Elevate to WithSecure™

Présentation du service - WithSecure™ Elevate

Février 2023

WITH secure

Sommaire

1 Présentation

Ce document décrit en détail notre service Elevate to WithSecure™. Ce service vous permet de faire remonter un cyberincident potentiel à WithSecure™, en vue d'une analyse plus poussée.

Elevate to WithSecure™ est un service à la demande. Il repose sur l'analyse des indices techniques issus des Broad Context Detections fournies par WithSecure™ Elements EDR.

1.1 Elevate to WithSecure™

Pour détecter et répondre efficacement aux attaques des hackers les plus redoutables, les entreprises doivent miser à la fois sur une analyse avancée des menaces et sur les conseils d'experts en cybersécurité.

Les clients de WithSecure™ Elements EDR peuvent bénéficier du service intégré Elevate to WithSecure™. Ce service offre une analyse professionnelle, à la demande, des cyberincidents. L'analyse repose sur les Broad Context Detections (ou simplement « détections ») assurées par WithSecure™ Elements EDR. Sur la base de cette analyse, nous pouvons vous fournir des conseils de réponse adaptés aux techniques, outils et processus utilisés par le hacker.

Si le profil de risque de votre entreprise indique une forte probabilité de cyberincident grave, nous vous recommandons de combiner Elevate to WithSecure™ avec nos services Incident Response et Incident Readiness. Ces services, vendus séparément, vous sont brièvement présentés à la fin de ce document.

1.2 Processus Elevate

Lorsque le professionnel chargé de gérer Elements EDR déclenche une escalade de détection vers WithSecure™, le processus Elevate commence. Débute alors une première phase appelée Threat Validation, au cours de laquelle la détection est validée. La plupart des cas sont résolus durant cette phase.

Si la détection est validée comme sérieuse ou comme étant une véritable attaque, le professionnel en charge d'Elements EDR peut demander à passer à une seconde phase facultative appelée : **Threat Investigation**. Au cours de cette seconde phase, la détection fait l'objet d'un examen approfondi et des propositions concrètes sont fournies pour assurer une réponse efficace.

Si la phase Threat Investigation détermine que le **seuil d'incident majeur** est atteint, l'expert en cybersécurité WithSecure™ recommandera une escalade vers une mission de réponse à incident.

1.2.1 Phase « Threat Validation »

Dans la phase de **Threat Validation**, les analystes de WithSecure™ déterminent la nature de la détection et la classent dans l'une des quatre catégories ci-dessous :

1. Menace réelle
2. Activité suspecte à laquelle il faut réagir
3. Activité suspecte pouvant être acceptée comme un comportement à risque dans l'environnement cible
4. Faux positif

Pour une validation efficace, un dialogue est nécessaire entre les analystes WithSecure™ et professionnel chargé de gérer WithSecure™ Elements EDR. Cette collaboration a lieu via le Elements Security Center, par lequel le service Elevate a été déclenché.

Sur la base de ces échanges et des informations contextuelles disponibles, les analystes WithSecure™ peuvent fournir des résultats de validation plus rapides. Ils peuvent notamment : comprendre le phénomène à l'origine de la remontée Elevate, déterminer quel élément pose problème et valider toutes les caractéristiques de la détection.

Si la détection est confirmée comme étant une véritable menace, les analystes WithSecure™ expliquent ce résultat. Ils fournissent des conseils de réponse, ainsi qu'une analyse du déroulement de l'enquête.

Si la détection est catégorisée comme suspecte, les analystes WithSecure™ peuvent recommander des vérifications supplémentaires pour mieux cerner le contexte de la détection. Forte de ces recommandations, l'entreprise peut choisir de continuer seule ou de requérir une assistance optionnelle.

Un faux positif est une détection injustifiée, d'ordre purement technique : il s'agit d'une simple activité standard perçue comme malveillante. Ces faux positifs peuvent être liés à l'impact imprévu d'un ajustement ou à la mise à jour des règles de détection.

Si un utilisateur interne légitime mène une activité suspecte, la détection n'est pas considérée comme un faux positif. Toute activité suspecte, qu'elles soient légitime ou malveillante, qu'elle soit le fait d'acteurs externes ou internes, justifie une investigation et une validation. C'est l'objectif même du service Elevate.

1.2.2 Phase « Threat Investigation »

Si la validation n'a pas suffi à écarter tout danger, ou si la détection est considérée comme une véritable menace, alors le client peut demander une phase optionnelle de **Threat Investigation**.

Au cours de cette étape, les analystes WithSecure™ effectuent une analyse plus poussée de la détection. Ils analysent :

1. les anomalies, les pics, les creux et les régularités observées dans la télémétrie des actifs et des connexions réseau,
2. les données fournies par la détection elle-même comme l'activité anormale des programmes, l'exécution de scripts inattendus et l'exécution inattendue d'outils système depuis des processus standard.
3. et enfin, le recoupement de ces données avec les renseignements sur les menaces que nous observons dans nos opérations partout dans le monde.

Une fois que l'analyste WithSecure™ a déterminé le type de menace en cours, il présente ses conclusions au professionnel chargé de gérer Element EDR.

Dans le cas où une attaque avérée est en cours, il propose des mesures visant à empêcher des dommages supplémentaires. L'accent est mis sur les mesures d'endiguement à court terme pour empêcher la menace de se propager, par exemple en isolant les systèmes touchés ou en mettant hors ligne les appareils infectés.

À l'issue de la phase de **Threat Investigation**, WithSecure fournit les résultats de son enquête avec des mesures d'intervention concrètes visant à maîtriser la menace.

Si la gravité du cas atteint le **seuil d'incident majeur**, ou si le professionnel ayant sollicité le service Elevate n'est pas en mesure de remédier à l'incident, les analystes WithSecure™ recommandent l'escalade vers un processus complet de réponse totalement distinct, pour contenir les menaces et les neutraliser. Ce processus de réponse n'est pas couvert par le service Elevate to WithSecure™ et est proposé séparément. Pour plus d'informations et pour connaître les critères définissant le seuil d'incident majeur, voir la section 5 : Services complémentaires.

2 Disponibilité du service

Pour utiliser le service, les conditions suivantes doivent être remplies :

- Abonnement WithSecure™ Elements EDR valide
- Agent(s) WithSecure™ Elements déployé(s)
- Abonnement valide au module complémentaire Elevate to WithSecure™
- Accès à la console de gestion WithSecure™ Elements

2.1 Horaires de service

Le service WithSecure™ Elevate est disponible 24h/24, 7j/7 et 365 jours par an. Notre objectif est d'amorcer la phase de validation des menaces dans les 2 heures suivant la demande Elevate. Une fois la validation terminée, vous visualisez instantanément les résultats sur votre WithSecure™ Elements Security Center.

2.2 Langue disponible

Elevate to WithSecure™ est uniquement disponible en anglais.

3 Collecte et rétention des données

Pour faire remonter les détections via la fonction Elevate, un agent WithSecure™ Elements EDR doit être installé sur au moins un périphérique. Les agents sont installés sur des appareils choisis par le client sur son réseau, pour détecter et conserver les données relatives aux anomalies de sécurité. L'agent envoie ensuite ces données à WithSecure™ pour analyse.

L'agent EDR WithSecure™ Elements collecte des données basées sur les événements, à partir de l'appareil sur lequel il est installé. Ces données d'événement sont les suivantes :

- Identifiants techniques de l'utilisateur
- Noms de domaine et connexions réseau
- Métadonnées concernant la création de processus, les comportements observés sur le réseau et les accès aux systèmes et sous-systèmes

L'agent collecte des informations sur les applications installés sur les appareils ayant été équipés d'une sonde. Il récolte également des informations sur le système/réseau, ainsi que d'autres mesures.

Les données collectées sont stockées de manière identifiable tant que leur traitement peut s'avérer nécessaire, sur la base de l'engagement du client avec WithSecure™ Elements EDR. Au moment de la rédaction du présent document, les données sont stockées en continu pendant un (1) an durant l'engagement client, et sont supprimées dans les deux (2) mois suivant la fin de cet engagement. Les données collectées manuellement sont stockées en continu pendant trois (3) mois.

Pour plus de détails, consultez notre politique de confidentialité EDR sur www.withsecure.com

En savoir plus

4 Licences

WithSecure™ Elevate est proposé sous licence, par le biais de deux types de tokens : l'un pour les Threat Validations, et l'autre pour les Threat Investigations. Ces tokens sont proposés dans plusieurs packs de taille variable. Par exemple : 2/1. Dans cet exemple, la licence contient 2 tokens de validation et 1 token d'investigation.

Les tokens ont une période de validité variable qui correspond à la période de validité de l'abonnement WithSecure™ Elements EDR (12, 24 ou 36 mois). Les tokens non utilisés expirent à la fin de cette période de validité.

Si la détection examinée date de plus de 7 jours, un token Threat Investigation est utilisé pour le service Elevate. Si la détection est de moins de 7 jours, elle est d'abord validée avec un token Threat Validation.

Pour plus d'informations sur la licence Elevate ou sur les services de réponse et de préparation proposés séparément, n'hésitez pas à contacter votre représentant local WithSecure™.

5 Services complémentaires

Si votre profil de risque indique une forte probabilité d'incident grave, nous vous recommandons de compléter le service Elevate to WithSecure™ avec deux autres services : Incident Response et Incident Readiness, vendus séparément.

5.1 Incident Response - Réponse aux incidents

Si la gravité du cas Elevate atteint le **seuil d'incident majeur**, les analystes de WithSecure™ recommandent une escalade vers un processus distinct et complet d'Incident Response, pour contenir la menace et la neutraliser. Incident Response n'est pas couvert par le service Elevate to WithSecure™.

Le **seuil d'incident majeur** est considéré comme atteint lorsque la situation répond à l'un des critères suivants :

- Elevate to WithSecure™ a passé plus de 2 heures sur l'incident sans résolution prévue dans l'heure qui suit
- Plus de cinq appareils ont été infectés dans l'environnement cible
- Un actif critique a été corrompu
- Un appareil corrompu identifié ne dispose pas de la couverture Elements EDR

Les services Incident Response sont assurés par l'équipe WithSecure™ Global Incident Response. Cette équipe fonctionne 24h/24, 7j/7. Elle est spécialisée dans les cyber-crises majeures et traite les incidents en direct pour certaines des plus grandes organisations mondiales (des entreprises du Dow Jones, du NASDAQ et du FTSE 100, ainsi que des agences et des ministères gouvernementaux).

Les services Incident Response font l'objet d'une documentation spécifique et sont vendus séparément. Dans certains cas, en raison de la classification des données, un contrôle gouvernemental peut également être requis, ainsi qu'un reporting continu auprès des régulateurs ou des clients.

WithSecure™ recommande à ses clients d'acquérir **WithSecure™ Incident Response Retainer** : ainsi, ils peuvent bénéficier d'accords de niveau de service (SLA), d'une couverture contractuelle pour une réponse immédiate, et de tarifs journaliers réduits pour la réponse aux incidents. Les clients ne disposant pas d'un contrat Retainer peuvent solliciter Incident Response en tant que client de passage. Les frais sont plus élevés pour les clients de passage et leurs dossiers sont traités en fonction des disponibilités. À l'inverse, les clients ayant signé un contrat bénéficient d'un support apporté dans les 72 heures.

5.2 Incident Readiness - Préparation aux incidents

En disposant d'une bonne préparation, il est possible de minimiser le recours à la réponse réactive, de rationaliser les coûts de réponse et d'améliorer la collaboration entre leurs différents services.

Nos activités de préparation vous permettent de déterminer votre capacité de réponse initiale et de la renforcer par le biais de playbooks, d'exercices de simulation, et via des formations permettant à vos équipes de mieux configurer vos outils.

Les services de préparation aux incidents permettent aux entreprises de :

- Renforcer leurs compétences de First Responder et de maîtriser les principaux scénarios de risques et d'incidents.
- Améliorer leurs systèmes de réponse et de continuité opérationnelle en créant des plans, des processus et des playbooks.
- Définir les processus de gestion des crises et des incidents majeurs.
- Communiquer et agir de manière coordonnée durant les phases de réponse, de gestion de crise et de reprise post-incident.
- S'améliorer en continu en intégrant une culture de préparation aux cyberincidents au sein de l'entreprise.

Qui sommes-nous ?

WithSecure™ est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités. Notre protection basée sur l'IA sécurise les endpoints et protège les environnements cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

W / T H®
secure