

B|ACKNOISE

EFFICACITÉ DE LA SÉCURITÉ OPÉRATIONNELLE

RAPPORT ANNUEL
BLACKNOISE 2023

PUBLIÉ LE : 31/01/2024

SOMMAIRE

INTRODUCTION	3
RÉSULTATS 2023	5
Breach & Attack Simulation (BAS)	6
Les simulations réalisées	7
L'évaluation des défenses	9
L'évaluation des risques	11
Focus sur les sources	13
CONSTATS	15
Améliorer la stratégie de défense	16
Optimiser les coûts	17
Communiquer : scoring & risques	18
PERSPECTIVES 2024	19
Plan pour 2024	20

INTRODUCTION

Pour la 2^e année, BlackNoise publie son rapport annuel sur l'efficacité de la sécurité opérationnelle.

Ce rapport analyse les capacités réelles de défense Cyber organisées autour de la détection et de la réaction observées en 2023. Il est basé sur l'analyse des données collectées et anonymisées lors des simulations d'attaques et des tests de validation de sécurité exécutés en 2023.

Le contexte d'exécution des simulations d'attaques en 2023 s'inscrit autour de **3 enjeux**.



**CYBER
SCORING**



**STRATÉGIE
DÉFENSE**



**OPTIMISATION
COÛTS**

1 Améliorer la stratégie de défense.

L'amélioration continue des conditions de sécurité est une composante de l'ADN des opérations Cyber. En 2023, cette amélioration s'est concentrée sur 2 axes principaux :

- Améliorer la qualité de l'information sur la menace Cyber par l'optimisation des flux de CTI.
- Raccourcir la vitesse de détection (MTTD)¹ en cas d'incident de sécurité en améliorant la configuration et la qualité des mécanismes de détection (logs, data et scénarios d'alerte et process de qualification).



2 Donner aux dirigeants une photo du niveau de risque réel. (Cyber Scoring).

La demande des dirigeants sur l'état de sécurité réel est de plus en plus forte et ne peut plus reposer sur une base déclarative. En Europe, elle s'est accélérée notamment avec le poids croissant des réglementations NIS2, CRA, DORA.



3 Optimiser les coûts des opérations Cyber.

Dans le contexte actuel, les dirigeants et les équipes Cyber cherchent à optimiser leurs investissements. Cela porte à la fois sur les budgets alloués aux actions « offensives » d'audits et de contrôle (pentests, opérations de type Red Team, etc.) mais aussi sur les budgets des capacités « défensives » qui concernent les logiciels, services ou effectifs en place. L'automatisation des tests de détection et de validation de la sécurité est donc perçue comme un levier permettant de mieux utiliser et affecter :

- Les capacités d'audit traditionnelles.
- Les moyens technologiques et humains en charge de la défense.



Ces 3 enjeux sont toujours prépondérants dans la stratégie des responsables sécurité pour 2024 et s'inscrivent dans un temps long.

¹ Mean Time To Detect : Temps moyen de détection

**RESULTATS DES
SIMULATIONS
D'ATTAQUES
2023**

1

1. **Breach & Attack Simulation**^(BAS)

Les solutions de BAS² permettent l'exécution automatique de scénarios d'attaque Cyber sur une infrastructure ciblée. Le scénario se compose des étapes techniques caractéristiques d'une activité malveillante (aussi appelée « Kill Chain »³). La simulation vise à mesurer les capacités de défense sur 3 composantes :

Le niveau global de résistance de l'infrastructures aux différentes stratégies d'attaques connues



La capacité et l'efficacité de la détection (MTTD)⁴



La vitesse et l'efficacité de la réaction défensive (MTTR)⁵



La solution attribue un score d'efficacité selon les résultats obtenus. Ce score dépend de différents critères tels que la performance de la détection face à un événement (inexistante, partielle, optimale), la qualification précise de l'événement par les outils et/ou les analystes, etc.

² Breach & Attack Simulation solution

³ Modélisation des Cyber-attaques par une décomposition du mode opératoire des attaques en plusieurs étapes. Principe importé du monde militaire et appliqué pour la 1ère fois au monde informatique par la société Lockheed Martin en 2011. Plusieurs modélisations ont été proposées par des sociétés ou organismes, dont le modèle ATT&CK du MITRE.

⁴ Mean Time To Detect

⁵ Mean Time To React

2. Les **simulations** d'attaques réalisées

Les chiffres de 2023

Les simulations d'attaques exécutées en 2023 ont ciblé des infrastructures informatiques d'ETIs ou de grands groupes de tous secteurs (public, aéronautique, industrie minière, chimie, finance, service, retail, ...).

+300

**SIMULATIONS
D'ATTAQUES**

13k

**ÉVÉNEMENTS
TECHNIQUES**

+300 simulations d'attaques adressant tout type d'environnement IT.

- Les environnements de type SI de gestion restent les environnements les plus représentés en 2023 (87% des simulations). Cela s'explique notamment par les menaces qui pèsent sur ces environnements et par la concentration, depuis de nombreuses années, des efforts de sécurisation (EDR et NDR en tête).
- Les environnements industriels (infrastructures variées d'usine, site de production, réseau logistique) ont été directement ciblés par 7% des simulations. Les enjeux Cyber relatifs à ces environnements gagnent en attention de la part des dirigeants ; le déploiement de services et de solutions de surveillance et sécurisation s'accélèrent fortement.
- Les simulations d'environnements cloud, principalement de type IaaS ou PaaS émergent et représentent 6% des simulations avec une accélération marquée sur le second semestre.

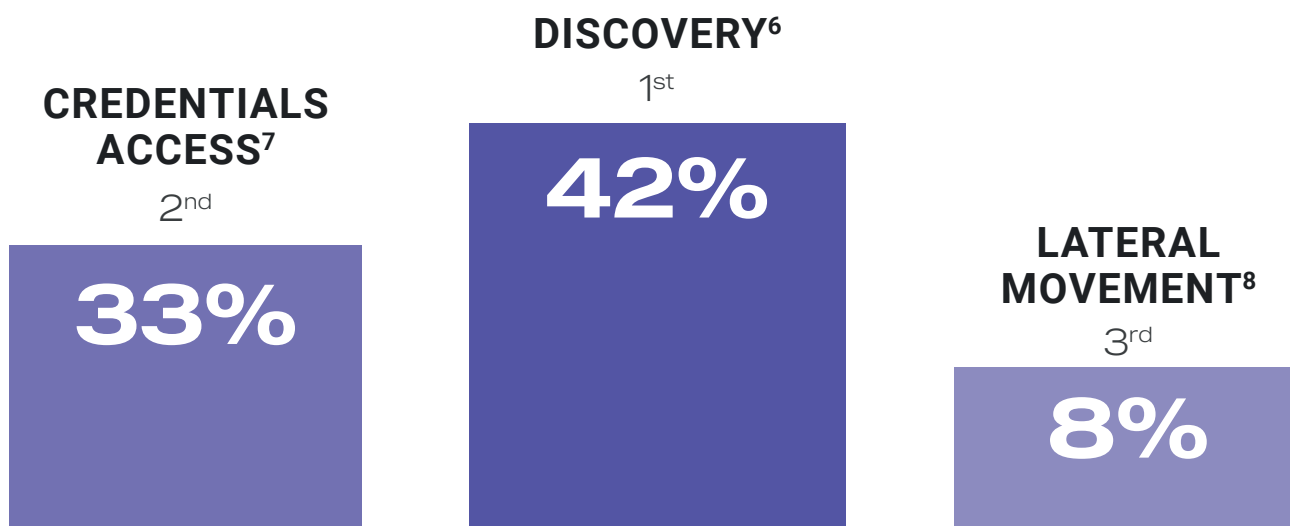
Répartition des 13k events.

Les simulations d'attaques couvrent l'ensemble de la chaîne de compromission Cyber. Ces simulations ont permis d'exécuter une moyenne de 42 événements techniques par campagne sur l'ensemble des catégories du référentiel MITRE ATT&CK®.

Dans la continuité des constats de 2022, la catégorie « Discovery » est la plus représentée parmi les événements exécutés. Elle regroupe les actions de découverte que mène un adversaire pour mieux connaître le réseau interne et ses systèmes. Ces actions permettent aussi d'évaluer la surface d'attaque du réseau, c'est-à-dire à identifier les cibles d'intérêt Cyber qui constitueraient des points d'entrée exploitables.

La forte représentation de cette catégorie dans les simulations exécutées tient au fait qu'elle regroupe de très nombreuses techniques différentes et un champ d'application particulièrement large. C'est également une étape clé des modes opératoires déployés par les adversaires. Reproduire cette diversité sous forme de simulations permet d'évaluer la capacité de détection des attaques, avant que les actions les plus impactantes ne se concrétisent.

Le top 3 des Tactiques du MITRE ATT&CK® les plus exécutées est le suivant :



Avis d'expert

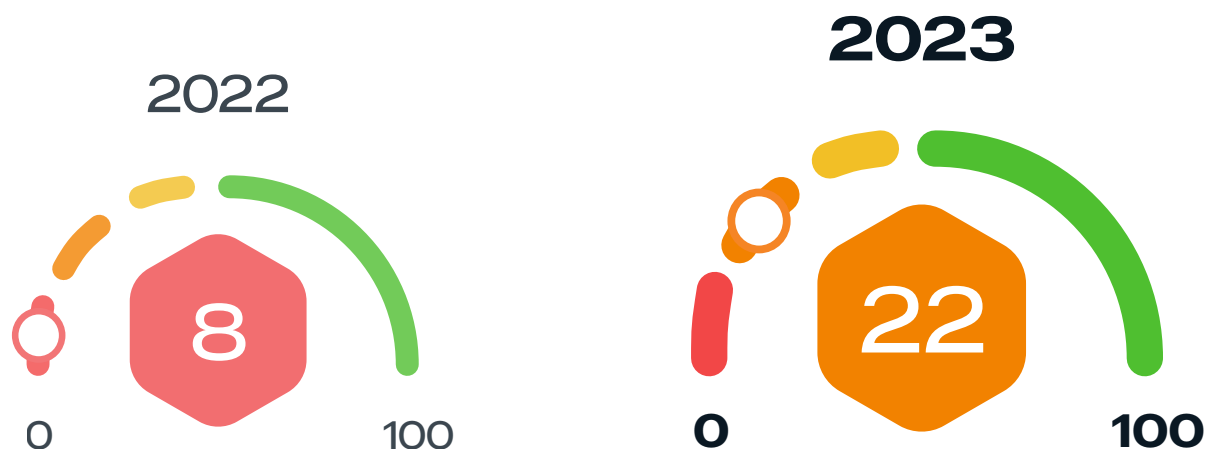
Les outils natifs du système d'exploitation sont souvent utilisés pour atteindre cet objectif de collecte d'informations. Les adversaires exploitent massivement de tels outils, échappant ainsi à la détection. Cette méthode, qui porte le nom de « living-off-the-land » (LotL), est fortement présente depuis plusieurs années et 2023 l'a confirmé.

⁶ <https://attack.mitre.org/tactics/TA0007/>

⁷ <https://attack.mitre.org/tactics/TA0006/>

⁸ <https://attack.mitre.org/tactics/TA0008/>

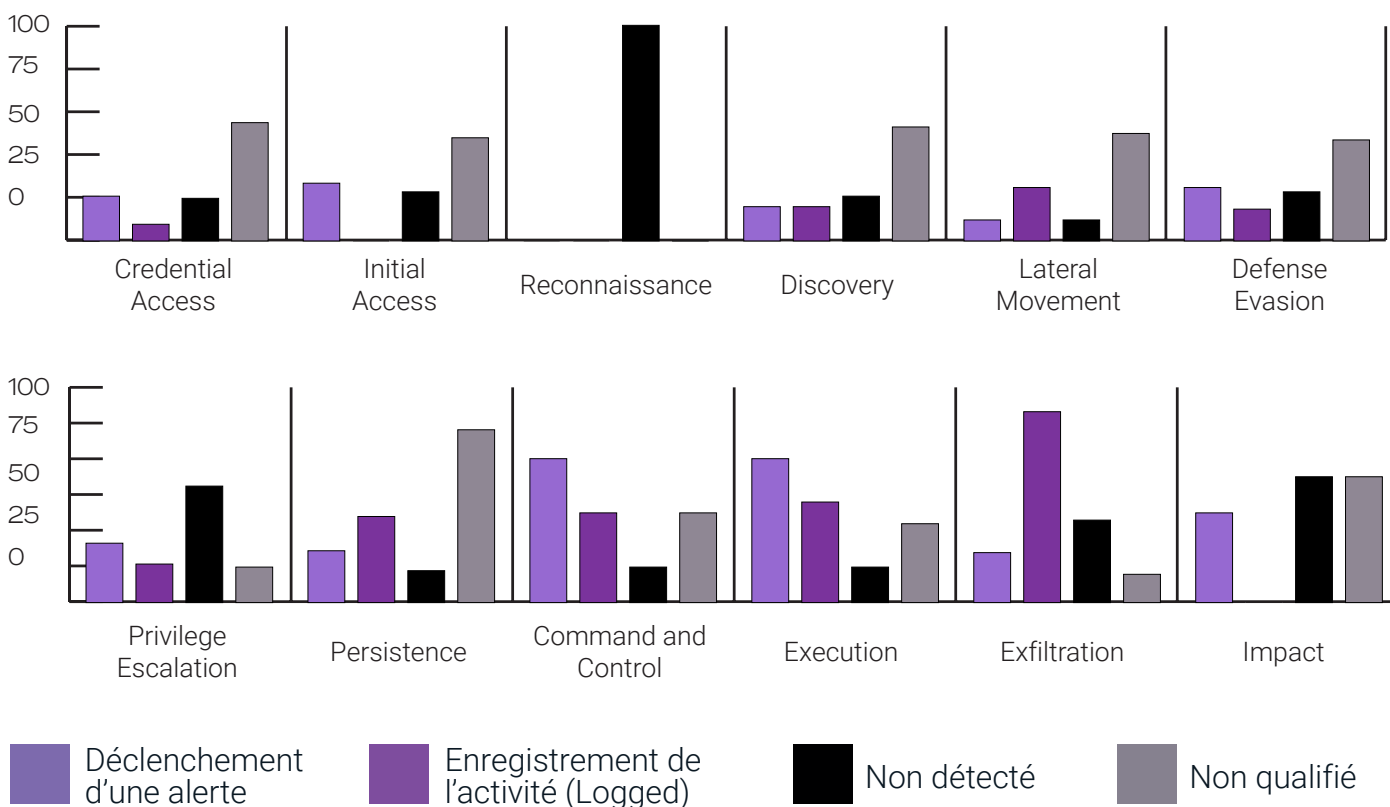
3. L'évaluation des capacités de défense



Le taux de détection moyen est en progression par rapport à l'an dernier, bien qu'il reste relativement faible. L'évolution à la hausse, même très relative, traduit une amélioration générale des capacités de défense.

Celle-ci s'explique par 2 facteurs clés : la maturité de technologies telles que l'EDR et la compétence des équipes SOC. Mais cette valeur, prise dans l'absolu, démontre également l'urgence de faire progresser toute la chaîne de défense.

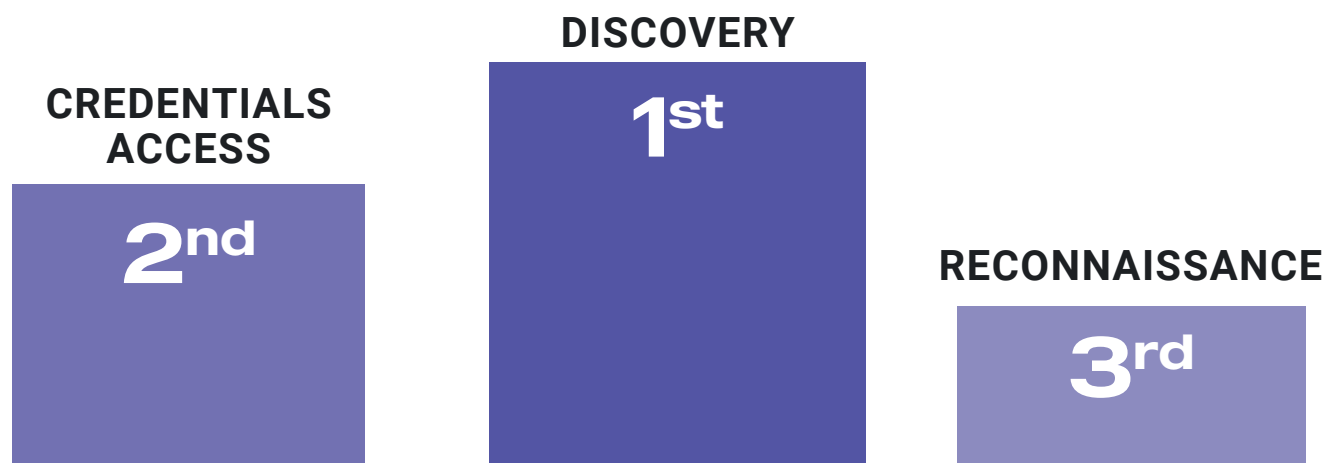
La projection des capacités de détection selon les tactiques du MITRE ATT&CK® est la suivante :



LES TOPS 2023



LES FLOPS 2023



Les « tops » démontrent que la détection s'avère plus efficace sur les phases avancées de la Kill Chain. L'activité des adversaires est principalement décelée au travers d'actions sensibles, à fort impact et avec une probabilité de faux positif faible, réalisées sur les systèmes. La surveillance se focalise sur la finalité des attaques donc principalement au niveau des endpoints, et l'EDR est l'atout majeur de cette détection. Les actions d'exfiltration peuvent également être détectées par des outils plus axés réseau comme les firewalls, IPS/IDS ou NDR.

Au contraire, les phases en amont de la Kill Chain sont plus délicates à déceler. Les scans réseau massifs et agressifs, les bruteforces de comptes, et même les récupérations massives d'informations techniques sur les systèmes ou l'AD qui permettent de mieux connaître l'environnement ciblé sont peu identifiés⁹. Cette réalité s'explique par une multitude de facteurs déjà évoqués en 2022 :

- Les outils déployés ne disposent pas toujours de réelles capacités de détection efficaces de telles actions, ou leur configuration n'est pas optimale pour y répondre. Il s'agit plutôt de solutions palliatives face à un problème peu considéré.
- Le volume de données techniques généré par la surveillance de tels comportements (notamment les scans réseau) engendre plusieurs contraintes : un coût de stockage prohibitif des logs, une forte complexité à identifier un signal pertinent dans un tel volume de données et un seuil de notification inadéquat qui induit un excès de faux positifs.

D'autres approches seront évoquées dans la 2^{de} section de ce rapport pour apporter des réponses efficaces et à moindre coût à cette faible capacité de détection face à de tels comportements adverses.

« Les attaques sont **moins bien détectées** en amont qu'au milieu ou en aval de la **Kill Chain** ».

4. L'évaluation des risques

EXTERNAL ATTACK

Premier constat : peu de simulations adressent les périmètres externes exposés sur Internet et l'efficacité des moyens de détection sur ces périmètres est très relative. Cela s'explique par le fait que ces périmètres sont historiquement peu couverts par les SOC. Ces derniers concentrent principalement leurs efforts, technologiques et humains, sur le périmètre interne.



⁹ Cf. les techniques de type LotL décrites précédemment

INSIDER THREAT

Le risque lié aux adversaires sans compétences techniques avancées et ayant accès au réseau interne (attaquants ayant pu pénétrer le SI grâce à un phishing par exemple, employés, sous-traitants, etc) est celui qui présente l'écart-type le plus fort. Les structures les plus matures détectent généralement bien ces scénarios et savent neutraliser la menace rapidement.

Les structures moins avancées affichent tout de même une capacité à adresser ce risque mais sur un périmètre restreint et bien délimité (le SI de « gestion » avec les postes de travail et l'AD, un environnement cloud avec des applicatifs très sensibles, etc.).



ESPIONNAGE / DESTRUCTION

Le risque d'espionnage ou de destruction ciblé concerne les modes opératoires issus d'APT ou équivalents. Ces attaques sont généralement ciblées et orchestrées par des groupes Cybercriminels expérimentés, parfois financés ou soutenus par des États. Elles sont souvent menées sur le long terme, les phases initiales se concentrant sur l'exécution discrète d'actions préparatoires avant de déclencher des actions liées à l'objectif final.

Ces risques peuvent également englober les attaques de la chaîne d'approvisionnement, où les Cybercriminels ciblent délibérément un fournisseur ou un partenaire moins sûr pour atteindre leur objectif final, à savoir des cibles plus sensibles.

La complexité technique de ces scénarios conjuguée à la furtivité des modes opératoires rend la détection difficile, ce qui explique le niveau d'exposition au risque plus important. Il est à préciser que seules les structures les plus matures en termes de capacités défensives s'orientent vers ce genre de simulations.



DATA BREACH

Le risque de fuite de données est mieux adressé que l'an dernier grâce à une amélioration constatée sur les capacités de détection et de blocage des exfiltrations de données. Les actions de collecte des données qui constituent la phase amont de tels scénarios restent cependant non décelées.



5. Focus sur les principales sources de détection

Les 3 principaux outils ayant permis de détecter les simulations exécutées sont les suivants :

EDR **68%**
des simulations détectées



Firewall/ IPS/IDS **28%**
des simulations détectées



SIEM **24%**
des simulations détectées



L'EDR est encore cette année un outil majeur de l'arsenal défensif, sa contribution au nombre d'événements détectés le démontre. La qualité des alertes remontées couplée à un faible temps de réaction fait indéniablement de ce type de solution un atout fondamental pour détecter les actions des adversaires opérées sur les systèmes, des plus basiques aux plus complexes.

« L'EDR, roi de la détection : **2/3 des actions** adverses sont détectées grâce à lui ».

Cette stratégie centrée sur la détection de quelques types d'actions sur les endpoints présente toutefois un risque : en cas de défaillance de l'EDR, toute la chaîne de détection et de réaction peut donc être inopérante. Les attaquants l'ont bien compris et cherche souvent à désactiver rapidement l'EDR ou à le rendre silencieux.



EDR

SIEM

Firewall/ IPS/IDS

Avis d'expert

Pourquoi le SIEM n'est-il qu'en 3^e position ?

Nous constatons que la gestion des incidents de sécurité (au sens détection puis déclenchement de mesures de remédiation) est majoritairement réalisée directement depuis des solutions de type EDR, NDR, MDR. Même si les solutions de type SIEM sont plus anciennes et largement déployées compte tenu de leur maturité, elles ont tendance à être moins utilisées dans la réalisation quotidienne des opérations de détection et de remédiation.

Les usages des SIEM évoluent vers un service de type datalake permettant de conserver des traces exploitables à posteriori. Mais un couplage EDR + SIEM s'avère encore plus redoutable pour la défense.

**CONSTATS BASÉS
SUR LES RÉSULTATS
DE 2023**

2

Améliorer la stratégie de défense



1 *Hum... Il manque un truc là...?*

Une stratégie de détection efficace repose sur 2 fondamentaux : la surface de couverture et l'accès aux données nécessaires pour la surveillance (logs).

La mise en lumière des angles morts sur ces 2 fondamentaux par les simulations d'attaques est donc indispensable.

Cette stratégie doit également tendre vers une défense en profondeur au moyen de plusieurs dispositifs de détection et de réactions complémentaires. Cela doit permettre de mieux anticiper les attaques par une détection des comportements malveillants le plus en amont possible ; mais aussi de pallier à d'éventuels dysfonctionnements de l'EDR.

2 *Merci de patienter, nous allons prendre votre appel...*

S'assurer que les informations de détection remontent bien et que les personnes concernées sont joignables.

C'est un des SPOFs les plus couramment identifié : le numéro d'astreinte n'est pas le bon, personne ne répond, le mail d'alerte tombe dans les spams ou n'est tout simplement pas envoyé, la notification d'alerte est noyée dans le flux de faux positifs, etc.

3 *Ah ? Normalement ça aurait dû sonner...*

Mettre en œuvre un contrôle permanent des scénarios de surveillance les plus critiques. Il y a de nombreuses raisons qui peuvent mettre en échec un scénario de détection (logs non générés ou non transmis à la solution de surveillance, modification de la configuration du système qui désactive des contrôles, modification de la signature de l'attaquant, etc.).

La réalisation de tests réguliers pour valider cela est indispensable et de plus en plus systématisée.

4 *Attraper les attaquants avec du miel*

Poser des leurres. Stratégie ancestrale, redoutablement efficace et peu coûteuse, le piégeage revient en force depuis 2 ans dans les stratégies de détection et se décompose en plusieurs tactiques telles que le positionnement de fichiers servant de canaris (honey file) ou le déploiement de honeypot, honey account, honey email, etc.

5

Go, go, go !

Pour les structures les plus matures, les efforts se concentrent sur l'amélioration de la vitesse de réaction. La vitesse d'exécution des attaques, et en particulier des phases destructives (ransomware, wiper), exige une capacité de réaction tout aussi rapide qui repose sur 3 briques :

- Automatisation de la réaction avec des solutions du type SOAR ou avec un EDR, par exemple. Très peu généralisée dans la réalité.
- Existence de processus techniques, par exemple : déploiement et réplication rapide d'une politique de filtrage stricte sur une chaîne de firewall.
- Connaissance par les analystes du process applicable pour qualifier la gravité d'un incident. « *Pour se défendre vite et efficacement, il faut déjà qualifier la gravité au bon niveau* ».

Optimiser les coûts

6

Faire mieux avec ce que l'on a

Une meilleure exploitation des outils déjà en place se reflète dans la maîtrise des coûts de licences.

Exploiter ce qui est présent pour une meilleure détection, utiliser les fonctionnalités de remédiation automatique des solutions de détection (cf. key learning précédent), rationaliser la rétention des logs, etc. autant d'évolutions constatées en 2023.



7

Le système D(étection)

Le retour en grâce des stratégies « lowcost » illustrées en premier lieu par les honeypot, honeyaccount, honneyemail contribue aussi à l'optimisation des coûts.

8

La confiance n'exclut pas le contrôle, le contrôle optimise les coûts.

Les services de type MSSP se voient souvent confier la fonction stratégique de primo-intervenant sur les incidents Cyber. Ils sont généralement chargés de la détection et de la qualification initiale d'activités malveillantes et 2 SPOFs sont régulièrement identifiés dès les étapes initiales du processus de réponse aux incidents, et ont un impact significatif sur le ROI de ces services :

- Une erreur de qualification de la gravité, qui impacte la suite du processus d'alerte et entraîne une perte de temps significative dans la réaction.
- Un dysfonctionnement dans la chaîne d'alerte qui entraîne une latence dans le partage de l'information avec le management et les experts mobilisés en soutien.

Les clients des services MSSP souhaitent s'assurer de la fiabilité du processus de réponse aux incidents et tester régulièrement la maîtrise des 2 points de fragilité ci-dessus.

9

Revoir l'usage, sans remettre en cause.

Repenser la stratégie d'audit technique traditionnel : affecter les pentests et les redteams sur les environnements et cibles sur lesquels les résultats apportés par les BAS sont les meilleurs, afin d'optimiser l'utilisation et le coût du « touché humain ».

Communiquer Scoring & Risques



10

Des KPIs issus du terrain.

La conscience du risque Cyber est maintenant et durablement ancrée dans la stratégie des entreprises. Mais sa quantification reste majoritairement subjective, construite sur des analyses ponctuelles, qualitatives et déclaratives.

Les dirigeants veulent mieux comprendre le niveau réel du risque et par extension évaluer objectivement l'efficacité de leur stratégie de défense et l'efficacité des investissements réalisés, au travers d'indicateurs concrets, lisibles et construits sur la base de données issues de la technique.

PERSPECTIVES

2024



3

ET POUR 2024 ?

Le renforcement des capacités de détection pour identifier les menaces les plus furtives n’est pas une priorité de premier niveau. La conscience du risque est réelle, mais la capacité à y répondre globalement et efficacement dépend de ressources qui sont toujours en construction.

Deux arguments ressortent concernant les enjeux Cyber de cette stratégie :

- D’une part, elle favorise a priori une rationalisation des coûts.
- D’autre part à moyen terme, elle ouvre une perspective de gains d’efficacité importants avec la généralisation de l’IA défensive dans les infrastructures en nuage. Même si la réalité technique de ces nouveaux services est encore floue.

Les instances de Direction ont des attentes de plus en plus fortes sur l’efficacité de la Cyber sécurité. Le phénomène, alimenté par la conscience de la menace, se renforce par le poids des réglementations européennes à venir NIS2, DORA & CRA.

Globalement, l’efficacité des équipes opérationnelles se renforce significativement. Le niveau de connaissance technique, de formation et d’expérience des équipes opérationnelles (SOC, CSIRT, CERT) offre aux entreprises des capacités de réponse qui s’améliorent en permanence. Maintenir cette efficacité avec des exercices opérationnels et des tests réguliers se généralise chez les acteurs les plus avancés.

		Tendance 2023	Tendance 2024
TENDANCE TECHNOLOGIQUE	Déploiement de leurres (stratégie de Honey-x)	➡	↗
	Tests réguliers d’attaques ciblant l’Active Directory	➡	↗
	Généralisation d’EDR sur les environnements bureautiques	↗	↗
	Déploiement d’EDR sur les environnements industriels		➡
	Utilisation des algorithmes d’IA générative pour renforcer et assister les analystes		➡
	Généralisation de la remédiation automatique	➡	↗
TENDANCE ORGANISATIONNELLE	Réalisation de Scoring Cyber Tech		↗
	Surveillance des environnements externes (apps web, API ...)		➡
	Surveillance des environnements SaaS au niveau applicatif		➡
	Suivi régulier des performances de détection (MTTD)		↗
	Entraînement régulier des équipes opérationnelles pour optimiser la réaction (MTTR)		➡

B|ACKNOISE

LIVRABLE ÉDITÉ PAR LE GROUPE ERIUM

erium.fr/blacknoise

contact@erium.fr