les employés faisant l'objet de mesures disciplinaires. Cela permet de réduire les risques d'accès non autorisé ou de manipulation malveillante des informations.
- **Mettre en place une surveillance accrue** des activités des employés concernés. Cela inclut le suivi des accès aux fichiers, des modifications de données et des tentatives d'exfiltration. Une surveillance proactive permet d'anticiper et de détecter rapidement les comportements à risque.

Commentaire :

Il est essentiel de maintenir un équilibre entre la protection des données de l'entreprise et le respect des droits des employés. Une surveillance trop intrusive pourrait être perçue comme une atteinte à la vie privée et risquerait de démotiver davantage l'employé, accentuant les tensions. Une approche mesurée est recommandée pour éviter de telles répercussions négatives.

Documentation :

- AWS : Audit de l'accès aux fichiers dans FSx pour Windows
- Windows Server : Configuration des journaux d'accès sur Kaspersky

Restructuration de l'entreprise/réduction des effectifs

Description :

Lors d'une restructuration de l'entreprise ou d'une réduction des effectifs, les employés concernés peuvent ressentir de l'incertitude ou de l'angoisse, ce qui peut les pousser à agir de manière imprévisible. Pendant ces périodes, il est fréquent que des employés cherchent à sécuriser des informations pour leur avenir professionnel ou tentent d'extraire des données avant leur départ. De plus, les mouvements massifs de personnel peuvent créer des vulnérabilités dans les processus de sécurité. Il est donc crucial de surveiller les activités des employés pendant ces périodes de transition pour détecter et prévenir toute tentative de fuite ou d'exfiltration de données.

Proposition de processus de protection :

- **Réduire immédiatement les privilèges d'accès** de l'employé en limitant son accès aux informations sensibles et aux systèmes critiques. Cette mesure vise à réduire les risques d'accès non autorisé aux données critiques.
  Attention : Cette mesure doit être effectuée avec soin pour éviter de créer un climat de méfiance ou de panique parmi les employés touchés par la restructuration.
- **Mettre en place une surveillance en temps réel** de toutes les activités de l'employé, incluant le suivi de l'accès aux fichiers, des transferts de données, ainsi que des tentatives de modification ou de suppression de données. Une surveillance proactive permet d'identifier rapidement tout comportement suspect.

Commentaire :

La surveillance en temps réel est plus intrusive et exhaustive, couvrant non seulement la restriction d'accès, mais aussi le comportement général de l'employé. Cela permet de détecter et de réagir à une large gamme de menaces, y compris des tentatives de contournement des restrictions. Il est essentiel de trouver un équilibre entre la sécurité des données et le bien-être des employés durant ces périodes difficiles.

Documentation :

N/A

Correspondance avec les concurrents

Description :

Une tentative de transfert d'informations sensibles ou stratégiques peut indiquer une intention de quitter l'entreprise pour rejoindre un concurrent. Ces échanges peuvent potentiellement compromettre des secrets commerciaux, des informations confidentielles sur les clients ou les projets en cours, ainsi que des éléments critiques de la propriété intellectuelle. Une telle situation nécessite une attention particulière, car les employés en contact avec des concurrents peuvent être tentés d'utiliser ou de divulguer des informations internes pour négocier un poste ou obtenir un avantage compétitif, mettant ainsi en péril la position de l'entreprise sur le marché.

Proposition de processus de protection :

- **Mettre en place une surveillance ciblée** des communications électroniques pour détecter les échanges avec des domaines ou des adresses e-mail associés à des concurrents connus. Cela permet d'identifier rapidement toute activité suspecte liée aux communications externes.
- **Bloquer automatiquement les communications** avec les adresses e-mail ou les domaines associés aux concurrents. En parallèle, il est conseillé d'activer une surveillance en temps réel des activités de l'employé pour détecter tout comportement suspect, incluant les tentatives de transfert de données sensibles ou de copies non autorisées.

Commentaire :

Le blocage direct des communications avec les concurrents est une mesure qui doit être appliquée avec discernement. Cette action peut avoir des implications légales et doit être justifiée par des preuves solides de comportements inappropriés. Une approche équilibrée est essentielle pour éviter des répercussions indésirables sur les relations professionnelles.

Documentation :

N/A

Tentative d'accès à des zones restreintes

Description :

Un employé tentant d'accéder à des zones non autorisées peut rechercher des informations sensibles, manipuler des données critiques ou commettre des actes de sabotage. Cette situation est particulièrement préoccupante lorsqu'elle concerne des zones critiques pour la sécurité, telles que les serveurs de données, les salles des serveurs ou des bases de données contenant des informations confidentielles. Une gestion rigoureuse de ces accès est essentielle pour protéger les actifs de l'entreprise et prévenir les incidents de sécurité potentiels.

Proposition de processus de protection :

- **Mettre en place un système de contrôle des accès** qui enregistre les tentatives d'accès non autorisées et alerte les responsables de la sécurité lorsque de telles tentatives sont détectées. Cette approche permet de suivre les événements et de mener des enquêtes si nécessaire.
- **Déployer un système de gestion des accès basé sur les rôles** avec des contrôles d'accès rigoureux et une surveillance en temps réel des tentatives d'accès aux zones restreintes. En cas de tentative non autorisée, des alertes automatisées doivent être envoyées, et des actions correctives doivent être mises en place pour restreindre les accès et enquêter sur les activités suspectes.

Commentaire :

Une approche stricte et proactive est essentielle pour garantir la sécurité des zones restreintes. Les systèmes de gestion des accès doivent être régulièrement mis à jour pour refléter les changements dans les rôles et responsabilités des employés, et les enquêtes doivent être menées rapidement pour minimiser les risques. Une vigilance constante est nécessaire pour protéger les actifs de l'entreprise.

Documentation :

- CNIL : Accès aux locaux et contrôle des horaires sur le lieu de travail
- ANSSI : Sécurisation des systèmes de contrôle d'accès physique et vidéoprotection

Activité en dehors du champ d'application normal

Description :

L'activité en dehors du champ d'application normal fait référence aux comportements ou actions d'un employé qui s'écartent de ses tâches habituelles et des responsabilités normalement associées à son rôle. Cela peut inclure des accès à des systèmes ou des données qui ne sont pas pertinents pour ses fonctions, des heures de travail atypiques, ou des actions inhabituelles telles que des téléchargements ou des transferts de données importants. De telles anomalies peuvent indiquer des tentatives de compromission de la sécurité, une intention de saboter les systèmes, ou un accès non autorisé à des informations sensibles. Il est crucial de détecter et d'investiguer ces activités pour prévenir des incidents potentiels.

Proposition de processus de protection :

- **Mettre en place des alertes** pour signaler les activités qui sortent du champ d'application normal des employés, telles que les accès à des systèmes ou à des données non pertinentes pour leur rôle. Cette mesure permet de détecter des comportements atypiques et de les examiner pour déterminer s'ils sont justifiés ou non.
- **Utiliser des outils d'analyse comportementale et de surveillance en temps réel** pour suivre et analyser les activités des employés. Ces outils doivent identifier les écarts par rapport aux comportements habituels, détecter automatiquement les actions inhabituelles, telles que les accès non autorisés ou les heures de travail atypiques, et déclencher des alertes pour une enquête approfondie.

Commentaire :

Certaines solutions EDR (Endpoint Detection and Response) sont capables de détecter ces changements de comportement. Il est conseillé de se renseigner auprès de l'éditeur pour connaître les fonctionnalités spécifiques et la capacité d'analyse comportementale des outils disponibles sur le marché.

Documentation :

- N/A

Activité en dehors des heures normales

Description :

L'activité en dehors des heures normales de travail se réfère aux actions d'un employé réalisées en dehors des plages horaires habituelles de son poste. Cela inclut des connexions tardives à des systèmes, des téléchargements ou des transferts de données pendant la nuit, ainsi que des modifications de fichiers en dehors des heures de bureau. De telles activités peuvent être des indicateurs de comportements suspects, tels que des tentatives de vol de données, de sabotage, ou d'autres actions malveillantes susceptibles de compromettre la sécurité de l'entreprise. Il est crucial de surveiller ces comportements pour identifier rapidement des incidents potentiels et protéger les informations sensibles.

Proposition de processus de protection :

- **Configurer des alertes** pour détecter les connexions et les activités en dehors des heures normales de travail. Ces alertes doivent être examinées pour déterminer si elles sont légitimes ou si elles nécessitent une investigation plus approfondie.
- **Mettre en place une surveillance continue et une analyse** des activités en dehors des heures normales. Utiliser des outils capables de détecter les connexions inhabituelles et les actions non autorisées en temps réel. Les systèmes doivent générer des alertes automatiques pour toute activité suspecte, et des enquêtes doivent être menées pour comprendre la raison de ces anomalies et minimiser les risques.

Commentaire :

Le blocage des comptes en dehors des horaires de travail reste une solution possible pour une part importante des personnels administratifs. Cela pourrait aider à prévenir certaines activités inappropriées, tout en tenant compte des besoins opérationnels.

Documentation :

- Active Directory : Comment définir les heures de connexion dans Active Directory

Modification/Suppression des journaux

Description :

La modification ou la suppression des journaux (logs) représente une menace significative pour la sécurité, car cela peut masquer des activités malveillantes, des accès non autorisés ou des tentatives de sabotage. Les journaux sont essentiels pour la traçabilité des actions et la détection des incidents de sécurité. Si un employé ou un attaquant parvient à modifier ou supprimer ces journaux, il peut effacer les preuves de ses actions et rendre plus difficile la détection et l'analyse des incidents. Il est crucial de protéger les journaux contre toute altération pour garantir l'intégrité des informations et maintenir une capacité d'audit efficace.

Proposition de processus de protection :

- **Mettre en place des contrôles d'accès rigoureux** pour les journaux, en limitant les droits de modification et de suppression uniquement aux administrateurs autorisés. De plus, configurer des alertes pour détecter les tentatives de modification ou de suppression des journaux, et effectuer des audits réguliers pour vérifier leur intégrité.
- **Implémenter une solution de gestion des journaux** avec des fonctionnalités de protection avancées, telles que l'archivage immuable et la journalisation en lecture seule. Assurer une surveillance continue des journaux pour détecter toute tentative de modification ou de suppression, et réaliser des audits réguliers et détaillés pour garantir l'intégrité et la sécurité des journaux.

Commentaire :

La protection des journaux est fondamentale pour maintenir la transparence, la responsabilité et l'intégrité des systèmes informatiques. Les journaux fournissent des preuves cruciales en cas d'incidents de sécurité, d'audits internes ou d'enquêtes réglementaires. Une gestion rigoureuse et sécurisée des journaux permet non seulement de détecter et de répondre rapidement aux menaces potentielles, mais aussi de se conformer aux exigences légales et aux normes de l'industrie. Les contrôles d'accès doivent être strictement appliqués, et les mécanismes de protection des journaux doivent être régulièrement vérifiés et testés pour garantir leur efficacité.

Documentation :

- Windows : Security Log Event

Plusieurs personnels quittant pour la même entreprise

Description :

Lorsqu'un groupe d'employés quitte une entreprise pour rejoindre le même concurrent ou une entreprise similaire, cela soulève des inquiétudes quant à des pratiques de recrutement agressives, la fuite potentielle de secrets commerciaux ou d'informations sensibles, et des actions de sabotage organisées. Ce phénomène peut indiquer un intérêt concerté pour des informations stratégiques, des tentatives de transfert de connaissances critiques, ou un plan coordonné pour nuire à l'entreprise d'origine. Il est crucial de surveiller ces mouvements pour identifier les risques et mettre en place des mesures préventives afin de protéger les actifs et les informations de l'entreprise.

Proposition de processus de protection :

- **Mettre en place des alertes** pour suivre les départs des employés vers des entreprises concurrentes ou similaires. Cette surveillance peut inclure l'examen des tendances et des motifs dans les départs pour identifier des regroupements inhabituels. Réaliser des enquêtes sur les raisons des départs et leur impact potentiel sur la sécurité des informations.
- **Implémenter une surveillance proactive des départs d'employés**, en mettant en place des mesures telles que des vérifications approfondies des antécédents des nouveaux employeurs, des analyses des communications entre les employés sortants et les recruteurs, et des contrôles renforcés des informations et des accès avant le départ. Mettre en œuvre des mesures de sécurité additionnelles pour protéger les informations sensibles et les secrets commerciaux.

Commentaire :

Bien que le départ de plusieurs employés vers une même entreprise puisse soulever des préoccupations légitimes, il est essentiel de gérer ces situations de manière équilibrée pour éviter des tensions inutiles ou des perceptions négatives. Une communication ouverte avec les employés peut aider à atténuer les inquiétudes et à préserver un climat de confiance.

Documentation :

- N/A

Emploi de courte durée inhabituel

Description :

Un emploi de courte durée inhabituel se réfère à une situation où un employé quitte l'entreprise après une période de travail exceptionnellement courte, souvent sans raison évidente ou explicite. Ce phénomène peut être le signe de divers problèmes potentiels, tels que des tentatives de compromettre la sécurité de l'entreprise avant de partir, la collecte ou l'exfiltration de données sensibles, ou même des comportements frauduleux. Les départs précoces peuvent également indiquer un processus de recrutement ou de gestion des talents inadéquat, ou des problèmes au sein de l'organisation qui pourraient affecter la rétention des employés. Une attention particulière doit être portée à ces cas pour comprendre les causes sous-jacentes et minimiser les risques associés.

Proposition de processus de protection :

- **Mettre en place des alertes** pour identifier les employés dont la durée d'emploi est exceptionnellement courte. Examiner les motifs des départs et les activités associées à la période d'emploi pour détecter des anomalies ou des comportements inhabituels. Réaliser des entretiens de sortie approfondis pour recueillir des informations sur les raisons du départ.
- **Déployer une surveillance plus rigoureuse** des employés ayant une durée d'emploi très courte, en analysant les accès et les actions réalisées durant leur période de travail. Mettre en œuvre des contrôles d'accès renforcés et une gestion des données plus stricte pour ces employés. En cas de départ prématuré, effectuer des enquêtes approfondies pour évaluer les risques et assurer que les informations sensibles ont été protégées.

Commentaire :

La gestion des employés avec une durée d'emploi courte nécessite une approche équilibrée. Il est important de comprendre les raisons sous-jacentes des départs rapides, tout en prenant des mesures appropriées pour protéger les informations sensibles et prévenir les comportements frauduleux. Une communication ouverte et un processus d’intégration solide peuvent également aider à améliorer la rétention des employés.

Documentation :

- N/A

Suppression de traces / fichiers

Description :

La suppression de traces se réfère à l'élimination ou à la modification des informations qui pourraient être utilisées pour retracer les actions passées d'un utilisateur ou d'un système. Cela inclut des pratiques telles que la purge des données de navigation, l'effacement de l'historique des commandes, la suppression des journaux (logs), ou la modification des métadonnées associées à des fichiers ou des transactions. Ce comportement peut indiquer des tentatives malveillantes de dissimuler des activités frauduleuses, d'éviter des audits ou de masquer des accès non autorisés à des informations sensibles.

Proposition de processus de protection :

- **Mettre en place des alertes** pour identifier les suppressions ou modifications anormales des traces, telles que les historiques de navigation ou les journaux d'activité. Il est également crucial d'examiner les raisons de ces actions et leur fréquence pour détecter d'éventuels comportements suspects. Des audits réguliers des journaux doivent être réalisés pour vérifier l'intégrité des informations enregistrées.
- **Déployer une surveillance rigoureuse** pour détecter la suppression de traces, en analysant les tentatives de purge ou de modification des journaux et des historiques. Il est essentiel de mettre en œuvre des mécanismes de contrôle d'accès renforcés pour limiter les actions de suppression aux utilisateurs autorisés. En cas de détection d'une suppression de traces, mener une enquête approfondie pour évaluer l'impact sur la sécurité et la conformité des systèmes.

Commentaire :

N/A

Documentation :

- **Navigateur internet :**
    - Chrome : “C:\Users[username]\AppData\Local\Google\Chrome\User Data\Default\History”
    - Firefox : “C:\Users[username]\AppData\Roaming\Mozilla\Firefox\Profiles[randomfoldername]\places.sqlite”
    - Edge : “C:\Users[username]\AppData\Local\Microsoft\Edge\User Data\Default\History”
    - Opera : “C:\Users[username]\AppData\Roaming\Opera Software\Opera Stable\History”
- **Windows Server :** Comment détecter qui a supprimé un fichier

Mise en place de chiffrement

Description :

Si un employé interne ou un acteur malveillant tente de contourner les systèmes de sécurité en chiffrant ou déchiffrant des données sensibles sans autorisation, cela peut indiquer une tentative de compromettre des informations critiques ou de couvrir des actions frauduleuses. Un tel comportement pourrait entraîner des fuites de données, des atteintes à la confidentialité, et une perte de disponibilité des informations au sein de l'organisation.

Proposition de processus de protection :

- Mettre en place des mécanismes de surveillance basiques pour détecter les tentatives de chiffrement ou de déchiffrement anormales par les employés.
- Déployer un système de détection avancé pour identifier rapidement toute tentative non autorisée de chiffrement ou déchiffrement des données sensibles.

Commentaire :

Certaines solutions de protection sont capables de détecter le déploiement de chiffrement sur les fichiers. Il convient de se renseigner auprès de l'éditeur.

Documentation :

Obligation : donner son mot de passe

Modification de la configuration du BIOS

Description

La modification non autorisée de la configuration du BIOS, comme le changement de l'ordre de boot ou l'activation de services supplémentaires (Bluetooth, NFC, etc.), représente un risque majeur pour la sécurité de l'organisation. Ces actions peuvent indiquer une tentative de compromettre le système en permettant le démarrage à partir de médias externes non sécurisés, l'installation de logiciels malveillants, ou l'accès à des fonctionnalités restreintes. Un tel comportement pourrait conduire à une compromission complète du système, rendant possible le vol de données, l'installation de logiciels espions, ou d'autres activités malveillantes, ce qui mettrait en péril l'intégrité des systèmes de l'entreprise.

Proposition de processus de protection :

- Mettre en place des alertes pour détecter toute modification du BIOS, telles que le changement de l'ordre de boot ou l'activation de services supplémentaires.
- Restreindre l'accès au BIOS aux administrateurs autorisés en utilisant des mots de passe robustes et, si possible, l'authentification multifactorielle (MFA).
- Effectuer des contrôles périodiques de la configuration du BIOS pour identifier toute modification non autorisée ou suspecte.

Commentaire

N/A

Documentations

- Intune : Configuration du BIOS avec Intune

Collecte

La phase de collecte marque le début de l'activité potentiellement sur des données peuvent signaler un comportement suspect.

À ce stade, le risque n'est pas encore confirmé, mais les premières actions suggèrent que le personnel pourrait commencer à manipuler des informations sensibles de manière non autorisée ou à minima dangereuse.

Bien que ces actions ne constituent pas encore une preuve totale d'une intention malveillante, elles représentent des signes précurseurs qui nécessitent une surveillance accrue et une évaluation approfondie pour éviter que ces comportements ne se développent en menaces avérées pour l'entreprise.

Téléchargement massif

Description

Le téléchargement massif de données provenant d'applications, de serveurs de fichiers, de courriels ou de l'intranet constitue un comportement suspect pouvant indiquer une tentative d'exfiltration de données sensibles ou d'informations critiques. Ce phénomène peut signaler qu'un employé cherche à collecter un volume important de données en vue de les utiliser à des fins non autorisées, compromettant ainsi la sécurité des informations et les opérations de l'entreprise. Les téléchargements massifs peuvent également suggérer une préparation à un départ imminent, du sabotage interne, ou des violations potentielles des politiques de sécurité de l'entreprise. Il est donc essentiel de surveiller et d'enquêter sur ces activités pour protéger les données et prévenir les risques associés.

Proposition de processus de protection :

- Mettre en place des alertes pour détecter les téléchargements massifs de données à partir de divers systèmes, tels que les serveurs de fichiers, les courriels, ou l'intranet.
- Analyser les modèles de téléchargement pour identifier les anomalies et déterminer si elles nécessitent une investigation plus approfondie.
- Déployer une surveillance en temps réel et une analyse approfondie des activités de téléchargement, en intégrant des outils capables de détecter les volumes importants de données transférées.
- Mettre en place des contrôles d'accès renforcés et des mécanismes d'audit pour suivre et limiter les téléchargements massifs.
- En cas de détection de comportements suspects, effectuer des enquêtes détaillées pour évaluer les intentions et la sécurité des informations.

Commentaire

Pour la mise en place de ce point, il est nécessaire d’avoir une bonne connaissance de son infrastructure et de l'utilisation qui en est faite d’une manière générale.

Documentations

N/A

Création de sauvegardes

Description

Lorsqu'un employé commence à collecter des données à partir de divers dépôts et à les sauvegarder sur un disque dur externe ou un autre support au moment de son annonce de départ, cela peut indiquer une intention de transférer des informations sensibles ou critiques hors de l'entreprise. Cette activité peut signaler une tentative de vol de données, de sabotage ou de préparation à un départ avec des informations confidentielles.

Proposition de processus de protection :

- Déployer une surveillance proactive des activités de copie et de sauvegarde des systèmes, avec des outils capables de détecter les transferts de données massifs et les sauvegardes vers des supports externes.
- Mettre en place des contrôles d'accès stricts pour les sauvegardes système et configurer des alertes en temps réel pour toute tentative de copie de données sensibles.
- En cas de détection de comportements suspects, mener des enquêtes détaillées pour évaluer les risques et assurer la protection des informations.

Commentaire

La mise en place de fichiers « canary » au sein de dossiers critiques peut être une solution pour identifier des ouvertures de fichiers sensibles hors de l'entreprise. La copie des sauvegardes système est une activité sensible qui nécessite une surveillance étroite pour prévenir les abus potentiels. Bien que les sauvegardes puissent être nécessaires pour des raisons légitimes, les tentatives de transfert de grandes quantités de données hors de l'entreprise doivent être examinées avec soin pour éviter les fuites d'informations.

Documentations

- Mise en place de quota : Quota Management
- Blocage USB via Intune : Restrict USB with Intune
- Blocage USB via GPO : Manage USB Flash Drive with GPO

Impression d’écran

Description

La prise de captures d'écran par un employé pour contourner les contrôles de sécurité représente un comportement préoccupant. Lorsqu'un employé utilise cette méthode pour recueillir des informations afin d'éviter les restrictions de sécurité ou de dissimuler une piste de vérification, il peut s'agir d'une tentative délibérée de collecter des données sensibles sans laisser de trace. En capturant des images des informations à l'écran et en les exportant ultérieurement, l'employé cherche à contourner les mécanismes de protection des données tout en évitant d'enregistrer directement les informations dans des fichiers, ce qui pourrait attirer l'attention.

Proposition de processus de protection :

- Implémenter des solutions de sécurité avancées qui détectent et bloquent la capture d'écran des informations sensibles, comme des outils de prévention de la perte de données (DLP) capables de surveiller les tentatives de capture et de copie d'écran.
- Configurer des alertes en temps réel pour signaler les activités suspectes et mener des enquêtes détaillées pour comprendre les intentions et protéger les informations.

Commentaire

N/A

Documentations

- Désactivation de capture d'écran sous Office : Désactivation de la capture d'écran

Exfiltration

La phase d'exfiltration marque le point critique où les indices de comportement suspect ont évolué vers une confirmation plus que probable d'une activité dangereuse voire malveillante.

À ce stade, le doute est plus fort que jamais, car les preuves suggèrent que des données sont activement transférées hors de l'entreprise.

L'exfiltration est souvent le résultat d'une intention délibérée de voler ou transmettre des informations et peut indiquer une violation grave des politiques de sécurité.

Téléversement vers un service de partage de fichier tiers

Description

Le téléversement de données vers un service de partage de fichiers tiers représente une activité préoccupante qui peut signaler une tentative d'exfiltration d'informations sensibles ou confidentielles. Lorsque des employés transfert des données de l'entreprise vers des plateformes externes, telles que des services de stockage en ligne non approuvés ou des applications de partage de fichiers, cela peut indiquer une intention de contourner les contrôles internes de sécurité ou de préparer une fuite de données. Cette activité est particulièrement risquée si les services utilisés ne sont pas validés par l'entreprise ou s'ils ne respectent pas les normes de sécurité nécessaires pour protéger les informations sensibles.

Proposition de processus de protection :

- Mettre en place des alertes pour détecter les transferts de données vers des services de partage de fichiers tiers.
- Configurer des contrôles pour limiter l'accès aux plateformes de partage non autorisées et analyser les tendances de téléversement pour identifier des comportements inhabituels.
- Effectuer des vérifications périodiques des activités de partage de fichiers pour évaluer les risques.
- Déployer une solution de sécurité qui surveille et bloque automatiquement les transferts de données vers des services de partage de fichiers non approuvés (DLP).
- En cas de détection d'une activité suspecte, mener des enquêtes détaillées pour évaluer la nature des données transférées et prendre les mesures correctives nécessaires.

Commentaire

Il est recommandé, en amont, d'identifier la population interne dont l'activité justifie le téléversement massif (ex : service communication) et de définir, au besoin, un seuil à partir duquel les alertes ne nécessitent pas d'actions et sont considérées comme « normales ». Malgré ce seuil, il est important de conserver une trace de cette activité.

Documentations

- Microsoft PureView DLP : Documentation

E-mail externe avec pièces jointes / volumétrie importante

Description

Lorsque des employés envoient un volume élevé de messages ou des e-mails contenant des pièces jointes volumineuses vers des adresses externes, cela peut indiquer un comportement suspect visant à transférer des informations confidentielles hors de l'entreprise. Ces activités peuvent contourner les contrôles de sécurité internes et masquer une fuite potentielle de données.

Proposition de processus de protection :

- Mettre en place des alertes pour surveiller l'envoi de volumes élevés d'e-mails ou de pièces jointes de grande taille vers des adresses externes.
- Analyser les tendances d'envoi et les modèles de taille des pièces jointes pour identifier des comportements atypiques.
- Effectuer des vérifications régulières pour évaluer la légitimité des transferts d'e-mails et des pièces jointes volumineuses.
- Configurer des contrôles automatisés pour bloquer ou signaler les envois d'e-mails avec des pièces jointes volumineuses ou un volume anormalement élevé.
- En cas de détection d'activités suspectes, réaliser des enquêtes approfondies pour déterminer la nature des données transférées et les intentions possibles.

Commentaire

N/A

Documentations

- Exemple de fuite de données via la signature mail : Lien

Téléversement vers un périphérique de stockage amovible

Description

Lorsqu'un employé copie des fichiers importants ou volumineux vers un périphérique de stockage amovible, cela peut indiquer une intention de contourner les contrôles de sécurité internes ou de préparer une exfiltration de données. Ce comportement est particulièrement préoccupant si le périphérique n'est pas contrôlé ou s'il est utilisé de manière inhabituelle.

Proposition de processus de protection :

- Analyser les utilisations des périphériques pour identifier les transferts inhabituels ou volumineux.
- Configurer des contrôles de base pour limiter l'accès aux périphériques de stockage non approuvés et surveiller les activités de copie de données sur ces périphériques.
- Déployer des outils de prévention de la perte de données (DLP) pour surveiller les transferts de fichiers et détecter les tentatives de copie de données sensibles.

Commentaire

N/A

Documentations

- Blocage USB via Intune : Documentation Intune
- Blocage USB via GPO : Documentation GPO

Impression massive de documents

Description

Lorsque des employés impriment des volumes importants de documents ou des fichiers contenant des données sensibles, cela peut indiquer une tentative de transfert ou de collecte d'informations hors des systèmes de contrôle de l'entreprise. Une telle activité peut signaler des intentions d'exfiltration de données ou de préparation d'activités malveillantes.

Proposition de processus de protection :

- Mettre en place des alertes pour surveiller les volumes d'impression élevés ou les impressions de documents sensibles. Analyser les tendances d'impression pour détecter des comportements inhabituels.
- Configurer des contrôles pour limiter l'accès à l'impression de documents confidentiels et effectuer des vérifications régulières des logs d'impression pour identifier des anomalies.
- Implémenter des solutions de sécurité qui surveillent et contrôlent les activités d'impression, notamment les outils de prévention de la perte de données (DLP) qui peuvent restreindre l'impression de documents sensibles.

Commentaire

N/A

Documentations

- Activer les logs du serveur d’impression : Documentation IT Connect

Mesures proactives

Les mesures proactives visent à renforcer la résilience de l'organisation face aux menaces internes en mettant en place des pratiques et des contrôles préventifs.

Ces mesures ne ciblent pas directement les comportements suspects observés mais contribuent à créer un environnement plus sécurisé et à réduire les risques.

En adoptant ces mesures proactives, l'organisation améliore non seulement sa capacité à prévenir les incidents de sécurité mais aussi à réagir de manière plus efficace en cas de menace avérée.

DLP

La mise en place de solutions de prévention de la perte de données (DLP) est essentielle pour surveiller et protéger les informations sensibles. Ces outils permettent de détecter et de bloquer les transferts non autorisés de données, tout en assurant une gestion rigoureuse des politiques de sécurité pour éviter les fuites.

Surveillance des sauvegardes

La surveillance des sauvegardes, en incluant le suivi des accès, des modifications et des lieux de stockage, garantit que les copies de données critiques sont sécurisées et protégées contre les manipulations non autorisées. Ce contrôle permet de détecter rapidement toute activité suspecte liée aux sauvegardes et de prendre des mesures correctives si nécessaire.

Collaboration entre les équipes

La collaboration avec le service des ressources humaines est cruciale pour aligner les politiques de sécurité avec la gestion des employés. Cette coopération aide à identifier les risques liés aux changements dans le personnel, tels que les départs ou les transferts, et à mettre en place des mesures adaptées pour sécuriser les données.

Le partenariat avec le service juridique permet d'assurer que les pratiques de sécurité respectent les régulations en vigueur et de gérer les implications légales liées à la sécurité des informations. Ce service aide également à élaborer des politiques et des procédures conformes aux exigences légales et à gérer les incidents de sécurité de manière appropriée.

Avertir l'équipe de sécurité dès le moindre doute est une pratique proactive clé. En signalant immédiatement toute activité suspecte ou comportement inhabituel, les équipes de sécurité peuvent réagir rapidement, enquêter sur les incidents potentiels et prendre des mesures pour prévenir les risques avant qu'ils ne se concrétisent.

Rôle Based Access

La mise en place du "Role Based Access" assure que les employés n'ont accès qu'aux informations nécessaires à l'exercice de leurs fonctions. En restreignant les accès aux données sensibles uniquement aux personnes autorisées, cette approche minimise le risque de fuites internes.

Méthode AGDLP : https://neptunet.fr/agdlp/

Mobile Device Management

Les smartphones et tablettes sont devenus des extensions incontournables des PC, offrant aux employés une flexibilité accrue pour accéder aux ressources de l'entreprise, qu'ils soient au bureau ou en déplacement. Cependant, cette commodité s'accompagne de risques significatifs.

Cas particulier : les équipes de sécurité internes

Les équipes de sécurité, en raison de leur rôle, peuvent parfois se considérer au-dessus des règles de sécurité qu'elles appliquent aux autres employés. Ces équipes disposent souvent d'exclusions de règles, de privilèges étendus, et d'un accès quasi illimité aux systèmes sensibles, ce qui les place en première ligne en termes de potentiel de menace interne. De plus, le fait qu'elles s'auto-surveillent peut entraîner un manque de vigilance, voire de la complaisance, dans le respect des protocoles de sécurité.

Ce risque est accentué par des pratiques telles que le téléversement de fichiers sensibles ou de samples de logiciels malveillants vers des sandbox publiques sans une évaluation rigoureuse des implications.

De telles actions peuvent involontairement exposer des informations critiques à des acteurs externes, compromettant ainsi la sécurité de l'entreprise.

Exemple avec des fichiers Zed : https://static.sstic.org/videos2024/540p/zed-files__aux_frontires_du_rel.mp4