BLACKNOISE

EFFICACITÉ DE LA SÉCURITÉ OPÉRATIONNELLE

DEEP PURPLE REPORT 2025

Version 1.0
Publiée le : 15/03/2025

ERIUM

SOMMAIRE

INTRODUCTION

Pour la troisième année, le **Deep Purple Report** de BlackNoise dresse un état des lieux stratégique de l'efficacité des dispositifs de cybersécurité, à partir des retours concrets de simulations d'attaques menées en 2024. Si les capacités de détection progressent, portées par les solutions EDR/XDR, elles restent trop centrées sur les endpoints et doivent désormais évoluer vers une approche globale, capable d'anticiper des attaques plus complexes et ciblées.

Face à un contexte réglementaire exigeant (NIS 2, DORA, TIBER-EU) et des menaces toujours plus sophistiquées, les organisations doivent investir dans la Security Validation : des tests réguliers, automatisés et à grande échelle qui permettent à la fois d'optimiser les technologies existantes, de renforcer la réactivité des équipes opérationnelles et de garantir la continuité des activités.

Plus qu'un enjeu technique, la maîtrise de la détection et de la réponse aux attaques devient un levier clé de résilience, de conformité et de protection du business dans un environnement numérique sous tension économique et géopolitique.

Pierre TEXIER
CTO

Arnaud LE MEN
CEO

Contexte et méthodologie

Le **Deep Purple Report** de BlackNoise synthétise les résultats techniques des simulations exécutées par la solution de BAS[1] au cours de l'année 2024. Cette approche automatisée permet d'évaluer le niveau de détection et de réaction face à différents scénarios d'attaque. Elle met en évidence des indicateurs clés des dispositifs de défense tels que le **MTTD** (Mean Time To Detect) et le **MTTR** (Mean Time To React). Afin de faciliter l'analyse des résultats, tous les tests exécutés par la solution sont liés au modèle ATT&CK du MITRE[2].

La solution attribue un score d'efficacité selon les résultats obtenus à chaque campagne de simulation d'attaques. Ce score dépend de différents critères comme la performance de la détection face à un événement (inexistante, partielle, optimale), la qualification précise de l'événement par les outils et les analystes, la rapidité de la détection, etc.

Les chiffres de 2024

+500
Simulations d'attaques

18k
Evènements techniques

1 Breach & Attack Simulation solution
2 https://attack.mitre.org/
3 ETI : Entreprise de Taille Intermédiaire

Les simulations d'attaques réalisées en 2024 par BlackNoise et prises en compte dans ce **Deep Purple Report** ont ciblé des infrastructures informatiques d'ETIs[3] ou de grands groupes de tous secteurs (public, télécommunications, aéronautique, transport, finance & assurance, service, distribution, …).

La typologie des environnements testés est caractérisée par les éléments suivants :

- Forte représentativité des SI de gestion (plus de 3/4 des campagnes)
- Part des environnements industriels stable par rapport à l'an dernier (~6%)
- Croissance des environnements cloud, avec une amorce des tests ciblant les SaaS par rapport aux années précédentes

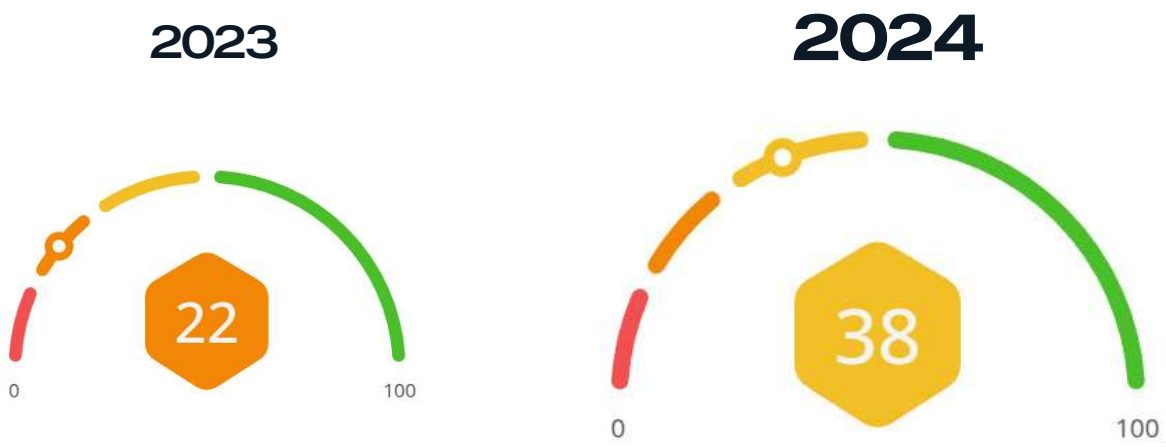
PARTIE 1

RESULTATS DES SIMULATIONS D'ATTAQUES 2024

1.1) Evaluation des capacités de défense

Synthèse

Les capacités de détection progressent de nouveau, tant sur la couverture des techniques d'attaques que sur la rapidité de détection. Elles se concentrent encore très majoritairement sur les endpoints.



Le taux de détection moyen observé par BlackNoise est en **progression par rapport à l'an dernier** (+72%) et démontre une maturité générale plus forte des dispositifs de défense. Cette amélioration est caractérisée au niveau technologique par une maturité et une maîtrise des outils déployés (EDR, XDR/SIEM, NDR, Honeypots, etc.), mais aussi l'expertise et l'organisation des équipes SOC[4] et CSIRT[5] / CERT[6].

Il est à préciser que les chiffres sont assez proches, indépendamment de la typologie du SOC : équipe interne, service externalisé (opéré par un MSSP) ou modèle hybride.

La progression du taux de détection affiche un écart type significatif entre les acteurs qui effectuent des simulations d'attaques régulières et ceux qui démarrent cette activité d'entrainement.

[4] SOC : Security Operations Center
[5] CSIRT : Computer Security Incident Response Team
[6] CERT : Computer Emergency Response Team

LES TOPS 2024

CREDENTIAL ACCESS

1st

DEFENSE EVASION

2nd

PERSISTENCE

3rd

Les 5 techniques ayant le meilleur taux de détection sont :

- T1003: OS Credential Dumping
- T1558: Steal or Forge Kerberos Tickets
- T1562: Impair Defenses
- T1548: Abuse Elevation Control Mechanism
- T1036: Masquerading: Rename System Utilities

LES FLOPS 2024

RECONNAISSANCE

1st

COMMAND & CONTROL

2nd

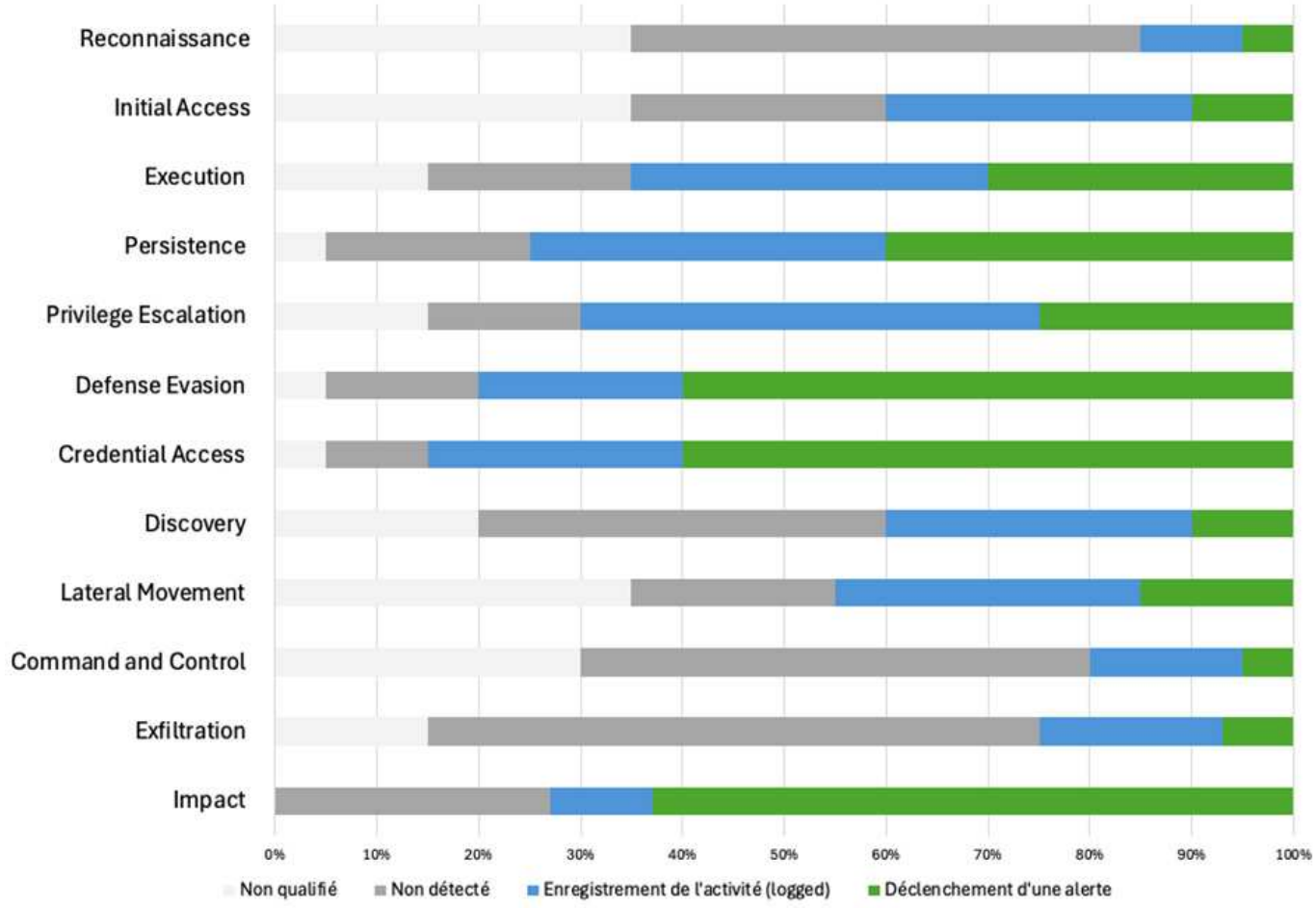
EXFILTRATION

3rd

Les 5 techniques ayant le moins bon taux de détection sont :

- T1048: Exfiltration Over Alternative Protocol
- T1567: Exfiltration Over Web Service: Exfiltration to Cloud Storage
- T1046: Network Service Discovery
- T1087: Account Discovery
- T1078: Valid Accounts: Default Accounts

Projection des capacités de détection observées par BlackNoise selon les tactiques du MITRE ATT&CK®



Il ressort tout d'abord que les mesures de détection s'avèrent plus efficace sur les phases intermédiaires de la Kill Chain (hormis l'impact final). Dans la continuité de notre rapport 2024, le comportement des adversaires est principalement décelé au travers d'**actions sensibles, à fort impact et avec une probabilité de faux positif faible**, réalisées techniquement sur les systèmes d'exploitation. La surveillance se focalise sur la **finalité des attaques** donc principalement **au niveau des endpoints**, et l'EDR, couplé à un XDR/SIEM, sont les atouts majeurs de cette détection.

Les techniques d'attaques associées aux catégories "Credential Access" et "Discovery" ne figurent plus parmi les "Flops". Or de nombreuses méthodes d'exécution associées à ces catégories reposent sur des modes opératoires qui exploitent des techniques dites de « Living-off-the-land » (LOTL). Ce constat démontre une progression, certes maîtrisée mais réelle, de l'identification de ces techniques par les moyens de défense.

Précisions sur les techniques de « Living-off-the-land » (LOTL)

Les techniques de LOTL utilisent des outils, applications ou processus standard qui sont déjà en place sur le système, par exemple powershell, certutil, teams, etc. Les processus Windows natifs suivants ont notamment été observés et testés par BlackNoise : cmd.exe, explorer.exeregsvr32.exe, svchost.exe, taskhost.exe. Ces composants logiciels, utilisés par les administrateurs, sont également employés par les attaquants pour collecter des informations ou exécuter des commandes système. Cette approche complexifie la détection de tels comportements offensifs car elle évite de déployer de nouveaux logiciels et dissimule les traces dans un "bruit" légitime.

Enfin, comme les années précédentes, le **Deep Purple Report** met en évidence qu'il est plus difficile de repérer les premières étapes de la Kill Chain. Les scans réseau massifs, les tentatives de piratage de comptes et les récupérations d'informations techniques sur les systèmes ou l'AD - qui aident à mieux comprendre l'environnement ciblé - sont rarement détectés. Cela s'explique par plusieurs raisons :

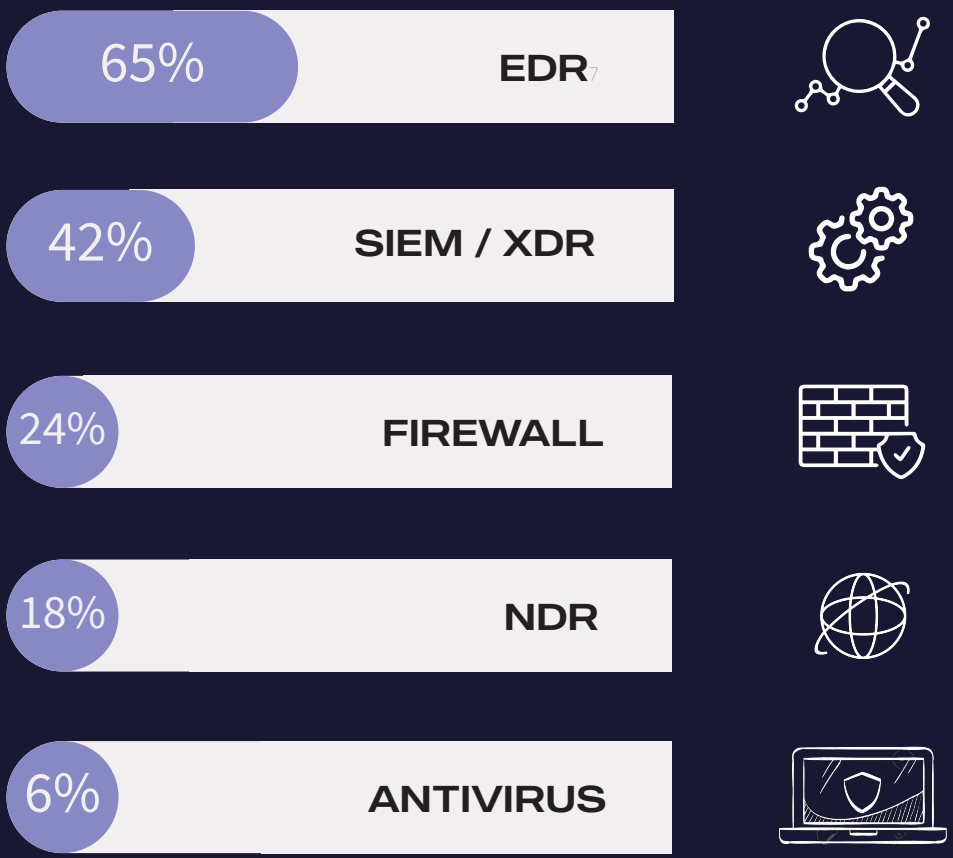
- La capacité de détection de ce type d'activité, dépend des choix technologiques de défense déployés. La surveillance des environnements réseaux est souvent secondaire, parfois ignorée ou simplement désactivée pour limiter la génération d'un volume de donnée trop important.
- Le volume de données généré par la surveillance de ces comportements (comme les scans réseau) pose plusieurs problèmes : un coût de stockage élevé pour les logs, une grande difficulté à trouver des informations utiles dans ce volume de données important, et un seuil de notification mal ajusté qui entraîne trop de faux positifs.

1.2) Focus sur les principales sources de détection

Synthèse

La principale source de détection repose sur l'analyse des comportements d'attaquants décelés sur les endpoints par les EDR/XDR/SIEM. La détection se fait principalement grâce à des règles telles que Sigma ou via des approches heuristiques.

Les 5 principales technologies ayant permis de détecter les simulations exécutées sont les suivantes :



[7] Endpoint Detection and Response. Détecte les comportements anormaux ou malveillants sur les terminaux.
[8] Extended Detection and Response. Plateforme qui corrèle et centralise les données provenant de plusieurs couches de l'infrastructure IT pour détecter les comportements malveillants. Agrège donc des données provenant de différentes sources, pas uniquement des endpoints.
[9] Network Detection and Response. Surveille le trafic réseau pour identifier les activités malveillantes. Contrairement aux firewalls, les NDR sont capables de détecter des menaces en analysant les modèles de trafic et les comportements des utilisateurs et des applications, et pas uniquement via des signatures.

L'EDR demeure encore cette année un **outil essentiel de l'arsenal défensif,** enrichi par des solution globale de type SIEM/XDR, qui renforce l'agrégation de différentes sources permettant de capter des signaux d'origines variées. La **qualité des alertes** générées, associée à un **temps de réaction réduit**, fait indéniablement de ces solutions un atout fondamental pour détecter les actions des adversaires sur les systèmes.

Le pare-feu, qui se concentre sur les menaces de la couche réseau, est désormais complété par des technologies de type NDR, capables de détecter des comportements d'attaques plus élaborés ciblant également les endpoints.

Les organisations disposant des budgets adéquats s'orientent de plus en plus vers l'intégration de solutions complémentaire (EDR, SIEM/XDR et NDR) qui permettent de créer une **défense en profondeur**, capable de détecter et de répondre à une variété de menaces. Les mesures de détection et de réaction **multicouches** vers lesquelles tendent ainsi les organisations apportent une couverture de sécurité redondante, plus complète et proactive. **L'intégration et l'interconnexion accrues des solutions de sécurité**, qui permettent une corrélation des alertes plus efficace, y contribuent fortement.

Il convient de préciser que le déploiement de solutions UEBA[10] apparait dans le radar BlackNoise cette année. Ces solutions constituent un levier stratégique pour détecter proactivement les comportements anormaux, indicateurs potentiels de compromission ou de menace interne, grâce à une approche comportementale surpassant les limites des mécanismes classiques basés sur les signatures. La croissance des usages SaaS, conjuguée à l'augmentation des attaques à l'encontre des services cloud et le renforcement de la maturité de ces solutions de détection, devrait conduire à une intégration de ces solutions dans le Top 5 prochainement.

Recommandations

- *Renforcer la détection au niveau des endpoints en enrichissant la configuration de l'EDR face à des techniques plus furtives.*
- *Déployer des capacités de détection et de réaction à plusieurs niveaux pour identifier et bloquer les menaces à plusieurs stades, mais aussi palier le contournement d'un des dispositifs par les attaquants (agrégation par un XDR/SIEM, prise en charge de la couche réseau par un NDR, etc.)*

[10] UEBA : User and Entity Behavior Analytics

PARTIE 2

TENDANCES

2.1) La détection des menaces sur les endpoints : approche combinée

La détection des menaces sur les terminaux à l'aide d'une solution EDR ou XDR repose sur 2 composantes, qui peuvent être décorréllées l'une de l'autre :

- Le **moyen d'exécution** de l'action malveillante
- La **finalité de l'action** malveillante (la "payload")

Les données analysées par BlackNoise montrent que l'efficacité de cette détection **varie en fonction des choix techniques opérés** par les adversaires.

Des écarts de détection significatifs sont parfois constatés lorsque l'outil de défense (Antivirus, EDR ou XDR) se fonde sur l'identification du moyen d'exécution, tel que l'utilisation des vecteurs *cmd* ou *PowerShell* par exemple. Le 1er vecteur présente un taux de détection meilleur que le 2nd ; avec un nombre de comportements malveillants identifiés plus élevé, mais aussi avec un degré de criticité souvent plus important pour une même action. **Une même action peut ainsi passer inaperçue selon le vecteur d'exécution employé** car elle peut ne pas être jugée avec la même criticité, même si l'effet final recherché par l'attaquant reste inchangé.

Concernant le taux de détection plus faible des actions exploitant *PowerShell*, plusieurs explications peuvent être avancées :

- *PowerShell* est un outil plus riche et plus complexe que *cmd.exe*. Il présente donc un risque de faux-positifs plus élevé, contrairement à *cmd.exe* qui est plus limité et dont les usages présentent moins d'ambiguïté.
- La distinction entre activité légitime et malveillante est plus complexe avec *Powershell* car il fait partie des outils d'administration usuels aujourd'hui ; cela expliquerait que *PowerShell* soit de plus en plus détourné par les attaquants (cf LOTL).
- *PowerShell* est un outil plus récent que *cmd.exe* ; il est donc possible que les signatures et les heuristiques soient mieux développées pour détecter des comportements anormaux dans cmd.exe.
- *PowerShell* offre des possibilités d'obfuscation et d'évasion avancées.

Retour d'expérience

Des cas de détection variables par un même EDR ont été observés selon la version de PowerShell installée sur la machine. La détection fonctionnait bien avec une version antérieure à PowerShell 7.1, mais était inefficace sur les versions plus récentes.

Pour éviter un blocage intempestif des usages de *PowerShell*, les outils de détection sont souvent configurés pour être plus tolérants. Cela conduit à ignorer certaines actions ou à réduire leur niveau de sévérité.

Cette difficulté **s'accentue avec des techniques plus sophistiquées**, telles que l'exécution par injection de DLL sous Windows, qui contournent plus aisément les mécanismes de surveillance traditionnels. Ainsi, la détection efficace des menaces sur les terminaux nécessite une **approche combinée**, prenant en compte non seulement les moyens d'exécution mais aussi la finalité des actions pour identifier et neutraliser les activités malveillantes de manière plus fiable.

Recommandations

Renforcer la détection au niveau des endpoints en enrichissant la configuration de l'EDR quel que soit le vecteur d'exploitation utilisé

2.2) Une réaction majoritairement manuelle

Remédiation peu automatisée

Très peu de mesures de remédiation sont déclenchées de façon totalement automatique, que ce soit par les outils de détection ou via des outils d'orchestration comme les SOAR[11]. Les processus de remédiation reposent principalement sur des **actions semi-automatisées**, pré-configurées par l'outil et soumises à validation d'un intervenant humain.

Ce constat est également partagé dans le rapport "Detection and response survey 2024" du SANS :

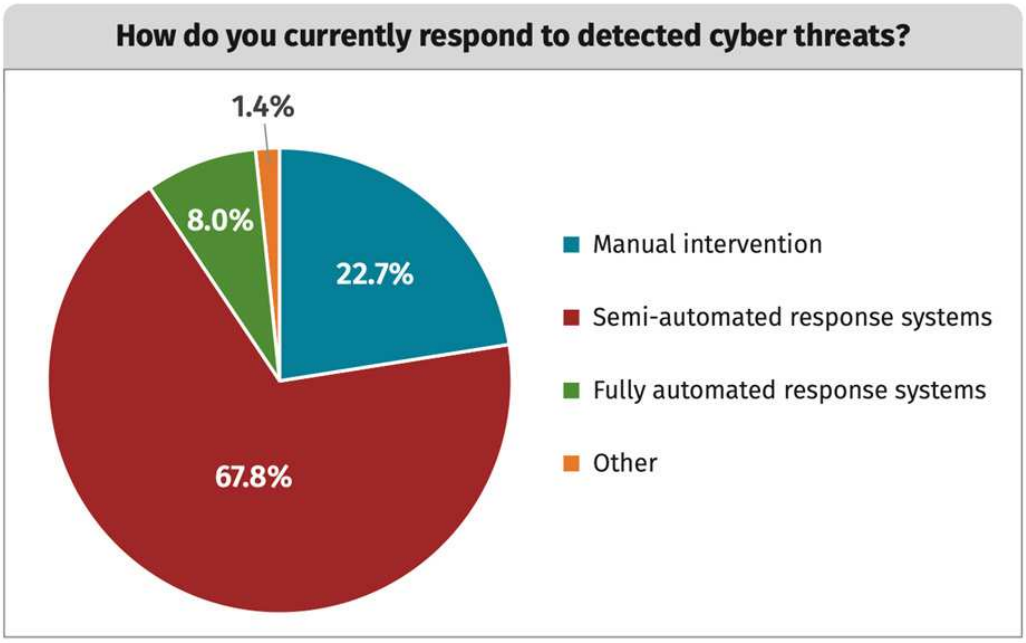


Figure 5. Threat Response Methods

[11] SOAR : Security Orchestration, Automation and Response

Bien que l'automatisation progresse légèrement, **l'expertise humaine reste indispensable** pour gérer les faux positifs, adapter les actions aux contextes métiers spécifiques et éviter les effets de bord. Le manque de personnel qualifié, la complexité d'intégration et les risques d'interruption de service limitent une automatisation massive. Des standards comme OpenC2[12] apparaissent pour faciliter l'automatisation entre différentes solutions.

L'approche la plus couramment adoptée, dite de semi-automatisation, consiste à tirer parti de la puissance des outils et de l'interconnexion entre solutions afin d'**enrichir les alertes** avec des données techniques précises. Cette stratégie vise à placer les équipes d'intervention dans des conditions optimales, en leur fournissant les informations nécessaires pour prendre rapidement les meilleures décisions, tout en conservant le contrôle final sur le déclenchement des contre-mesures.

L'utilisation de l'IA pour enrichir ces approches est indéniable et constitue un facteur clé qui renforcera la valeur de automatisation et son bénéfice.

Retour d'expérience

L'analyse des résultats obtenus par BlackNoise montre que les actions techniques de réaction, lorsqu'elles sont déclenchées, se concentrent principalement sur les mesures suivantes :

- *Arrêt des processus incriminés*
- *Suppression de fichiers douteux*
- *Isolation réseau de la machine ciblée par l'attaque via l'activation d'un firewall local bloquant les flux entrants et sortants*

[12] https://openc2.org/

Concentration sur la cible plutôt que sur la source

Les mesures listées précédemment montrent que la remédiation semi-automatique se concentre initialement sur la cible afin de **contenir la propagation de l'attaque**. Par exemple, dans le cas d'une isolation réseau, c'est la machine compromise qui est isolée du reste du réseau, mais **la source de l'attaque est souvent ignorée**. En conséquence, l'attaquant peut poursuivre ses actions et compromettre d'autres systèmes.

Pour parvenir à une **remédiation plus proactive visant à neutraliser la source de la menace** il faut être en mesure d'identifier précisément la source de l'attaque pour déployer des contre-mesures ciblées et adéquates ; par exemple un isolement réseau de la machine « attaquante » par désactivation du port Ethernet auquel elle est connectée ou une redirection de ses flux vers un environnement spécifique. Cela requiert des capacités avancées de détection, capables de remonter des informations techniques précises (jusqu'au port physique du switch impliqué dans le cas cité), et de pouvoir déployer rapidement ce type de configuration sur les équipements réseau.

Ce constat illustre un point important : **la détection n'est pas qu'une affaire de rapidité**. Il faut certes réagir vite mais une détection performante, permettant d'enclencher une réaction adaptée, implique des données de qualité.

Manque d'entrainement et de coordination entre les équipes

Enfin, l'efficacité de la réaction repose également sur une **coordination rigoureuse entre les équipes de sécurité** (SOC, CSIRT/CERT) **et les équipes IT responsables des infrastructures**. Ces dernières doivent être en mesure d'appliquer rapidement les contre-mesures défensives. Cela implique l'élaboration de procédures détaillées et adaptées aux différents scénarios de cyberattaques, avec des mises à jour régulières basées sur les tendances de menaces et les retours d'expérience, qui doivent idéalement être appuyés par des playbooks actionnables rapidement.

L'exécution régulière de simulations d'attaques contribue à tester et améliorer cette coordination :

- Évaluation de l'efficacité des processus de détection et de réponse
- Validation de la pertinence des données techniques disponibles
- Accélération de la corrélation des informations
- Optimisation de la mise en œuvre des mesures de remédiation

Il est fondamental d'entrainer régulièrement les équipes sur leurs outils (afin de se familiariser avec les interfaces et les requêtes d'analyse poussées) et les process d'intervention pour gagner en efficacité le jour J. La mise en place de formations continues grâce aux simulations de cyberattaques, dans une approche **Purple Team**, permet renforcer l'expertise et l'engagement des analystes.

Recommandations

- *Tendre vers l'automatisation de la remédiation, au moins par des réponses semi-automatisées qui enrichissent les données et suggèrent des playbooks de contre-mesures*
- *Entrainer les équipes pour les aguerrir à l'utilisation des outils en place et faciliter la coordination entre SOC, CSIRT/CERT et IT.*
- *Remonter à la source des attaques pour neutraliser l'origine, et ne pas uniquement contenir les cibles impactées*

2.3) Le tsunami de vulnérabilités

Le recensement et la correction des failles est une course sans fin

Face à l'essor des menaces et à la multiplication des surfaces d'attaque, l'approche traditionnelle ne suffit plus à garantir une protection efficace des systèmes d'information. L'évolution des infrastructures informatiques s'appuie désormais sur des composants plus nombreux et moins maîtrisés. La dépendance accrue aux **bibliothèques logicielles tierces** – reconnue comme un risque de type « **supply chain** » - en est un exemple caractéristique ces dernières années.

Plus largement, entre 2013 et 2023, le nombre de CVE identifiées est passé de 5 000 à 28 000, avec une croissance annuelle moyenne de 20 %. En 2024, cette tendance s'est aggravée avec un record historique de 40 000 CVE, soit une augmentation de 38 % en un an[13].

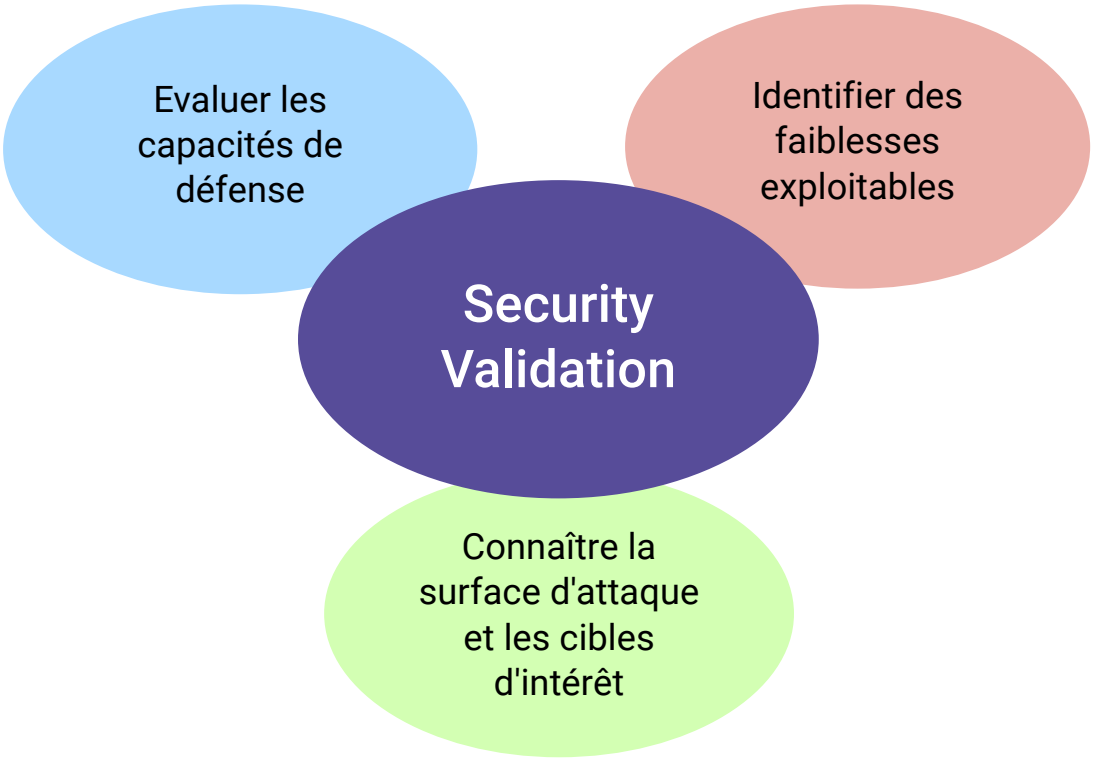
[13] https://www.yeswehack.com/news/cve-surge-record-jump-vulnerabilities

Maintenir à jour le système de CVE devient difficile. Le NIST ne peut plus gérer seul ce travail titanesque. En avril 2024, l'organisation a annoncé son intention de créer un consortium d'acteurs privés et/ou publics pour reprendre la gestion de la NVD (National Vulnerability Database)[14].

Le CISA tient justement à jour une source officielle des vulnérabilités qui ont été exploitées dans la nature : le catalogue KEV (Known Exploited Vulnerability)[15]. L'agence recommande vivement à toutes les organisations d'examiner et de surveiller le catalogue KEV et de donner la priorité à la correction des vulnérabilités répertoriées afin de réduire la probabilité d'une compromission par des acteurs connus de la menace.

Limites des méthodes classiques

Dans ce contexte, les approches habituelles d'identification des failles telles que les pentests, les Red Teams ou les scans de vulnérabilités montrent leurs limites face à une explosion du nombre de vulnérabilités à couvrir. Il faut préparer le coup d'après en considérant que l'adversaire est en mesure d'exploiter ces failles. La défense en profondeur se doit de considérer le 2nd niveau : assurer la détection pour enclencher efficacement les contre-mesures en vue de contenir l'attaque.



[14] https://nvd.nist.gov/general/news/nvd-program-transition-announcement
[15] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Pour cela, l'exploitation de schémas d'attaque linéaires n'est pas suffisante. Une action technique menée par un adversaire peut être exécutées de manières multiples. Ainsi, l'automatisation et la parallélisation de tests variés sont essentielles pour **tester un large éventail de scénarios** et renforcer la défense contre les menaces actuelles et futures.

Exemple

Pour illustrer ce propos par un exemple simple, un scan de ports effectué avec Nmap sera facilement repérable. Une autre variante consiste à utiliser des outils open-source alternatifs qui peuvent contourner les mécanismes de détection. Mais l'exécution manuelle de requêtes via Netcat permet d'obtenir le résultat du point de vue de l'attaquant tout en utilisant un « signal » plus complexe à détecter.

2.4) Une détection comportementale dans le cloud

Dans les environnements cloud, les SOC concentrent leurs efforts sur la détection comportementale, en surveillant les actions inhabituelles des utilisateurs susceptibles de signaler des violations des politiques de sécurité. Par exemple, dans Microsoft 365, des opérations telles qu'un téléchargement massif de fichiers depuis SharePoint ou OneDrive peuvent indiquer une tentative d'exfiltration de données, tandis que des accès non autorisés à des boîtes mail peuvent révéler des activités d'espionnage. De même, des connexions depuis des localisations inhabituelles ou à des horaires atypiques, bien que parfois masquées par l'usage de VPN, constituent des indicateurs pertinents de compromission de compte.

Une évolution notable dans cette approche, constatée par BlackNoise, est l'adoption du **User and Entity Behavior Analytics (UEBA)** qui s'appuie sur l'apprentissage automatique pour détecter des comportements inhabituels et prédire les menaces potentielles. L'UEBA permet d'identifier des modèles anormaux, comme une connexion inhabituelle depuis un pays où l'utilisateur ne se rend jamais, une escalade de privilèges suspecte ou encore des tentatives répétées d'accès à des ressources sensibles.

Contrairement aux systèmes traditionnels basés sur des règles fixes, l'UEBA analyse continuellement les comportements pour établir des bases de référence dynamiques et identifier les écarts significatifs. L'UEBA est particulièrement adapté à la détection des attaques visant les environnements SaaS car il permet de détecter des menaces difficiles à repérer avec des règles classiques.

Pour les environnements de type PaaS ou IaaS, la détection des attaques repose encore sur les couches système et réseau grâce aux mécanismes habituels : heuristique, corrélation des logs , analyse des flux, etc.. Pour ces modèles de cloud, la détection diffère finalement peu des environnements habituels.

Mais ces environnements font également face à des attaques conçues pour exploiter les technologies et produits créés spécifiquement pour le cloud, comme Microsoft Entra ID par exemple. Le **Deep Purple Report** de BlackNoise met en évidence une plus faible capacité de détection actuelle à couvrir les composantes techniques spécifiques aux nouveaux environnements cloud.

2.5) La conformité NIS2 et DORA

Une croissance importante des simulations d'attaques au bénéfice des travaux de conformité vers NIS2 et DORA (mais aussi dans le cadre de TIBER-EU) a été constatée au cours du 2nd semestre 2024.

La conformité à ces réglementations impose notamment la mise en place de mesures de surveillance des incidents et d'une gouvernance claire en matière de cybersécurité. Les entités concernées doivent respecter des obligations de reporting, en déclarant tout particulièrement rapidement les incidents significatifs aux autorités compétentes et en renforçant leur coopération en cas de cyberattaques ou d'incidents opérationnels. Ces obligations imposent une capacité efficace et constante des moyens de détection et de réaction face aux attaques.

Les simulations d'attaques y contribuent sur deux axes majeurs :

- Tester les **capacités technologiques** en contrôlant les mécanismes de sécurité et de détection
- Évaluer le **dispositif organisationnel** en examinant les processus en place

L'objectif est d'assurer une **coordination optimale** entre les différentes équipes impliquées, en intégrant des protocoles précis de réponse aux cyberattaques.

CONCLUSION

Cette édition 2025 du Deep Purple Report de BlackNoise confirme des avancées notables des moyens de cyber défense, notamment dans la couverture des techniques d'attaque et la rapidité de détection. Celle-ci est toujours prépondérante sur les endpoints.

Cependant, malgré ces progrès, la remédiation demeure majoritairement manuelle, ce qui souligne l'urgence d'adopter des solutions d'automatisation. L'intégration de l'IA dans les processus de sécurité est devenue essentielle pour analyser efficacement les comportements suspects et accélérer la réponse aux incidents. Ces évolutions doivent aussi conduire à accentuer la stratégie de neutralisation des attaques, pour dépasser la simple logique de confinement des cibles.

Enfin, les simulations d’attaques automatisées sont de plus en plus utilisées pour répondre aux exigences de conformité Européenne comme NIS 2 et DORA, afin de renforcer les besoins de préparation des organisations face aux menaces.

BLACKNOISE

www.blacknoise.co

contact@blacknoise.co