FICHE PRODUIT

THREAT INTELLIGENCE

Étendez votre visibilité sur la sécurité,
de votre réseau local au cyberespace mondial

DES EXPERTS EN CYBERSÉCURITÉ
À VOS CÔTÉS

qu'est-ce qu'une **solution de Threat Intelligence ?**

Le service Threat Intelligence d'ESET vous offre des informations sur les attaques ciblées, sur les menaces persistantes avancées (APT), sur les attaques zero-day et sur les activités botnet à l'échelle mondiale.

Les ingénieurs peinent souvent à mettre en lumière ces éléments, car ils peuvent uniquement accéder aux informations du réseau local de leur entreprise.

Pourquoi choisir le **Threat Intelligence?**

Le service Threat Intelligence permet de trier des volumes considérables d'informations, puis de transmettre les données les plus pertinentes pour chaque organisation.

SURCHARGE D'INFORMATIONS

Les attaques zero-day, les menaces persistantes avancées, les attaques ciblées et les botnets concernent tous les secteurs, dans tous les pays. Malheureusement, face au nombre considérable de menaces différentes, les organisations peinent à identifier les mesures de protection et d'atténuation proactives les plus importantes. Résultat : elles s'efforcent de mettre en lumière des informations utiles à partir d'ensembles de données limités, notamment au sein de leurs réseaux locaux, ou en utilisant des ensembles de données volumineux fournis par des sources externes. Le service Threat Intelligence permet de trier des volumes considérables d'informations, puis de transmettre les données les plus pertinentes pour chaque organisation.

Avec Threat Intelligence, les entreprises peuvent prioriser les menaces émergentes rapidement et facilement, ce qui leur laisse plus de temps pour mettre en place de nouvelles défenses proactives adéquates.

PROACTIVITÉ VS RÉACTIVITÉ

Avec l'apparition de nouvelles méthodes d'attaque et de menaces inédites, le monde de la cybersécurité ne cesse d'évoluer. En cas d'attaque ou de faille de données, les entreprises sont souvent surprises par la défaillance de leurs défenses, ou ignorent totalement qu'une attaque a eu lieu. Quand elles finissent par la découvrir, elles se hâtent de mettre en place des solutions d'atténuation pour éviter de futures attaques identiques. Mais cette approche ne les protège pas des menaces reposant sur d'autres types de vecteurs d'attaque.

Le service Threat Intelligence offre des informations sur les risques à venir et les menaces inconnues pour permettre aux organisations de renforcer leurs défenses et d'adopter une approche de cybersécurité proactive.

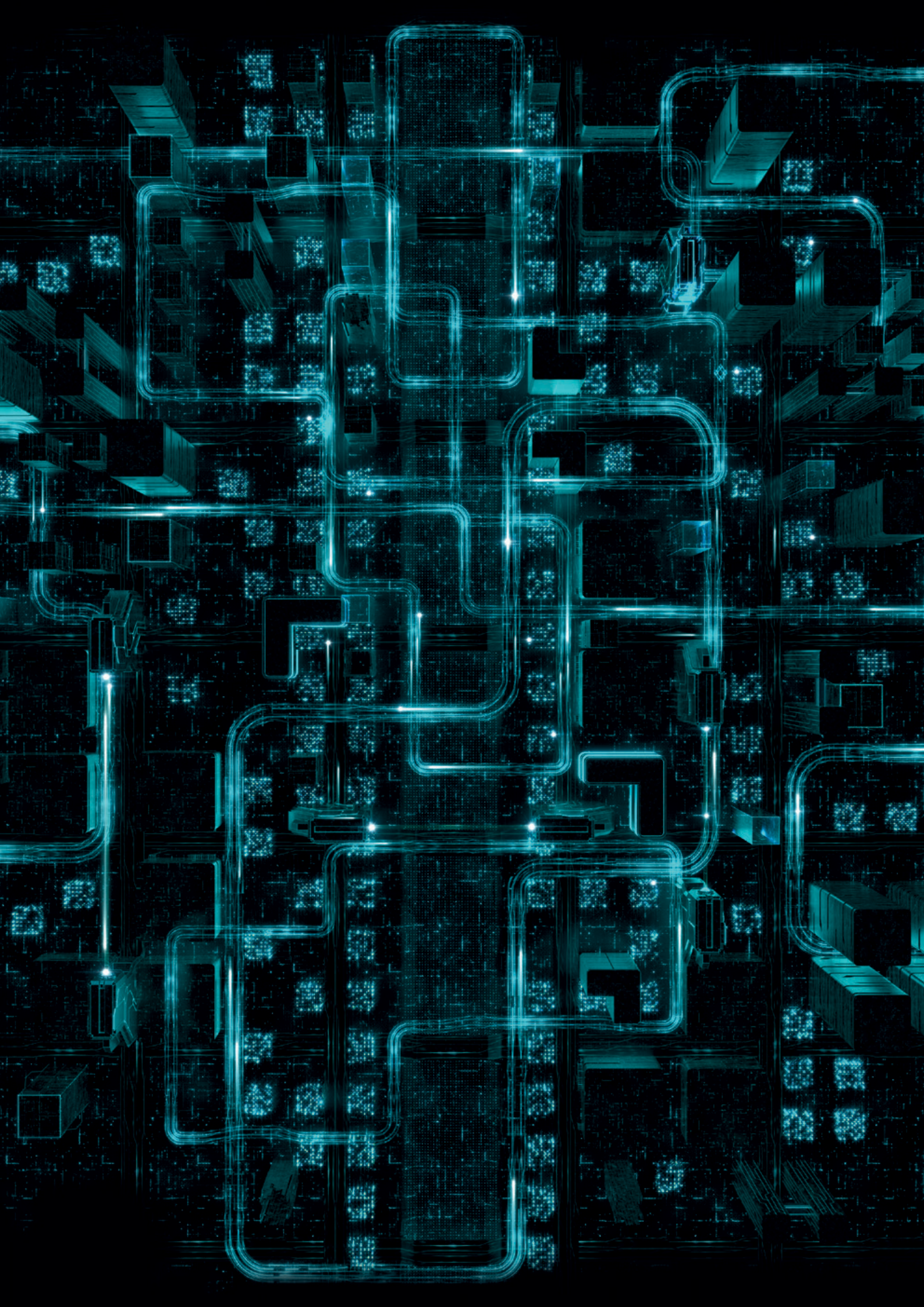
ASSISTANCE INTERVENTION EN CAS D'INCIDENT

En cas de faille de données, les équipes de sécurité doivent généralement trouver la cause de l'incident ainsi que les appareils affectés. Pour cela, elles procèdent souvent manuellement, en cherchant les anomalies signalant des défaillances dans le réseau de leur entreprise.

Avec Threat Intelligence, ces équipes d'intervention peuvent comprendre parfaitement la cause des failles et y réagir rapidement. Grâce aux informations sur la nature des menaces, sur le comportement des malwares, sur les vecteurs d'attaque et sur les indicateurs de défaillance, les équipes de sécurité peuvent accélérer le délai d'intervention en ayant une vue complète sur l'attaque et en connaissant les éléments à rechercher.

En cas d'attaque ou de faille de données, les entreprises sont souvent surprises par la défaillance de leurs défenses, ou ignorent totalement qu'une attaque a eu lieu.

Grâce aux informations sur la nature des menaces, sur les vecteurs d'attaque et sur les indicateurs de défaillance, les équipes de sécurité peuvent accélérer le délai d'intervention en ayant une vue complète sur l'attaque et en connaissant les éléments à rechercher.



Les avantages ESET

EXPERTISE HUMAINE ÉTAYÉE PAR LE MACHINE LEARNING

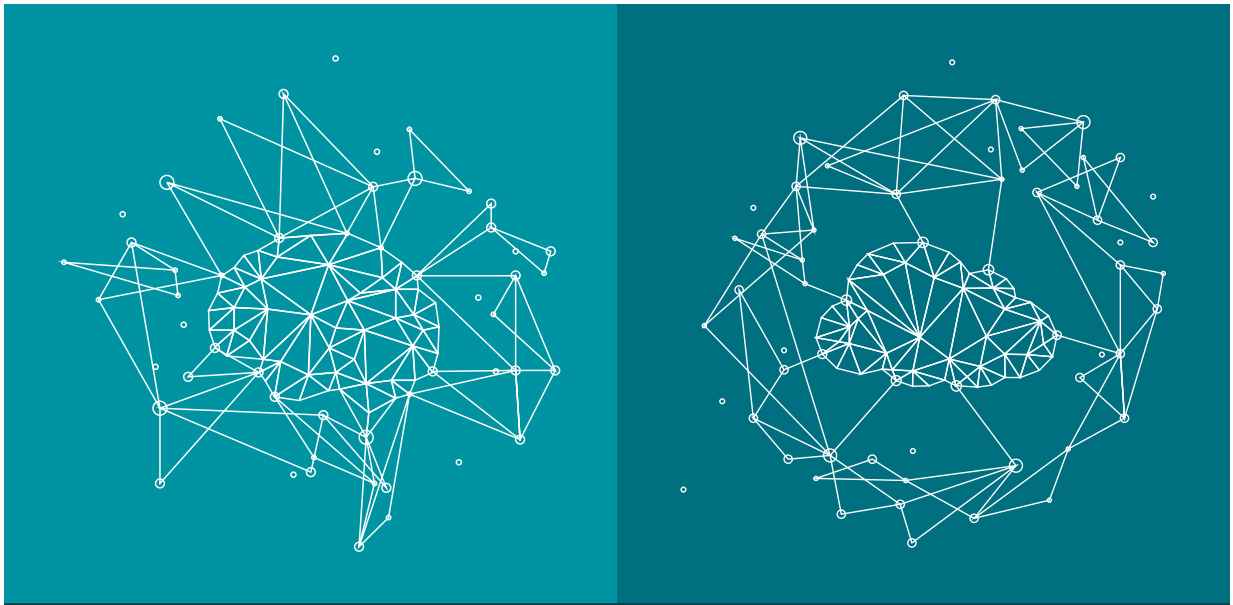
Notre approche s'appuie fortement sur l'utilisation du machine learning pour automatiser les décisions et évaluer les menaces potentielles. Mais la technologie seule ne suffit pas : elle doit être gérée par des équipes de spécialistes. L'expertise humaine est essentielle à la précision des informations sur les menaces, étant donné que leurs auteurs sont des personnes réelles.

SYSTÈME DE RÉPUTATION

Les produits ESET Endpoint incluent un système de réputation Cloud offrant des informations pertinentes sur les menaces les plus récentes et sur les types de fichiers inoffensifs. Baptisé LiveGrid®, notre système de réputation vérifié par nos centres R&D repose sur 110 millions de capteurs à l'échelle mondiale. Depuis son tableau de bord, les clients peuvent consulter des informations et des rapports d'une fiabilité à toute épreuve.

PRÉSENCE MONDIALE

Acteur du secteur de la sécurité depuis plus de 30 ans, ESET compte 22 bureaux à l'échelle mondiale et 13 centres R&D. La société est également présente dans plus de 200 pays et régions. Cela nous permet d'offrir à nos clients une perspective mondiale sur les dernières tendances et menaces.



Expertise humaine étayée par le machine learning. LiveGrid®, notre système de réputation vérifié par nos centres R&D, repose sur 110 millions de capteurs à l'échelle mondiale.

Cas d'utilisation

Prévention proactive des menaces

Les entreprises veulent éviter les communications entrantes et sortantes des infiltrations dans leur réseau.

SOLUTION

- ✓ Threat Intelligence envoie des alertes proactives aux équipes de sécurité concernant les attaques ciblées et les serveurs de commande et contrôle (C&C) récemment identifiés à l'échelle mondiale.
- ✓ Threat Intelligence offre également des flux de données pouvant être intégrés aux outils SIEM ou aux appareils UTM pour bloquer les connexions entrantes ou sortantes des éléments malveillants, ce qui permet d'éviter les fuites de données ou les incidents.
- ✓ Les entreprises peuvent définir des règles et des mesures d'atténuation pour éviter l'apparition des ransomware dans leur organisation.

SOLUTIONS ESET COMPLÉMENTAIRES RECOMMANDÉES

- ✓ **ESET Endpoint Security**
- ✓ **ESET Enterprise Inspector**

Améliorer la réaction aux incidents et le processus d'enquête

En cas d'infection, les entreprises doivent identifier et éliminer toutes les sources de l'attaque à l'échelle de leur réseau.

SOLUTION

- ✓ ESET Threat Intelligence offre des informations sur le fonctionnement des menaces, ce qui permet de réduire le temps passé à collecter des données et à enquêter en transmettant directement la menace à la solution pour analyse.
- ✓ Vous pouvez ainsi rechercher et éliminer les infections à l'échelle de votre organisation à l'aide des données fournies par le service Threat Intelligence.

SOLUTIONS ESET COMPLÉMENTAIRES RECOMMANDÉES

- ✓ **ESET Endpoint Security**
- ✓ **ESET Enterprise Inspector**

" Comme on le dit à l'hôpital, mieux vaut prévenir que guérir. "

— Jos Savelkoul, team leader du service TIC, hôpital Zuyderland, Pays-Bas. +10 000 employés

Atténuation des menaces

La plupart des entreprises se contentent d'éliminer les menaces sans mettre en place de mesures d'atténuation pour éviter l'apparition de nouvelles infections dans leurs systèmes.

SOLUTION

- ✓ Après une infection par malware, les entreprises peuvent envoyer un fichier au système d'analyse d'échantillons automatisée développé par ESET.
- ✓ Cette solution produit des données fiables sur le comportement du malware que les entreprises peuvent utiliser pour mettre en place des mesures d'atténuation ciblant les vecteurs d'attaque utilisés par le malware en question.

SOLUTIONS ESET COMPLÉMENTAIRES RECOMMANDÉES

- ✓ **ESET Endpoint Security**
- ✓ **ESET Mail Security**
- ✓ **ESET Enterprise Inspector**
- ✓ **ESET Dynamic Threat Defense**

" Les solutions de sécurité d'ESET protègent nos systèmes et envoient des alertes au service IT de Primoris en cas de menaces et infections sérieuses comme les ransomware. "

— Joshua Collins, Responsable des opérations des centres de données, Primoris Services Corporation, États-Unis. +4 000 employés

Fonctionnalités techniques ESET Threat Intelligence

FLUX DE DONNÉES EN TEMPS RÉEL

Les flux de données d'ESET Threat Intelligence utilisent le format STIX/TAXII compatible avec de nombreux systèmes, ce qui facilite leur intégration aux outils SIEM existants. Cela permet de renforcer la prestation de services et de transmettre des informations à jour sur les menaces actuelles, afin d'anticiper et d'éviter l'apparition des menaces sur le réseau. ESET propose actuellement trois types de flux : botnet, fichiers malveillants et flux de domaine. Tous ces flux contenant de nouvelles métadonnées sont actualisés toutes les 5 minutes.

RAPPORTS PRÉVENTIFS SUR LES MENACES

Basés sur les règles YARA permettant d'identifier des programmes, activités ou configurations similaires, les rapports analysent les menaces en cours de préparation ou actives dans les systèmes de certaines organisations ou certains clients.

API ROBUSTE

ESET Threat Intelligence inclut une API complète et compatible avec l'automatisation des rapports, les règles YARA et bien plus encore, pour assurer l'intégration aux autres systèmes des organisations.

ENVOI D'ÉCHANTILLONS ANDROID

ESET Threat Intelligence permet de surveiller les malware ciblant les applications mobiles des entreprises. Il s'agit d'une fonctionnalité particulièrement importante pour les banques et les acteurs disposant de leurs propres applications mobiles. À tout moment, les entreprises peuvent envoyer leur application Android à ESET Threat Intelligence pour effectuer une analyse complète du fichier .apk.

RÈGLES YARA

Les règles YARA permettent aux ingénieurs de sécurité de définir des règles personnalisées pour obtenir des informations spécifiques à leur entreprise. Une fois ces règles définies, les organisations bénéficient d'informations utiles, comme par exemple le nombre d'occurrences à l'échelle mondiale, les URL contenant du code malveillant, le comportement des malware dans les systèmes, l'origine de la détection, et bien plus encore.

ANALYSE D'ÉCHANTILLONS AUTOMATISÉE

Crée un rapport personnalisé concernant le fichier ou hash transmis avec des informations utiles qui améliorent la prise de décision et les enquêtes en cas d'incident.

Tableau de bord ESET Threat Intelligence

Rapports préventifs sur les menaces et flux

Rapports

RAPPORT CIBLÉ SUR LES MALWARES

Informe l'utilisateur des attaques potentielles en cours de préparation ou actives ciblant son organisation. Ce rapport inclut des extraits de règles YARA, des informations sur la réputation, des binaires similaires, des informations sur les fichiers, des sorties sandbox, etc.

RAPPORTS D'ACTIVITÉ BOTNET

Offre des données régulières et quantitatives sur les familles de malware identifiées et sur les variantes de botnet malveillant. Le rapport offre des informations décisionnelles sur les serveurs de commande et contrôle (C&C) utilisés pour gérer les botnet, des échantillons de botnet, des statistiques hebdomadaires mondiales et une liste des organisations ciblées par le malware.

RAPPORT SUR LES CERTIFICATS SSL FALSIFIÉS

Ce rapport est généré lorsqu'ESET détecte un nouveau certificat SSL généré par un organisme de certificats présentant des similarités avec le certificat fourni par le client au cours du déploiement initial. Le rapport peut par exemple mentionner les campagnes d'hameçonnage basées sur l'utilisation de ce certificat. Il liste également les caractéristiques clés du certificat, les correspondances YARA et les données du certificat.

RAPPORT CIBLÉ SUR L'HAMEÇONNAGE

Ce rapport présente des données sur l'ensemble des activités d'e-mailing ciblant l'organisation. Il inclut des informations sur les campagnes d'hameçonnage comme l'ampleur de la campagne, le nombre de clients, des captures d'écran des URL, des aperçus des e-mails d'hameçonnage, l'emplacement des serveurs, et bien plus encore.

Flux

FLUX BOTNET

Inclut trois types de flux permettant de vérifier plus de 1 000 cibles par jour, avec des informations sur le botnet lui-même, les serveurs impliqués et les cibles des attaques. Les flux fournissent des données directes, notamment concernant la détection, le hash, la date de la dernière activité du serveur, les fichiers téléchargés, les adresses IP, les cibles, et bien plus encore.

FLUX DE DOMAINE

Inclut les domaines considérés comme malveillants, avec notamment le nom du domaine, l'adresse IP, la détection des fichiers téléchargés via l'URL et la détection des fichiers ayant essayé d'accéder à l'URL.

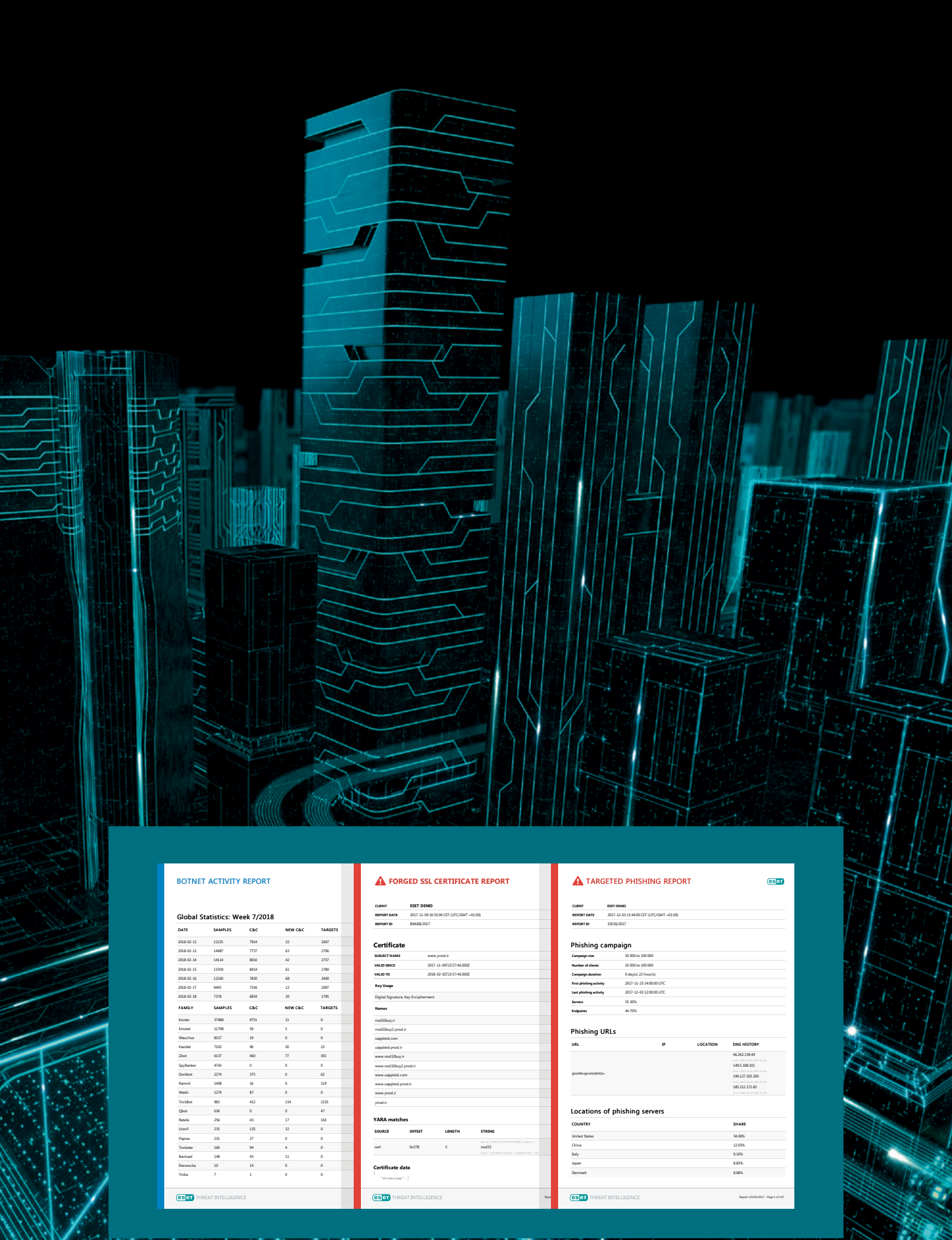
FLUX DE FICHIERS MALVEILLANTS

Inclut les exécutables considérés comme malveillants et reconnaît et partage les informations sur les formats SHA1, MD5 et SHA256, ou encore sur la détection, la taille et le format des fichiers.

FLUX PERSONNALISÉS

ESET peut fournir de nouveaux flux basés sur les exigences des entreprises. Les flux existants sont également personnalisables en fonction des besoins des clients.

La disponibilité des rapports et des flux d'ESET Threat Intelligence varie selon les pays. Contactez votre représentant ESET local pour en savoir plus.



BOTNET ACTIVITY REPORT

Global Statistics: Week 7/2018

DATE	SAMPLES	C&C	NEW C&C	TARGETS
2018-02-12	12225	7914	32	2647
2018-02-13	14487	7737	63	2706
2018-02-14	14114	8016	42	2737
2018-02-15	13359	8414	61	2789
2018-02-16	12160	7830	68	2640
2018-02-17	9445	7356	12	2697
2018-02-18	7378	6834	20	1795

FAMILY	SAMPLES	C&C	NEW C&C	TARGETS
Kovter	37988	9751	13	0
Emotet	11798	59	5	0
Wauchos	8157	19	0	0
Kasidet	7102	96	20	23
Zbot	6137	460	77	301
SpyBanker	4743	0	0	0
Dorkbot	2274	375	0	62
Ramnit	1408	16	0	119
Waski	1274	87	0	0
TrickBot	983	412	114	2135
Qbot	636	0	0	47
Retefe	256	43	17	163
Ursnif	235	135	32	0
Papras	231	27	0	0
Tovkater	166	94	4	0
Banload	148	45	11	0
Elenoocka	10	14	0	0
Tinba	7	1	0	0

FORGED SSL CERTIFICATE REPORT

CLIENT	ESET DEMO
REPORT DATE	2017-11-09 16:55:06 CET (UTC/GMT +01:00)
REPORT ID	89A88/2017

Certificate

SUBJECT NAME	www.ynod.ir
VALID SINCE	2017-11-04T23:57:46.000Z
VALID TO	2018-02-02T23:57:46.000Z

Key Usage

Digital Signature, Key Encipherment

Names

nod32buy.ir
nod32buy2.ynod.ir
uappleid.com
uappleid.ynod.ir
www.nod32buy.ir
www.nod32buy2.ynod.ir
www.uappleid.com
www.uappleid.ynod.ir
www.ynod.ir
ynod.ir

YARA matches

SOURCE	OFFSET	LENGTH	STRING
cert	0x378	5	nod32

Certificate data

{
  "@timestamp": [

TARGETED PHISHING REPORT

CLIENT	ESET DEMO
REPORT DATE	2017-12-03 13:44:00 CET (UTC/GMT +01:00)
REPORT ID	32E30/2017

Phishing campaign

Campaign size	10 000 to 100 000
Number of clients	10 000 to 100 000
Campaign duration	9 day(s) 22 hour(s)
First phishing activity	2017-11-23 14:00:00 UTC
Last phishing activity	2017-12-03 12:00:00 UTC
Servers	55.30%
Endpoints	44.70%

Phishing URLs

URL	IP	LOCATION	DNS HISTORY
gooddrugsale[dot]su			46.242.139.49 149.5.188.101 199.127.103.200 185.212.172.83

Locations of phishing servers

COUNTRY	SHARE
United States	34.69%
China	12.03%
Italy	9.10%
Japan	8.83%
Denmark	8.68%

À propos d'ESET

ESET, acteur mondial de la sécurité informatique, est désigné comme unique Challenger dans le Gartner Magic Quadrant 2018, « Endpoint Protection »

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe, qui protègent en temps réel les entreprises et les particuliers du monde entier contre des menaces de cybersécurité en constante évolution.

En tant qu'entreprise privée non endettée, nous sommes libres de mener toutes les actions nécessaires pour offrir à nos clients une protection optimale et complète.

ESET EN QUELQUES CHIFFRES

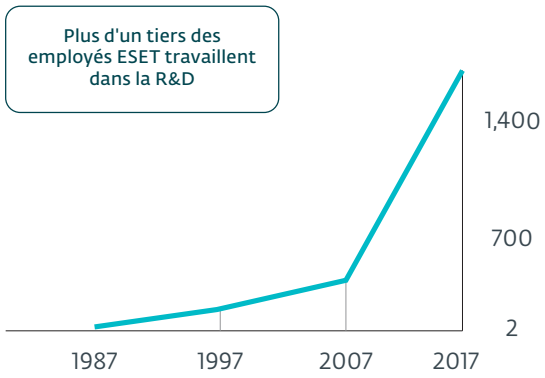
+110 millions
d'utilisateurs partout dans le monde

+ 400 000
Clients Entreprises

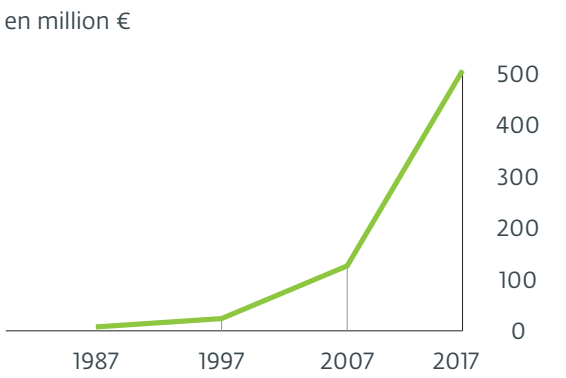
+ 200
pays et territoires couverts

13
centres R&D dans le monde

EMPLOYÉS ESET



CHIFFRE D'AFFAIRES ESET



*Gartner ne recommande aucun fournisseur, produit ou service mentionnés dans ses rapports d'études. Les opinions exprimées par Gartner dans ses publications ne doivent pas être interprétées comme des faits établis. Gartner décline toute responsabilité, expresse ou tacite, relative à cette étude, notamment toute garantie de valeur commerciale ou d'adéquation à un usage particulier.

QUELQUES-UNS DE NOS CLIENTS

HONDA

Protégé par ESET depuis 2011

Licence prolongée 3 fois, étendue 2 fois

GREENPEACE

Protégé par ESET depuis 2008

Licence prolongée/étendue 10 fois

Canon

Protégé par ESET depuis 2016

Plus de 14 000 endpoints

T . .

Partenaire de sécurité FAI depuis 2008

2 millions d'utilisateurs

NOS RÉCOMPENSES LES PLUS PRESTIGIEUSES

SE Labs AAA ENTERPRISE ENDPOINT OCT-DEC 2016

THE CHANNEL CO. CRN ★★★★★ PARTNER PROGRAM GUIDE WINNER 2017

AV comparatives Approved Business Product 2017

SC MEDIA RECOMMENDED

" Avec ses excellentes fonctionnalités anti-malware, sa simplicité de gestion et sa présence internationale, ESET fait partie des meilleurs candidats du marché pour les appels d'offres de solutions de sécurité. "

KuppingerCole Leadership Compass

Enterprise Endpoint Security: Anti-Malware Solutions, 2018

ENJOY SAFER TECHNOLOGY™

30 ANNÉES D'INNOVATION POUR PROTÉGER VOTRE VIE NUMÉRIQUE

Consultez notre catalogue complet des solutions et services sur :

WWW.ESET.COM/NA/BUSINESS

Besoin de renseignements ? Contactez-nous :

+33 (0)1.72.59.42.01

info.afrique@eset-nod32.fr