WithSecure™ Elements Identity Security

Gagnez en visibilité sur les attaques basées sur l'identité

January 2025

Introduction

WithSecure™ Elements Identity Security est une solution d'Identity Threat Detection and Response (ITDR). Elle protège les organisations contre les attaques basées sur l'identité en détectant les identités potentiellement compromises de Microsoft Entra ID et permet aux analystes de répondre rapidement aux menaces pour minimiser leur impact sur l'entreprise. Faisant partie de la famille de produits Elements XDR, Identity Security empêche les impacts majeurs du vol d'identifiants et des attaques contre les infrastructures de gestion des identités et des accès.

Les objectifs des attaquants n'ont pas changé, ils cherchent toujours à provoquer des perturbations et à voler des informations. Cependant, les attaques se concentrent de moins en moins sur le déploiement de charges utiles sur les endpoints et de plus en plus sur l'abus des identités (utilisateur et entité) et de leurs privilèges. L'équipe d'Incident Response de WithSecure observe une tendance croissante aux attaques centrées sur l'identité. Un rapport récent* a révélé que les identifiants volés sont devenus le point d'entrée le plus populaire pour les violations et que les violations initiées avec des identifiants volés ou compromis ont pris le plus de temps à identifier et à contenir.

De 2023 à 2024, il y a eu une augmentation de 71 % des attaques basées sur des identifiants d'utilisateur volés ou compromis. Les violations de données initiées avec des identifiants volés ou compromis ont pris le plus de temps à résoudre parmi les différents vecteurs d'attaque – près de 10 mois.***

Alors que les environnements informatiques d'aujourd'hui s'étendent au-delà des bureaux, vous avez besoin de plus que d'une hygiène de sécurité de base pour rester protégé. Bien qu'ils soient toujours utiles pour sécuriser les endpoints, les outils traditionnels de détection et de réponse (EDR) ne peuvent pas fournir de visibilité sur les identités et les services cloud accessibles de n'importe où. L'utilisation d'identités cloud Entra ID par les télétravailleurs et l'authentification aux outils tiers augmentent la surface d'attaque.

Les identités sont devenues un nouveau vecteur d'attaque lucratif, en particulier dans le cas de Microsoft Entra ID en tant que service cloud de gestion des identités et des accès (IAM). Entra ID joue un rôle central pour Microsoft 365, car il inclut également l'authentification multifactorielle et l'accès conditionnel. Il est utilisé par la plupart des organisations qui utilisent les services cloud Microsoft 365.

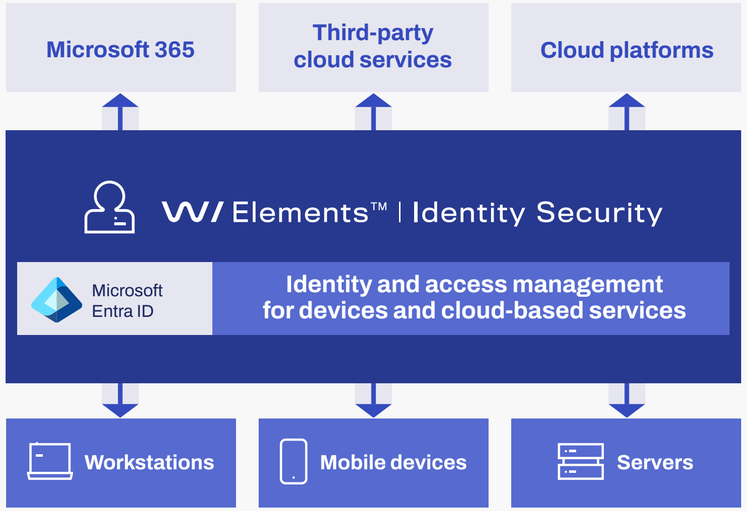
* IBM Cost of a Data Breach Report 2024
** IBM X-Force Threat Intelligence Index 2024

WithSecure™ Elements Identity Security vous permet de détecter et de répondre aux attaques basées sur l'identité en mettant en évidence les identifiants d'utilisateur potentiellement compromis, afin que les analystes puissent prendre des mesures pour protéger leur organisation. Les identifiants sont souvent collectés par les attaquants via des campagnes de phishing par mail ou en incitant les administrateurs à accepter des flux d'authentification non standard dans leur organisation. Elements Identity Security étend vos capacités de détection aux attaques basées sur l'identité au-delà des endpoints, pour sécuriser vos identifiants d'utilisateur.

Une fois qu'Elements Identity Security détecte une attaque, il facilite vos prochaines étapes de réponse. Toute activité détectée à partir d'un utilisateur potentiellement compromis est agrégée dans une détection de contexte large (Broad Context DetectionTM - BCD), de sorte que l'enquête puisse facilement se dérouler en un seul endroit, la plateforme cloud WithSecure Elements. Avec Elements Identity Security, vous pouvez répondre rapidement et facilement aux menaces d'identité pour minimiser les perturbations, par exemple en supprimant l'accès, en réinitialisant les mots de passe ou en mettant fin aux sessions pour arrêter les attaquants dans leur élan.

La couverture de détection pour Entra ID couvre une gamme de scénarios d'attaque récents, y compris la compromission des mails professionnels, où un attaquant obtient un accès non autorisé à un mail d'entreprise, qui peut ensuite être utilisé pour voler des données ou obtenir frauduleusement des fonds. En plus d'une large gamme de techniques, les phases d'attaque MITRE sont couvertes, à savoir : l'accès initial, la persistance, l'élévation des privilèges, l'évasion de la défense et l'accès aux identifiants.

Le service combine également les alertes natives de Microsoft Entra ID Protection* avec les autres activités capturées par WithSecure Elements Identity Security et agrège ces données. Cela permet aux clients d'avoir une vue complète des actions récentes effectuées par des comptes suspects ou compromis à partir d'un seul tableau de bord.



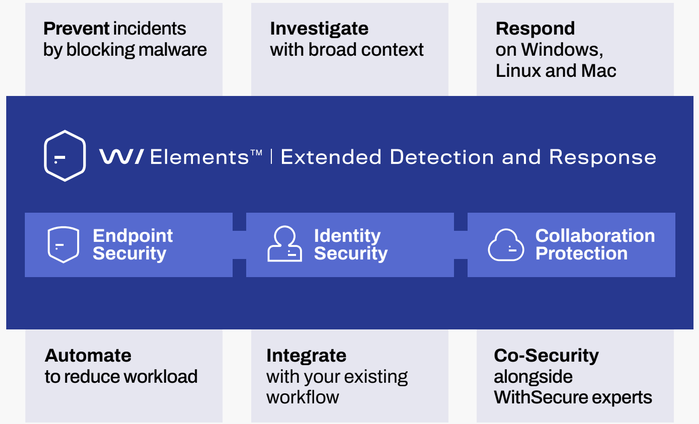
*Nécessite également une licence séparée pour Microsoft Entra ID Protection, qui est un produit qui alerte sur les connexions à risque (faisant partie des licences groupées de Microsoft comme Entra ID P1 et au-delà).

Fait partie de WithSecure™ Elements XDR

WithSecure™ Elements Identity Security est un module de WithSecure™ Elements Extended Detection and Response (XDR) et a été conçu pour les environnements informatiques d'aujourd'hui. Non seulement Elements XDR permet aux organisations de comprendre et de répondre aux menaces avancées sur les endpoints, les identités, les mails et les outils de collaboration, mais ses contrôles préventifs avancés automatisés permettent de limiter le nombre d'incidents et d'attaques de niveau inférieur.

Elements XDR vous permet d'identifier toute la chaîne d'attaque qui constitue une menace pour votre entreprise, en s'étendant au-delà des endpoints à différentes parties de l'attaque à travers les plateformes cloud, les identités et les mails. Reconnaître les attaques tôt vous donne, non seulement, une longueur d'avance pour répondre, mais vous permet également de réduire les coûts en diminuant les répercussions qui suivent les compromissions.

Elements XDR fait partie de notre plateforme cloud complète « Elements » qui comprend une large gamme d'outils et de capacités : Exposure Management, gestion automatisée des correctifs, threat intelligence dynamique et analyses comportementales continues. Les utilisateurs d'Elements Cloud peuvent facilement accéder à l'expertise de WithSecure avec nos services de co-sécurité qui offrent de l'aide pour comprendre et résoudre les détections complexes ou des incidents majeurs généralisés, par exemple.



Quelle est la différence entre EDR et XDR ?
Les solutions EDR se concentrent sur la détection et la réponse aux menaces pour les endpoints, tandis que WithSecure Elements XDR est une solution unifiée plus étendue pour protéger les environnements informatiques d'aujourd'hui. Elle minimise l'impact des attaques grâce à des contrôles préventifs avancés automatisés permettant de limiter le nombre d'incidents et d'attaques de niveau inférieur. Les outils alimentés par l'IA permettent une détection, une enquête et une réponse rapides aux menaces dans un contexte plus large – sur les endpoints, les identités, les mails et d'autres services cloud de collaboration. WithSecure Elements Identity Security est une solution ITDR pour protéger les organisations contre les attaques basées sur l'identité, inclus dans Elements XDR. WithSecure Elements Endpoint Detection and Response (EDR) fait également partie de notre offre Elements XDR, dans le cadre de notre solution d'Endpoint Security qui combine Elements EDR et Elements EPP (Endpoint Protection).

Comment fonctionne la tarification pour Elements Identity Security ?
Le prix est basé sur le nombre de comptes utilisateur Entra ID, donc tous les utilisateurs de chaque* tenant doivent être ajoutés. Vous pouvez obtenir Elements XDR avec protection pour les identités sans avoir besoin d'investir dans les abonnements les plus chers de Microsoft Entra ID comme P1 et P2, grâce à Elements Identity Security. Nous offrons un prix groupé pour Elements Identity Security avec Elements Endpoint Security (EPP + EDR).

Pourquoi avez-vous encore besoin de EPP et EDR (Elements Endpoint Security)?
Les attaquants cherchent constamment de nouvelles façons d'échapper à la détection. C'est un jeu perpétuel du chat et de la souris entre les attaquants et les défenseurs. L'exploitation croissante des Entra IDs indique un manque de couverture efficace contre les attaques basées sur l'identité. Cette tendance est susceptible de continuer jusqu'à ce qu'il y ait une adoption généralisée des outils ITDR, rendant les attaques si difficiles que les attaquants doivent chercher de nouvelles méthodes. L'augmentation des attaques liées à l'identité ne diminue pas l'importance de se protéger contre les menaces affectant les endpoints. Les ransomwares restent une menace importante pour de nombreuses organisations. Pour des informations plus détaillées, veuillez consulter nos derniers rapports sur la threat intelligence.

*La solution est compatible avec plusieurs tenants.

Pourquoi WithSecure™ Elements Identity Security ?

Protégez vos actifs les plus ciblés : vos utilisateurs. L'identité est la couche entre vos endpoints, les services cloud et les plateformes que votre organisation utilise. La protection des endpoints, les capacités de détection et de réponse protègent vos appareils, mais vous avez besoin de Elements Identity Security comme prochaine extension pour protéger votre environnement informatique.

Basé sur l'expérience d'attaques réelles de notre équipe d'Incident Response

Sécurisez vos travailleurs à distance en utilisant une logique de détection créée à partir d'attaques réelles ciblant les identités.

Empêchez l'utilisation des identifiants volés

Détectez les identifiants compromis et les attaques basées sur l'identité en obtenant une visibilité au-delà de l'endpoint.

Détectez la compromission Wdes emails professionnels

Détection éprouvée des techniques les plus coûteuses pour les organisations.

Agissez rapidement pour minimiser l'impact

Utilisez nos capacités de réponse Entra ID pour mettre fin aux sessions et désactiver l'accès des utilisateurs.

Enquêtez dans un large contexte

Toute activité détectée à partir d'un utilisateur potentiellement compromis est agrégée afin que l'enquête sur l'activité suspecte puisse être effectuée à partir d'un seul endroit central.

Services flexibles

Faites plus avec des ressources limitées en gérant facilement Elements XDR et en accédant à des services flexibles chaque fois que nécessaire.

Avantages

Protégez vos travailleurs à distance

Les solutions EDR traditionnelles ne protègent pas tous les actifs auxquels accède vos télétravailleurs. Les services cloud deviennent de plus en plus courants dans les environnements informatiques d'aujourd'hui et reposent souvent sur Entra ID, grâce à l'utilisation de fonctionnalités telles que l'authentification unique (SSO). Avec Elements Identity Security, vous pouvez étendre les capacités de détection au-delà des endpoints pour couvrir les identités et répondre rapidement aux menaces basées sur l'identité.

Enquêtez avec Broad Context Detection™

Les Broad Context Detections™ (BCD) réduisent la fatigue des alertes en agrégeant automatiquement les événements pertinents, en évaluant la gravité globale et en permettant des enquêtes à partir d'une vue consolidée. Les activités suspectes effectuées par les utilisateurs peuvent être examinées à travers une vue complète des actions récentes entreprises par des comptes potentiellement compromis. Avec les BCD, vous pouvez examiner les attaques sur une chronologie pour trouver des schémas, voir les événements pertinents et agir rapidement – avec nos recommandations. L'analyse comportementale en temps réel, l'analyse de la réputation et l'analyse des big data sont utilisées aux côtés du machine learning pour placer les détections dans leur contexte tout en tenant compte des niveaux de risque et de l'importance de chaque hôte affecté.

Nos divers mécanismes de détection créent des alertes de haute fidélité. Nous utilisons une combinaison de signes dans l'évaluation des risques et dans d'autres détections pour identifier les actions qu'un attaquant utiliserait après avoir obtenu un accès initial. Ces signes incluent des actions telles que la création d'enregistrements d'application, l'ajout de justificatifs aux principes de service et l'ajout de principes de service avec des noms similaires à ceux de Microsoft pour dissimuler les actions. La combinaison de ces types de signes permet de réduire les faux positifs, car nous pouvons être plus sûrs que la BCD est malveillante si elle contient plusieurs détections suspectes.

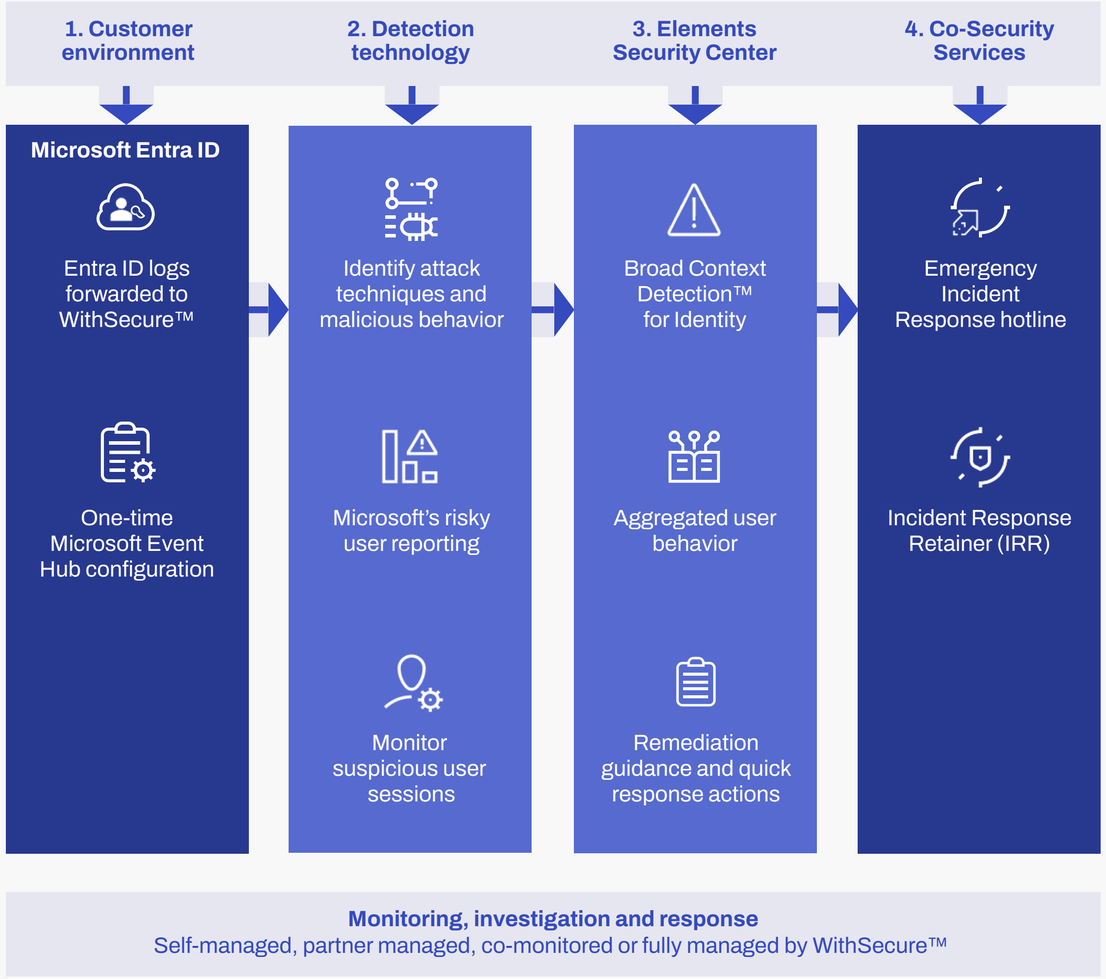
Détectez et répondez aux attaques basées sur l'identité

Protégez-vous contre les risques des attaques basées sur l'identité en ayant une visibilité sur les identifiants d'utilisateur compromis. Les identifiants sont souvent volés à l'aide de campagnes de phishing par mail qui récoltent les identifiants à partir de faux sites web qui incitent les administrateurs à accepter des flux d'authentification non standard dans leur organisation. Utilisez des alertes centrées sur l'utilisateur pour enquêter sur toute activité suspecte détectée à partir d'un utilisateur potentiellement compromis. En étant alerté, vous pouvez répondre rapidement lorsque des activités suspectes se produisent, vous permettant de minimiser l'impact des attaques avant que des données critiques pour l'entreprise ne soient volées. Chaque Broad Context Detection™ inclut des conseils de remédiation et des actions de réponse rapide, ce qui facilite une action rapide.

GenAI Luminen™

Utilisez notre assistant sur la plateforme Elements Cloud pour comprendre les attaques basées sur l'identité et les concepts clés (disponibilité de l'assistant pour la solution Identity Security prévue pour le premier semestre 2025*). Luminen™ GenAI analyse et fournit des explications compréhensibles sur les Broad Context Detections™ de WithSecure Elements XDR, enrichies de données pertinentes de renseignement sur les menaces externes. Il permet aux équipes informatiques d'aider immédiatement les utilisateurs de tout niveau d'expérience à mieux comprendre le contexte et l'impact des détections, leur permettant de se concentrer sur ce qui est le plus important.

Comment cette solution fonctionne-t-elle ?



1. Il y a une configuration unique de Microsoft Event Hub pour capturer les logs Entra ID de l'environnement du client*. L'intégration est configurée en trois parties : initialement en créant le tenant dans Elements Security Center ; puis en déployant l'infrastructure dans le tenant Microsoft ; et enfin en ajoutant la chaîne de connexion dans Elements Security Center, afin que la collecte de données puisse commencer.

2. Les logs Entra ID de Microsoft sont envoyés à WithSecure via un Microsoft Event Hub hébergé par le client. La technologie de détection de WithSecure identifie les techniques d'attaque et les comportements malveillants en utilisant les rapports d'utilisateurs à risque de Microsoft et en surveillant les sessions utilisateur suspectes.
   - Les logs collectés sont les logs de connexion et d'audit, les logs de connexion utilisateur non interactifs, les logs de connexion des principes de service, les logs de connexion des identités managés, les alertes et événements à risque de Microsoft des utilisateurs et des principes de service**.

3. Dans Elements Security Center, les détections liées à l'identité sont agrégées en incidents potentiels. Broad Context Detection™ pour l'identité apparaîtra comme une méthode pour comprendre le comportement utilisateur agrégé. Chaque Broad Context Detection™ inclut des conseils de remédiation et des actions de réponse rapide.

4. Souvent, la prochaine étape d'une enquête est de confirmer que l'activité est attendue et légitime. Par conséquent, généralement, le partenaire doit contacter l'utilisateur final pour valider l'activité dans le contexte de l'organisation. Cependant, la surveillance, l'enquête et la réponse peuvent être automanagées par le client ou managées par un partenaire. Il existe également des services de co-sécurité supplémentaires pour la réponse aux incidents disponibles auprès de WithSecure, par exemple notre service Incident Response Retainer (IRR). Nous offrons également une hotline de support d'urgence pour la réponse aux incidents 24/7/365.

*Il y a également une intégration unique pour la capacité de réponse, qui accorde le consentement du tenant client à une application de réponse Azure de WithSecure Elements. Cette connexion sera utilisée par la plateforme Elements pour émettre des tâches de réponse dans le tenant client.

** Plus d'informations sur les données collectées et leur objectif peuvent être trouvées dans la politique de confidentialité d'Elements.

Prévenez les impacts majeurs du vol d'identifiants avec notre technologie

Couverture de détection étendue

La couverture de détection des attaques liées à l'identité pour Microsoft Entra ID couvre une gamme de phases MITRE ATT&CK. Celles-ci incluent l'accès initial, la persistance, l'élévation des privilèges, l'évasion de la défense et l'accès aux identifians. La couverture de détection couvre une gamme de scénarios d'attaque récents, par exemple la compromission des courriels professionnels, où un attaquant obtient un accès non autorisé à un courriel d'entreprise qui peut ensuite être utilisé pour voler des données ou obtenir frauduleusement des fonds. Elements Identity Security peut également détecter des scénarios tels que des comptes compromis suspectés, l'utilisation des identifiants volés, une activité d'identité et d'accès suspecte ou des déplacements atypiques.

Les cookies et les tokens de session peuvent être volés par un site web malveillant Adversary-in-the-Middle (AitM) pour être réutilisés dans une attaque de prise de contrôle de session. Les circonstances dans lesquelles ces cookies et tokens, comme l'emplacement et l'appareil, sont réutilisés peuvent être des propriétés traçables de l'activité de session. Cela peut ensuite être utilisé pour détecter une activité suspecte. Notre solution suit les métadonnées de l'appareil et l'emplacement de l'activité de session, entre autres types de données, nous permettant d'évaluer la probabilité d'une session malveillante.

Facteurs de risque pour déterminer la protection de la connexion

WithSecure utilise de nombreux facteurs pour déterminer les risques d'un événement de connexion :

- **Géolocalisation** – Nous couvrons toute une série d'anomalies de déplacement impossible à partir de connexions réussies et échouées.
- **Force brute** – Il peut y avoir des centaines de connexions échouées pour des cas de déplacement impossible. Pour réduire le bruit, celles-ci sont agrégées ensemble et utilisées pour déterminer le risque ultime de la connexion, plutôt que d'alerter l'utilisateur sur des tentatives de force brute individuelles.
- **Anomalies du protocole OAuth** – Nous identifions des anomalies dans les événements de connexion OAuth, qui pourraient être de nouvelles ressources, applications ou clients.
- **Métadonnées de l'appareil** – Les différences dans les appareils et leurs métadonnées peuvent indiquer une session compromise et donc, augmenteront le risque de la connexion.
- **MFA (Authentification multifactorielle)** – Nous utilisons les métadonnées MFA pour évaluer à quel point un événement de connexion est suspect.
- **Principal inconnu** – Si le principal n'a pas été utilisé dans un événement de connexion pour l'organisation, cela augmentera le score de risque global de l'événement.

Visibilité étendue via l'intégration Entra ID

WithSecure Elements Identity Security s'intègre à Microsoft Entra ID (précédemment connu sous le nom d'Azure AD) en tant que service cloud de gestion des identités et des accès (IAM) le plus utilisé. Entra ID est obligatoire pour les services cloud Microsoft 365, et il peut être utilisé pour l'authentification à travers des services cloud tiers. Elements Identity Security capture les événements Entra ID basés sur l'identité pertinents, y compris les logs de connexion et d'audit, et les combine avec les alertes natives de Microsoft Entra ID Protection (si ce produit Microsoft est utilisé). Avec la combinaison de ces deux types d'événements basés sur l'identité, vous avez une visibilité étendue sur les attaques basées sur l'identité.

Déplacement impossible

Le déplacement impossible ou atypique est détecté par la solution. Cela fonctionne en détectant les cas où le déplacement physique sur de longues distances n'est pas possible dans un temps donné entre les connexions.

Compromission des mails professionnels

La compromission des mails professionnels (Business Email Compromise - BEC) est un type d'attaque d'identité où les auteurs se font passer pour un utilisateur interne en volant d'abord leurs identifiants. Cela leur permet ensuite d'envoyer un mail pour tromper d'autres individus au sein de la même organisation afin d'envoyer de l'argent ou de divulguer des informations sensibles. WithSecure a construit des détections basées sur des cas réels de réponse aux incidents de compromission des mails professionnels où les données du client Microsoft Outlook ont été utilisées.

Minimiser le bruit

En raison de la nature probabiliste des événements de connexion, il y a toujours un équilibre délicat entre la sur-alerte et les détections manquées. En développant le produit, nous avons soigneusement affiné nos détections et construit des mécanismes de suppression du bruit. Ces mécanismes incluent des aspects tels que :

- Suppression des alertes sur les donneurs d'ordre répétés dans un court laps de temps (histogrammes)
- Agrégation des activités ensemble pour déterminer un score de risque basé sur l'activité de l'utilisateur, plutôt que sur des événements de connexion uniques
- Examen du comportement à travers l'organisation pour réduire les anomalies avec le déplacement impossible (bien que l'utilisation du VPN puisse être un problème ici, nous atténuons ce problème en utilisant des statistiques de métadonnées de connexion courantes de l'entreprise).

Réponse d'identité

La réponse est une partie importante de la prévention des impacts majeurs des attaques et donc, un composant critique d'Elements Identity Security. Les actions de réponse rapide disponibles fonctionnent par une intégration directe entre Elements Cloud et votre instance Entra ID. Les actions de réponse incluent :

1. Terminer la session en cours
2. Réinitialiser le mot de passe
3. Bloquer l'accès utilisateur.

Qu'est-ce qu'un Event Hub ?
Un Event Hub est un mécanisme de collecte et de transfert de logs qui collecte les logs et les transfère à WithSecure.

Combien coûtera un Event Hub ?
Il y a un petit coût associé à l'utilisation des Event Hubs, généralement 15 euros par mois, veuillez consulter les coûts associés à Microsoft pour plus de détails.

Quelle est l'approche de rétention des données chez WithSecure ?
Les données liées aux Broad Context Detections (BCD) sont stockées pendant la durée de vie du service. Veuillez consulter notre politique de confidentialité pour plus d'informations.

Mesures de cybersécurité unifiées pour une protection étendue

Nous guidons les clients à travers les méandres de la cybersécurité depuis plus de 30 ans et notre solution de cybersécurité modulaire, WithSecure™ Elements, intègre dans une vue unifiée nos solutions XDR, Exposure Management ainsi que nos services de co-sécurité.

Une bonne cybersécurité ne peut pas être dans un silo. Tout d'abord, en utilisant une pile d'outils de cybersécurité fragmentée, vous devez constamment passer d'un portail à un autre. La fatigue des alertes est réelle, et gérer plusieurs flux de travail séparés est complexe, ce qui rend difficile la priorisation. Ensuite, la gestion n'est pas la seule inefficacité. Les solutions dans une configuration comme celle-ci ne coopèrent pas – et peuvent être complètement ignorantes les unes des autres. Cela signifie des silos, des détections manquées, des réponses lentes et finalement une posture de sécurité plus faible. Pour surmonter les défis d'un monde cloisonné, WithSecure™ Elements unifie les capacités de cybersécurité de base en une seule plateforme intelligente.

Plus d'éléments signifient plus de résultats, mais vous pouvez construire votre propre suite de cybersécurité cloud en choisissant des modules technologiques. Vous pouvez facilement introduire de nouvelles capacités et augmenter ou diminuer l'utilisation au fil du temps et selon vos besoins. Lorsque vous renforcez votre pile de cybersécurité avec une combinaison unifiée d'Exposure Management, de XDR ou encore de services de co-sécurité, vous pouvez repousser un spectre complet de menaces cyber. Les technologies unifiées fonctionnent ensemble comme une seule et sont faciles et efficaces à gérer à partir d'un seul portail, WithSecure™ Elements Security Center.

Elements Identity Security offre un ensemble cohérent avec le reste des solutions Elements, le rendant familier aux utilisateurs existants et facile à utiliser pour les nouveaux utilisateurs. Notre modèle de tarification transparent et nos modèles de licence cohérents à travers les solutions Elements facilitent la gestion des logiciels. Les équipes de sécurité et les partenaires peuvent examiner tous les produits Elements en une seule fois. Au lieu de solutions ponctuelles cloisonnées, WithSecure™ Elements vous donne les moyens de protéger votre environnement informatique de manière unifiée et efficace. Les technologies intelligentes sont alimentées par une IA avancée et une automatisation, allégeant la charge pour vous et votre équipe. Vous pouvez également déléguer la gestion de la sécurité à nos partenaires certifiés, et libérer du temps pour vous concentrer sur des activités plus stratégiques.

WithSecure™ Elements – Consolidez votre cybersécurité

Unifiez vos technologies de sécurité

Les composants de sécurité fonctionnent ensemble de manière transparente en utilisant un ensemble de données partagé et sont gérés via un portail unique, WithSecure™ Elements Security Center.

Vue de la situation en temps réel

Visibilité en temps réel de votre environnement, incluant une vue complète de l'activité, des risques et comment les prioriser.

Construisez votre suite

Personnalisez votre palette de sécurité avec différents modules.

Intégrez facilement

Connectez facilement les données de sécurité avec vos systèmes SIEM, SOAR, gestion de la sécurité, monitoring ou reporting tiers.

Adaptez-vous aux changements

Sans engagement, avec des options de licences flexibles, allant de l'utilisation basée sur la consommation (usage-based) aux licences annuelles.

Conditions techniques

Systèmes supportés
Étant donné que Elements Identity Security est conçu pour protéger Microsoft Entra ID dans le cadre de notre solution Elements XDR, vous devez avoir des droits administratifs sur les tenant Entra ID concernés pour configurer votre protection. Après la configuration initiale, tout ce dont vous avez besoin est un navigateur web et un accès Internet pour gérer Elements Identity Security dans le cadre de Elements XDR.

Langues
Anglais, finnois, français, allemand, italien, japonais, polonais, portugais (Brésil), espagnol (Amérique latine), suédois et chinois traditionnel (Taïwan).

Installation
Vous devez pouvoir vous connecter en tant qu'administrateur global sur le compte Azure pour exécuter le script dans Azure Cloud Shell et avoir votre ID de tenant, ID d'abonnement et emplacement de déploiement connus et prêts avant de commencer le déploiement. La licence doit être attribué à un groupe de gestion Azure.

Conditions de licence Elements
Elements Identity Security nécessite une sosucription à WithSecure Elements Endpoint Security, qui inclut les capacités de protection des endpoints (EPP) et de détection et réponse des endpoints (EDR).

Conditions de licence Microsoft
Il n'y a pas d'exigences de licence Microsoft pour Identity Security. Si le client dispose d'une licence P2 pour Entra ID, nous offrons une logique de détection pour utiliser les rapports de risque de Microsoft Entra ID Protection et désactiver l'accès conditionnel (une fonctionnalité qui nécessite une licence P2).

Autorisations Microsoft
Les rôles privilégiés suivants au sein du tenant Entra ID sont nécessaires pour la capacité de réponse :

- Permission Graph API : User.ReadWrite.All
- Rôle privilégié Azure : Administrateur

Bien que WithSecure ait mis en place des mesures pour réduire ce risque, les autorisations mentionnées ci-dessus ont des privilèges élevés que les attaquants pourraient exploiter. Les impacts potentiels incluent :

a) Création de nouveaux comptes utilisateur pour maintenir un accès non autorisé dans l'environnement
b) Attaques par déni de service (DoS) ciblant les administrateurs et les utilisateurs Entra ID
c) Accès non autorisé à des données sensibles, telles que les noms, adresses e-mail et fonctions

Limitations
Notez que le client est autorisé à 200 millions d'événements à travers les sources de logs Entra ID chaque mois. Si le nombre d'événements traités dépasse cette limite, un ajustement de prix peut être nécessaire. Pendant le déploiement, le client exécutera un script qui configure des alertes Azure pour lorsque le(s) Microsoft Event Hub(s) atteint sa capacité maximale. Le client est responsable de s'assurer que les Event Hubs ne dépassent pas leur capacité maximale, car cela affectera la prestation de services, WithSecure ne recevant plus tous les événements du tenant du client. Veuillez soumettre un ticket au service client de WithSecure si de telles alertes sont reçues d'Azure.

Coûts associés à Microsoft
La configuration du Microsoft Event Hub qui est déployée utilise des Event Hubs de niveau Standard. Le coût mensuel est basé sur le nombre d'unités de débit (TU). Le nombre de TU dépend de la charge. Les Event Hubs de niveau Standard coûtent environ 25 € par mois par unité de débit (TU). Les coûts associés aux Event Hubs sont décrits sur la page de tarification des Event Hubs de Microsoft Azure. Le coût par événement reçu via l'Event Hub est actuellement de 0,026 € par million d'événements. D'après nos données, le volume d'événements mensuel varie de 6 millions à 300 millions d'événements. Veuillez trouver plus d'informations sur le sujet dans notre guide utilisateur Identity Security.

WithSecure™ Elements – Réduisez les risques cyber, la complexité et l'inefficacité

WithSecure™ Elements Identity Security est disponible en tant que capacité intégrale SUR la plateforme de cybersécurité modulaire WithSecure™ Elements.

WithSecure™ Elements offre aux clients une protection complète dans une plateforme unifiée et un centre de sécurité facile à utiliser. La plateforme centralisée combine des capacités de sécurité prédictives, préventives et réactives puissantes en une protection intelligente contre les menaces allant des ransomwares aux attaques ciblées. Notre simplicité inégalée permet aux clients de se concentrer sur ce qui leur est le plus précieux.

Les packages de produits modulaires et les modèles de tarification flexibles offrent aux clients la liberté d'évoluer. WithSecure™ Elements peut faire partie de l'écosystème du client. Il peut être facilement connecté à leurs systèmes SIEM, SOAR, gestion de la sécurité, monitoring ou reporting.

Essayez Elements dès aujourd'hui

Contactez-nous pour sécuriser vos travailleurs à distance contre l'augmentation des attaques ciblant les identités.

Contactez-nous

A propos de WithSecure

WithSecure™ est le partenaire européen de référence en matière de cybersécurité. Grâce à un large réseau de revendeurs & MSSPs certifiés, nous fournissons des solutions de cybersécurité pour répondre aux besoins spécifiques des PME/PMI. Les racines européennes de WithSecure en matière de protection des données nous demandent la plus haute exigence en matière de confidentialité, souveraineté des données ainsi que sur notre conformité réglementaire.

Avec plus de 35 ans d'expérience dans le secteur, WithSecure™ propose aux entreprises une offre complète de solutions proactives et réactives afin de minimiser la surface d'attaques des entreprises et ainsi limiter le risque cyber. Pour répondre au mieux aux exigences du marché, WithSecure™ propose à ses partenaires des modèles commerciaux flexibles, garantissant un succès mutuel.

Les solutions WithSecure™ s'articulent autour d'une plateforme cloud de cybersécurité appelée « Elements ». Celle-ci intègre de manière transparente des technologies IA, une expertise humaine ainsi que des services de co-sécurité. De plus, elle permet aux PME de disposer de capacités modulaires pour la protection endpoint et cloud (EPP), la détection et la réponse aux menaces (EDR) ainsi que la gestion de l'exposition aux risques cyber (Exposure Management).

WithSecure™ Corporation a été fondée en 1988 et est cotée sur le NASDAQ OMX Helsinki Ltd.

WITH secure