PRÉSENTATION

THREAT INTELLIGENCE

Flux de renseignements uniques et rapports sur les menaces émanant des meilleurs professionnels du secteur

Progress. Protected.

Perspective unique sur le paysage des menaces

OBTENEZ DES INFORMATIONS UNIQUES

ESET recueille des renseignements sur les menaces à partir d'un éventail unique de sources et possède une expérience inégalée sur le terrain, qui vous aide à lutter contre des attaques de plus en plus sophistiquées.

CONSERVEZ UNE LONGUEUR D'AVANCE SUR LES ATTAQUANTS

ESET est au cœur de l'action, surveillant spécifiquement les endroits où nous avons détecté des groupes de pirates qui ciblent les entreprises occidentales : la Russie, la Chine, la Corée du Nord, l'Iran. Vous serez le premier à être informé des nouvelles menaces.

PRENEZ RAPIDEMENT DES DÉCISIONS CRUCIALES

Anticipez les menaces et prenez plus rapidement de meilleures décisions grâce aux rapports ESET complets et aux fils d'actualité. Réduisez votre exposition aux menaces actuelles, signalées par les experts.

AMÉLIOREZ VOTRE POSTURE DE SÉCURITÉ

Grâce aux flux de renseignements ESET, améliorez vos moyens de recherche des menaces et de remédiation, bloquez les menaces persistantes avancées et les ransomwares, et renforcez votre architecture de cybersécurité.

AUTOMATISEZ LES ENQUÊTES SUR LES MENACES

La technologie ESET recherche constamment des menaces, dans plusieurs couches et depuis la phase d'avant le démarrage jusqu'aux périodes d'inactivité. Bénéficiez de la télémétrie sur tous les pays où ESET détecte des menaces émergentes.

L'avantage ESET

Expertise humaine s'appuyant sur le machine learning. LiveGrid®, notre système de données de réputation, se compose de 110 millions de capteurs dans le monde entier et est vérifié par nos centres de recherche.

EXPERTISE HUMAINE S'APPUYANT SUR LE MACHINE LEARNING

L'utilisation du machine learning pour automatiser les décisions et évaluer les menaces éventuelles est un élément essentiel de notre approche. Mais la force du système dépend des personnes qui le soutiennent. L'expertise humaine est primordiale pour fournir les informations les plus fiables possibles sur les menaces, car les auteurs de menaces sont des adversaires intelligents.

LIVEGRID®, LE SYSTÈME DE DONNÉES DE RÉPUTATION

Les produits ESET pour endpoints intègrent LiveGrid®, notre système de données de réputation dans le Cloud qui fournit des informations pertinentes sur les menaces les plus récentes et les fichiers inoffensifs. Il se compose de 110 millions de capteurs dans le monde entier, et les résultats sont vérifiés par nos centres de recherche. Les clients bénéficient ainsi du plus haut niveau de confiance lorsqu'ils consultent les informations et les rapports dans leur console.

ORIGINES EUROPÉENNES, PRÉSENCE MONDIALE

Basé dans l'Union européenne, ESET est présent dans le secteur de la sécurité depuis plus de 30 ans, avec 22 bureaux dans le monde, 13 centres de recherche, et une présence dans plus de 200 pays et territoires. Cela permet d'apporter à nos clients une perspective mondiale sur les tendances et les menaces les plus récentes.

Rapports sur les menaces persistantes avancées

NOS MEILLEURES ÉTUDES À VOTRE SERVICE

Notre équipe de recherche est bien connue dans le milieu de la cybersécurité grâce à notre blog primé We Live Security. Les excellentes études de l'équipe et les résumés des activités des groupes de pirates sont disponibles, avec des informations beaucoup plus détaillées. Les clients d'ESET bénéficient d'un aperçu exclusif sur la totalité du contenu de We Live Security.

UN CONTENU PERTINENT ET EXPLOITABLE

Les rapports fournissent un contexte enrichi sur ce qui se passe et pourquoi. Grâce à cela, les entreprises peuvent se préparer à l'avance à ce qui pourrait arriver. Nos experts veillent à ce que le contenu soit facile à comprendre.

PRENEZ RAPIDEMENT DES DÉCISIONS CRUCIALES

Tout cela aide les entreprises à prendre des décisions cruciales et leur procure un avantage stratégique dans la lutte contre la cybercriminalité. Elles peuvent comprendre ce qui se passe du « côté obscur d'Internet » et s'y préparer rapidement en interne.

ACCÈS À UN ANALYSTE ESET

Chaque client qui commande l'offre APT Reports Premium aura également accès à un analyste ESET pendant quatre heures par mois. C'est l'occasion de discuter de sujets plus en détail et d'essayer de résoudre les questions en suspens.

AVEC LES RAPPORTS SUR LES MENACES, VOUS OBTENEZ

- Un accès à des analyses techniques privées et approfondies
- Des rapports de synthèse sur les activités des groupes de pirates
- Un résumé mensuel pour vos cadres supérieurs
- Un accès direct à un professionnel de la cybersécurité ESET
- Un accès à notre serveur MISP

ANALYSES APPROFONDIES

L'offre comprend des rapports mensuels d'analyse technique approfondie décrivant les campagnes récentes, les nouveaux outils et les sujets associés. Vous recevrez également toutes les deux semaines un rapport récapitulatif des activités qui décrit les toutes dernières campagnes menées par différents groupes de pirates que les chercheurs d'ESET ont suivies, ainsi que leurs cibles et, bien sûr, les indicateurs de compromission (IoC) qui y sont associés. Les rapports de synthèse mensuels regroupent les informations de tous les rapports d'analyse technique et de synthèse d'activité publiés au cours du mois précédent sous une forme plus courte et plus digeste.

La disponibilité des rapports et des flux ESET Threat Intelligence varie selon les pays. Veuillez contacter votre représentant ESET local pour plus d'informations.

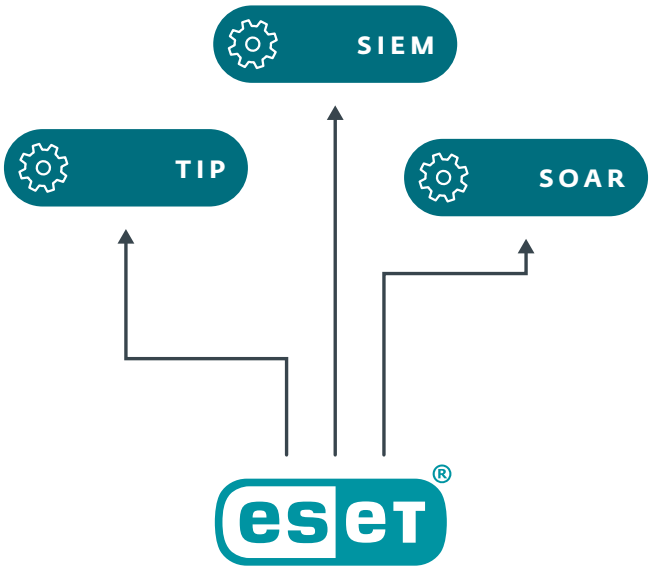
Intégrez ESET Threat Intelligence à votre système

L'intégration de la télémétrie ESET est simple et enrichira votre **TIP**, **SIEM** ou **SOAR**

Nous disposons d'une **API complète avec une documentation exhaustive**

Nous fournissons des données dans des **formats standardisés** tels que des flux JSON et STIX via TAXII, afin que l'intégration dans n'importe quel outil est possible

Pour IBM QRadar, Anomali, ThreatQuotient et Logpoint, nous disposons de **manuels d'intégration étape par étape** afin de faciliter et d'accélérer la mise en œuvre, et nous en ajoutons continuellement d'autres



Cycle de vie d'ESET Threat Intelligence

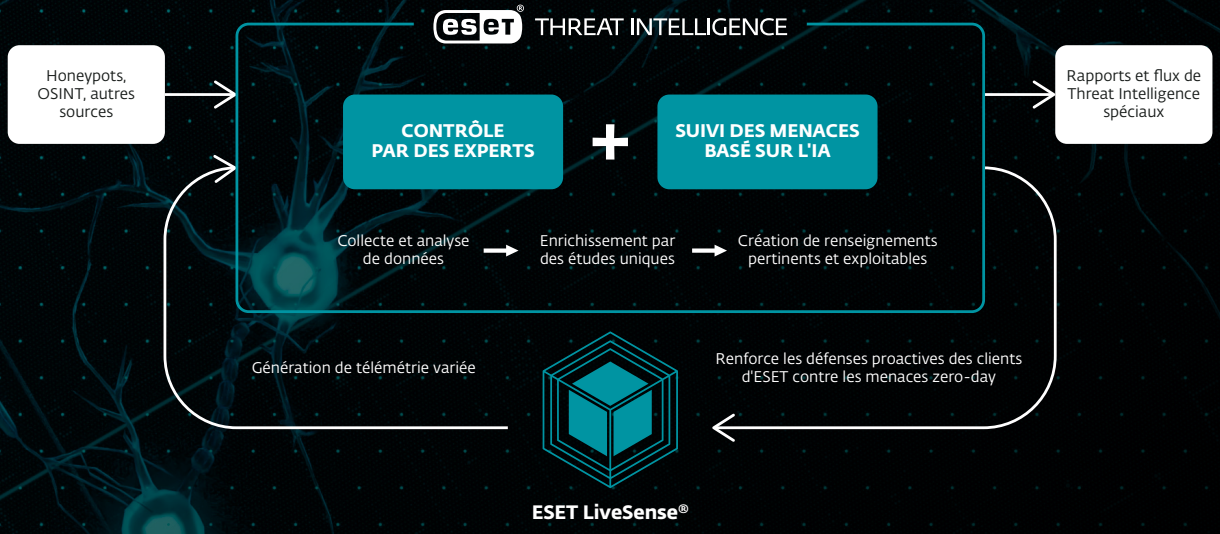
La création de nos renseignements est en fait un cycle d'auto-renforcement.

Il utilise la vaste gamme de télémétrie générée par ESET LiveSense, notre technologie de sécurité multi-couche intégrée à la plateforme ESET PROTECT.

La télémétrie recueillie est complétée par différentes sources supplémentaires, telles que les honeypots ou l'OSINT.

Elle est ensuite traitée par nos robustes systèmes de repérage et de traitement des malwares s'appuyant sur l'IA. Ces systèmes sont capables de découvrir des menaces et d'ajouter de nombreuses informations contextuelles pour enrichir les renseignements.

En tant qu'élément crucial, nos experts en Threat Intelligence supervisent le produit final et veillent à ce qu'il contienne toujours des données actualisées pour vous aider à prendre de meilleures décisions plus rapidement.



Flux d'informations propriétaires ESET

Enrichissez votre visibilité sur le paysage mondial des menaces, à partir d'une télémétrie unique. Les flux ESET sont émis par nos centres de recherche dans le monde entier, et fournissent une vision d'ensemble pour bloquer rapidement les indicateurs de compromission dans votre environnement. Ils sont aux formats JSON et STIX 2.1.

FLUX DE FICHIERS MALVEILLANTS

Ce flux fournit des informations en temps réel sur les échantillons de malwares récemment découverts, ainsi que sur leurs caractéristiques et leurs IOC. Il vous aide à comprendre quels fichiers malveillants sont découverts et vous permet de les bloquer de manière proactive avant qu'ils ne causent des dommages. Le flux contient des domaines malveillants, y compris des hachages de fichiers, des horodatages, le type de menace détecté et d'autres informations détaillées.

FLUX DE DOMAINES

Ce flux peut être utilisé pour bloquer les domaines considérés comme malveillants. Il comprend les noms de domaine, les adresses IP et les dates qui leur sont associées. Le flux classe les domaines en fonction de leur gravité, ce qui vous permet d'adapter votre réponse en conséquence, par exemple en ne bloquant que les domaines les plus risqués.

FLUX D'ADRESSES IP

Ce flux partage les adresses IP considérées comme malveillantes et les données qui leur sont associées. La structure des données est très similaire à celle utilisée pour les flux de domaines et d'URL. Le principal objectif est de comprendre quelles adresses IP malveillantes sont actuellement répandues, bloquer celles les plus dangereuses, repérer celles qui le sont moins, et approfondir les recherches.

FLUX D'URL

Tout comme le flux de domaines, le flux d'URL concerne des adresses spécifiques. Il comprend des informations détaillées sur les données relatives aux URL, ainsi que des informations sur les domaines qui les hébergent. Toutes les informations sont filtrées pour n'afficher que les résultats les plus fiables.

FLUX DE BOTNETS

S'appuyant sur le réseau exclusif de suivi des botnets d'ESET, le flux des botnets présente trois types de sous-flux : botnets, C&C et cibles. Les données fournies comprennent des éléments tels que la détection, le hachage, la date la dernière activité, les fichiers téléchargés, les adresses IP, les protocoles, les cibles et d'autres informations.

FLUX D'APT

Ce flux est constitué d'informations sur les menaces persistantes avancées produites par les recherches d'ESET. En général, le flux est un export du serveur MISP interne d'ESET. Toutes les données partagées sont également expliquées plus en détail dans les rapports sur les APT. Le flux d'APT fait également partie des rapports sur les APT, mais peut être acheté séparément.

Avec les flux ESET, vous obtenez

- ✓ DONNÉES PRÉCISÉMENT SÉLECTIONNÉES
- ✓ CONTEXTE EXPLOITABLE
- ✓ FAIBLE TAUX DE FAUX POSITIFS
- ✓ ACTUALISATIONS FRÉQUENTES
- ✓ API COMPLÈTE

La disponibilité des rapports et des flux d'ESET Threat Intelligence varie selon les pays. Veuillez contacter votre représentant ESET local pour plus d'informations.

À propos d'ESET

Cybersécurité de nouvelle génération pour les entreprises

NOUS NE NOUS CONTENTONS PAS DE STOPPER LES MENACES, NOUS LES ANTICIPONS

Contrairement aux solutions conventionnelles qui se concentrent sur la réaction aux menaces une fois qu'elles se sont déclenchées, ESET offre une approche inégalée axée sur la prévention via l'IA et soutenue par l'expertise humaine, la renommée mondiale de sa Threat Intelligence, et un vaste réseau de R&D dirigé par des chercheurs reconnus dans le secteur, tout cela au service de l'innovation continue de notre technologie de sécurité multicouche.

Bénéficiez d'une protection sans pareil contre les ransomwares, l'hameçonnage, les menaces zero-day et les attaques ciblées grâce à notre plateforme de cybersécurité XDR primée, qui combine des fonctionnalités nouvelle génération pour la prévention, la détection et la recherche proactive de menaces. Nos solutions hautement personnalisables incluent un support hyperlocal. Elles ont un impact minimal sur les performances des endpoints, et sont en mesure d'identifier et de neutraliser les menaces émergentes avant qu'elles ne se déclenchent, garantissent la continuité des activités et réduisent les coûts de mise en œuvre et d'administration.

Dans un monde où la technologie permet le progrès, protégez votre entreprise avec ESET.

ESET EN QUELQUES CHIFFRES

+ 1 Md
internautes protégés

+ 400 k
entreprises clientes

200
pays et territoires

13
centres de recherche

RECONNAISSANCE DU SECTEUR

ESET a reçu des éloges dans plus de 700 avis recueillis sur Gartner Peer Insights

ESET est récompensée pour sa contribution à la communauté avec le prix Tech Cares 2023 de TrustRadius

RECONNAISSANCE DES ANALYSTES

IDC ANALYZE THE FUTURE

En 2023, IDC a placé ESET dans le top 5 des fournisseurs de Threat Intelligence et a mis en évidence le profil d'ESET Threat Intelligence.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET a été reconnu parmi les « Top Player » pour la quatrième année consécutive dans le rapport Advanced Persistent Threat (APT) Protection Market Quadrant de Radicati en 2023.

MITRE ATT&CK™

ESET est l'un des principaux éditeurs indépendants de logiciels de cybersécurité et figure dans le top 10 des 354 contributeurs du framework MITRE ATT&CK.

CERTIFICATION DE SÉCURITÉ ISO

ESET est conforme à ISO/CEI 27001:2013, une norme de sécurité internationalement reconnue et applicable dans la mise en œuvre et la gestion de la sécurité de l'information. La certification est accordée par l'organisme de certification tiers accrédité SGS. Elle démontre la conformité totale d'ESET aux meilleures pratiques du secteur.

QUELQUES-UNS DE NOS CLIENTS

Protégés par ESET depuis 2017 : 9 000 endpoints

Protégé par ESET depuis 2016 : +4 000 boîtes mail

Protégés par ESET depuis 2016 : 32 000 endpoints

Partenaire de sécurité FAI depuis 2008 : 2 millions d'utilisateurs

QUELQUES-UNES DE NOS RÉCOMPENSES

★★★★★

« L'IMPLÉMENTATION S'EST DÉROULÉE TRÈS SIMPLEMENT. EN COLLABORATION AVEC LE PERSONNEL TECHNIQUE BIEN FORMÉ D'ESET, NOUS AVONS PU METTRE EN ŒUVRE NOTRE NOUVELLE SOLUTION DE SÉCURITÉ ESET EN QUELQUES HEURES. »

Responsable informatique, Diamantis Masoutis S.A., Grèce, plus de 6 000 postes

★★★★★

« NOUS AVONS ÉTÉ TRÈS IMPRESSIONNÉS PAR L'ASSISTANCE DONT NOUS AVONS BÉNÉFICIÉ. EN PLUS DE L'EXCELLENT PRODUIT, L'EXCELLENTE PRISE EN CHARGE A ÉTÉ CE QUI NOUS A VRAIMENT CONDUIT À MIGRER TOUS LES SYSTÈMES DE PRIMORIS VERS ESET. »

Joshua Collins, Directeur des opérations du centre de données, Primoris Services Corporation, USA, plus de 4 000 postes

Digital Security
Progress. Protected.