Guide d'achat de solutions de gestion des menaces internes

Ce guide d'achat met en évidence les fonctionnalités les plus importantes d'une solution de gestion des menaces internes (ITM, Insider Threat Management). Il fait la synthèse des connaissances acquises par Proofpoint au cours de l'élaboration de programmes ITM efficaces pour des entreprises de toutes tailles, à travers le monde et dans tous les secteurs. Ce guide vous aidera à tous les stades de votre parcours, que vous commenciez à aborder cette problématique ou que vous souhaitiez moderniser votre solution ITM existante.

Sécurité centrée sur les personnes

Pour protéger les données contre les menaces internes, vous avez besoin d'une solution qui prend en charge un modèle de sécurité centré sur les personnes. Ce type de modèle offre une visibilité complète sur les comportements à risque des utilisateurs et sur leurs interactions avec les données sensibles. Vous bénéficiez ainsi d'informations contextuelles importantes quant à leurs intentions lorsque leurs actions semblent porter préjudice à l'entreprise, que ce soit de manière délibérée ou non.

Grâce à une solution centrée sur les personnes, vous pouvez rapidement évaluer les risques internes en vous basant sur des indicateurs comportementaux. Considérés de manière globale, sur la durée et dans le contexte d'autres activités, ces indicateurs peuvent révéler qu'un utilisateur est susceptible de nuire à l'entreprise et que son comportement mérite un examen plus approfondi afin de déterminer la réponse appropriée à y apporter.

Éléments incontournables d'une solution ITM

Si vous souhaitez bloquer les menaces internes, vous devez être en mesure de les identifier, de protéger l'environnement de façon adéquate, et de prévenir et neutraliser les incidents liés à ces menaces particulières. Pour limiter le risque de menaces internes, toutes ces opérations doivent être coordonnées de façon proactive.

Identifier

Vous devez vous doter d'une solution qui offre une visibilité sur les comportements à risque avant que toute menace interne se manifeste. Ainsi, vous devez pouvoir identifier les comportements anormaux sur la base de valeurs de référence. La solution doit permettre la surveillance des utilisateurs à risque, comme les utilisateurs avec accès à privilèges, les collaborateurs quittant l'entreprise ou susceptibles de le faire, les sous-traitants, les cadres et les utilisateurs faisant l'objet d'une investigation. L'identification des utilisateurs à risque peut aussi prendre en compte des déclencheurs particuliers tels que la modification du statut d'un collaborateur (licenciement, démission), les changements au sein de la structure d'entreprise (fusion, acquisition, réorganisation), sans oublier les comportements préoccupants (expressions de mécontentement, litiges d'ordre financier, etc.).

Chaque entreprise doit décider des contrôles de prévention à mettre en œuvre en fonction de ses objectifs métier, de sa culture d'entreprise et de sa rapidité d'innovation.

Protéger

La solution ITM adoptée doit contribuer à protéger les données et systèmes sensibles à l'aide de contrôles de sécurité centrés sur les personnes. Les règles doivent intégrer des indicateurs comportementaux pour renforcer la protection contre les comportements à risque.

Il est important d'empêcher un utilisateur d'enfreindre, volontairement ou non, les règles de sécurité par une formation adéquate, des rappels en temps réel et une fonctionnalité de blocage. Bien évidemment, il n'est ni possible, ni souhaitable de bloquer toutes les activités : la prévention ne doit pas devenir un frein à la productivité des utilisateurs. Chaque entreprise doit décider des contrôles de prévention à mettre en œuvre en fonction de ses objectifs métier, de sa culture d'entreprise et de sa rapidité d'innovation.

Une solution ITM doit également offrir un moyen flexible et efficace de gérer l'accès aux données utilisateur. La solution déployée doit être dotée de contrôles d'accès assurant aux analystes en sécurité une visibilité sur les données uniquement dans les cas où cela s'avère nécessaire.

Détecter

Une solution ITM doit proposer des alertes et des actions en temps réel associées aux comportements des utilisateurs. Les activités à risque susceptibles de déclencher des alertes sont notamment les suivantes :

- Dissimulation d'informations
- Élévation de privilèges
- Contournement de contrôles de sécurité
- Exfiltration de données
- Téléchargement de logiciels non approuvés
- Sabotage informatique
- Création d'une porte dérobée (backdoor)
- Accès non autorisé
- Utilisation inacceptable

En cas de violation d'une règle, la solution doit pouvoir capturer les détails (qui, quoi, quand et où) de l'activité utilisateur afin de proposer un contexte précis et des informations pertinentes sur le comportement et les intentions associés. La solution doit également enregistrer des captures d'écran pour pouvoir fournir des preuves irréfutables dans le cadre des investigations. Elle doit aussi présenter la flexibilité nécessaire pour répondre de façon dynamique au comportement à risque et n'enregistrer des captures d'écran qu'après qu'une alerte a été générée, ce qui contribue à protéger la confidentialité de l'utilisateur et permet aux analystes en sécurité de gagner en efficacité.

Les utilisateurs négligents sont la principale cause de fuites de données et de menaces internes. Bien qu'animés de bonnes intentions, ces utilisateurs commettent des erreurs, qui peuvent avoir des répercussions désastreuses.

Répondre

Il est important d'enquêter et d'intervenir rapidement et efficacement en cas d'incident. Plus il faut de temps pour neutraliser une menace interne, plus celle-ci peut faire des dégâts sur le plan des résultats financiers et de la réputation. Les workflows d'investigation constituent un élément critique pour suivre le statut d'un incident, particulièrement lorsque celui-ci doit être remonté à des groupes externes à l'équipe de sécurité, comme les équipes en charge des RH, des questions juridiques, de la conformité et de la confidentialité, qui doivent parfois être impliquées dans une enquête sur un incident. Une solution ITM robuste doit aussi être intégrée à un système de gestion des événements centralisé, tel qu'un SIEM, déjà exploité par l'équipe d'analystes en sécurité.

Trois scénarios principaux de fuite de données

Il existe trois types principaux de menaces internes. Tous sont imputables à une intervention humaine. Une solution ITM centrée sur les personnes doit pouvoir identifier ces trois types, à savoir :

- **Utilisateurs négligents.** Personnes qui manquent de rigueur et commettent des erreurs.
- **Utilisateurs malveillants.** Personnes qui cherchent à nuire à l'entreprise.
- **Utilisateurs compromis.** Personnes dont les identifiants de connexion ont été subtilisés par un cybercriminel extérieur.

1. Utilisateurs négligents et erreurs courantes

Selon le rapport Data Loss Landscape 2024 de Proofpoint, les utilisateurs négligents sont la principale cause de fuites de données et de menaces internes. Il s'agit d'utilisateurs animés de bonnes intentions, mais commettant des erreurs. Souvent, ils souhaitent simplement faire leur travail le plus efficacement possible, mais leurs erreurs peuvent avoir de graves conséquences : perturbation des activités, atteinte à la réputation, position concurrentielle fragilisée, infractions et amendes réglementaires, actions en justice, etc.

Voici quelques exemples d'actions à risque de ces utilisateurs :

- Envoi d'emails au mauvais destinataire, avec ou sans pièce jointe
- Partage de données sensibles sur des sites d'IA générative
- Consultation de sites de phishing
- Installation de logiciels non autorisés
- Partage public de fichiers et données sensibles
- Envoi par email de données personnelles à un compte de messagerie personnel
- Enregistrement de données sensibles de l'entreprise sur des terminaux personnels

Les utilisateurs malveillants sont dangereux, car ils sont idéalement placés pour voler des données sensibles et nuire à l'entreprise. Ils sont motivés par leur intérêt personnel.

Protection contre la négligence

Une solution ITM efficace permet de détecter et de prévenir les activités à risque. Elle offre également aux utilisateurs négligents un accompagnement qui leur permet d'identifier et de modifier leurs comportements à risque.

Fonctionnalités indispensables d'une solution ITM :

- **Classification.** Vérifiez que la messagerie, les données et les contenus font l'objet d'une surveillance continue à la fois manuelle et par l'intelligence artificielle (IA) pour identifier et classer les utilisateurs à risque. Lorsqu'un utilisateur est considéré à haut risque, le système lui attribue un score de risque pour protéger les données en conséquence.
- **Surveillance.** La solution doit surveiller les comportements et activités à risque comme l'utilisation non autorisée d'applications et du Web, la modification des noms et types de fichiers de documents sensibles, l'accès à des données sortant du cadre de leur travail, ou encore l'exfiltration de nombreux documents confidentiels. La surveillance des groupes à haut risque peut permettre d'identifier les utilisateurs qui nécessitent une surveillance plus approfondie.
- **Prévention.** Il convient d'empêcher les utilisateurs d'exfiltrer des données sensibles à partir de l'endpoint : emails avec ou sans pièce jointe envoyés au mauvais destinataire, clés USB, chargements Web, synchronisation cloud, partage réseau, impression, etc. S'ils commettent une erreur, ces utilisateurs doivent recevoir instantanément un message d'avertissement contextuel leur permettant de la corriger et de prévenir l'incident en temps réel, sans intervention de l'administrateur. Si nécessaire, les utilisateurs peuvent fournir une justification d'accès aux données. L'équipe de sécurité peut alors autoriser ou refuser cette demande.
- **Formation continue.** Les utilisateurs négligents ignorent souvent que leur comportement est dangereux. Une solution ITM doit proposer aux utilisateurs des formations et sensibilisations, par le biais de notifications de comportements dangereux et de liens vers les règles de l'entreprise.

2. Utilisateurs malveillants

Les utilisateurs malveillants sont dangereux, car ils sont idéalement placés pour voler des données sensibles et nuire à l'entreprise. De plus, ils sont motivés par leur intérêt personnel. Les collaborateurs quittant l'entreprise constituent le type d'utilisateurs internes le plus à risque, mais il en existe d'autres.

Les principales menaces liées aux utilisateurs internes malveillants sont les suivantes :

- **Fraude.** Acte de tromperie provoquant des perturbations de l'activité.
- **Sabotage.** Action causant des dommages à un système ou la destruction de données.
- **Vol.** Extraction de toute information propriétaire qui possède une valeur pour l'entreprise.
- **Espionnage.** Extraction et vente de données de valeur, de secrets commerciaux et autres à un concurrent ou à un adversaire.

Un système centré sur les personnes surveille certains utilisateurs de plus près que d'autres, et applique des contrôles d'accès plus stricts aux utilisateurs les plus à risque.

Si les utilisateurs internes malveillants sont si dangereux, c'est parce qu'ils occupent une position de confiance. À ce titre, ils peuvent attendre leur heure pour exploiter leur accès à privilèges, mettre la main sur des données précieuses et exploiter des failles de sécurité. En outre, les entreprises créent souvent des vulnérabilités en permettant à leurs collaborateurs de consulter et de stocker des données sur leurs terminaux personnels, ce qui facilite le vol de données sensibles et les actes dommageables.

Protection contre les utilisateurs malveillants

Un système centré sur les personnes peut surveiller certains utilisateurs de plus près que d'autres et appliquer des contrôles d'accès plus stricts aux utilisateurs les plus à risque. Il peut en outre bloquer de façon proactive les activités malveillantes en se basant sur des facteurs de risque tels qu'une démission ou un licenciement.

Fonctionnalités indispensables d'une solution ITM :

- **Visibilité.** Une visibilité sur les mouvements des données et les comportements offre une vue d'ensemble et des informations contextualisées sur l'activité d'un utilisateur et ses intentions. Des données télémétriques sur les interactions des utilisateurs avec les données et les systèmes doivent être collectées, par exemple en cas de changement de nom d'un fichier sensible ou de son chargement sur un site Web non autorisé ou dans un dossier de synchronisation cloud. Si un utilisateur télécharge des applications non autorisées, altère des contrôles de sécurité ou installe un navigateur TOR, ces activités à risque doivent également être surveillées. Une vue chronologique contextualisée des événements vous aidera à comprendre les tenants et aboutissants (qui, quoi, quand, où) des activités des utilisateurs et vous informera sur les actions effectuées par un utilisateur avant et après une alerte.
- **Bibliothèque de menaces.** Une bibliothèque d'alertes complète pour les scénarios les plus courants de menaces internes (fraude au temps de travail, exfiltration de données, contournement des contrôles de sécurité, etc.) est essentielle. Cela vous permettra d'être rapidement opérationnel, avec des règles permettant d'identifier les indicateurs comportementaux les plus fréquents.
- **Investigations.** Optez pour une solution qui fournit des métadonnées et des captures d'écran détaillées des activités utilisateur, qui pourront servir de preuves dans le cadre des investigations numériques. Les workflows collaboratifs sont importants pour gérer les incidents liés aux menaces internes. Comme les enquêtes sur les incidents internes impliquent des parties prenantes externes à l'équipe de sécurité (équipes en charge des RH, des questions juridiques, de la confidentialité et de la conformité, par exemple), il vous faudra partager des rapports sur les risques liés aux utilisateurs dans des formats faciles à consulter et à interpréter, comme des documents PDF.
- **Contrôles de la confidentialité.** Une solution ITM robuste est dotée de fonctionnalités telles que des contrôles d'accès basés sur des attributs, le masquage et l'anonymisation des données, ainsi que la prise en charge de centres de données multirégions. Elle vous permettra ainsi de répondre aux exigences en matière d'emplacement et de confidentialité des données, et d'éliminer les biais lors des investigations. Elle doit permettre de modifier de façon dynamique et flexible les règles de surveillance d'un utilisateur en temps réel si ce dernier déclenche une alerte, ce qui préserve la confidentialité en n'enregistrant des captures d'écran que lorsque cela s'avère nécessaire.

3. Utilisateurs compromis

Les comptes des utilisateurs compromis peuvent être contrôlés et utilisés de manière inappropriée par un cybercriminel externe. Avec ces comptes piratés, les cybercriminels disposent d'un accès privilégié à vos données et systèmes. La situation est d'autant plus problématique qu'il arrive souvent que les systèmes internes soient compromis depuis plusieurs mois avant que l'attaque ne soit repérée.

Les cyberpirates externes exploitent les vulnérabilités du facteur humain. L'ingénierie sociale, et le phishing en particulier, est l'une des techniques les plus couramment employées pour manipuler les utilisateurs. Cela n'est guère surprenant au vu du taux de réussite de ces types d'attaques : 71 % des entreprises ont subi une attaque de phishing fructueuse.

Quelques exemples de techniques de phishing courantes :

- Envoi de liens malveillants, de pièces jointes malveillantes et de demandes de données
- SMiShing (phishing par SMS)
- Phishing via les réseaux sociaux
- Attaques par téléphone (TOAD, Telephone-Oriented Attack Delivery)
- Piratage de la messagerie en entreprise (BEC, Business Email Compromise)
- Authentification multifacteur (MFA)

L'objectif des cybercriminels est toujours le même : obtenir un accès à des données et systèmes de valeur, afin de les exploiter à leur avantage ou à des fins lucratives.

Protection contre les utilisateurs compromis

Une solution ITM doit offrir visibilité et contexte afin d'aider à déterminer si le comportement d'un utilisateur est inhabituel. Si un utilisateur est enclin à cliquer sur des liens de phishing, par exemple, vous pouvez surveiller cet utilisateur à risque afin de repérer tout comportement inhabituel. Vous pouvez aussi protéger les données en vous assurant qu'elles ne pourront être consultées par des personnes précises que si cela est absolument nécessaire.

Fonctionnalités indispensables d'une solution ITM :

- **Surveillance proactive.** Grâce à la création et à l'enregistrement d'explorations personnalisées, vos équipes peuvent traquer régulièrement les exfiltrations de données et autres activités à risque. Les personnes très attaquées ou VAP (Very Attacked People), qui ont tendance à cliquer sur des liens ou pièces jointes malveillants ou à interagir avec des applications vulnérables, peuvent faire l'objet d'une surveillance afin de déceler tout comportement inhabituel, pouvant indiquer qu'il s'agit d'utilisateurs compromis. La même approche peut être adoptée pour d'autres groupes à haut risque, comme les collaborateurs qui quittent l'entreprise ou les utilisateurs avec des accès à privilèges. Comme il est impossible d'identifier par avance tous les utilisateurs internes dangereux, la solution ITM doit pouvoir modifier de façon dynamique et flexible les règles de surveillance d'un utilisateur en temps réel si ce dernier déclenche une alerte.
- **Contrôles adaptatifs de l'accès.** Vous pouvez appliquer des règles d'accès conditionnelles aux données, par exemple pour placer des pays, des réseaux ou des adresses IP à haut risque sur liste d'autorisation et/ou de blocage. Vous pouvez également limiter l'accès aux données sensibles à certains utilisateurs et groupes à privilèges, et n'autoriser les chargements et les téléchargements que sur des terminaux managés. Grâce à un contrôle d'accès basé sur les attributs, vous pouvez respecter les exigences en matière de confidentialité.
- **Intégrations.** Une solution ITM efficace complétera votre système de sécurité en ajoutant du contexte aux événements. Elle s'intègre facilement à divers outils, notamment :
  - Orchestration, automatisation et réponse aux incidents de sécurité (SOAR)
  - Gestion des événements et des incidents de sécurité (SIEM)
  - Réponse aux incidents
  - Gestion des tickets
- **Architecture moderne.** Une plate-forme native au cloud peut prendre en charge des centaines de milliers d'utilisateurs. Une solution ITM doit collecter des données télémétriques par le biais d'un agent léger qui ne nuit pas à la productivité des utilisateurs et ne présente aucune incompatibilité avec d'autres solutions.

Conclusion

Protéger votre entreprise contre les risques externes, qu'ils soient intentionnels ou involontaires, exige une solution ITM permettant une approche proactive. Une telle solution doit vous offrir une visibilité sur les comportements à risque et une capacité de réponse à la fois dynamique et automatique. Au vu de la collaboration transversale requise pour gérer les risques liés aux menaces internes, cette solution doit permettre des workflows d'investigation et être capable de collecter des preuves irréfutables, telles que des captures d'écran, pour étayer et accélérer les investigations. Enfin, une solution ITM doit pouvoir évoluer avec votre activité, exploiter vos investissements existants et proposer un accès flexible et des contrôles de la confidentialité pour préserver la conformité. Adopter une solution ITM disposant de ces fonctionnalités vous aidera à protéger votre entreprise contre les risques internes, tout en soutenant efficacement votre équipe de sécurité.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

1212-001-03-01 9/24