Livre blanc

Vulnérabilités logicielles :

Découvrez comment renforcer la sécurité de votre infrastructure informatique avec une gestion proactive des vulnérabilités et des patchs.

Romain RAVON

Digital Security
Progress. Protected.

Digital Security
Progress. Protected.

Table des matières

Introduction

L'évolution rapide des menaces numériques a rendu la détection et la gestion des vulnérabilités plus capitale que jamais. Les acteurs malveillants développent constamment de nouvelles techniques pour exploiter les failles logicielles et mettent en péril les données d'entreprises de toutes tailles.

Prenons l'exemple d'une bijouterie. Afin de garantir la sécurité des bijoux, plusieurs dispositifs ont été mis en place : une porte verrouillée, des caméras de sécurité ainsi qu'un coffre-fort pour les pièces ayant le plus de valeur.

Imaginons maintenant que le coffre-fort présente un défaut de conception connu. La marque de production du coffre-fort a conscience de ce défaut et a communiqué ouvertement à ce sujet lors de sa campagne de rappel visant à remplacer cet élément défectueux. Ce défaut peut être assimilé à une faille de sécurité référencée sous une CVE. Pour une raison de temps et du fait que le bijoutier ne peut pas se permettre de passer 2 jours sans coffre-fort le temps d'en recevoir un nouveau, il décide de le garder.

Un groupe de cambrioleurs découvre eux aussi au cours de leurs recherches que ce coffre-fort est défaillant et par conséquent facile à forcer. Il décide donc d'échafauder un stratagème pour contourner les autres sécurités de la bijouterie et atteindre le coffre-fort. Ainsi une fois devant le coffre, il leur suffit d'exploiter la vulnérabilité de ce dernier pour s'emparer des trésors qu'il renferme.

Il faut retenir de cette analogie qu'une faille de sécurité ne sera pas forcément la porte d'entrée d'un attaquant, mais qu'elle permettra d'effectuer une action illégitime, facilement ou presque. Dans le cas présent, il convient de s'assurer que chaque organe de sa bijouterie est fonctionnel et sécurisé et si ce n'est pas le cas, prendre les mesures correctives pour les remettre en état de fonctionnement optimal.

C'est une situation similaire que rencontrent les entreprises qui ne mettent pas en œuvre une gestion rigoureuse des vulnérabilités et des patchs dans leurs systèmes informatiques. Le cybercrime, qui coûte 11 000 milliards de dollars à l'économie mondiale en 2023 — incluant les coûts des rançons et les pertes brutes liées à la cessation d'activité —, montre bien que même si les failles ne sont pas la cause majeure de ce montant, elles démontrent la profitabilité croissante de l'activité des cybercriminels.

Ce livre blanc est votre guide pour comprendre comment sécuriser ces ouvertures et protéger votre entreprise contre les menaces numériques.

Chapitre 1

Comprendre les vulnérabilités et les CVE

Pour maintenir la sécurité des systèmes d'information, il convient de comprendre la nature et la gestion des vulnérabilités informatiques. En effet, elles représentent des faiblesses ou des failles dans un système informatique qui, si exploitées, peuvent entraîner une violation de la sécurité. Un attaquant peut accéder à des informations sensibles et perturber les opérations normales. Il peut également prendre le contrôle total du système affecté. Notez que les attaquants ont la possibilité de rester dissimulés dans le système pendant une période prolongée, tant que la faille n'est pas détectée et corrigée. Ils exploitent cette invisibilité pour collecter progressivement des données ou préparer des attaques plus conséquentes.

DÉFINITION

Une vulnérabilité informatique est une **faiblesse dans la conception d'un logiciel qui peut être exploitée par une menace** ou un attaquant pour un usage détourné, tout en utilisant un logiciel légitime, ce qui dupe souvent l'utilisateur.

Ces vulnérabilités existent en raison :

- D'erreurs de programmation ;
- De configurations incorrectes ;
- Ou de l'utilisation de composants (bibliothèque) logiciels eux-mêmes vulnérables.

Ces faiblesses peuvent affecter divers composants d'un système, y compris le matériel, les logiciels, le réseau et les données.

+29 000

vulnérabilités et expositions communes (CVE) répertoriées en 2023 soit **une hausse de 15 %** par rapport à l'année précédente

Les vulnérabilités sont particulièrement dangereuses, car **elles octroient aux cybercriminels le moyen d'infiltrer les systèmes**. Par exemple, la faille CVE-2017-0144, mieux connue sous le nom d'EternalBlue, était une vulnérabilité dans le protocole SMB de Microsoft Windows.

Après son identification, elle a été exploitée par le ransomware WannaCry pour déployer en masse une attaque qui a causé des perturbations globales.Elle a affecté des milliers d'organisations en chiffrant leurs données et en demandant une rançon pour leur déchiffrement.

DÉCOUVRIR L'EXISTENCE D'UNE FAILLE

Il existe plusieurs façons de découvrir l'existence d'une faille informatique :

- **Une faille peut être détectée en interne chez l'éditeur** lors d'une revue de code par exemple. C'est le meilleur cas de figure. Il permet ainsi de conserver cette faille secrète jusqu'à l'édition et la mise à disposition du correctif, en espérant qu'elle n'aura jamais été découverte et exploitée par un groupe malveillant.
- **Certains éditeurs organisent des Bug Bounty avec des hackers éthiques (white hat)** qui prennent le rôle d'un attaquant afin de trouver de potentielles failles et les remontent directement à l'éditeur moyennant une prime. Ces failles sont gardées secrètes jusqu'à l'édition et la mise à disposition du correctif.
- **La découverte d'une exploitation malveillante par des attaquants.** Il s'agit ici du pire cas de figure. Ces derniers découvrent une faille et l'exploitent durant leurs multiples attaques informatiques.

C'est suite à une ou plusieurs atteintes que les experts en cybersécurité, découvriront la faille et pourront ainsi la remonter à l'éditeur.

Il faut donc encore attendre parfois plusieurs jours pour que l'éditeur soit en capacité de proposer un correctif.

Les failles découvertes et ensuite enregistrées comme CVE sont rendues publiques.

C'est pourquoi il est capital d'appliquer au plus tôt le correctif sous peine d'être victime de cette faille connue aussi bien du grand public que des attaquants.

QU'EST-CE QU'UNE CVE ?

Le système Common Vulnerabilities and Exposures (CVE) est un catalogue public de vulnérabilités de sécurité notoires. Chaque entrée dans le système CVE, intitulé CVE ID, est unique et fournit une référence standard pour chaque vulnérabilité connue. Cela permet aux professionnels de la sécurité et aux administrateurs système de discuter, de gérer et de résoudre les vulnérabilités de manière uniforme et coordonnée.

Le programme CVE a été lancé en 1999 par le MITRE, une organisation à but non lucratif qui gère des projets de recherche et développement pour le gouvernement fédéral américain.

Le système CVE est aujourd'hui largement utilisé par les fabricants de sécurité, les organisations de recherche en sécurité et les agences gouvernementales pour partager des informations fondamentales sur les vulnérabilités de sécurité.

CLASSIFICATION DES CVE

Les vulnérabilités dans le système CVE sont souvent évaluées à l'aide du Common Vulnerability Scoring System (CVSS).

Le CVSS est un cadre ouvert qui sert à attribuer des scores numériques aux vulnérabilités, en fonction de leur sévérité.

Le score est calculé en tenant compte de divers facteurs, tels que la complexité de l'exploitation, l'impact sur la confidentialité, l'intégrité et la disponibilité, et d'autres métriques liées au contexte de l'exploitation.

Les scores CVSS sont généralement divisés en trois niveaux :

- Faible (0.0 - 3.9)
- Moyen (4.0 - 6.9)
- Élevé (7.0 - 10.0)

Score **CVSS**

10.0

EXEMPLE : LA VULNÉRABILITÉ CVE-2021-44228

Cette vulnérabilité, plus connue sous le nom de Log4Shell, est une faille critique avec un score CVSS de 10.0, indiquant son extrême gravité.

Cette vulnérabilité affecte la bibliothèque de logging Apache Log4j, largement utilisée par de nombreuses applications Java à travers le monde.

Elle permet une exécution de code à distance, offrant à un attaquant la possibilité d'exécuter du code arbitraire sur un système vulnérable simplement en envoyant des chaînes de caractères malveillantes.

Peu après sa divulgation, cette faille a été exploitée à grande échelle, compromettant des applications web et services en ligne dans le monde entier.

Log4Shell a démontré à quel point une vulnérabilité critique peut rapidement affecter d'innombrables systèmes dans un laps de temps très court.

MAÎTRISER CES FAILLES

La gestion des CVE implique la surveillance continue des nouvelles vulnérabilités, l'évaluation de leur applicabilité au contexte spécifique d'une organisation, et la priorisation des correctifs et des mises à jour en fonction de la sévérité des risques. Une gestion pertinente des CVE maintient la sécurité des systèmes informatiques.

Elle comprend généralement les étapes suivantes :

1. **Identification :** utilisation de scanners de vulnérabilités et d'autres outils pour diagnostiquer les vulnérabilités potentielles dans les systèmes.
2. **Évaluation :** analyse de l'impact potentiel et de la facilité d'exploitation des vulnérabilités identifiées.
3. **Priorisation :** classement des vulnérabilités en fonction de leur sévérité, de l'impact potentiel et des ressources disponibles pour les corriger.
4. **Correction :** déploiement de correctifs et de mises à jour pour rectifier les vulnérabilités.

+38 %

des applications
exécutent encore des versions vulnérables de Log4j en décembre 2023, malgré la gravité de la faille identifiée.

La gestion proactive des vulnérabilités s'avère incontournable pour prévenir les exploits et les attaques qui peuvent tirer parti des vulnérabilités non corrigées.

Comprendre le fondement des vulnérabilités et gérer avec efficacité les failles de sécurité sont deux actions primordiales. Les organisations doivent adopter des stratégies de cybersécurité qui détectent et corrigent les vulnérabilités de manière opportune.

Elles doivent également anticiper les menaces potentielles pour rester résilientes face aux attaques cyberattaques de plus en plus sophistiquées.

ESET est reconnu comme autorité de numérotation CVE (CNA) dans le cadre du programme CVE. Cette reconnaissance renforce le rôle d'ESET dans l'avancement des normes de sécurité dans l'écosystème informatique.

Chapitre 2

Les scanners de vulnérabilités et gestionnaires de patchs

La sécurité informatique est une course constante entre les développeurs de sécurité et les cybercriminels. Pour rester en tête, les entreprises déploient des outils spécialisés pour identifier et corriger les vulnérabilités avant qu'elles ne soient exploitées .

La gestion des patchs est le processus par lequel les entreprises identifient, téléchargent et installent des mises à jour sur leurs systèmes informatiques. Ces correctifs peuvent corriger des bugs, améliorer les performances, et surtout, fermer les failles de sécurité

FONCTIONNEMENT

Les scanners de vulnérabilités sont des **outils automatisés conçus pour rechercher les failles de sécurité dans les réseaux**, les systèmes et les applications.

Ils examinent passivement ou activement les systèmes à la recherche de toutes les corruptibilités connues.

Pour ce faire, ils partent d'une **base de données de signatures de vulnérabilités** qui est régulièrement mise à jour.

Ces outils réalisent des inspections détaillées des configurations, des codes, et des services web, en effectuant le rapprochement entre les versions utilisées et les versions comportant des CVE.

RÉDUCTION DES RISQUES

La détection des vulnérabilités à un stade précoce **réduit considérablement le risque d'attaques réussies**. Le scanner permet de découvrir les vulnérabilités et d'évaluer le niveau de risque associé à chaque faille détectée. Ce processus autorise ainsi une priorisation efficiente des réponses.

CORRECTION RAPIDE

La rapidité de déploiement des patchs est un facteur critique. Les failles telles que celles identifiées par les CVE doivent être corrigées rapidement pour éviter des exploitations malveillantes car en effet, une faille est rendue public auprès des utilisateurs mais auprès de cybercriminels.

La gestion des correctifs permet de s'assurer que toutes les corrections nécessaires sont appliquées dès qu'elles deviennent disponibles.

Chaque logiciel peut présenter **7 à 8 vulnérabilités** (CVE) par an. Pour une entreprise utilisant 250 logiciels différents, **cela représente environ 1 750 failles potentielles** chaque année, soit près de 5 vulnérabilités par jour.

CONFORMITÉ ET NORMES DE SÉCURITÉ

Un pilotage pertinent des patchs **aide également les entreprises à rester conformes aux normes** de sécurité industrielles et réglementaires.

De nombreuses régulations, comme le RGPD en Europe ou le HIPAA aux États-Unis, exigent que les organisations prennent des mesures proactives pour protéger les données contre les menaces de sécurité.

Ne pas appliquer les correctifs de sécurité en temps opportun peut entraîner des **amendes substantielles**, en plus d'augmenter le risque de brèches de données.

IMPACT DU CLOUD & MISES À JOUR AUTOMATIQUES

Avec l'adoption croissante des services basés sur le cloud, la capacité à gérer les mises à jour sécurité a été grandement améliorée. Le cloud offre un avantage distinct en termes de gestion des patchs grâce à la possibilité de mises à jour automatiques.

MISES À JOUR SANS INTERVENTION

Les fournisseurs de cloud peuvent déployer des correctifs automatiquement à travers leurs infrastructures.

Cela réduit ainsi le besoin d'intervention manuelle et la possibilité d'erreur humaine.

Même les vulnérabilités les plus récentes sont rapidement et efficacement adressées sans que les utilisateurs aient à prendre des mesures.

RÉDUCTION DES TEMPS D'ARRÊT

Les mises à jour automatiques et planifiées réduisent également les temps d'arrêt des systèmes, car elles peuvent nécessiter des redémarrages. C'est inhérent pour maintenir une continuité d'activité dans un environnement commercial qui dépend de plus en plus de la technologie numérique

SÉCURITÉ HOMOGÈNE

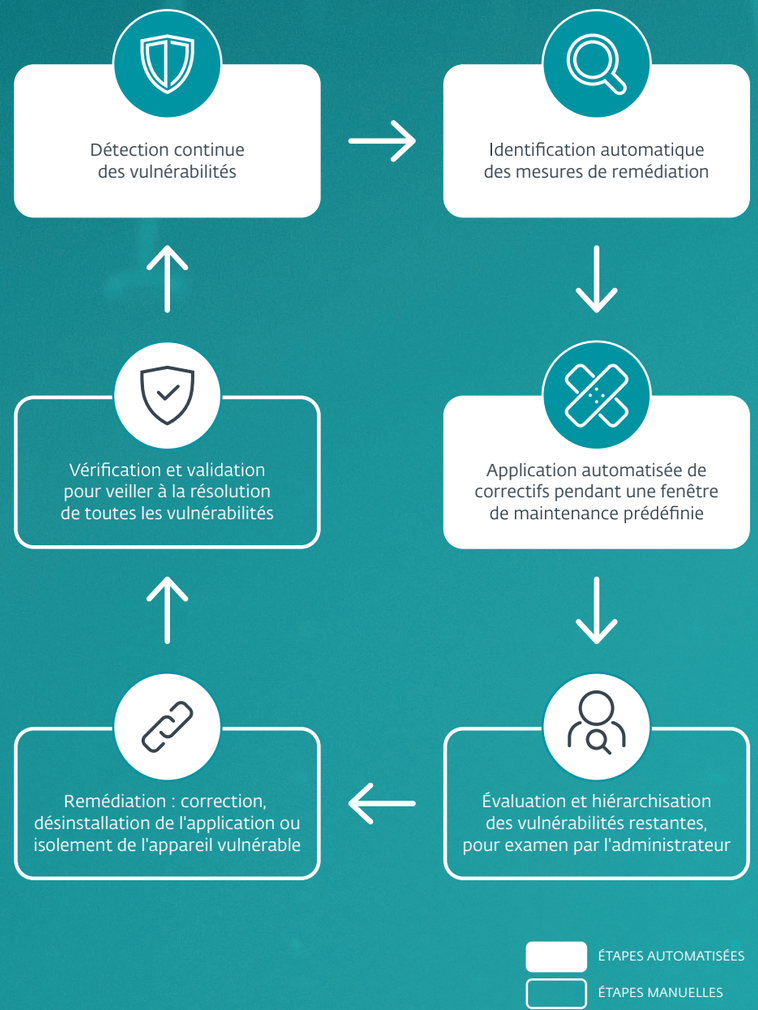
Enfin, les mises à jour automatiques garantissent que tous les composants du système sont maintenus à jour sur l'ensemble du réseau.

Cela évite les incohérences dans les versions de logiciel qui pourraient autrement introduire des vulnérabilités dans l'environnement Les scanners de vulnérabilités et les gestionnaires de patchs sont indispensables pour une stratégie de cybersécurité solide.

Ils permettent de détecter et de corriger les vulnérabilités de manière proactive mais aussi de maintenir les systèmes à jour et conformes aux normes de sécurité actuelles.

Aujourd'hui, les menaces évoluent rapidement et ces outils protègent les actifs numériques et physiques des entreprises contre les cyberattaques.

Leur intégration dans les stratégies de sécurité informatique est non seulement recommandée, mais nécessaire pour tout environnement soucieux de sa sécurité numérique.



Chapitre 3

Pourquoi ESET est-il le partenaire idéal ?

Dans le domaine de la cybersécurité, les entreprises doivent s'assurer que leurs défenses soient robustes mais aussi capables d'anticiper et de répondre aux menaces émergentes.

ESET, avec sa solution complète ESET Vulnerability & Patch Management intégrée à la plateforme ESET PROTECT, offre une sécurité avancée, une gestion efficace des vulnérabilités, et une automatisation des correctifs, faisant d'ESET le partenaire idéal pour sécuriser les infrastructures informatiques modernes.

AUTOMATISATION

ESET Vulnerability & Patch Management effectue des analyses automatiques des logiciels et applications.

Cette solution propose une visibilité instantanée sur les vulnérabilités grâce à des rapports en temps réel accessibles via la console ESET PROTECT.

Cette automatisation assure que les vulnérabilités soient rapidement identifiées et que les correctifs nécessaires soient appliqués sans délai, en choisissant parmi diverses stratégies d'application des correctifs pour optimiser la protection sans perturber les opérations courantes.

PERSONNALISATION

La solution permet également une grande personnalisation dans l'application des patchs. Les entreprises peuvent configurer leurs propres plannings de correctifs automatiques ou manuels, en ajustant les politiques pour prioriser les ressources critiques et programmer les patchs des autres ressources pendant les heures creuses pour minimiser les interruptions.

ORCHESTRATION

L'intégration d'ESET Vulnerability & Patch Management à ESET PROTECT renforce la capacité des organisations à orchestrer de manière globale la sécurité de leurs systèmes.

ESET PROTECT est une plateforme unifiée qui déploie une protection complète contre toutes les formes de malware, y compris les ransomwares, et prévient les menaces de type zero-day sur tous les endpoints, les serveurs et les messageries.

VUE D'ENSEMBLE

Grâce à ESET PROTECT, les entreprises bénéficient d'une vue d'ensemble complète de leur sécurité. La plateforme centralise la gestion des menaces et la réponse aux incidents. Elle fournit une visibilité totale sur les risques de sécurité à travers une console unique. Cela octroie une meilleure coordination entre les équipes informatiques et métiers, et améliore la réactivité face aux incidents de sécurité.

65 %

des entreprises victimes d'une cyberattaque ont subi un impact négatif sur leur activité les cybercriminels est insoutenable.

70 %

des entreprises victimes ont opté pour une assurance cyber les cybercriminels est insoutenable.

69 %

des entreprises victimes estiment que le coût de la lutte contre les cybercriminels est insoutenable.

AVANTAGES CLÉS DE LA PLATEFORME

Cette plateforme prodigue de nombreux bénéfices :

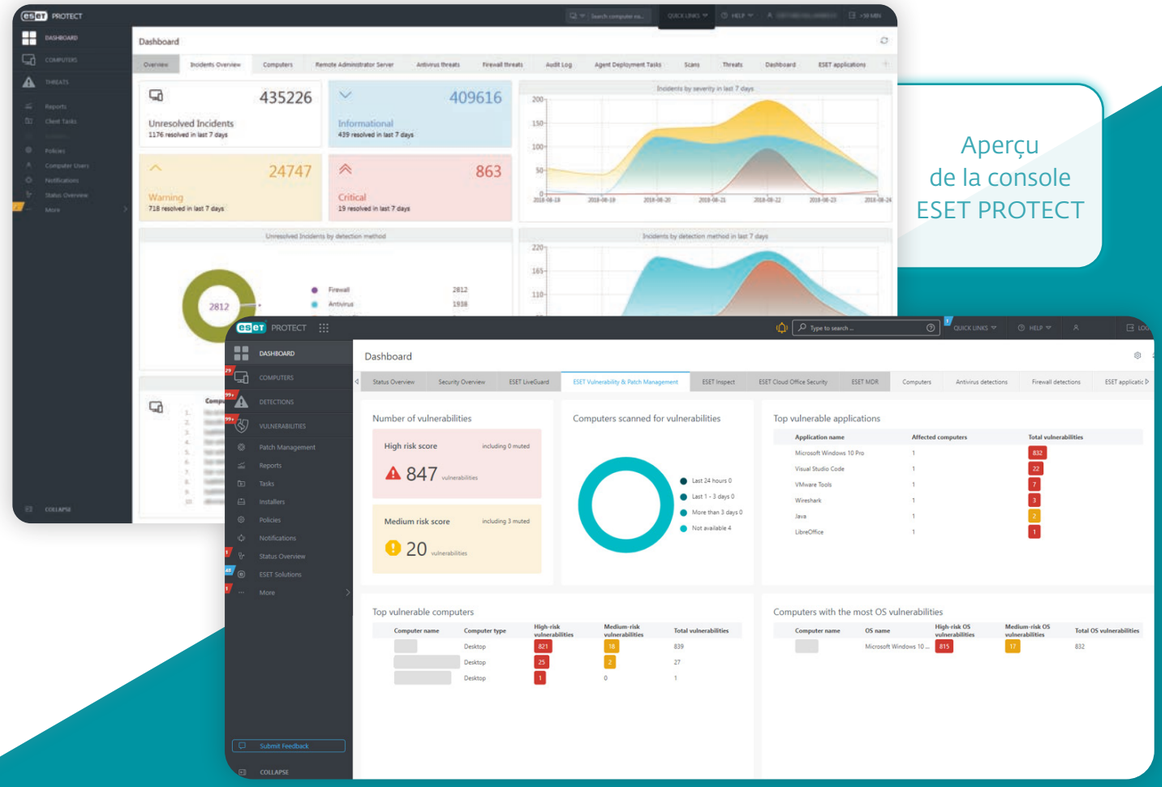
- **Réduction de la complexité :** ESET PROTECT simplifie la gestion de la sécurité grâce à des workflows automatisés et une administration centralisée.
- **Flexibilité et contrôle :** la fonctionnalité multiplateforme et les options de personnalisation permettent de gérer la sécurité de manière flexible et adaptée aux besoins spécifiques de chaque organisation.personnalisation permettent de gérer la sécurité de manière flexible et adaptée aux besoins spécifiques de chaque organisation.
- **Prévention proactive :** la plateforme utilise l'intelligence artificielle et l'expertise humaine pour détecter et neutraliser les menaces avant qu'elles ne causent du tort.

ESET déploie des outils avancés pour la gestion des vulnérabilités et des correctifs.

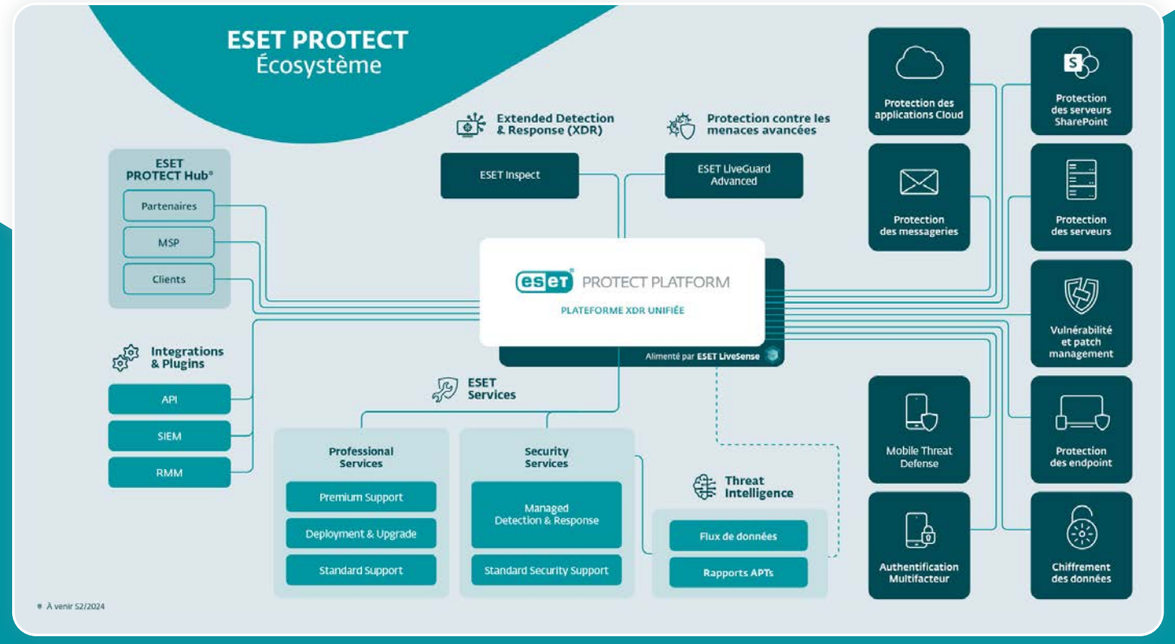
De plus, une plateforme complète propose une sécurité globale et intégrée. En utilisant ESET Vulnerability & Patch Management avec ESET PROTECT, les entreprises développent une protection efficace de leurs systèmes, minimisent leur exposition aux cyberattaques, et restent conformes aux exigences réglementaires et aux meilleures pratiques de l'industrie.

Cela se traduit par une sécurité renforcée, une meilleure gestion des risques et une réduction des coûts opérationnels associés à la gestion de la sécurité informatique.

Par sa capacité à intégrer une protection de pointe dans une solution de gestion unifiée et facile à utiliser, ESET se positionne comme le partenaire idéal pour les entreprises qui souhaitent renforcer leur cyberdéfense.



Aperçu de la console ESET PROTECT



La plateforme ESET PROTECT fournit une **visibilité approfondie** sur le réseau ainsi que des **fonctionnalités étendues**. Le tout à partir d'un tableau de bord unique et intuitif.

Conclusion

Synthétiser et agir

Tout au long de ce livre blanc, vous avez découvert les complexités de la détection des vulnérabilités et de la gestion des patchs dans le contexte de la cybersécurité actuelle. Les points suivants résument les éléments fondamentaux à retenir.

1.

Les vulnérabilités non détectées peuvent mener à des compromissions majeures. La solution ESET Vulnerability & Patch Management permet d'appliquer un patch au plus vite, dès qu'il est édité.

2.

La mise en œuvre rapide des correctifs protège les systèmes contre les failles connues. Une gestion pertinente des correctifs réduit considérablement le champ d'exposition aux menaces.

3.

Les outils d'ESET offrent des capacités d'automatisation et de personnalisation avancées qui facilitent et accélèrent l'application des patchs, permettant ainsi aux entreprises de se concentrer sur leur cœur de métier.

4.

ESET fournit une solution intégrée qui aide à la gestion des vulnérabilités et des correctifs. Elle propose également une protection globale contre un large éventail de menaces, y compris les ransomwares et les attaques zero-day.

À propos d'ESET

Quand la technologie engendre le **progrès**, ESET est là pour **le protéger**.

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour offrir une protection complète et multicouche contre les menaces de cybersécurité aux entreprises et aux particuliers du monde entier.

ESET est depuis longtemps un pionnier des technologies de machine learning et dans le Cloud qui préviennent, détectent et traitent les malwares. ESET est une société privée qui encourage la recherche et le développement scientifiques dans le monde entier.

Canon

protégé par ESET depuis 2016
plus de 32 000 endpoints

T · ·

partenaire FAI depuis 2008
2 millions d'utilisateurs

Allianz Suisse

protégé par ESET depuis 2016
plus de 4 000 boîtes mail

MITSUBISHI MOTORS
Drive your Ambition

protégé par ESET depuis 2017
plus de 9 000 endpoints

Plus de 30 ans
d'innovation continue

1er éditeur Européen
de solutions de sécurité

Focus continu sur la
technologie

Croissance continue
depuis sa création

www.eset.com/fr