PRÉSENTATION

INSPECT

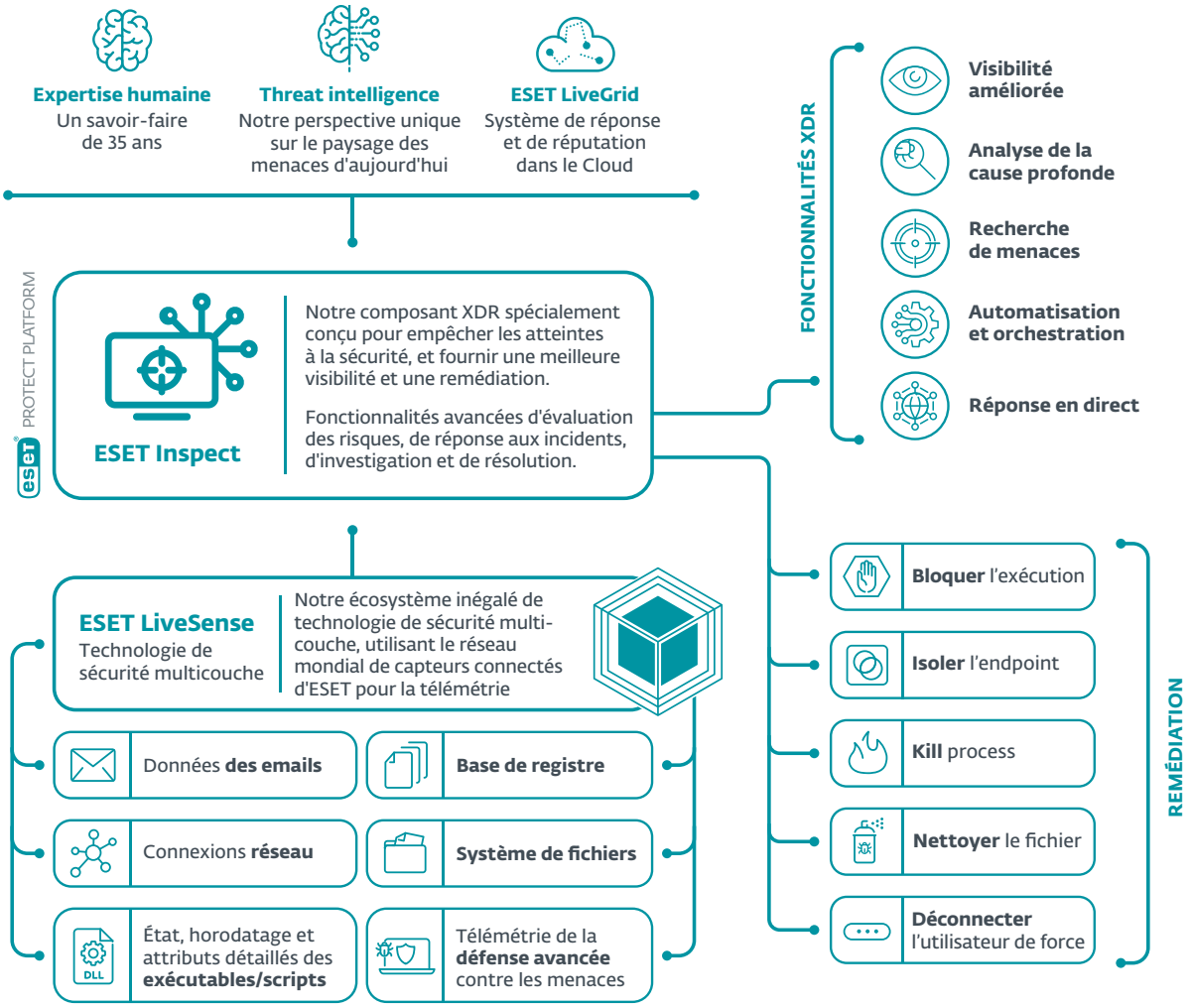
Le module XDR de la plateforme ESET PROTECT pour la prévention et la remédiation des intrusions, et l'amélioration de la visibilité

Progress. Protected.

Qu'est-ce qu'une **solution de détection et de réponse étendues (XDR) ?**

ESET Inspect, le module XDR de la plateforme ESET PROTECT, est un outil d'identification des comportements anormaux et des failles de sécurité, d'évaluation des risques, de réponse aux incidents, d'enquêtes et de remédiation.

Il permet aux intervenants de surveiller et d'évaluer toutes les activités du réseau et des appareils connectés en cas d'incident. Il permet également d'automatiser au besoin les actions correctives immédiates. Les 800 règles de détection d'ESET (leur nombre continu d'augmenter) permettent une recherche étendue des menaces.



Les avantages ESET

PRÉVENTION, DÉTECTION ET RÉPONSE TOTALES

Analyse et remédiation rapide de tout problème de sécurité dans votre réseau. La sécurité multicouche sous-jacente d'ESET, dans laquelle chaque couche envoie des données à ESET Inspect, analyse de grandes quantités de données en temps réel afin qu'aucune menace ne passe inaperçue.

SOLUTION D'UN FOURNISSEUR PRIVILÉGIANT LA SÉCURITÉ

ESET lutte contre les cybermenaces depuis plus de 30 ans. En tant qu'entreprise à vocation scientifique, elle est depuis longtemps à la pointe du développement de technologies autours du machine learning, du Cloud, et maintenant de XDR.

MIEUX VAUT PRÉVENIR QUE GUÉRIR

L'approche d'ESET en matière de l'XDR est étroitement liée à ses produits de prévention primés. Grâce à son engagement à développer une technologie de détection de haute qualité, la technologie de prévention d'ESET est une des meilleures du secteur.

VISIBILITÉ DÉTAILLÉE SUR LE RÉSEAU

Avec des règles de détection transparentes (ESET en compte plus de 800), des indicateurs de compromis (IoC) avancés et une fonctionnalité de recherche, un examen approfondi des exécutables fonctionnant sur votre réseau vous permettra d'identifier tout ce qui est suspect.

FLEXIBILITÉ DU DÉPLOIEMENT

Nous vous laissons décider de la manière de déployer votre solution de sécurité : ESET Inspect peut être hébergé sur vos propres serveurs sur site ou dans le Cloud, ce qui vous permet d'adapter votre configuration en fonction de vos objectifs de coût total de possession et de vos moyens matériels.

CRÉATION AUTOMATISÉE D'INCIDENT

Obtenez une visibilité parfaite grâce à des incidents créés automatiquement et élégamment présentés. ESET Inspect corrèle de grandes quantités de données pour trouver les causes profondes des événements et les compiler en incidents détaillés afin que vous puissiez les résoudre immédiatement.

PRÊT À L'EMPLOI IMMÉDIATEMENT

La solution d'ESET est prête à l'emploi dès son installation, et est suffisamment puissante pour être configurée de façon granulaire par les équipes expérimentées de recherche de menaces.

MITRE ATT&CK

Les détections d'ESET Inspect s'appuient sur le cadre MITRE ATT&CK™ (Adversarial Tactics, Techniques, and Common Knowledge), qui fournit des informations complètes en un clic, même sur les menaces les plus complexes.

SYSTÈME DE RÉPUTATION

Le filtrage étendu permet aux ingénieurs en sécurité d'identifier toutes les applications connues à l'aide du système robuste de réputation d'ESET. Le système d'ESET intègre une base de données de centaines de millions de fichiers bénins afin de garantir que les équipes de sécurité puissent se consacrer à des fichiers inconnus, et potentiellement malveillants, et non sur des faux positifs.

AUTOMATISATION ET ORCHESTRATION

Adaptez facilement ESET Inspect au niveau de détail et d'automatisation dont vous avez besoin. Choisissez le niveau d'interaction souhaité, ainsi que le type et la quantité de données à stocker, lors de la configuration initiale et à l'aide de profils d'utilisateurs prédéfinis, puis laissez le mode apprentissage cartographier l'environnement de votre entreprise et suggérer au besoin des exclusions pour les faux positifs.

eset Digital Security
Progress. Protected.

Fonctionnalités

SYSTÈME DE GESTION DES INCIDENTS

Regroupez des objets tels que des détections, des ordinateurs, des exécutables ou des processus en unités logiques afin de visualiser les événements malveillants potentiels sur une chronologie, avec les actions associées des utilisateurs. ESET Inspect suggère automatiquement à l'intervenant tous les événements et objets pertinents qui peuvent grandement l'aider dans les étapes de triage, d'enquête et de résolution d'un incident.

OPTIONS DE RÉPONSE EN DIRECT

ESET Inspect est fourni avec des actions facilement accessibles en un clic, telles que le redémarrage et l'arrêt d'un endpoint, l'isolement des endpoints du reste du réseau, le lancement d'une analyse à la demande, l'arrêt de tout processus en cours d'exécution, et le blocage de toute application en fonction de son hachage. De plus, grâce à l'option de réponse en direct d'ESET Inspect, appelée Terminal, les professionnels de la sécurité peuvent bénéficier de la suite complète d'options d'investigation et de remédiation dans PowerShell.

ANALYSE DES CAUSES PROFONDES

Visualisez facilement l'analyse des causes profondes et l'arborescence complète des processus de toute chaîne d'événements potentiellement malveillants, accédez au niveau de détail souhaité, et prenez des décisions éclairées en vous référant aux explications et au contexte fournis par nos experts en malwares sur les causes bénignes et malveillantes.

API PUBLIQUE

ESET Inspect comprend une API REST publique qui permet d'accéder aux détections et de les exporter, et d'accéder à leurs interventions pour permettre une intégration efficace avec des outils de SIEM, de SOAR, de tickets et bien d'autres.

MULTIPLES INDICATEURS DE COMPROMIS

Consultez et bloquez des modules en fonction de plus de 30 indicateurs différents, y compris le hachage, les modifications de la base de registre, les modifications de fichiers et les connexions réseau.

RECHERCHE DE MENACES

Utilisez de puissantes requêtes de recherche d'indicateurs de compromis et appliquez des filtres aux données brutes pour les trier en fonction de la popularité des fichiers, leur réputation, leur signature numérique, leur comportement ou d'autres informations contextuelles. La mise en œuvre de plusieurs filtres facilite et automatise la recherche des menaces et la réponse aux incidents, avec la possibilité de détecter et de stopper les menaces persistantes avancées et les attaques ciblées.

ACCÈS À DISTANCE SÛR ET FLUIDE

La fluidité des services de sécurité et de réponse aux incidents dépend de la facilité d'accès à ces services, qu'il s'agisse de la connexion de l'intervenant à la console ou de la connexion aux endpoints. La connexion fonctionne en quasi temps réel, même avec les mesures de sécurité maximales appliquées, le tout sans avoir recours à des outils tiers.

ISOLEMENT EN UN CLIC

Définissez des politiques d'accès au réseau pour stopper rapidement les mouvements latéraux des malwares. Isolez un appareil compromis du réseau en un seul clic via l'interface d'ESET. Retirez également facilement des appareils de la quarantaine.

DÉTECTION DES ANOMALIES ET DES COMPORTEMENTS

Vérifiez les actions effectuées par un exécutable et utilisez le système de réputation LiveGrid® d'ESET pour déterminer rapidement si les processus exécutés sont fiables ou suspects. La surveillance des incidents anormaux liés aux utilisateurs est possible grâce à des règles conçues pour être déclenchées par un comportement, et non par de simples détections de malwares ou des signatures. Le regroupement des ordinateurs par utilisateurs ou par services permet aux équipes de sécurité de déterminer si un utilisateur est autorisé à effectuer une action spécifique ou non.

RAPPORTS INTERACTIFS SUR LES COMPORTEMENTS

Vous rencontrez un fichier suspect ? Soumettez-le à ESET LiveGuard Advanced et son puissant sandbox dans le cloud pour une analyse approfondie. En quelques instants, vous pouvez consulter un rapport interactif sur les comportements du fichier, les modifications apportées au système, les appels d'API, etc. et les bloquer.

TAGGING

Attribuez et retirez des balises pour un filtrage rapide des objets tels que les ordinateurs, les alarmes, les exclusions, les tâches, les exécutables, les processus et les scripts. Les balises sont partagées entre les utilisateurs, et peuvent être attribuées en quelques secondes une fois qu'elles sont créées.

DÉTECTION DES VIOLATIONS DES POLITIQUES DE SÉCURITÉ

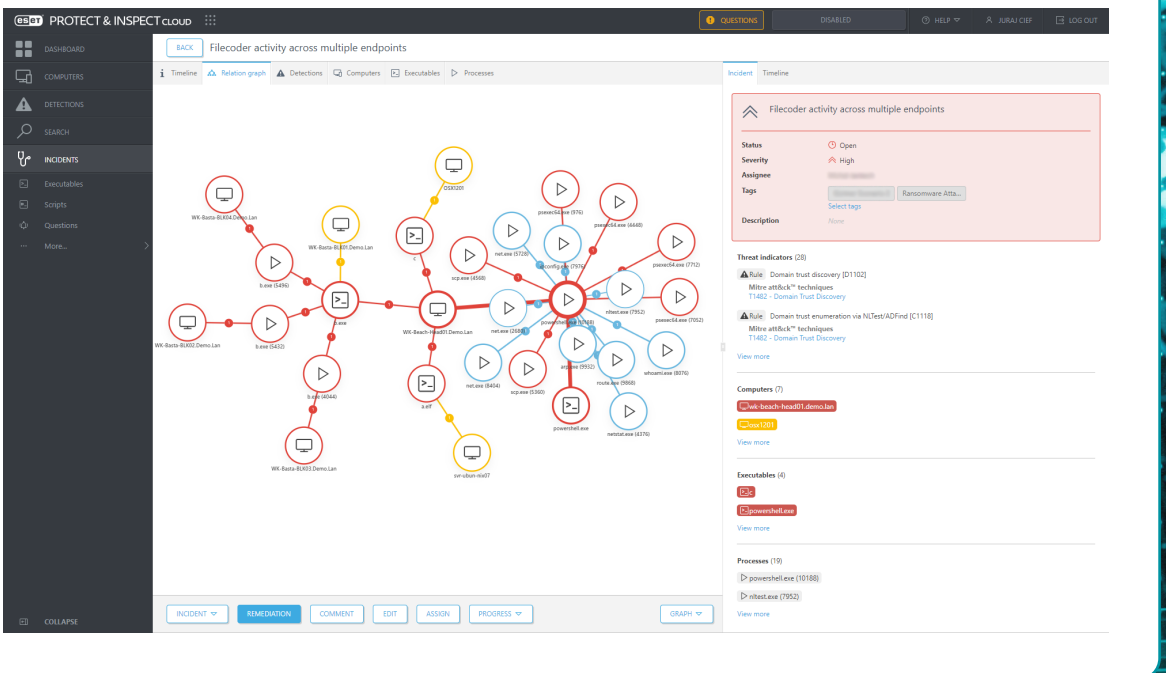
Bloquez l'exécution de modules malveillants sur tout ordinateur du réseau de votre entreprise. L'architecture ouverte d'ESET Inspect permet de détecter les violations des politiques de sécurité concernant l'utilisation de logiciels spécifiques tels que les applications de téléchargement de torrents, de stockage dans le Cloud, de navigation via Tor ou d'autres logiciels indésirables.

ARCHITECTURE OUVERTE ET INTÉGRATIONS

ESET Inspect intègre une détection unique s'appuyant sur les comportements et la réputation, qui est totalement transparente pour les équipes de sécurité. Toutes les règles sont facilement éditables via XML et peuvent être facilement personnalisées et créées pour répondre aux besoins d'environnements d'entreprise spécifiques, y compris les intégrations avec des solutions de SIEM.

NOTATION SOPHISTIQUÉE

Hiérarchisez la gravité des alarmes grâce à une fonctionnalité de notation qui attribue une valeur de gravité aux incidents, et permet à l'administrateur d'identifier rapidement les ordinateurs présentant une probabilité plus élevée d'incident potentiel.



eset Digital Security
Progress. Protected.

Cas d'utilisation

Détection des comportements et des récidives

PROBLÈME

Dans votre réseau, vous avez des utilisateurs récidivistes, c'est-à-dire que les mêmes utilisateurs continuent d'être infectés à chaque fois. Est-ce dû à un comportement à risque ? Ou sont-ils plus souvent visés que d'autres utilisateurs ?

SOLUTION

- ✓ Déterminez facilement les utilisateurs et les appareils à problème.
- ✓ Effectuez rapidement une analyse des causes profondes pour déterminer la source des infections.
- ✓ Corrigez les vecteurs d'infection trouvés tels que les emails, le web ou les périphériques USB.

Recherche et blocage des menaces

PROBLÈME

Votre système d'alerte précoce ou votre centre d'opérations de sécurité (SOC) émet un nouvel avertissement quant à une menace. Quelles sont vos prochaines étapes ?

SOLUTION

- ✓ Récupérez des données sur les nouvelles menaces ou les menaces à venir, à partir du système d'alerte précoce.
- ✓ Analysez tous les ordinateurs pour vérifier si une nouvelle menace y est présente.
- ✓ Recherchez dans tous les ordinateurs des indicateurs de compromis indiquant que la menace existait avant l'alerte.
- ✓ Empêchez la menace de s'infiltrer dans le réseau et de s'y propager.

Configuration/ réponse faciles sans équipe de sécurité requise

PROBLÈME

Toutes les entreprises ne disposent pas d'équipes de sécurité spécialisées, et la création et la mise en œuvre de règles de détection avancées peuvent s'avérer difficiles.

SOLUTION

- ✓ Plus de 300 règles préconfigurées sont intégrées.
- ✓ Réagissez facilement en cliquant simplement sur un bouton unique pour bloquer, stopper ou mettre des appareils en quarantaine.
- ✓ Des propositions et des étapes de remédiation sont intégrées aux alarmes.
- ✓ Les règles sont modifiables via le langage XML, ce qui permet de les affiner facilement ou d'en créer de nouvelles.

Visibilité sur le réseau

PROBLÈME

Certaines entreprises s'inquiètent des applications dont se servent les utilisateurs sur les systèmes. Vous devez non seulement vous préoccuper des applications installées traditionnellement mais également des applications portables qui ne sont pas réellement installées. Comment pouvez-vous les contrôler ?

SOLUTION

- ✓ Visualisez et filtrez facilement toutes les applications installées sur tous les appareils.
- ✓ Visualisez et filtrez tous les scripts sur tous les appareils.
- ✓ Bloquez facilement l'exécution d'applications ou de scripts non autorisés.
- ✓ Notifiez les utilisateurs des applications non autorisées et désinstallez-les automatiquement.

Détection approfondie des menaces des ransomwares

PROBLÈME

Une entreprise souhaite disposer d'outils supplémentaires pour détecter les ransomwares de manière proactive, en plus d'être avertie rapidement en cas d'observation d'un comportement de type ransomwares sur le réseau.

SOLUTION

- ✓ Règles pour détecter les applications exécutées à partir de dossiers temporaires.
- ✓ Règles pour détecter les fichiers Office (Word, Excel, PowerPoint) qui exécutent des scripts ou des exécutables supplémentaires.
- ✓ Alerte lorsqu'un module de ransomware courant apparaît sur un appareil.
- ✓ Visualisation des alertes Ransomware Shield émises par les solutions ESET Endpoint Security dans la même console.

Enquêtes et remédiation en fonction du contexte

PROBLÈME

Les données ne sont utiles qu'à la mesure du contexte qui les sous-tend. Pour prendre les bonnes décisions, vous devez savoir quelles sont les alertes, sur quels appareils elles se produisent, et quels utilisateurs les déclenchent.

SOLUTION

- ✓ Identifiez et classez tous les ordinateurs à l'aide d'Active Directory, de regroupements automatiques ou de regroupements manuels.
- ✓ Autorisez ou bloquez des applications ou des scripts en fonction des groupes d'ordinateurs.
- ✓ Autorisez ou bloquez des applications ou des scripts en fonction des utilisateurs.
- ✓ Recevez des notifications uniquement pour certains groupes.

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

+ 400 k
entreprises clientes

200
pays et territoires

13
centres de recherche

QUELQUES-UNS DE NOS CLIENTS

MITSUBISHI MOTORS
Drive your Ambition

Protégés par ESET depuis 2017 : 9 000 endpoints

Allianz Suisse

Protégé par ESET depuis 2016 : +4 000 boîtes mail

Canon
Canon Marketing Japan Group

Protégés par ESET depuis 2016 : 32 000 endpoints

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

RECONNAISSANCES

AV comparatives APPROVED Business Security DEC 2023

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 2024

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**.

kuppingercole ANALYSTS

ESET est **reconnu comme un leader du marché** et un leader en général du MDR, selon le KuppingerCole Leadership Compass 2023.