Réduire la complexité de la cybersécurité

Une approche critique pour une cybersécurité axée sur la prévention

Digital Security
Progress. Protected.

Table des matières

Introduction

Les logiciels ont conquis le monde il y a de nombreuses années, et vont maintenir leur emprise grâce à de nouveaux développements tels que l'essor de l'IA. Malheureusement, les progrès des logiciels continueront d'introduire des risques que les entreprises ont déjà des difficultés à gérer, et les équipes de sécurité trouveront leur travail beaucoup plus difficile qu'il ne devrait l'être. Le coupable ? **La complexité de la cybersécurité**.

Même les petites entreprises dont l'infrastructure informatique est théoriquement plus réduite ne sont pas épargnées par le problème de la complexité. Par exemple, les problèmes de compétences généralisés rendent la gestion d'outils complexes encore plus difficile. Le télé-travail, qui est courant dans la plupart des entreprises, peut étendre la surface d'attaque et la complexité informatique de manière imprévisible lorsque les employés utilisent leurs propres appareils et des réseaux personnels non sécurisés.

Il est essentiel que les équipes informatiques et de sécurité trouvent des moyens plus efficaces et plus cohérents de surmonter cette complexité pour trai-ter les menaces multivecteurs qui évoluent rapidement.

Pour répondre à cette problématique, ESET a compilé ce livre blanc, qui offre un aperçu essentiel des principaux défis auxquels les organisations sont confrontées dans leur lutte contre la complexité de la cybersécurité. Et plus important encore, il fournit des stratégies et des conseils pratiques pour réussir.

Vous apprendrez notamment comment les éléments suivants peuvent contribuer à **réduire la complexité** :

- L'IA et l'automatisation, qui permettent de faire monter en compétence les équipes de sécurité et **réduire les efforts manuels** tout en augmentant la productivité
- La **protection** holistique **multicouche** fournie par une plateforme unique pour lutter de manière proactive contre les menaces tout en améliorant la visibilité sur l'environnement
- L'**externalisation** de certaines opérations de sécurité (SecOps) auprès d'un prestataire tiers de services de détection et en réponse managées (**MDR**)
- Une **approche Zero Trust** qui peut atténuer les risques liés au télétravail et à l'accès aux données à distance

80 %

des entreprises

reconnaissent que l'utilisation de plusieurs solutions ponctuelles nuit à l'efficacité de leurs équipes en ce qui concerne la détection, la réponse et la reprise après un incident.

Source : *Indice CISCO de préparation à la cybersécurité, 2024.*

S'attaquer à la complexité est l'une des premières étapes de la mise en œuvre d'une approche de la cybersécurité axée sur la prévention, conçue pour minimiser les cyber-risques en remédiant aux processus, aux solutions ou même aux services de sécurité conçus de manière inefficace.

L'objectif est de **créer des SecOps efficaces** pour renforcer la cyber-résilience sans compromis.

Comprendre la complexité de la cybersécurité

Que signifie exactement la complexité dans le contexte de la cybersécurité ? Cela comporte plusieurs aspects et pourrait notamment signifier :

1. **Nombre et type d'outils de sécurité** que les équipes informatiques doivent gérer et les processus qu'elles doivent suivre pour assurer la sécurité d'une organisation.

2. De même, cela pourrait concerner les **systèmes informatiques distribués et hétérogènes** qu'ils doivent défendre : téléphones mobiles, ordinateurs, réseaux Cloud étendus par le télétravail.

3. Et bien sûr, il peut s'agir de l'**évolution rapide du paysage des menaces**, que de nombreuses équipes de sécurité internes ont des difficultés à suivre.

En fait, l'un des plus grands défis que doivent relever ces professionnels de la sécurité informatique, souvent débordés et manquant de ressources, est la vitesse à laquelle apparaissent de nouvelles tactiques, techniques et procédures (TTP) des auteurs de menaces.

Leur travail est également rendu beaucoup plus difficile par le fait qu'ils doivent travailler avec des **données cloisonnées**, des **outils difficiles à utiliser** et des **budgets limités** tout en étant confrontés à une surface d'attaque étendue et en expansion.

À quoi ressemble la cybersécurité ?

En définitive, la complexité est un grand ennemi de la cybersécurité. C'est pourquoi la compréhension de l'impact qu'elle peut avoir sur une entreprise typique est la première étape pour la résoudre. On la trouve principalement dans :

DES OUTILS ET DES SOLUTIONS MULTIPLES

La direction des entreprises considère souvent la cybersécurité comme une question secondaire. C'est regrettable, car les dépenses réactives à la suite d'un incident ou d'une failles de sécurité sont généralement fragmentés et conduisent à des investissements dans des solutions ponctuelles qui ne répondent qu'à un seul cas d'utilisation.

Ainsi, plutôt que de **résoudre la cause sous-jacente d'une atteinte à la sécurité**, ces solutions se concentrent sur un seul aspect de l'infrastructure de sécurité, ce qui complique les tâches quotidiennes de l'équipe informatique. Cela pousse les équipes de sécurité à travailler en mode « chaise tournante », en devant constamment passer d'une interface à l'autre et d'un portail d'administration à l'autre.

Les entreprises de taille moyenne de 1 à 5 000 postes utilisent environ

51

solutions

dans leur organisation.

Source : *Pentera : Enquête sur l'état du pentesting en 2024*.

Les grandes entreprises de 10 000 postes utilisent environ

58

solutions

dans leur organisation.

Source : *Pentera : Enquête sur l'état du pentesting en 2024*.

Quoi qu'il en soit, les menaces se cachent invariablement dans le manque d'interopérabilité et de visibilité créé par ces outils. Par ailleurs, une grande partie du temps du service informatique est consacrée à l'apprentissage de nouveaux outils plutôt qu'à la résolution de problèmes importants. Une entreprise moyenne utilise des dizaines de solutions de sécurité, et la plupart prévoient d'augmenter le nombre de fournisseurs dans leur infrastructures au cours des prochaines années.

COMPLEXITÉ DES OUTILS DE SÉCURITÉ

Il n'y a pas seulement trop d'outils de sécurité. Ceux dont disposent les entreprises sont souvent trop complexes, avec des interfaces peu intuitives ou des flux de travail médiocres. Cela peut **éroder la productivité** des équipes déjà en sous-effectif et les **empêcher d'optimiser toutes les fonctionnalités** à leur disposition.

Dans d'autres cas, les solutions pour grandes entreprises telles que SIEM sont achetées mais largement inutilisées parce que l'entreprise ne peut pas consacrer les ressources nécessaires à leur configuration et leur administration en continu.

TÉLÉTRAVAIL ET BYOD (APPAREILS PERSONNELS UTILISÉS POUR TRAVAILLER)

La complexité s'étend au-delà des outils de sécurité d'une organisation. Aujourd'hui, les entreprises sont plus nombreuses que jamais à bénéficier de la flexibilité qu'offre le télétravail à leurs employés. Aux États-Unis, près d'un tiers des salariés à des rôles professionnels, de direction ou similaires travaillent à domicile.

Cela se traduit généralement par un personnel plus heureux et plus productif, voire une réduction potentielle des coûts des bâtiments/bureaux. Mais ces mêmes organisations sont également exposées à un cyber-risque supplémentaire.

Le télétravail signifie que les employés peuvent se connecter à partir d'appareils et d'ordinateurs portables non protégés ou non corrigés, potentiellement à partir de réseaux personnels ou publics non sécurisés. Cela pourrait **mettre en péril les mots de passe de l'entreprise et fournir une voie d'attaque non surveillée** aux auteurs de menaces pour atteindre les réseaux et les données de l'entreprise.

73 %

des cadres dirigeants de services informatiques

estiment que les télétravailleurs présentent un risque plus élevé que les collaborateurs sur site.

Source : *OpenVPN : Enquête OpenVPN sur la cybersécurité des télétravailleurs, 2024*.

La protection de cet environnement informatique distribué peut entraîner des coûts d'administration et des casse-tête supplémentaires, surtout si l'on considère le nombre d'appareils internes et externes différents qu'une entreprise doit surveiller en même temps.

UN PAYSAGE DES MENACES ÉVOLUANT RAPIDEMENT

Le paysage des menaces est en constante évolution. À mesure que les défenseurs des réseaux et les fournisseurs de solutions de sécurité continuent de mettre en place des protections, leurs adversaires trouvent de nouveaux moyens de les contourner, dans une course aux armements sans fin. Les auteurs de menaces ont l'avantage de la surprise et n'ont besoin d'être chanceux qu'une seule fois pour pénétrer dans un réseau ou un entrepôt de données d'entreprise.

Ils disposent de nombreux moyens pour ce faire, grâce aux investissements continus dans l'infrastructure Cloud, les logiciels, les API et autres technologies numériques, qui ouvrent de nouvelles possibilités d'attaque.

Le nombre de vulnérabilités et d'expositions communes (**CVE**) **nouvellement découvertes** a atteint des sommets au cours de ces dernières années, tandis que l'on prévoit que de nouvelles TTP rendues possibles par l'IA augmenteront le volume et l'impact d'attaques telles que les ransomwares. Les chaînes d'approvisionnement complexes offrent aux adversaires des possibilités supplémentaires d'atteindre leurs cibles, et les mots de passe volés restent un talon d'Achille. L'utilisation d'identifiants volés a été à l'origine de près d'un tiers (31 %) des atteintes à la sécurité au cours de la dernière décennie, ce qui peut constituer un défi à gérer même pour les entreprises disposant de ressources suffisantes.

93 %

des entreprises

ont subi une atteinte à leur cybersécurité en raison de faiblesses dans leur chaîne d'approvisionnement / fournisseurs tiers en 2023.

Source : *Étude de cybersécurité WSJ Pro : Guide de gestion du cyber-risque pour les tiers*.

Le nombre de détections d'exploitations de vulnérabilités uniques

a augmenté de

68 %

au cours des cinq dernières années, ce qui indique une diversification des méthodes d'attaque.

Source : *Fortinet : Rapport sur le paysage mondial des menaces, 2023*.

PÉNURIES ET LACUNES EN MATIÈRE DE COMPÉTENCES DANS LA CYBERSÉCURITÉ

Un autre problème pour les petites et moyennes entreprises est que leurs équipes informatiques comportent rarement suffisamment de personnel dédié à la cybersécurité. Le déficit mondial de main-d'œuvre dans le domaine de la cybersécurité s'élève aujourd'hui à près de cinq millions, en augmentation de 19 % par an. Les petites entreprises qui ne sont pas en mesure de proposer les salaires de leurs homologues plus importantes ne peuvent acquérir les talents nécessaires.

Ces pénuries de compétences sont exacerbées par les contraintes budgétaires qui peuvent être plus dures pour les PME que pour les grandes entreprises, et par les outils et les processus de sécurité à forte intensité de main-d'œuvre qui réduisent la productivité. Le **personnel surchargé** est également plus susceptible de commettre des erreurs. Les lacunes en matière de compétences constituent un autre problème.

Un quart seulement (26 %) des recruteurs interrogés par l'ISACA estiment qu'au moins la moitié de leurs candidats sont bien qualifiés, le Cloud (47 %) et les contrôles de sécurité (35 %) étant deux des trois principaux domaines touchés par le manque de compétences.

Alors que la technologie continue de progresser et de devenir plus complexe, le danger est que **les compétences de sécurité informatique ne suivent pas le rythme**, ce qui donne un avantage supplémentaire aux auteurs de menaces.

SURCHARGE DE DONNÉES

Du point de vue des SecOps, le **grand nombre de solutions ponctuelles** utilisées par de nombreuses organisations **peuvent générer des données et des alertes** à un rythme effréné, et submerger les analystes au point de les empêcher d'établir correctement des priorités.

Les équipes perdent du temps à traiter des faux positifs et laissent des faux négatifs se faufiler et causer des dommages. Cela peut également conduire à du stress et à l'épuisement professionnel, ce qui a pour effet d'exacerber les tensions entre les collègues restants. La moitié des professionnels de la cybersécurité affirment avoir déjà vécu un épisode d'épuisement et 65 % ont envisagé de quitter leur emploi en raison du stress.

47 %

des travailleurs numériques

avaient des difficultés à trouver les informations dont ils ont besoin pour accomplir efficacement leur travail en raison du nombre croissant d'applications utilisées sur le lieu de travail en 2023.

Source : *Communiqué de presse de Gartner : L'enquête de Gartner révèle que 47 % des travailleurs numériques ont des difficultés à trouver les informations nécessaires pour accomplir efficacement leur travail, 2023*.

46 %

des personnes interrogées

chargées de la cybersécurité décrivent les effectifs actuels de l'équipe de cybersécurité de leur organisation comme « quelque peu insuffisants » en 2023.

Source : *Rapport de l'ISACA sur l'état de la cybersécurité dans le monde en 2023*.

Focus sur la prévention pour vaincre la complexité

Il n'est pas facile de s'attaquer à ce type de complexité. Mais avec une **approche axée sur la prévention** comme principe directeur, toute entreprise peut y parvenir. Pourquoi la prévention est-elle la plus judicieuse ?

En se concentrant sur le renforcement de la résilience des systèmes par une **meilleure cyber-hygiène**, en **bloquant d'emblée les menaces** et en **détectant et en contenant rapidement** celles qui se faufilent, les organisations ont les meilleures chances d'atténuer les risques avant qu'ils ne s'aggravent. Il s'agit d'améliorer la première ligne de défense, car la prévention est toujours meilleure (et moins chère) que la remédiation.

La prévention nécessite une sécurité robuste mais simple à mettre en œuvre, fortement automatisée, prête à l'emploi, sans aucune maintenance et conçue pour les PME, au prix correspondant. En bref, elle devrait privilégier **la simplicité à la complexité**. Dans cette optique, voici comment relever les défis de la complexité cités plus haut :

CONSOLIDATION DES OUTILS Une réponse simple à la surabondance d'outils consiste à consolider la sécurité axée sur la prévention sur une plateforme unique d'un fournisseur de confiance. C'est notamment ce que la plateforme **ESET PROTECT** propose. À partir d'une seule interface, elle protège l'ensemble de l'environnement informatique : endpoints, serveurs, appareils mobiles, applications Cloud et messagerie électronique.

Il s'agit d'assurer la prévention, la détection et la recherche proactive de menaces à partir d'un seul endroit, en comblant les lacunes de sécurité et en réduisant la charge de travail des équipes informatiques sous pression. La plateforme comporte également des intégrations transparentes avec des produits tiers qui augmentent encore sa valeur, réduisant ainsi la nécessité de recourir à des environnements de type « chaise tournante ».

Les technologies multicouches, notamment HIPS, Advanced Memory Scanner, UEFI Scanner, Deep Behavioral Inspection, Botnet Protection et DNA Detections, fonctionnent ensemble dans **ESET LiveSense**. Elles remplissent un large éventail de fonctions à partir d'une plateforme unique : blocage des malwares, signalement des comportements suspects et protection contre les botnets et les menaces ciblant les microprogrammes UEFI, entre autres.

INTERFACE UTILISATEUR SIMPLIFIÉE Les outils de cybersécurité ne sont pas tous complexes à utiliser. **ESET PROTECT** est facile à déployer et à utiliser grâce à son interface conçue pour le Cloud et cohérente sur l'ensemble de ses fonctionnalités. Sa console d'administration est accessible en tout lieu depuis n'importe quel appareil, et les tableaux de bord et les rapports peuvent être personnalisés en fonction des besoins de l'organisation. Un degré élevé d'automatisation intégrée permet d'optimiser davantage l'expérience utilisateur, tandis que

des fonctionnalités d'IA telles que le **générateur d'incidents** et **ESET AI Advisor** simplifient le travail des analystes de SecOps.

APPROCHE ZERO TRUST L'approche **Zero Trust** est la meilleure pour réduire les risques ciblant les environnements informatiques distribués, dans le Cloud et mobiles. Son principe est de ne faire confiance à personne par défaut. Cette approche implique une vérification fréquente de tous les utilisateurs et de tous les appareils, la mise en œuvre de politiques d'accès au moindre privilège, la segmentation du réseau, une surveillance continue, le chiffrement renforcé, etc.

La sécurité Zero Trust permet de maintenir des contrôles d'accès stricts, car elle est conçue pour réduire les risques que des acteurs malveillants accèdent aux réseaux d'entreprise et aux ressources dans le Cloud, et minimiser les possibilités d'effectuer des actions malveillantes s'ils y pénètrent.

ESET PROTECT offre de nombreuses fonctionnalités pour prendre en charge la sécurité Zero Trust : administration intégrée de la sécurité et de la protection des endpoints, chiffrement intégral des disques, sandbox Cloud, protection des applications Cloud, et plus encore. **ESET Secure Authentication** est un autre composant clé qui prend en charge l'authentification multifacteur (MFA).

DÉTECTION ET RÉPONSE MANAGÉES (MDR) Les pénuries de cybercompétences sont difficiles à combler sans une action globale et à long terme de la part des gouvernements et des éducateurs. Cependant, afin d'atténuer ce défi, les organisations peuvent externaliser certains aspects de leurs opérations lorsqu'il existe des solutions alternatives à forte valeur mais économiques.

ESET PROTECT MDR propose justement une telle option. La solution élimine la nécessité d'un investissement coûteux dans les technologies de SecOps, ainsi que les dépenses liées au personnel et à la formation continue. Mieux encore, elle garantit que les analystes experts d'ESET bien au fait des dernières études et informations sur les menaces, surveillent en permanence les environnements des clients 24/7/365 avec recherche des menaces et surveillance continues, afin que le personnel informatique interne puisse se concentrer sur d'autres priorités.

Elle peut également réduire les délais de détection des menaces, de 277 jours habituellement (ou 16 heures pour un SOC professionnel) à moins de 30 minutes, ce qui réduit considérablement les risques d'atteinte à la sécurité des données et les complications à long terme qui en découlent.

DÉFENSE PROACTIVE Les auteurs de menaces peuvent sembler avoir toutes les cartes en main. Mais en déployant l'IA dans le Cloud, sur les endpoints et sur l'ensemble du réseau, les entreprises peuvent analyser de vastes volumes de données, repérer les comportements suspects de manière proactive et stopper les menaces avant qu'elles n'aient une chance d'avoir un impact.

ESET PROTECT combine les données de la télémétrie du client avec la technologie **ESET Threat Intelligence** des experts de renommée mondiale d'ESET, ce qui permet d'obtenir des informations globales uniques sur tous les endpoints du réseau.

AUTOMATISATION ET IA En fait, l'IA et le machine learning (ML) peuvent jouer un rôle de taille pour minimiser la complexité de la cybersécurité des entreprises. Face à la surcharge de données et d'alertes qui affecte de nombreux analystes de SecOps, les assistants d'IA générative (GenAI) peuvent fournir des informations intuitives à partir de grands volumes de données, ce qui permet de mieux hiérarchiser les alertes et prendre des décisions éclairées.

C'est ce que fait **ESET AI Advisor**, qui s'intègre de manière transparente aux flux de travail quotidiens pour aider les équipes de SecOps à rationaliser leur utilisation de la technologie **XDR** et la Threat Intelligence. Ce faisant, il contribue également à combler les lacunes potentielles en matière de compétences dans la fonction en interagissant avec les analystes en langage naturel.

L'automatisation intelligente, qui s'appuie souvent sur l'IA, peut également réduire la charge de travail des équipes de sécurité en s'occupant des tâches manuelles et fastidieuses d'application de correctifs et de remédiation des incidents. **ESET PROTECT** est doté de flux de travail automatisés permettant de réduire les erreurs humaines, d'améliorer les résultats de sécurité et de concentrer les ressources limitées du personnel sur les tâches les plus importantes, tout en minimisant la complexité de la cybersécurité. Il permet même à de nombreux administrateurs informatiques d'éviter d'avoir à se connecter à la plateforme.

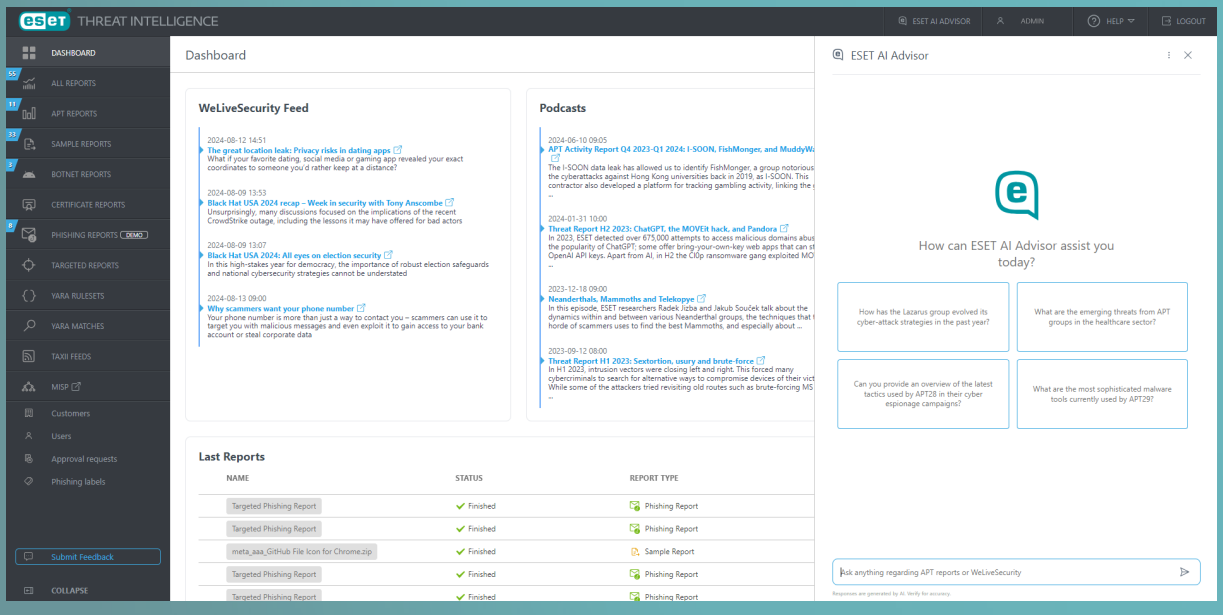

Image 1 : *Intégration d'ESET AI Advisor dans la console ESET Threat Intelligence.*

Conclusion : La simplicité au service des résultats

La plupart des entreprises ambitieuses se concentrent sur une croissance durable, mais cela n'est possible que si elles s'appuient sur des fondations sûres et robustes. La sophistication des menaces modernes et la complexité des systèmes informatiques et de l'infrastructure de sécurité des entreprises rendent cette tâche encore plus difficile. Les pénuries de compétences et les lacunes de sécurité ne font qu'aggraver le problème.

Cela représente une menace potentiellement importante pour leur activité. Un rapport de PwC affirme que la complexité de la cybersécurité pourrait entraîner des pertes financières liées à des atteintes à la sécurité des données, l'impossibilité d'innover et une réduction de la résilience opérationnelle.

La simplification devrait donc être une priorité pour les responsables informatiques. Heureusement, de nombreuses solutions sont disponibles. En regroupant la prévention, la détection et la recherche proactive de menaces sur une plateforme unique, intuitive et hautement automatisée comme **ESET PROTECT**, les équipes informatiques peuvent éliminer la complexité et optimiser les ressources internes.

Elles peuvent également se tourner vers un service managé comme **ESET MDR** pour réduire encore davantage la complexité de leurs opérations de sécurité. En prenant les devants de cette manière, elles seront en mesure de bloquer la plupart des menaces, et de trouver et contenir rapidement les autres.

ESET PROTECT est votre guichet unique pour ce type d'approche axée sur la prévention. Il réduit non seulement la complexité de l'administration, mais comprend également toutes les fonctionnalités robustes dont vous avez besoin aujourd'hui, dans une plateforme sécurisée pour l'externalisation de l'XDR et la mise en œuvre d'initiatives Zero Trust pour demain. En bref, c'est une feuille de route optimisée pour un avenir plus simple et plus sûr.

Découvrez les avantages des services de MDR d'ESET qui combinent l'IA et l'expertise humaine pour bénéficier d'une détection des menaces sans pareille et une réponse rapide aux incidents, et qui évitent de recourir à des spécialistes de la sécurité en interne.

EN SAVOIR PLUS

À propos d'ESET

Défense proactive.
Notre activité consiste à minimiser la surface d'attaque.

Prenez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre **approche préventive reposant sur l'IA et l'expertise humaine**.

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 protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie.

Prévention multicouche

IA de pointe associée à une expertise humaine

Threat Intelligence de renommée mondiale

Support hyperlocal et personnalisé

Digital Security
Progress. Protected.