PRÉSENTATION

THREAT INTELLIGENCE

Rapports et flux de renseignements uniques sur les menaces émanant des meilleurs professionnels du secteur

Progress. Protected.

Pourquoi ajouter ESET à votre infrastructure de CTI

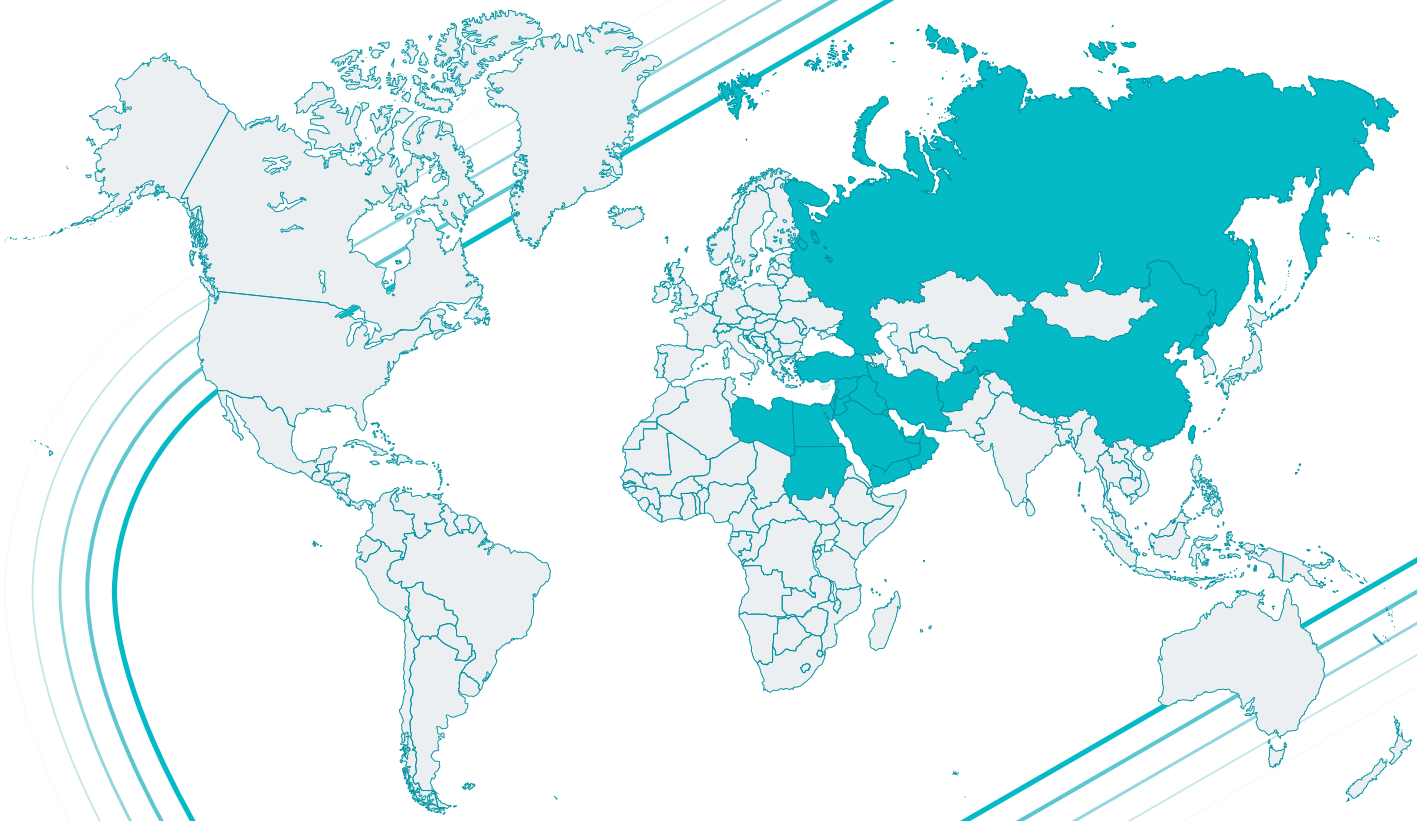
Comprendre le paysage actuel des menaces et les tactiques employées par les cybercriminels constitue un avantage crucial en termes de connaissances. Ces informations permettent aux organisations de **renforcer efficacement leurs systèmes de défense internes**. Des renseignements de haute qualité sont la pierre angulaire de toute stratégie solide de Cyber Threat Intelligence (CTI).

Depuis plus de 35 ans, ESET est une société privée, sans dettes et en constante croissance. Notre réussite repose sur une approche « Prevention First » s'appuyant sur l'IA doublée d'une expertise humaine. Un **système unique de Threat Intelligence mondiale au cœur de nos opérations s'appuie sur un vaste réseau de R&D** dirigé par des chercheurs reconnus dans le secteur. Nous prenons le temps de bien comprendre les cybermenaces, ce qui nous permet de défendre efficacement contre elles.

Quel que soit le degré d'avancement de vos solutions actuelles de CTI, l'intégration d'**ESET dans votre infrastructures vous apportera une valeur inégalée.** Nos flux complets de Threat Intelligence et nos rapports détaillés sur les auteurs de menaces vous permettent de conserver une longueur d'avance sur les menaces émergentes, et de renforcer vos défenses existantes grâce à des informations utiles et des études de pointe.

Tirez parti de la télémétrie unique d'ESET

La présence mondiale d'ESET, développée au fil des décennies, nous permet de disposer d'une **bibliothèque de renseignements riche et diversifiée** provenant de millions de nœuds. Contrairement à de nombreux concurrents, notre télémétrie est particulièrement forte dans les régions considérées comme **« plus intéressantes » d'un point de vue géopolitique** dans le monde de la cyberdéfense. Cette couverture unique se traduit directement par une intelligence de haut niveau. Grâce à la télémétrie d'ESET, vous **avez accès à des informations utiles de haute qualité** qui améliorent vos moyens de détection et de réponse aux menaces.

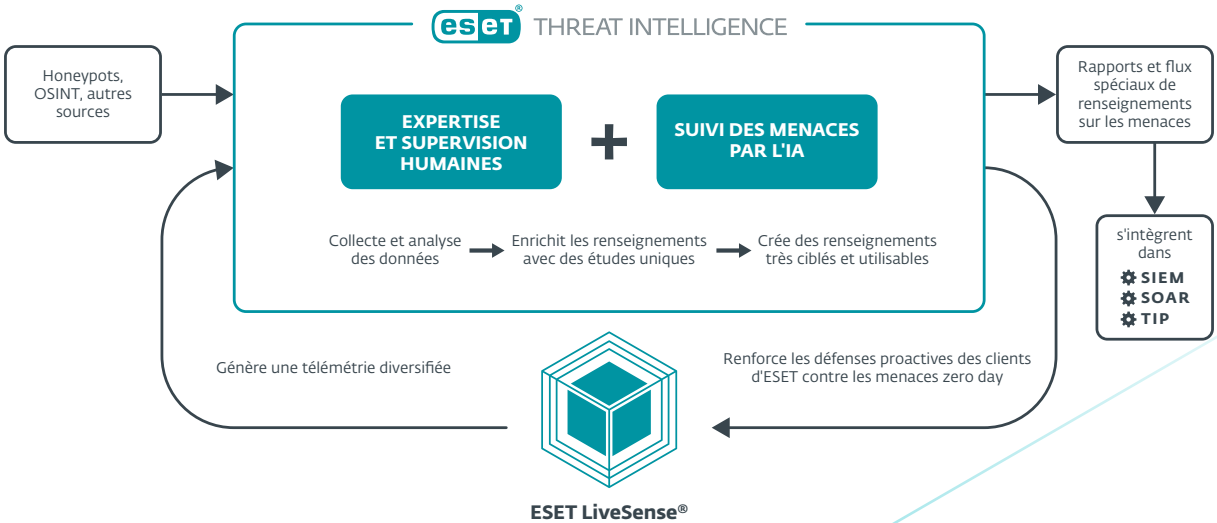


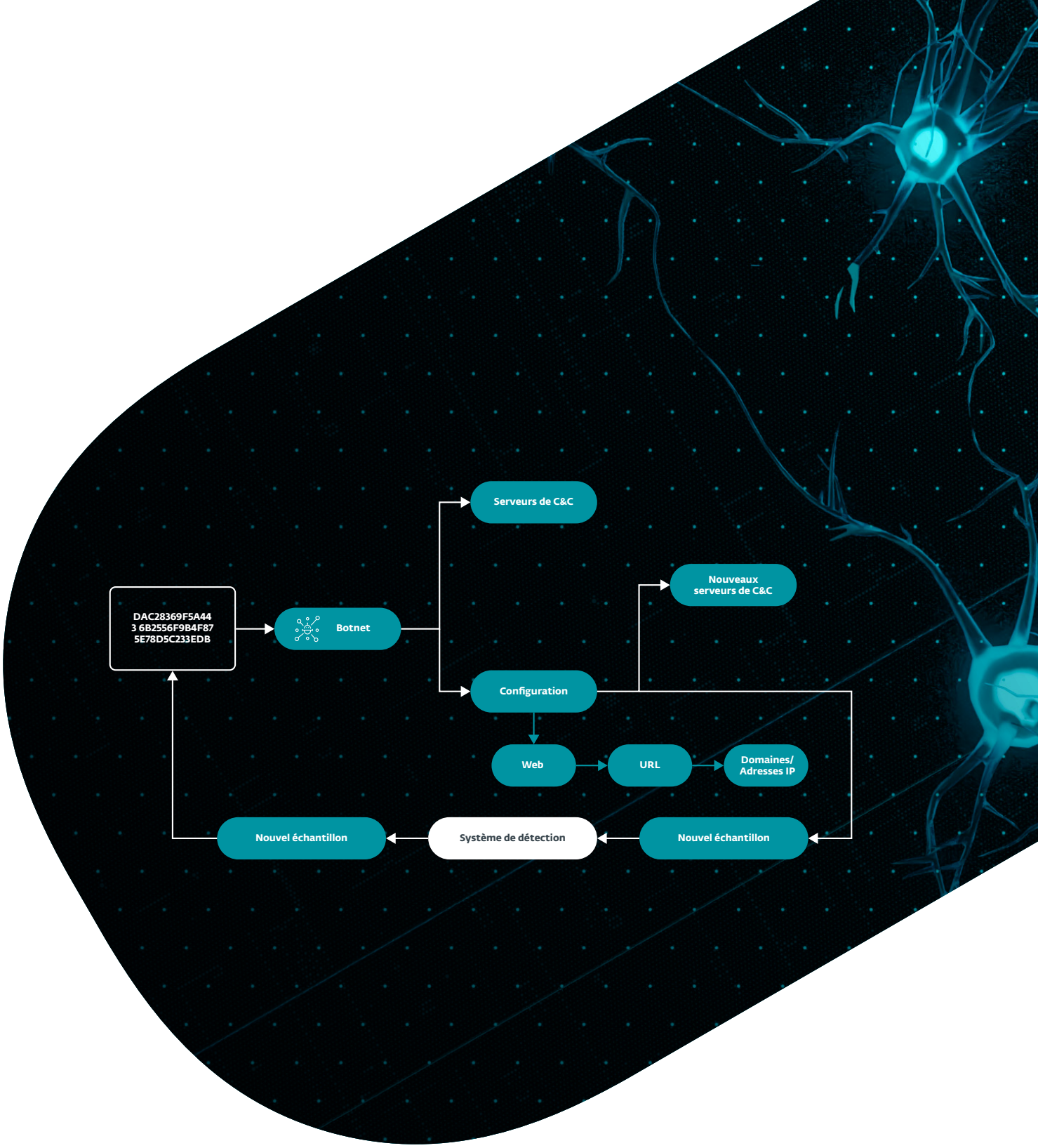
eset Digital Security
Progress. Protected.

Renseignements enrichis et connaissances utiles

La Threat Intelligence ne se limite pas à la collecte d'indicateurs et leur mise en forme ; ESET va bien au-delà. Nous utilisons des technologies de pointe et une expertise approfondie pour traiter et enrichir notre intelligence, afin de veiller à ce qu'elle apporte une valeur réelle à votre entreprise.

1. **Télémétrie complète :** Notre intelligence utilise une vaste gamme de télémétrie générée par ESET LiveSense, notre technologie de sécurité multicouche intégrée à la plateforme ESET PROTECT. Cela garantit une collecte étendue et approfondie de données provenant de diverses sources.
2. **Différentes méthodes de collecte :** Outre LiveSense, nous utilisons différentes méthodes de collecte et de surveillance, notamment des honeypots, des capteurs, des ressources OSINT, l'exploration du web (en clair et en profondeur) et le suivi des menaces. Il en résulte un volume important de données de haute qualité.
3. **Traitement avancé :** Une fois collectées, toutes les données sont traitées par de robustes systèmes en back-end, qui s'appuient sur l'IA pour classer et analyser les informations automatiquement. Seule l'intelligence la plus pertinente et les plus utiles est ainsi mise en évidence.
4. **Analyse d'experts :** Au-delà du traitement automatisé, notre équipe qualifiée d'analystes et de chercheurs spécialisés dans la Threat Intelligence joue un rôle crucial. Ils étudient et analysent en permanence les différents auteurs de menaces, leurs motivations, leurs TTP (tactiques, techniques et procédures) et leurs outils. Cette vérification humaine ajoute une couche supplémentaire de détails et de précision à notre intelligence, allant au-delà de ce que le machine learning et l'automatisation peuvent réaliser à eux seuls.





Les échantillons que nous recevons par télémétrie font l'objet d'une analyse comportementale et structurelle approfondie. Ce processus permet d'obtenir d'autres indicateurs utiles, ce qui enrichit encore notre veille sur les menaces. En examinant méticuleusement chaque échantillon, nous extrayons des informations précieuses qui améliorent la qualité et l'efficacité globales de notre intelligence, et vous permettent en retour de mieux comprendre le paysage des menaces.

Sécurité améliorée via des rapports APT détaillés

Rédigés dans un langage concis et utile pour améliorer la posture de sécurité de votre organisation, nos rapports sur les auteurs de menaces (APT) fournissent des informations détaillées sur les campagnes de malwares, leur diffusion et les acteurs impliqués. Accédez à notre serveur MISP et AI Advisor, et réservez des sessions en live avec les meilleurs experts d'ESET en Threat Intelligence pour obtenir des renseignements complets et utiles.

NOS MEILLEURES ÉTUDES À VOTRE SERVICE

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

UN CONTENU PERTINENT ET UTILE

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

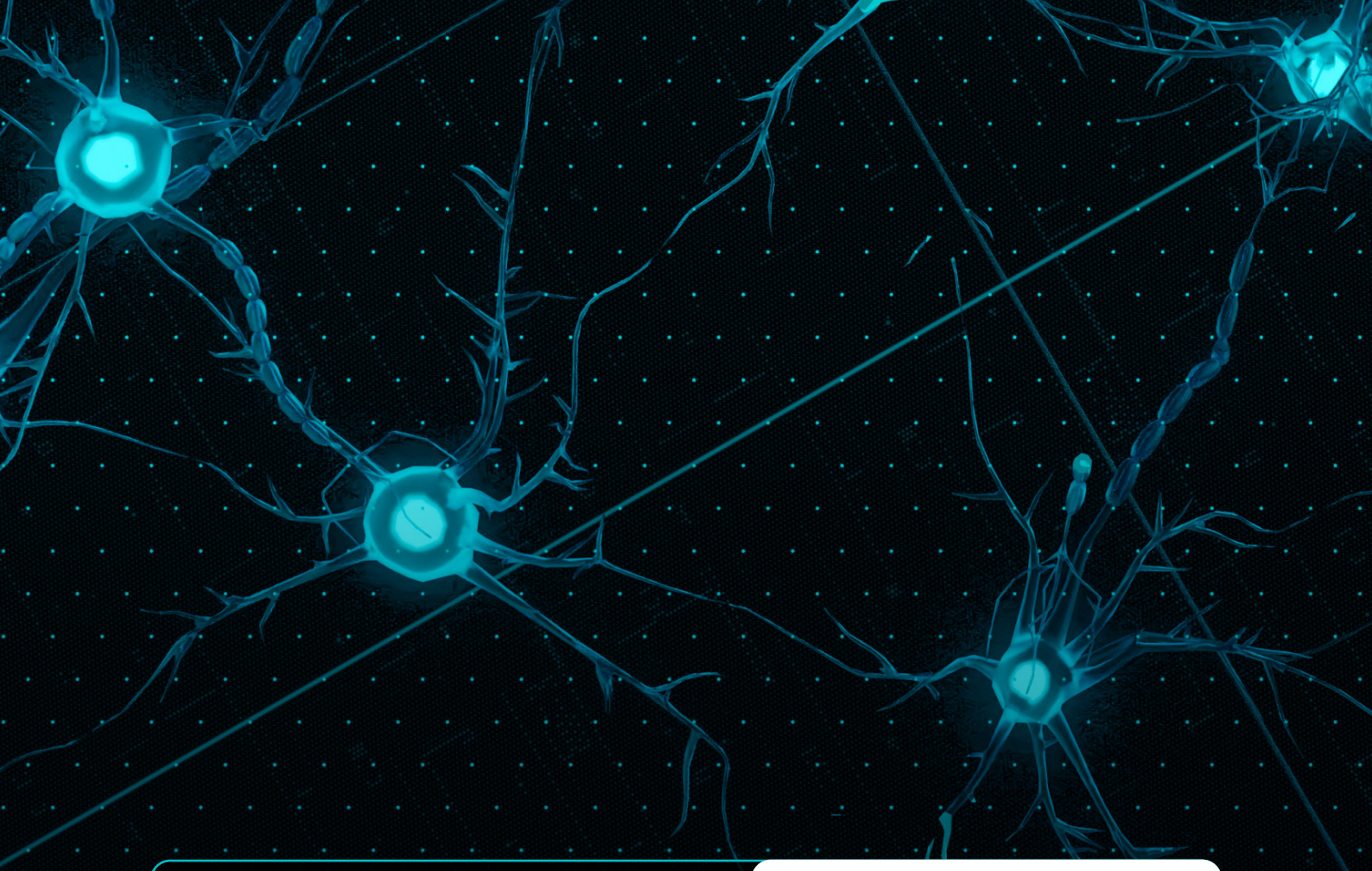
Tout cela aide les entreprises à prendre des décisions cruciales et leur procure un avantage stratégique dans la lutte contre la cybercriminalité. Elles peuvent comprendre ce qui se passe du « côté obscur d'Internet » et s'y préparer rapidement en interne.

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.

ESET AI ADVISOR

ESET AI Advisor utilise une IA avancée et notre expertise sur les auteurs de menaces pour fournir des informations à la demande et des mesures de protection contre les cyberattaques. Disponible sous la forme d'un chatbot, il répond aux questions de sécurité, propose des résumés sur les auteurs de menaces, compile des IoC (Indicateurs de Compromis) et des TTP, et génère des règles YARA pour une compréhension et une prévention rapides des menaces.



		APT Reports	APT Reports Advanced	APT Reports Ultimate
Résumé d'activité bimensuel	Rapports résumant les activités de tous les groupes de pirates étudiés, tel que détaillé ci-dessus (deux rapports par mois)	✓	✓	✓
Rapports d'analyse des menaces	Analyse technique personnalisée ou régulière des menaces les plus courantes (~30 par an)	✓	✓	✓
Aperçu mensuel	Compilation mensuelle des informations avec une vue d'ensemble des menaces	✓	✓	✓
Résumé mensuel	Index et résumé exécutif des rapports et des événements du mois	✓	✓	✓
Accès en avant-première à WeLiveSecurity	Accès en avant-première aux rapports sur les menaces et à une sélection d'articles WeLiveSecurity	✓	✓	✓
Flux des IoC des auteurs de menaces	Accès complet au flux STIX/TAXII contenant les IoC des rapports	✓	✓	✓
Accès au serveur MISP	Accès complet au serveur ESET MISP contenant toutes les informations disponibles dans les rapports	✗	✓	✓
ESET AI Advisor	Accès à ESET AI Advisor qui fournit des informations et des résumés des rapports disponibles sur les auteurs de menaces	✗	✓	✓
Accès aux analystes	Accès aux analystes via différentes plateformes telles que Teams et la messagerie, limité à quatre heures par mois (non cumulables, y compris le temps de préparation)	✗	✗	✓

Flux de données clairs et concis

Améliorez votre visibilité sur le paysage des menaces grâce à la télémétrie unique d'ESET. Nous fournissons des flux de données hautement structurés en JSON et STIX 2.1, qui s'intègrent de manière transparente dans les outils SIEM, TIP ou SOAR. Contrairement à de nombreux fournisseurs de Threat Intelligence, nous accordons une attention toute particulière afin que **nos flux soient méticuleusement filtrés et évalués** pour garantir leur pertinence. Cela permet aux systèmes de sécurité existants d'agir automatiquement en cas de besoin, et aux analystes de bénéficier d'une vue d'ensemble sur le paysage mondial des menaces.

- Des données riches en métadonnées, détaillées et préparées avec très peu de faux positifs
- Nous veillons à ce que les données soient peu volumineuses, très pertinentes et dédupliquées, avec un score de confiance
- Le résultat du filtrage avancé, avec les observations des chercheurs d'ESET
- Leader du marché, en particulier pour les données relatives aux botnets
- Faibles exigences en matière d'utilisation grâce à un contenu bien structuré
- Flux en temps réel ; uniquement des IoC récents et prévalents

FLUX DE DONNÉES MALVEILLANTES

Obtenez de précieuses connaissances grâce à ce flux en temps réel, qui fournit des informations sur les échantillons de malwares récemment découverts, leurs caractéristiques et leurs IoC. En tirant parti de ces données, vous pouvez bloquer de manière proactive les fichiers malveillants avant qu'ils ne causent des dommages. Le flux comprend des détails tels que les hachages de fichiers, les horodatages et les types de menaces identifiés.

FLUX DE RANSOMWARES

Luttez contre les ransomwares grâce à des données en temps réel sur les échantillons les plus répandus. Notre flux fournit des informations sur les familles de ransomware actives pour un blocage proactif. Gardez une longueur d'avance sur les menaces et protégez votre organisation contre les atteintes à la sécurité des données et les perturbations coûteuses.

FLUX DE BOTNETS

Tirez parti des informations fournies par le réseau propriétaire d'ESET de recherche de botnets grâce au flux de botnets. Il comprend trois sous-flux : botnets, serveurs de commande et de contrôle, et cibles. Le flux fournit des données essentielles, notamment les détails de la détection, les hachages de fichiers, les horodatages de la dernière communication, les fichiers téléchargés, les adresses IP, les protocoles et des informations ciblées.

IOC DES AUTEURS DE MENACES

Bénéficiez d'informations précieuses provenant du flux propriétaire d'ESET sur les auteurs de menaces, qui fournit des informations sur les menaces persistantes avancées (APT) basées sur les recherches d'ESET. Ce flux est exporté depuis le serveur interne MISP d'ESET et comprend des données qui sont détaillées dans les rapports sur les auteurs de menaces. Bien qu'il fasse partie de l'offre de APT Reports, le flux peut également être acheté séparément.

FLUX DE DOMAINES

Bloquez les domaines considérés comme malveillants, à partir du nom, de l'adresse IP et de la date qui leurs sont associés. 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'URL

Tirez parti du flux d'URL soigneusement élaboré, qui se concentre sur des adresses spécifiques. Il fournit des informations détaillées sur chaque URL et comprend des données sur les domaines qui les hébergent. Les résultats du flux sont classés de manière à ne présenter que les résultats les plus fiables, accompagnés d'explications compréhensibles pour les URL signalés.

FLUX D'ADRESSES IP

Recevez des données utiles à partir de ce flux, qui fournit des informations sur les adresses IP malveillantes. La structure des données ressemble beaucoup à celle des flux de domaines et d'URL. Il permet d'identifier les adresses IP malveillantes les plus courantes, de bloquer de manière proactive les adresses IP les plus graves, de détecter les adresses IP moins graves, et d'approfondir le travail d'enquête sur la base de données supplémentaires afin d'évaluer les dommages potentiels.

FLUX DE MENACES SUR ANDROID

Ce flux fournit des informations en temps réel sur les menaces Android les plus courantes et leurs IoC pour un blocage proactif. Créé à partir de la télémétrie d'ESET, il est mis à jour en temps quasi réel avec une déduplication quotidienne.

FLUX D'INFOSTEALERS

Sous-ensemble ciblé des menaces Android, le flux de voleurs d'informations sur Android fournit des détails spécifiques sur les échantillons de voleurs d'informations sur Android actuels et répandus, avec des données associées. Grâce à ces informations, vous obtenez des connaissances sur les familles de voleurs d'informations actives. Plus important encore, vous pouvez les bloquer de manière proactive avant qu'elles ne causent des dommages.

FLUX DES URL D'ESCROQUERIES

Restez à l'affût des escroqueries grâce à des données en temps réel sur les URL frauduleuses. Notre flux couvre les boutiques en ligne, les escroqueries à l'investissement, les escroqueries aux rencontres et les escroqueries aux cryptomonnaies. Créé à partir de toutes les sources ESET d'URL en temps quasi réel, avec déduplication toutes les 24 heures.

FLUX DES ESCROQUERIES AUX CRYPTOMONNAIES

Gardez une longueur d'avance sur les escroqueries aux cryptomonnaies grâce à des informations en temps réel sur les domaines, les URL et des données associées. Notre flux provenant de la télémétrie étendue d'ESET fournit des informations précoces et ciblées pour vous aider à bloquer les menaces de manière proactive et protéger vos ressources.

FLUX DES PIÈCES JOINTES MALVEILLANTES DANS LES EMAILS

La messagerie est une cible privilégiée pour les attaques. Notre flux fournit des données en temps réel sur les pièces jointes malveillantes provenant de la télémétrie ESET d'analyse des emails. Gardez une longueur d'avance sur les menaces grâce à des informations actualisées et exploitables qui protègent votre organisation.

FLUX DES URL D'HAMEÇONNAGE

Restez protégé grâce à des données en temps réel sur les URL d'hameçonnage les plus courantes. Notre flux, qui provient de la base de données ESET d'URL d'hameçonnage, est mis à jour en quasi temps réel avec une déduplication quotidienne. Empêchez les atteintes à la sécurité des données en identifiant et en bloquant les sites trompeurs avant qu'ils ne causent des dommages.

FLUX DE SMISHING

Restez protégé grâce à des données en temps réel sur les domaines d'hameçonnage par SMS (smishing), comprenant les URL et des données associées. Notre flux provenant de la télémétrie étendue d'ESET est mis à jour en quasi temps réel avec une déduplication quotidienne.

FLUX DES ESCROQUERIES PAR SMS

Protégez-vous contre les escroqueries par SMS grâce à notre flux en temps réel sur les domaines et les URL malveillants. Mis à jour en quasi temps réel à partir de la télémétrie étendue d'ESET et dédupliqué quotidiennement, ce flux vous aide à identifier et bloquer les menaces sophistiquées.

Découvrez la puissance d'ESET Threat Intelligence

Demandez une démonstration dès aujourd'hui et découvrez la valeur unique qu'ESET Threat Intelligence peut apporter à votre organisation. Avec un taux de renouvellement de 100 %, nos clients satisfaits témoignent de l'efficacité de nos solutions. Laissez-nous vous montrer comment nous pouvons améliorer vos défenses de cybersécurité.

Vous souhaitez voir par vous-même avant de demander une démo ?

Commencez par créer un compte de prévisualisation dans le portail ESET Threat Intelligence pour accéder aux flux et aux rapports sur les auteurs de menaces.

ESET Digital Security
Progress. Protected.

Voici ESET

Défense proactive. Minimisez les risques par la prévention.

Conservez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre approche axée sur l'IA et la prévention. Nous combinons la puissance de l'IA et l'expertise humaine pour améliorer l'efficacité et la facilité d'utilisation de la protection.

Bénéficiez d'une protection de haut niveau grâce à notre Threat Intelligence interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par des chercheurs reconnus.

ESET PROTECT, notre plateforme de cybersécurité XDR, combine des fonctionnalités de nouvelle génération de prévention, de détection et de recherche proactive de menaces, avec une gamme étendue de services de sécurité, notamment de détection et de réponse managés.

Nos solutions hautement personnalisables comprennent une assistance locale et ont un impact minimal sur les performances. Elles identifient et neutralisent les menaces connues et émergentes avant qu'elles ne puissent se déclencher. Elles favorisent la continuité des activités, et réduisent les coûts de mise en œuvre et d'administration.

ESET protège votre entreprise afin que vous puissiez maximiser le potentiel de la technologie.

ESET EN QUELQUES CHIFFRES

+ 1 Mrd
internautes protégés

+ 500 k
entreprises clientes

176
pays et territoires

11
centres de recherche

QUELQUES-UNS DE NOS CLIENTS

MITSUBISHI MOTORS
Drive your Ambition

Protégé par ESET depuis 2017 : 9 000 endpoints

Allianz Suisse

Protégé par ESET depuis 2016 : +4 000 boîtes mail

Canon
Canon Marketing Japan Group

Protégé par ESET depuis 2016 : 32 000 endpoints

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

RECONNAISSANCES

AV comparatives APPROVED Business Security JUL 2024

ESET est constamment **parmi les éditeurs les plus performants des tests indépendants** d'AV-Comparatives, et atteint les meilleurs taux de détection avec peu voire aucuns faux positifs.

G2 Leader WINTER 2025

ESET obtient régulièrement les meilleures notes sur la plateforme mondiale d'évaluation des utilisateurs G2, et ses solutions sont **appréciées par les clients du monde entier**.

IDC ANALYZE THE FUTURE

ESET a été reconnu comme un leader dans le domaine de la sécurité des endpoints dans l'évaluation des fournisseurs IDC MarketScape: Worldwide Modern Endpoint Security for Midsize Businesses 2024.