BLACKNOISE

RAPPORT ANNUEL

EFFICACITÉ DE LA DÉTECTION D'ATTAQUES : BAROMÈTRE BLACKNOISE

ANNÉE 2022

PUBLIÉ LE : 07/03/2023

ERIUM

SOMMAIRE

Ce document est interactif

Ce symbole indique un **hyperlien**

ANALYSE DES CAPACITÉS RÉELLES DE DÉFENSE CYBER

1

Les solutions de Breach and Attack Simultation (BAS) ont commencé à se développer en Europe et en France au cours de l'année 2022.

Elles apportent une nouvelle dimension au combat cyber : celle de la mesure de l'efficacité réelle de la détection et de la réaction. Les CISO's ne veulent plus se contenter des promesses des éditeurs de solutions cyber (xDR, DLP, IP/DS, PXY,...), ou des fournisseurs de services (SOC, NOC, MSSP,...).

Ils expriment le besoin d'une maîtrise renforcée de leurs moyens de SecOps en lien avec l'évolution de la nature des attaques cyber et la perte de contrôle liée à la cloudification.

Ce besoin repose sur deux axes :

Technologique

Humain

Les résultats de l'étude reposent sur 85 campagnes de simulation réalisées sur 11 pays en 2022

Une étude basée sur 85 campagnes …	… avec un mode opératoire unique
outillées par une solution de Breach & Attack Simulation	un protocole d'intervention validé par chaque entreprise/ organisation
5270 événements de sécurité malveillants exécutés	une détection des événements déclarative
tous profils d'organisation et tous secteurs d'activités (grands groupes, ETI, organisations publiques),	un typage « non détecté » pour les événements non identifiés
tous modèles de SOC confondus : interne, externe (MSSP) ou hydride	un recoupement systématique avec l'entreprise sur l'exhaustivité des attaques simulées

Les simulations d'attaques sont composées d'événements techniques liés entre eux et qui reproduisent des schémas d'attaques.

Les événements techniques sont tous rattachés au référentiel MITRE ATT&CK et ses 14 phases. **Pour simplifier l'analyse des résultats, les phases du référentiel ATT&CK sont regroupées sur les 3 grandes catégories suivantes :**

INITIAL ACCESS

- Network access
- Network sniffing
- Ports scans
- Service discovery
- AD enumeration
- Accounts bruteforce…

COMPROMISSION & LATERAL MOVEMENT

- Process/service exploitation
- Passwords/tickets dump
- Account creation
- AV/EDR bypass
- System modification
- CVE exploitation…

IMPACT & EXFILTRATION

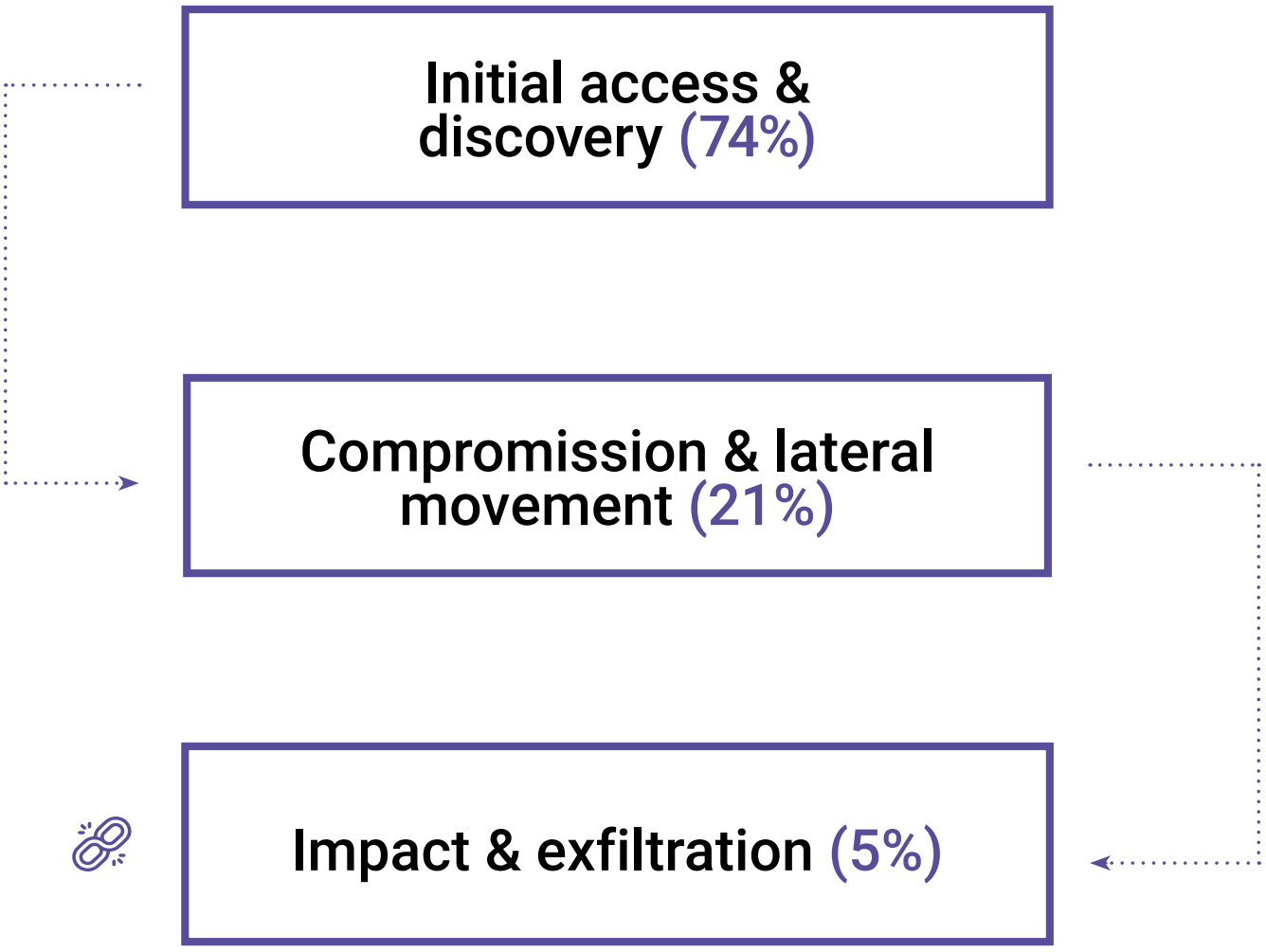
- Ransomware (encryption)
- Wiper (destruction)
- Cryptominer
- RAT (Remote Access Tool)
- Malware traffic (C&C)
- Cloud services exfiltration…

MITRE Att&ck simplified Cyber Kill Chain

DES TESTS SUR TOUTE LA CYBER KILL CHAIN

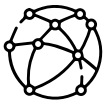
2

Le top 3 des simulations d'attaques les plus fréquemment jouées par catégorie du MITRE ATT&CK® (ie Tactic) est le suivant :



Initial Access et Discovery :
74% des événements, pourquoi ?

Les tests de la catégorie Initial Access & Discovery reproduisent les techniques de reconnaissance mises en œuvre par les attaquants pour cartographier la cible et identifier les composants (systèmes notamment) exploitables dans les phases suivantes de l'attaque :



LES RÉSEAUX INTERNES

LES SERVEURS

LES APPLICATIONS

Les tests de la sous-catégorie Credential Access visent l'obtention des comptes d'accès et **représentent 25% des événements simulés parmi les 74%.** Ces phases de découverte sont toujours verbeuses et représentent donc une part significative des événements simulés.

Compromission & Lateral Movement :
La suite logique…

Les phases de compromission sont plus fines et plus ciblées. Ce sont les marqueurs des premiers impacts potentiels sur les systèmes. Les stratégies de mise en œuvre sont multiples et dépendent directement de la finalité de l'attaque et du système (OS) sur lequel l'attaquant opère.

Impact & Exflitration :

L'attention des équipes de sécurité se focalise davantage sur les phases amont pour bloquer l'activité malveillante, avant même que l'impact ne soit déclenché, considérant qu'une telle exécution est le reflet de l'échec des phases de détection précédentes et de l'ensemble de la stratégie de défense.

Ceci explique le faible taux des événements simulés dans cette catégorie.

5270 ÉVÈNEMENTS

ont été executés dans les simulations d'attaques réalisées en 2022. Soit 62 événements en moyenne, par campagne

ENSEIGNEMENTS ET CONCLUSION POUR 2022

3

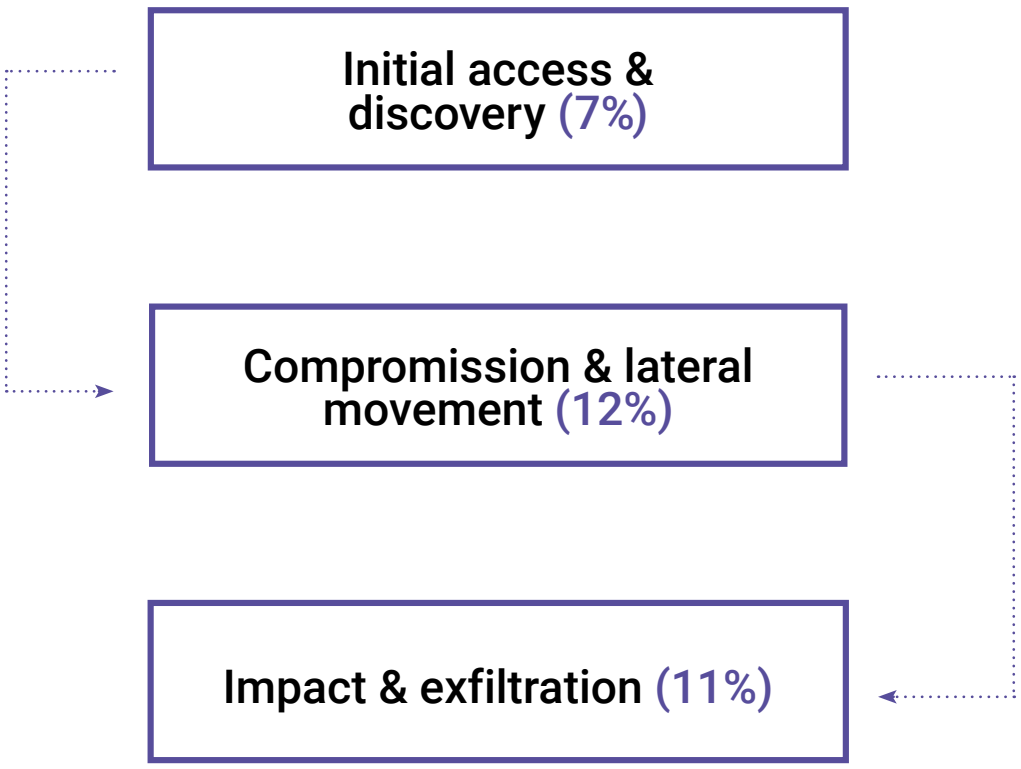
Key Learning #1 :

Le taux de détection global reste trop faible.

8%

En moyenne, le taux de détection des simulations d'attaque est de 8%. Si ce taux atteint tout de même 20% pour les entreprises les plus matures sur ce sujet, il reste largement perfectible.

Le niveau de détection des attaques par étape de la Kill Chain est le suivant :



Key Learning #2 :

L'EDR, une arme de détection efficace à challenger

75% L'EDR est la source de détection primaire dans 75% des cas.

Les solutions de type EDR sont de plus en plus déployées, et bien exploitées, elles représentent un atout fondamental pour la détection d'attaques sur des endpoints. On constate notamment que près d'un tiers des simulations d'élévation de privilèges sont détectées. Ces techniques, utilisées pour obtenir des autorisations de niveau de privilèges supérieurs, sont principalement identifiées grâce aux protections déployées sur les endpoints (postes de travail et serveurs) et en premier lieu par les EDR.

Dès lors qu'elles sont couplées à un SIEM, les alertes provenant de ces outils sont rapidement et correctement considérées par les équipes SecOps. Elles présentent le délai de réaction moyen le plus faible de notre analyse.

« Même s'il faut les challenger pour améliorer leur efficacité, les solutions de type EDR sont indéniablement un composant clé de l'arsenal défensif actuel des entreprises. Elles sont d'autant plus efficaces couplées avec un SIEM. »

Key Learning #3 :

Les attaques au niveau réseau passent sous les radars

83% 5 entreprises sur 6 ne détectent pas des scans de réseau massifs et agressifs

C'est un enseignement clé des tests réalisés : les attaques qui ne déclenchent pas d'exécution de code système sont peu détectées. Il s'agit notamment des simulations d'attaques menées :

- **Sur la couche réseau :** connexion d'équipement illégitime au réseau local, scans de ports, écoute du trafic, etc.
- **Sur les services systèmes, sans exécution de commandes** : reconnaissances des services, bruteforce de comptes, etc.
- **Pour des exfiltrations d'informations** : vers des serveurs C&C ou encore plus facilement vers des services cloud standards dont la finalité est détournée par les attaquants.

Cette réalité s'explique par une multitude de facteurs dont les principaux sont :

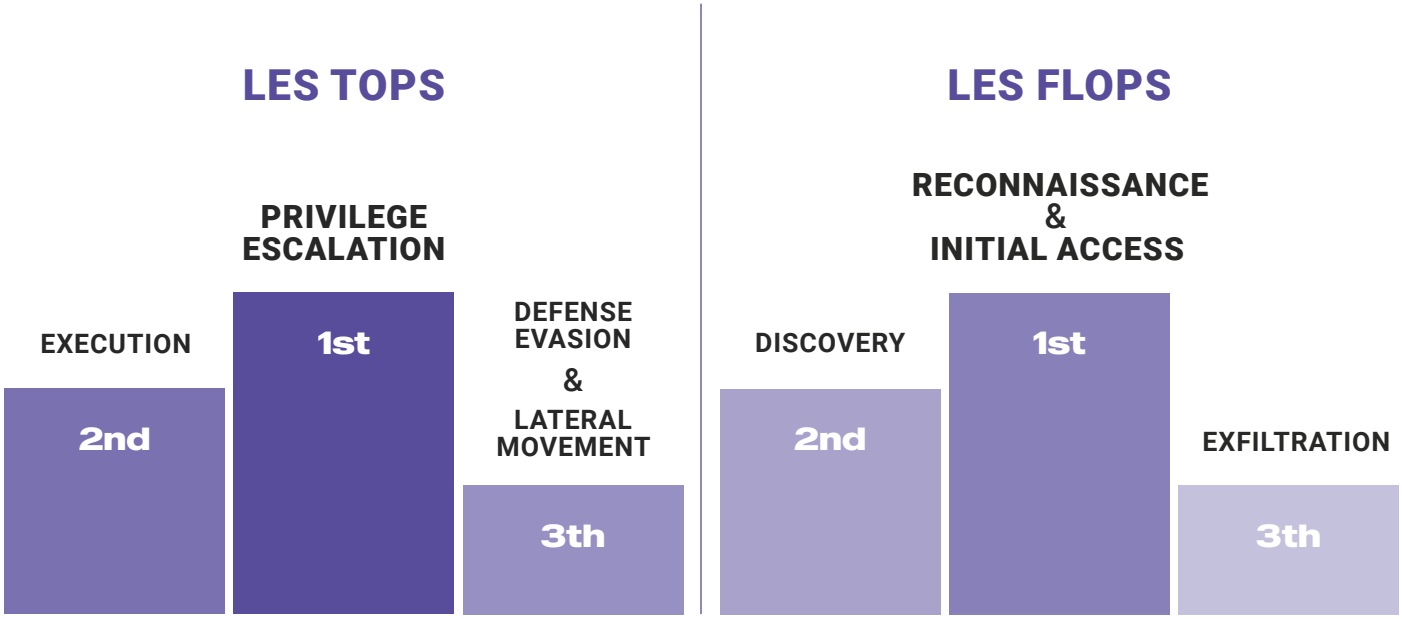
- **Un manque de technologies adéquates** : les attaquants en profitent (peu de solutions de type NDR, ID/PS déployées …)
- **Une configuration non-optimale des outils en place** : l'information n'est pas obtenue à la source ou les seuils de détection ne sont pas adaptés.
- **Une remontée / exploitation trop faible des logs** : les traces restent localement sur l'équipement qui les génère, sans remonter dans un SIEM ni donc déclencher d'alertes. Par exemple, les logs des firewalls sont souvent exclus : coût du volume de stockage, faible capacité à identifier un signal pertinent dans un tel volume de données, etc.
- **Des processus de traitement et de réaction des SOC parfois perfectibles** : notamment un seuil de notification inadéquat qui induit un excès de faux positifs.

Analyse des stratégies de détection adoptées par les organisations

Danger, zone de risque : une attaque est sensiblement moins bien détectée en amont (7% de détection) qu'au milieu ou en aval de la kill chain (respectivement 12 et 11%). En résumé, l'étude montre que les activités malveillantes qui touchent des endpoints (serveurs, postes de travails, application) sont globalement mieux détectées (12% de détection) que celles touchant les infrastructures réseaux (7% de détection). Cela s'explique notamment par la généralisation des solutions de type EDR.

- Dans la majorité des cas, la finalité d'une attaque est de toucher des serveurs connectés au réseau ciblé ; il semble donc naturel de focaliser la surveillance sur ces composants du système d'information.
- Détecter une activité malveillante sur un système présente un taux de faux positifs plus faible : une alerte sur un système a une plus grande probabilité d'être une réelle activité malveillante.

Détection des simulations selon les Technics du MITRE Att&ck



« POUR QUE LES RESPONSABLES DE SECOPS FASSENT L'IMPASSE SUR CETTE PHASE AMONT, IL FAUDRAIT DES TAUX DE DÉTECTION BIEN PLUS ÉLEVÉS DANS LES PHASES EN AVAL. »

Le faible taux de détection des actions de type Discovery au niveau système s'explique notamment par l'utilisation de plus en plus répandue de la technique du LotL, comme l'évoque l'ANSSI dans son panorama des menaces.

Détail intéressant, les événements relatifs à la persistance restent les plus difficiles à détecter au sein de la catégorie « Compromission & lateral movement ». Quand ces actions sont détectées, c'est généralement au moment de leur « création » (modification des clés de registre, création de tâches planifiées, configuration d'un root kit, positionnement de fichiers, etc.). Les attaquants parviennent ainsi à maintenir les accès obtenus pendant de longues durées et sans révéler leur présence.

Pour se dissimuler, les attaquants exploitent des outils légitimes présents sur les réseaux des victimes, échappant ainsi à la détection selon la technique du living-off-the-land (LotL) qui consiste à utiliser des outils déjà présents sur le réseau de la victime, notamment des outils d'administration comme PowerShell, pour arriver à leurs fins.

Ces constats ouvrent des opportunités pour de nouvelles approches de renforcement de la détection d'attaques

1

L'EDR est parfois utilisé en tant que source de détection primaire des scans de ports pour pallier l'absence de solutions purement dédiées à cet objectif. Cet usage détourné reste complexe à implémenter et présente des difficultés sur les étapes de configuration et de définition des seuils d'alerte.

2

La mise en place de **honeypots** pour remédier au manque d'outils de détection en amont de la kill chain. En disséminant de tels leurres à plusieurs endroits du réseau avec des configurations opportunes c'est terriblement efficace. Une activité réseau suspecte sur ces cibles de choix permet une levée d'alerte rapide.

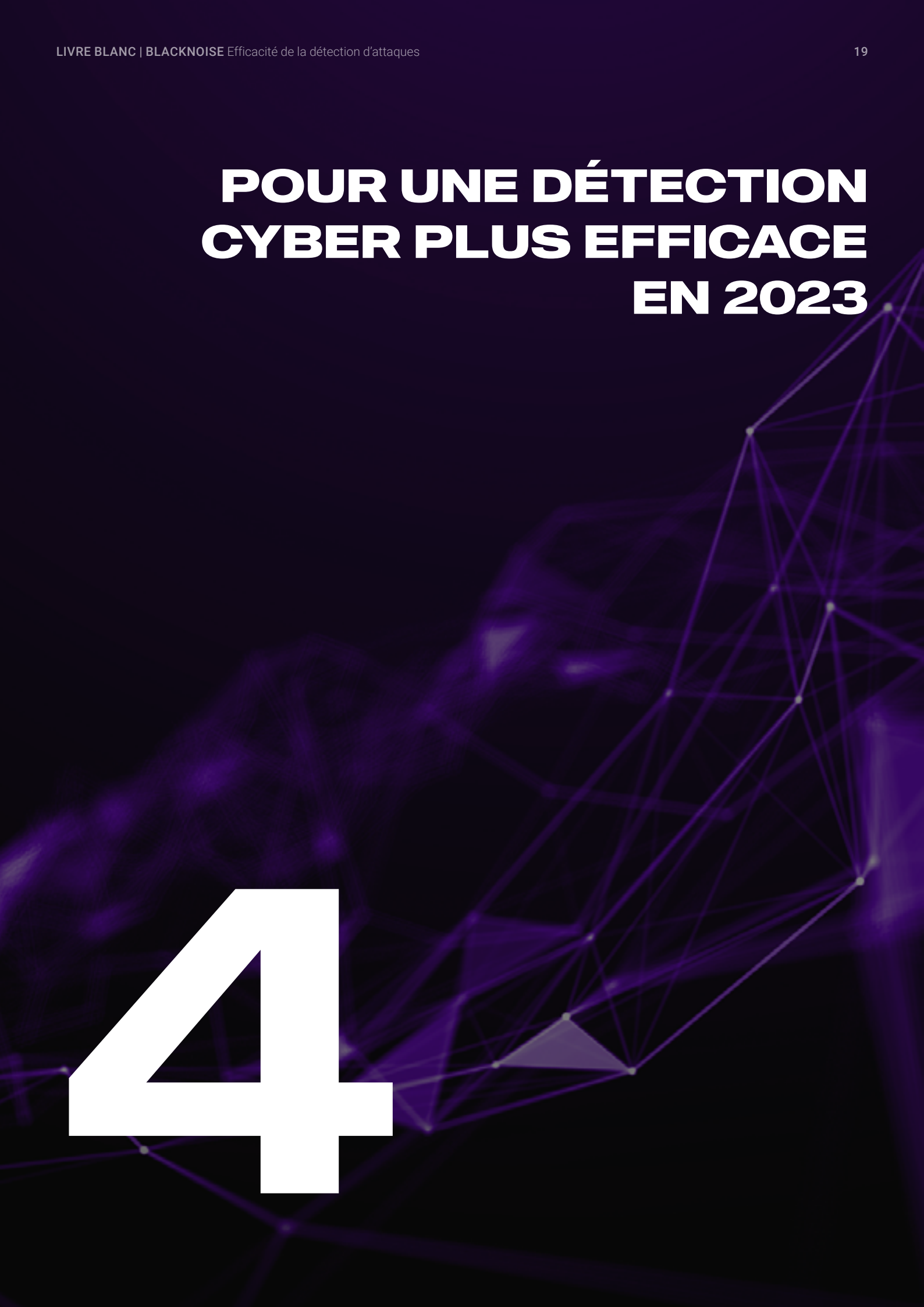
L'ÉCHEC DU MILLE-FEUILLE DES CYBER TECHS ?

Malgré un volume d'investissement en Cyber en forte croissance (9% à 14% de croissance du marché mondial selon différentes études), les résultats opérationnels ne sont pas à la hauteur des ambitions.

Les observations réalisées ne reflètent pas un manque de capacité technologique, mais un manque d'optimisation et d'efficacité de l'utilisation de ces technologies. Repenser la sécurité opérationnelle en y intégrant des contrôles d'efficacité et de non regression devient indispensable. Les solutions et services de sécurité doivent être challengés, régulièrement, sur l'ensemble de leurs capacités, avec des simulations d'attaques qui permettent de tester la sécurité «en vrai» !

C'est de cette manière que les organisations pourront contrôler et confirmer que leur cybersécurité est réellement opérationnelle et fonctionnelle, sans faire appel à de nouvelles briques techniques qui génèrent de la complexité.

POUR UNE DÉTECTION CYBER PLUS EFFICACE EN 2023



4

Une stratégie de cyberdéfense efficace doit permettre de détecter les attaques le plus en amont possible pour limiter la capacité de l'attaquant à toucher les systèmes vitaux.

Face à la découverte permanente de nouvelles vulnérabilités et à l'évolution des techniques d'attaques, la défense doit s'adapter constamment, et rapidement afin de dissuader l'attaquant.

Le système de défense repose sur trois pilliers :

Complexité

rendre complexe les techniques que doit déployer l'attaquant

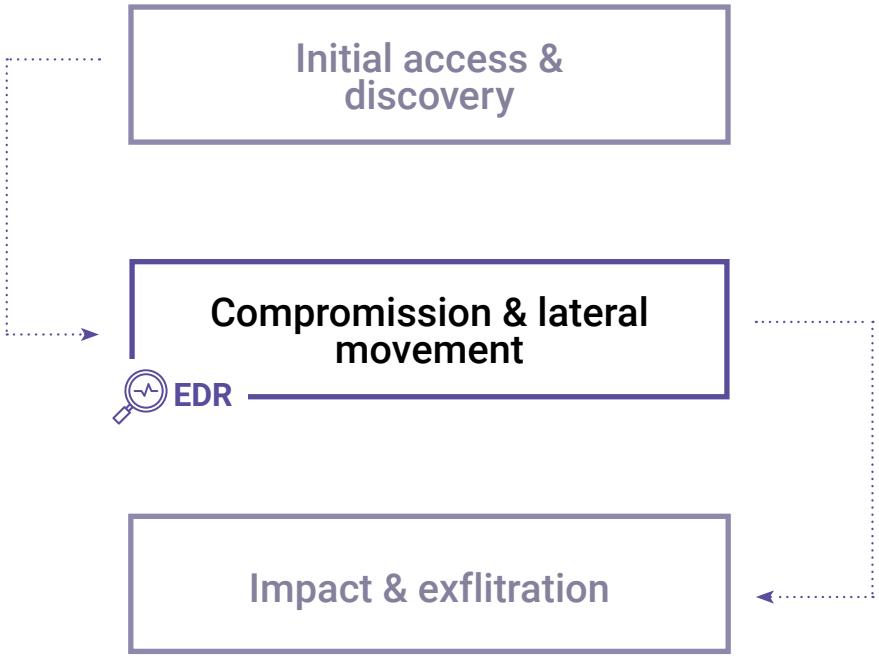
Coût

rendre l'attaque coûteuse en moyens, compétences et temps

Non standard

rendre impossible l'utilisation de modèles d'attaques standars

La capacité de détection se retrouve focalisée sur la zone centrale de la Kill Chain qui concerne les activités malveillantes sur les systèmes. Les entreprises se sont concentrées sur les actions exécutées au niveau des endpoints pour construire le principal maillon de la chaîne de défense.



Les autres types d'actions issus des modes opératoires des attaquants ne sont pas suffisamment détectés.

DANGER MAJEUR : dépendre excessivement de l'EDR, c'est accepté d'être en mode aveugle en cas de dysfonctionnement de celui-ci. Les attaquants l'ont parfaitement compris.

L'EDR serait-il leur meilleur ennemi ?

À quoi serons-nous attentifs en 2023 ?

Par analogie avec le déploiement de mesures de sécurisation complémentaires à différents niveaux techniques portés par une défense en profondeur, la capacité de détection doit également intégrer des sources à même de capter les signaux et de réagir à plusieurs niveaux.
Plus généralement, comme évoqué par l'ANSSI , le renforcement des moyens de détection est un axe clé pour une évolution vers un modèle Zero Trust.

Pour renforcer techniquement les capacités de détection et in fine permettre une défense efficace, 3 mesures clés s'imposent :

1. Une plus forte capacité à détecter les prémices d'une attaque lors des premières activités et interactions avec les environnements réseaux avec une stratégie de type Honeypot.

2. Une meilleure détection des actions destinées à acquérir une croissance approfondie des systèmes et de l'Active Directory, pierre angulaire du SI. De nombreuses commandes, qui s'appuient sur des outils natifs (LOLT attack, dualused tools), sont caractéristiques de comportements hostiles et restent peu détectées.

3. Un délai de neutralisation plus rapide de la menace en cas de comportement hostile détecté. Cela n'implique pas uniquement la dimension technologique. L'expérience montre que la réaction peine souvent par défaut d'organisation et de collaboration entre la cybersécurité et l'exploitation du SI. Des stratégies claires de qualification des menaces et des SLAs acceptables et tenus peuvent changer la vie des acteurs opérants sur le SI.

RETOUR DE TERRAIN

Un SIEM a été blacklisté par la plateforme d'envoi de mail interne lors d'une campagne intensive. Les simulations d'attaques ont généré de nombreuses alertes au niveau du SIEM qui a envoyé trop d'emails de notification. Le SOC ne recevait donc plus de messages. Un attaquant peut donc mettre hors service l'alerting du SIEM en le saturant d'événements non importants, menés à l'encontre de cibles secondaires.

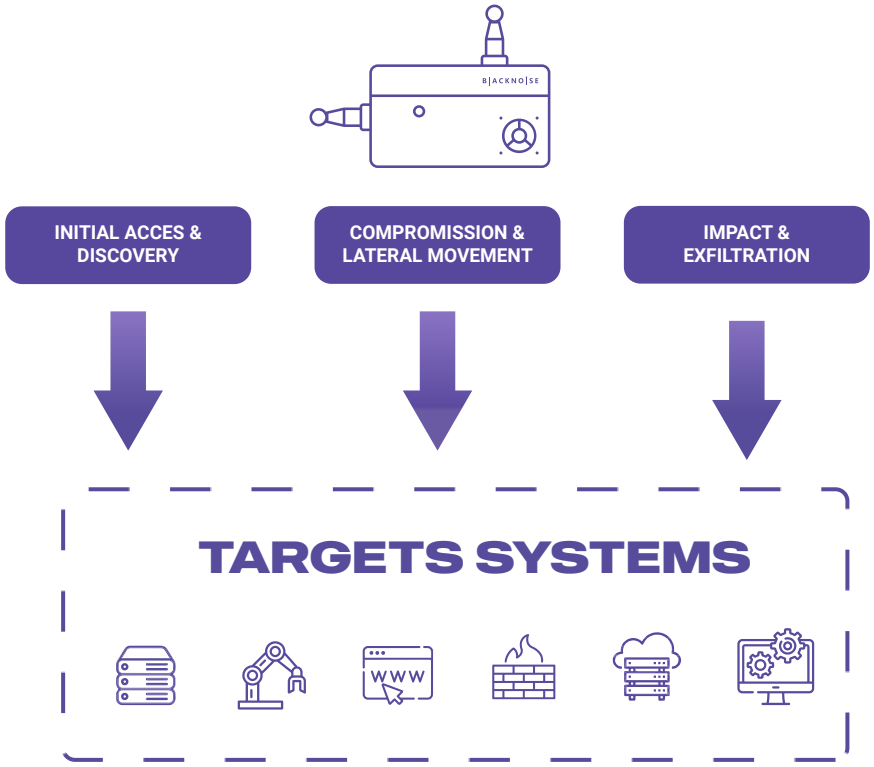
Il peut ensuite se concentrer sur son réel objectif avec un risque moindre de détection.

Breach and attack simulation :

COMMENT ÇA MARCHE ?

Une solution de « Breach & Attack Simulation » (BAS) doit simuler les modes opératoires des attaquants pour mesurer l'efficacité de la détection et de la réaction face aux attaques cyber. L'objectif est de mettre le système de défense sous stress-test pour vérifier l'efficacité de ses réactions.

Les solutions BAS reposent sur le principe de génération de bruit cyber, du joli bruit en reproduisant des patterns d'attaques réalistes sur toutes les étapes de la Cyber kill chain. Les meilleures solutions de BAS permettent de tester plusieurs modes opératoires pour chaque technique d'attaques considérée.



BLACKNOISE

LIVRABLE ÉDITÉ PAR LE GROUPE ERIUM

WWW.ERIUM.FR/SOLUTION/BLACKNOISE

CONTACT@ERIUM.FR

«L'EFFICACITÉ DE LA DÉTECTION D'ATTAQUES : BAROMÈTRE BLACKNO&ISE 2022

ERIUM