Livre blanc

Passer de l'EDR au XDR : quand franchir le pas

kaspersky bring on the future

Passer de l'EDR au XDR : quand franchir le pas

Il n'est plus nécessaire pour une organisation d'être médiatisée pour représenter un risque élevé. Cela témoigne d'un virage décisif dans le domaine de la cybersécurité. Traditionnellement, seules les grandes organisations étaient considérées comme des cibles rentables pour des cyberattaques plus avancées, ce qui justifiait des solutions de sécurité robustes destinées aux grandes entreprises. Toutefois, ces dernières années ont montré que les entreprises de taille moyenne sont devenues des cibles lucratives et stratégiques pour des attaques sophistiquées du même type.

Cette évolution oblige de nombreux directeurs des systèmes d'information (DSI) et spécialistes de la sécurité informatique à repenser leurs stratégies de cybersécurité. De plus, de nombreuses solutions actuelles — notamment celles utilisées par de petites équipes de sécurité ou des services informatiques plus généraux — ne suffisent plus à faire face au nombre croissant de menaces et à leur complexité.

Pourquoi les entreprises de taille moyenne deviennent-elles des cibles privilégiées pour les cybercriminels ?

Les entreprises dotées de petites équipes de cybersécurité sont devenues les cibles privilégiées des cyberattaques les plus avancées. D'après nos constats, les PME subissent en moyenne 16 attaques par an, et les grandes entreprises jusqu'à 18, selon leur secteur d'activité.[1] Mais pourquoi cet intérêt pour les petites entreprises qui, à première vue, ne devraient pas avoir besoin d'une protection aussi élevée ?

Un premier pas vers des organisations plus importantes

De nombreuses petites organisations constituent des liens essentiels avec les grandes entreprises. Les cybercriminels examinent souvent le réseau dans son ensemble et exploitent le point d'entrée le plus facile. Cela leur permet de perturber l'ensemble de la chaîne d'approvisionnement et de causer des dommages en cascade. Rien qu'en 2025, 54 % des grandes organisations citent les interdépendances de la chaîne d'approvisionnement comme le principal facteur de la complexité croissante de la cybersécurité.[2] Mais si les grandes organisations ont enregistré une augmentation de leur cyberrésilience par rapport à 2024, les petites organisations restent désavantagées, 35 % d'entre elles déclarant une cyberrésilience insuffisante.[2]

Un manque de personnel qualifié

La plupart des petites équipes de cybersécurité souhaitent améliorer leurs capacités de détection des menaces et de réponse aux incidents, mais ne disposent pas des ressources ou du budget nécessaires. En effet, selon des études récentes, 41 % des professionnels de la sécurité informatique déclarent une pénurie de personnel « légère » à « sévère » parmi les équipes de cybersécurité de leur organisation.[3] Bien souvent, cela signifie que les PME se reposent largement sur le personnel informatique général pour gérer les tâches liées à la cybersécurité. Non seulement cette situation met à rude épreuve les petites équipes, mais elle expose également les entreprises à des cybermenaces accrues en raison d'un manque de formation spécialisée. Malheureusement, les cybercriminels connaissent cette vulnérabilité et l'exploitent facilement.

Des cibles faciles pour des outils sophistiqués

Les organisations de taille moyenne se sont révélées des cibles faciles, beaucoup d'entre elles ne disposant pas de la cybersécurité nécessaire pour les protéger correctement contre les menaces complexes. Toutefois, être une « cible facile » peut s'expliquer par l'équipe informatique, mais aussi car les menaces sophistiquées sont plus faciles à déployer que jamais. Les petites entreprises utilisent généralement des solutions de sécurité informatique plus simples, comme la sécurité réseau, les EPP (Endpoint Protection Platforms) ou les CWPP (Cloud Workload Protection Platforms) — des solutions de plus en plus inefficaces face à des cybercriminels qui utilisent des outils sophistiqués pour contourner facilement les protections de base.

Les PME subissent en moyenne 16 piratages par an.[1]

Comment les outils et facteurs modernes facilitent la vie des pirates informatiques

Pour mieux comprendre l'augmentation rapide des attaques complexes, nous devons considérer la cybercriminalité comme plus qu'une simple menace technique, et plutôt comme une entreprise mondiale florissante. Les cybercriminels ont développé des modèles économiques évolutifs qui leur permettent de simplifier leurs opérations, de diversifier leurs sources de revenus et d'innover avec rapidité et précision. La montée en puissance des attaques sophistiquées s'accélère avec l'apparition de multiplicateurs de force : des outils avancés permettent désormais même aux cybercriminels peu expérimentés de lancer ce type d'attaques.

Les tactiques des cybercriminels évoluent constamment, et les nouvelles technologies et faiblesses systémiques permettent des attaques plus efficaces.

Vous trouverez ci-dessous les principaux outils et facteurs qui permettent aux pirates informatiques d'exploiter plus facilement les victimes.

Piratage informatique

Les attaques d'ingénierie sociale, comme le phishing, utilisent des techniques de manipulation qui exploitent votre équipe pour obtenir des informations privées, et les technologies d'IA ont facilité leur déploiement. Par exemple, un chatbot IA axé sur la cybercriminalité peut aider les pirates à créer des emails polis et des demandes Docusign frauduleuses. Avec un minimum d'effort, les attaquants peuvent contourner les signaux d'alerte traditionnels du phishing, personnaliser les e-mails frauduleux et utiliser des techniques de manipulation pour créer un sentiment d'urgence et d'authenticité. D'autres attaques d'ingénierie sociale suivent une approche en plusieurs étapes. L'attaque commence par l'envoi massif de spams qui finissent par forcer les employés à créer des tickets d'assistance légitimes. Les pirates se font ensuite passer pour l'assistance informatique, contactent les employés sur Microsoft Teams et les piègent avec des codes QR malveillants conçus pour fournir des outils de surveillance à distance qui peuvent être exploités pour accéder au réseau.

Spyware en tant que service

Les développeurs de logiciels espions louent ou vendent également l'accès à leurs outils, souvent par l'intermédiaire de forums sur le Dark Web ou de canaux malveillants. Les clients (généralement des pirates informatiques, des États-nations ou des harceleurs) paient pour accéder à des enregistreurs de frappe, des outils d'accès aux microphones/caméras, des kits de surveillance mobile, des outils d'accès à distance (RAT), des outils d'interception des navigateurs et des emails ou des traceurs GPS.

Ces outils peuvent être utilisés pour collecter et transmettre des informations à partir d'un appareil victime à l'insu de l'utilisateur ou sans son consentement.

Les ransomwares en tant que service (RaaS)

Les kits RaaS sont en fait des outils « prêts à l'emploi », qui permettent aux cybercriminels de lancer des cyberattaques sophistiquées avec peu d'intervention. Ils déploient des programmes malveillants capables d'adapter leur code sans effort pour éviter d'être détectés par les systèmes de sécurité (comme les antivirus ou les pare-feu). De nombreux cadres de cybersécurité sont donc insuffisants pour offrir une protection adéquate contre le RaaS, exposant ainsi les entreprises, les gouvernements et les particuliers à des situations à haut risque.[4]

Semblables aux modèles de logiciels en tant que service (SaaS), les kits RaaS permettent aux affiliés d'accéder à des outils de ransomwares, à une assistance technique 24h/24 et 7j/7, à des portails de traitement des paiements et à bien d'autres choses encore, à partir de seulement 40 $ par mois. Pour remettre les choses en perspective, une violation par ransomware moyenne coûte à sa victime 4,91 millions de dollars (y compris les temps d'arrêt, la perte de clients, les amendes, etc.).[5]

Logiciels obsolètes

De nombreuses entreprises peinent à suivre le rythme des correctifs et mises à jour, ce qui peut rendre leurs logiciels vulnérables. Les groupes de ransomwares, en particulier, exploitent les vulnérabilités de type zero-day en sachant qu'ils peuvent devancer la vitesse à laquelle les organisations appliquent les correctifs. En fait, 85 % des vulnérabilités critiques ne sont pas corrigées 30 jours après leur découverte, 47 % sont toujours présentes 60 jours plus tard, et 20 % s'attardent encore six mois après.[6]

En 2024, 41,6 % des incidents étaient liés à des ransomwares, contre 33,3 % en 2023. Les ransomwares devraient rester la principale menace pour les organisations du monde entier dans un avenir proche.[7]

La nécessité d'une protection avancée

Processus perturbés :

- Communications – 41 %
- Support client – 36 %
- Automatisation du marketing – 34 %
- Logistique – 32 %
- Développement/production de produits – 31 %
- CRM, ventes – 27 %
- Achats et paiements – 26 %
- Paie – 17 %

Les atteintes à la sécurité coûtent aux PME 1,5 fois les dépenses consacrées à la cybersécurité.[1]

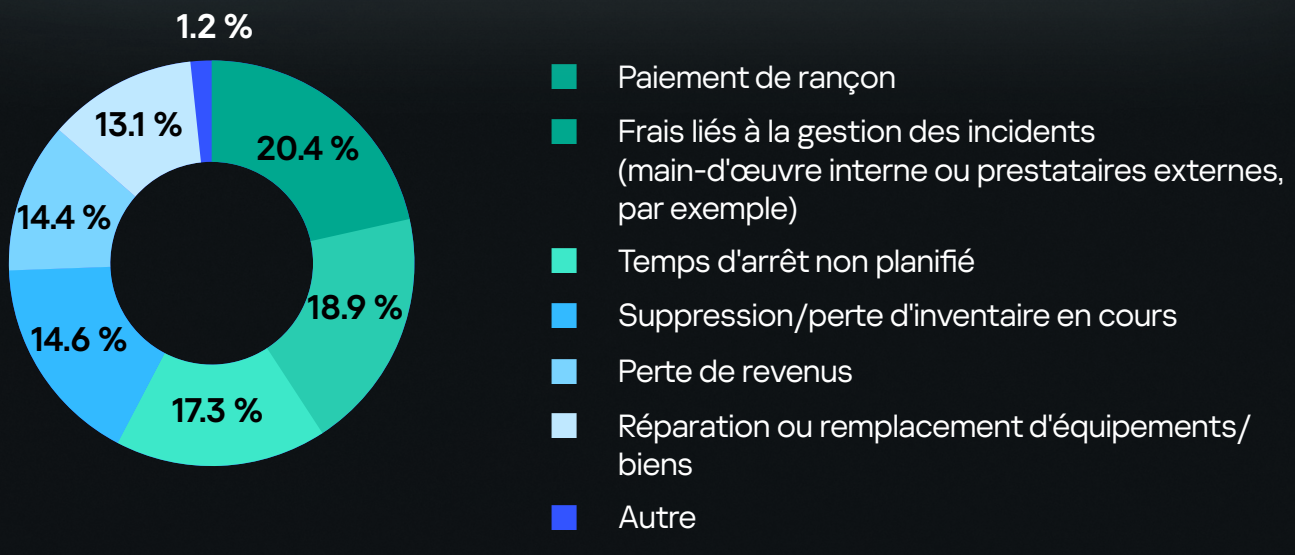
En parallèle de la hausse des cyberattaques complexes, des études récentes montrent que les coûts liés à la perte d'activité et à la gestion des incidents post-violation ont augmenté de près de 11 % par rapport à l'année précédente.[6] Cette hausse s'explique principalement par la sophistication des attaques, qui allongent la durée des cycles de violation.

Les cyberattaques sont désormais inévitables, mais la rapidité de détection et réponse détermine si un incident devient un événement mineur ou une violation catastrophique. Par exemple, en 2024, les trois types de violations par vecteur initial les plus longues à contenir étaient le phishing, les initiés malveillants et le vol/compromission d'identifiants. Il s'agit également de trois des quatre types de violation par vecteur initial les plus coûteuses, ce qui met en évidence le lien entre la durée et les dommages causés.[5]

Plus les pirates opèrent longtemps sans être détectés, plus ils infligent de dégâts. C'est là que le temps moyen de détection (MTTD) devient un indicateur clé de performance dans la gestion des incidents et témoigne de la capacité de votre équipe à détecter ou découvrir un incident. Par conséquent, votre temps moyen de réponse (MTTR) correspond au temps moyen nécessaire pour neutraliser la menace. L'automatisation des opérations de sécurité joue un rôle important dans l'amélioration de ces paramètres. En effet, ceux qui s'engagent dans l'automatisation des processus de sécurité rapportent des progrès, comme une amélioration de 46 % de leur temps moyen de réponse.[8]

La différence entre un incident circonscrit et une véritable catastrophe se résume souvent à la rapidité de la réaction. Le temps moyen de détection (MTTD) ne sert à rien sans temps moyen de réponse (MTTR). En effet, inutile de trouver une menace rapidement si vous ne pouvez pas l'arrêter tout aussi vite. Le temps, c'est de l'argent, et chaque seconde compte. Les organisations qui réagissent rapidement aux violations peuvent économiser des millions, répondre facilement aux exigences réglementaires et protéger leur réputation.

Coût moyen des violations de cybersécurité dans le secteur de l'alimentation et des boissons[9]



Quand l'EDR ne suffit plus

Pendant de nombreuses années, les outils de détection et de réponse au niveau des terminaux (EDR) ont constitué la base de toute stratégie de cybersécurité, à juste titre. L'EDR fournit aux équipes de cybersécurité des données précieuses et des outils de visualisation pour déterminer la cause première de la menace et déterminer si des mesures d'intervention supplémentaires sont nécessaires, surpassant largement les outils antivirus traditionnels en matière de capacité et d'efficacité.

Cependant, le paysage des menaces s'est considérablement développé, de même que l'importance de la réponse aux incidents et de l'investigation des menaces, complexifiant les besoins des organisations à haut risque au point que seules les fonctionnalités XDR peuvent les satisfaire.

Cependant, investir dans une solution XDR complète s'avère souvent impossible pour les petites entreprises sans le matériel, le budget ou le personnel qualifié pour traiter et analyser efficacement les données télémétriques.

Les petites et moyennes entreprises se trouvent donc dans une situation intermédiaire délicate où les solutions actuelles ne suffisent plus, mais où une solution XDR à l'échelle de l'entreprise est trop avancée, trop chère et trop peu pratique pour résoudre les problèmes actuels. Pendant ce temps, la surface d'attaque s'étend et votre équipe est submergée par le nombre d'alertes à analyser.

Mais comment savoir qu'il est temps d'agir ?

La lassitude des alertes pèse sur votre équipe

Si votre organisation utilise une série d'outils de cybersécurité qui génèrent de nombreuses alertes, votre équipe de sécurité informatique peut être rapidement débordée. C'est particulièrement vrai si votre équipe ne dispose pas d'un contexte suffisant pour classer ces alertes par ordre de priorité et les examiner efficacement. Ce processus peut s'avérer fastidieux et votre équipe risque de plus en plus de passer à côté d'une menace imminente si elle travaille manuellement. Votre équipe pourrait même finir en burnout et chercher à partir.

> « Lorsqu'un professionnel de la cybersécurité travaille bien, il ne se passe rien et ses tâches sont principalement routinières : il vérifie les journaux et les règles, examine les comptes et s'assure que les stratégies sont respectées. Ces étapes ne sont pas complexes, mais elles sont essentielles. Les faire manuellement conduit rapidement au burnout. »
>
> Ilya Markelov, responsable de la plateforme unifiée de Kaspersky

Si les plateformes EDR font un bon travail en signalant les anomalies au niveau des terminaux, elles manquent souvent d'un contexte plus général, nécessaire pour comprendre toute la portée d'une attaque. Par conséquent, les analystes sont contraints à un travail de détective. Il est donc essentiel de trouver un moyen de trier efficacement les alertes et d'obtenir une visibilité claire.

La surface d'attaque augmente, mais pas vos ressources

Le renforcement de la sécurité des systèmes est un élément essentiel pour aider les petites et moyennes entreprises à réduire la surface d'attaque. Par essence, le renforcement de la sécurité des systèmes consiste à identifier et à corriger les faiblesses de cybersécurité afin de minimiser les vecteurs d'attaque potentiels et d'éliminer les services ou fonctionnalités inutiles faciles à exploiter pour les pirates informatiques.

Cependant, le maintien de systèmes renforcés nécessite une surveillance et des correctifs permanents pour remédier aux nouvelles vulnérabilités, sans parler du fardeau de rester conforme à des réglementations en matière de cybersécurité fréquemment mises à jour. Il va sans dire qu'un renforcement efficace de la sécurité des systèmes s'avère souvent difficile pour une petite équipe aux ressources limitées.

Vos collaborateurs peinent à faire face à toutes les tentatives de phishing et d'ingénierie sociale

Malgré l'investissement dans l'EDR, vos employés peuvent encore être victimes d'attaques de phishing et d'ingénierie sociale. Il ne s'agit pas d'un échec de l'EDR, mais d'un signe que le paysage des menaces a évolué. L'EDR permet d'identifier les programmes malveillants connus, de surveiller le comportement du système et de signaler les anomalies, mais il n'est pas conçu pour prévenir l'erreur humaine, qui joue un rôle dans 22 % des violations.[5]

Les attaques de phishing n'ont pas besoin d'exploiter une vulnérabilité logicielle, mais une vulnérabilité dans le comportement humain. Un email bien conçu ou une page de connexion usurpée peuvent contourner les plateformes EDR les plus robustes en incitant un employé à fournir des identifiants ou à télécharger des fichiers malveillants.

Si vos employés ont du mal à reconnaître ces types d'attaques, cela indique clairement que votre stratégie de cybersécurité doit aller au-delà de l'EDR. Une défense proactive implique la mise en place d'une culture de la sécurité soutenue par une formation continue et des outils pour faciliter la protection de l'identité. Aller au-delà de l'EDR, c'est s'attaquer à l'ensemble des risques, en particulier ceux causés par l'ingénierie sociale.

Détection trop tardive des attaques

Lorsque les attaquants accèdent à votre système par des canaux légitimes, votre solution EDR peut détecter l'intrusion trop tard, une fois l'accès déjà accordé. IBM a constaté qu'en 2024, les organisations mettaient en moyenne 194 jours pour identifier une violation, et 64 jours supplémentaires pour la contenir.[5] Il ne s'agit pas d'un retard mineur. Il s'agit de nombreux mois d'exfiltration, de mouvement latéral et de persistance potentiels.

Chaque jour où un incident n'est pas détecté augmente le risque de vol de données confidentielles, de compromission des systèmes ou de déploiement d'un ransomware.

La réponse manuelle vous ralentit

Les entreprises dotées de plans de réponse aux incidents solides et régulièrement testés réalisent en moyenne 58 % d'économies par rapport aux autres.[10] Mais qu'est-ce qui rend un plan de réponse aux incidents « solide » ? En bref, il s'agit avant tout de rapidité. Les délais d'exécution des attaques modernes se raccourcissent rapidement : un ransomware peut, par exemple, verrouiller des systèmes critiques en quelques minutes seulement. Dans un paysage de menaces en constante évolution, la réponse aux incidents manuelle ne peut plus suivre le rythme.

Contrairement aux systèmes automatisés, la réponse manuelle est plus lente à réagir aux incidents de cybersécurité et le moindre retard peut entraîner une compromission et un risque plus importants.

L'importance de l'automatisation dans la réponse aux incidents ne doit pas être sous-estimée. En tirant parti de l'automatisation, les équipes peuvent identifier et contrer les menaces en temps réel, ce qui réduit considérablement la fenêtre d'exposition. En outre, cela permet à votre équipe de se concentrer sur d'autres tâches essentielles qui pourraient nécessiter leur expertise, et donc d'économiser du temps, de l'argent et des ressources.

Faut-il aller plus loin ?

Les solutions XDR complètes, bien que cruciales pour la protection contre les menaces avancées, ne correspondent pas encore aux besoins particuliers des petites équipes informatiques et de cybersécurité.

> Les obstacles qui rendent les entreprises de taille moyenne vulnérables aux cyberattaques complexes (budget limité, manque de ressources) sont les mêmes qui les empêchent de mettre en œuvre une protection avancée efficace.

Ces solutions spécialisées sont notoirement complexes à mettre en œuvre et à utiliser et nécessitent souvent une courbe d'apprentissage trop raide pour les petites équipes informatiques. Toutefois, la nécessité d'au moins quelques fonctionnalités XDR devient de plus en plus importante. D'après notre rapport d'analyse MDR, « en 2024, le temps moyen pour enquêter et signaler les cyberincidents a augmenté de 48 % par rapport à 2023, reflétant une augmentation significative de la complexité des attaques. L'analyse des règles de détection déclenchées et des indicateurs d'attaque (IoA), dont la grande majorité provenait d'outils XDR spécialisés, le confirme. Il s'agit d'un tournant par rapport aux années précédentes, au cours desquelles la détection par les journaux du système d'exploitation jouait un rôle important. Dans ce contexte, des outils spécialisés de type XDR deviennent essentiels pour détecter et examiner avec succès les menaces modernes. »[7]

Comment Kaspersky peut vous aider

Protection de niveau 'grande entreprise' optimisée pour les petites structures

Kaspersky NEXT XDR Optimum est conçu pour les petites équipes informatiques et de cybersécurité. Cette solution renforce la réponse aux incidents et développe l'expertise sans alourdir la charge de travail liée aux tâches routinières chronophages.

Grâce à l'automatisation de nombreux processus, vous pouvez vous concentrer sur ce qui compte le plus.

Une protection exceptionnelle des terminaux

Profitez d'une protection automatisée pour éviter les interruptions d'activité. Grâce à des outils anti-ransomwares et anti-malwares basés sur le ML et éprouvés par l'industrie, vous pouvez facilement prévenir les infections provenant de menaces connues et inconnues.

Corrigez les vulnérabilités par le renforcement de la sécurité des systèmes et les formations

Réduisez votre surface d'attaque en renforçant la sécurité de vos systèmes, en fonction du comportement réel de vos utilisateurs. Gagnez du temps grâce à la gestion centralisée des vulnérabilités, des correctifs et du chiffrement, et offrez à votre équipe toutes les formations nécessaires pour tirer le meilleur parti de vos nouvelles capacités en matière de cybersécurité.

Étendez vos capacités de détection et de réponse

Obtenez des informations sur les menaces et sur la manière dont elles se déplacent à l'intérieur et à l'extérieur des terminaux. Utilisez l'automatisation et la réponse guidée pour contrer les attaques, et les outils d'enquête essentiels pour suivre leur activité.

Formez toute votre équipe à jouer un rôle actif en matière de sécurité

Donnez à votre personnel informatique et à vos employés non techniques les connaissances et les compétences nécessaires pour rester en sécurité. Renforcez votre équipe de sécurité informatique tout en instaurant une culture de la sécurité au sein de votre personnel.

Contrôlez le Shadow IT grâce à une sécurité dans le cloud fiable

Réduisez la vulnérabilité de votre entreprise, et protégez vos données ainsi que vos employés en contrôlant le Shadow IT. Déterminez quels services cloud sont utilisés, bloquez les accès non autorisés et identifiez les données confidentielles stockées dans les applications Microsoft 365.

Réduisez la lassitude face aux alertes

La fonction d'agrégation des alertes de Next XDR Optimum, associée à une protection efficace et éprouvée des terminaux, réduit le nombre d'alertes à analyser pour les équipes. Cela augmente l'efficacité et réduit la lassitude liée aux alertes, et permet à votre équipe de se concentrer sur d'autres tâches essentielles.

Le XDR n'est plus réservé aux grandes entreprises

Découvrez une solution supérieure optimisée pour les petites équipes.

Kaspersky Next XDR Optimum

En savoir plus

Bibliographie :

[1] Kaspersky, B2B IT security risk tracker report, (Kaspersky, 2024)
[2] Tuteja, Akhilesh, 5 risk factors from supply chain interdependencies in a complex cybersecurity landscape, (World Economic Forum, 2025)
[3] Kaspersky, A portrait of a modern Infosec professional, (Kaspersky, 2024)
[4] Willie, Alan, The Evolution of Ransomware-as-a-Service (RaaS): AI's Role in Cybercrime and Countermeasures, (Stanford University, 2025)
[5] IBM, Cost of a Data Breach Report 2024, (IBM, 2024)
[6] Verizon, 2024 Data Breach Investigations Report, (Verizon, 2024)
[7] Kaspersky, Fortress under fire: cyber threat chronicles 2024, (Kaspersky MDR Analyst Report, 2024)
[8] Verizon, 2024 Data Breach Investigations Report, (Verizon, 2024)
[9] Kaspersky and VDC Extended Survey Findings, (Securing OT environments, 2024)
[10] IBM, Cost of a Data Breach Report 2022, (IBM, 2022)

www.kaspersky.fr

#kaspersky
#bringonthefuture