

B|ACKNOISE

ANNUAL REPORT

ATTACK DETECTION PERFORMANCE & EFFECTIVENESS: BLACKNOISE BAROMETER

YEAR 2022



SUMMARY

1

Analysis of actual **cyber defence** capabilities

2

Testing the entire **Cyber Kill Chain**

3

What did we learn in 2022?

4

Towards a **more effective cyber detection** in 2023



This document is interactive

This symbol indicates a **hyperlink**

ANALYSIS OF ACTUAL CYBER DEFENCE CAPABILITIES

1

Breach and Attack Simulation (BAS) solutions really started to be deployed in European countries in 2022.

They bring a new dimension to the cyber battlefield: Measurement of the real performance/effectiveness of detection and reaction. CISOs can no longer just rely on buzzwords and promises of delivery from cyber security vendors (xDR, DLP, IPS/IDS, Proxies...) or from service providers (SOC, NOC, MSSP, etc.).

They need better control of their OpSec resources, getting pace with the evolution of cyber attacks, and with the loss of governance related to the move to the Cloud .

Their expectations rely on at least 2 vectors:



Technological



Human

The results of the study are based on 85 simulation campaigns conducted in 11 countries in 2022

A study based on 85 campaigns ...	with a unique operating mode
tailored with a Breach & Attack Simulation solution	and a modus operandi that is adapted and tuned to the requirement of each organisation
5,270 malicious security events run	event detection validation based on a declarative mode
covers all types of organisation profiles (global companies, public sector, SMEs), from all sectors	an «undetected» type for unidentified events
all SOC types covered internal, external (MSSP) and hybrid	systematic facts and events cross-checking with the company on the completeness of simulated attacks

Attack simulations are composed of linked technical events that reproduce attack patterns. The technical events are all linked to the MITRE ATT&CK® repository and its 14 phases. **To simplify the analysis of the results, the phases of the ATT&CK® repository are regrouped into the following 3 main categories :**

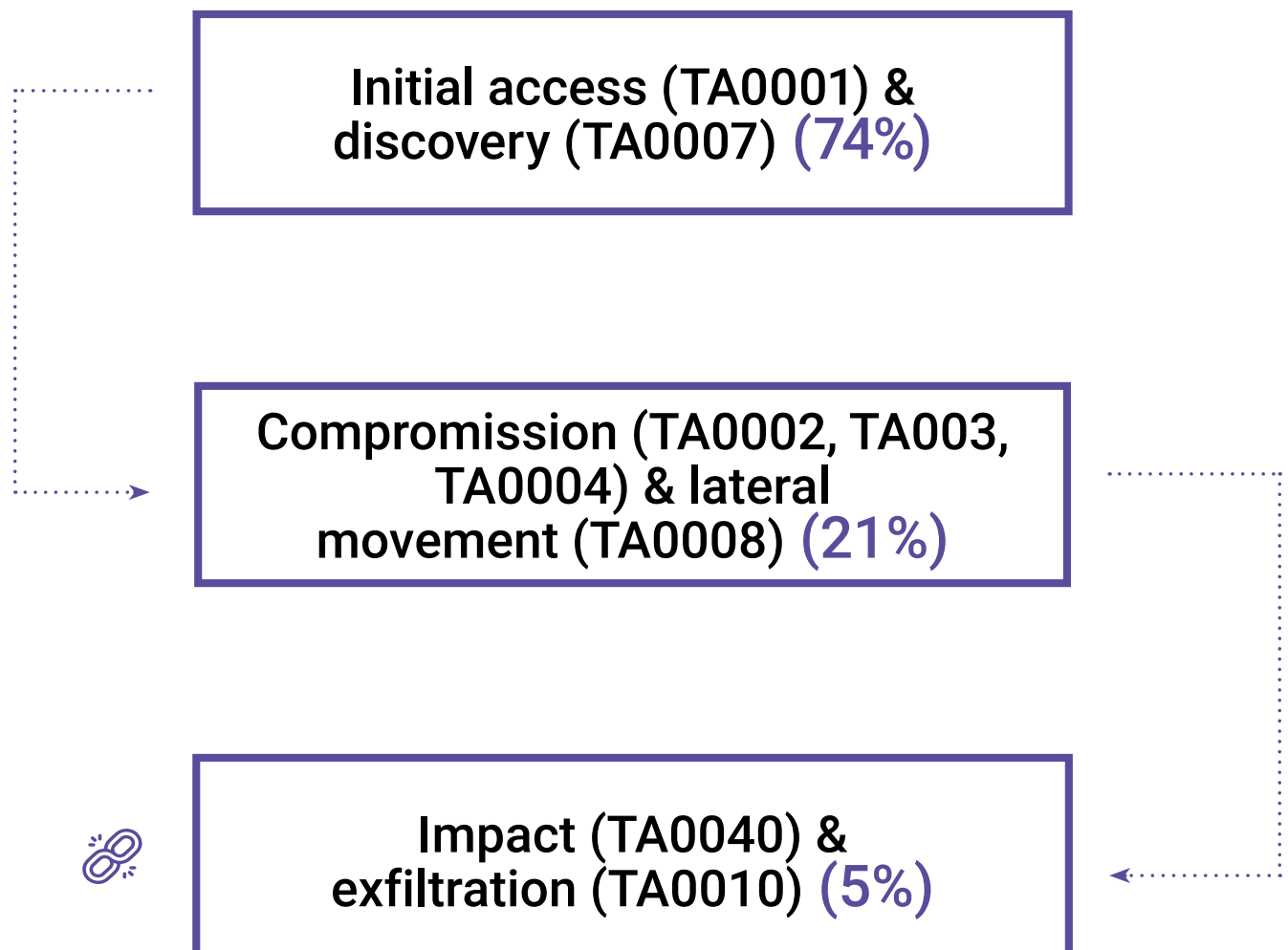
INITIAL ACCESS	COMPROMISSION & LATERAL MOVEMENT	IMPACT & EXFILTRATION
• Network access • Network sniffing • Ports scans • Service discovery • AD enumeration • Accounts bruteforce...	• Process/service exploitation • Passwords/tickets dump • Account creation • AV/EDR bypass • System modification • CVE exploitation...	• Ransomware (encryption) • Wiper (destruction) • Cryptominer • RAT (Remote Access Tool) • Malware traffic (C&C) • Cloud services exfiltration...

MITRE ATT&CK simplified Cyber Kill Chain

TESTS ENCOMPASS THE FULL CYBER KILL CHAIN SPECTRUM

2

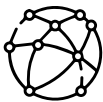
The top 3 most frequently played attack simulations by MITRE ATT&CK® category (ie Tactic) are as follows



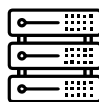
Initial Access and Discovery

74% of events, why?

The INITIAL ACCESS (TA0001) & DISCOVERY (TA0007) tests reproduce the reconnaissance techniques used by attackers to map the target and identify the components (notably systems) that can be exploited in the following phases of the attack:



INTERNAL NETWORKS



SERVER



APPLICATIONS

Tests in the Credential Access sub-category aim at obtaining access accounts and **represent 25% of the 74% of simulated events**. These discovery phases always generate a lot of noise, are verbose, and therefore represent a significant part of the simulated events.

Compromission & Lateral Movement

A logical continuation...

The compromise phases are more precise and targeted. They are the markers of the first potential impacts on systems. The implementation strategies are diverse and directly depend on the purpose of the attack and the targeted operating system (OS) against which the attacker operates.

Impact & Exfiltration

Security teams focus more on the upstream phases to block the malicious activity, even before the impact is triggered, considering that such an execution is a reflection of the failure of the previous detection phases and of the whole defence strategy.

This explains the low rate of simulated events in this category.

5270

EVENTS

were executed in the simulated attacks carried out in 2022. This represents an average of 62 events per campaign.

LESSONS LEARNT IN 2022 AND CONCLUSIONS

3

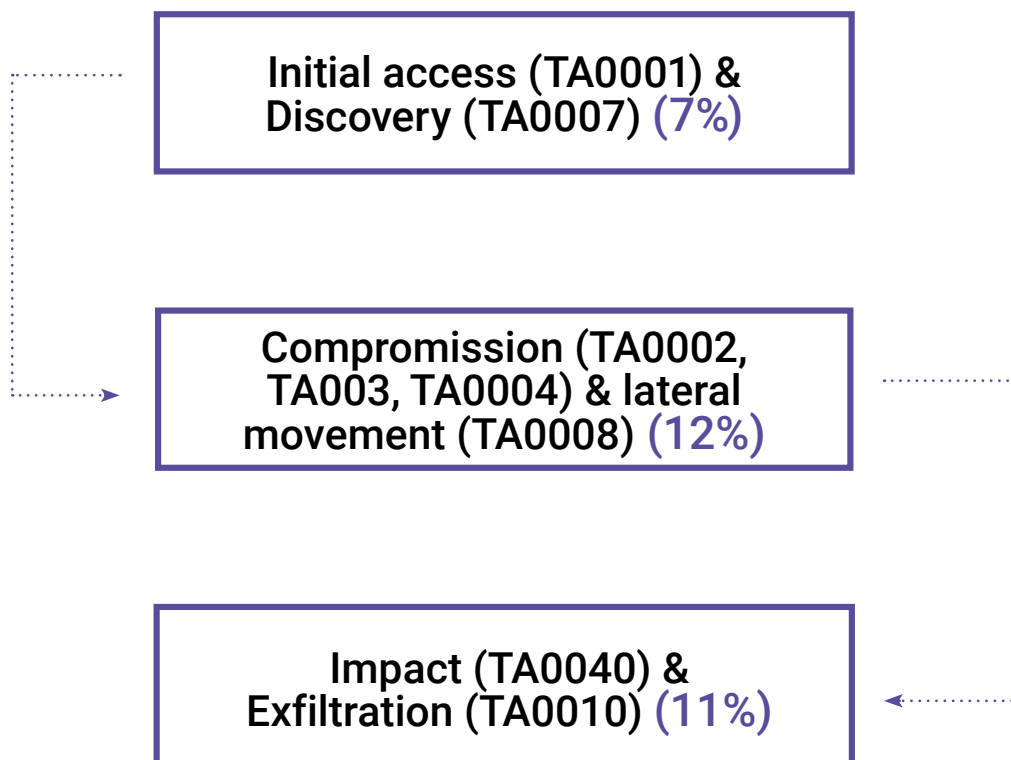
Key Finding #1

The overall detection rate remains too low.

8%

On average, the detection rate for simulated attacks is 8%. Although this rate reaches 20% for the most mature companies on this subject, it remains largely perfectible.

The level of attack detection per stage of the Kill Chain is as follows



Key Finding #2

EDR, a powerfull detection mechanism, which needs to be evaluated

75% EDR is the primary source of detection in 75% of cases.

Deployment of EDR solutions is becoming mainstream. When properly tuned, they are a key end-point component in the detection chain. A key finding is that EDR are able to detect almost a third of all simulated elevation of privileges (EoP). Such technique, used in conjunction of others are often used in the final step to achieve full compomise of a system.

When integrated in a SIEM, alerts generated by EDRs are promptly and properly handled by OpSec teams. This is another clear finding of this report; such alerts boast the lowest average response time in our analysis.

« Even if they require some effort to tune them and to keep them being efficient, EDR are definitely a critical must have component in the current defensive arsenal. EDR efficiency dramatically increase when integrated in a SIEM.»

Key Finding #3

Network level attacks mostly get undetected

83%

5 out of 6 companies fail to detect massive, aggressive network scans

A major finding is that some attacks are not detected such as those that do not generate system code execution activities. Similar issues occur when:

- **At the network layer:** connecting illegitimate equipment on a local network, port scans, traffic eavesdropping...
- **At the system level :** without command execution: service fingerprinting, bruteforcing...
- **In case of data exfiltration :** to C&C servers, cloud services providers - a best case scenario for attackers - or other third parties

There are many underlying reasons, and multiple factors, among which the most important ones are:

- **Gaps in the implemented defence technologies** to the benefit of attackers due to few or outdated NDR / IDS / IPS solutions
- **Quality issues with the configurations** of the existing security solutions such as by-default or poorly tuned configurations, which translates into lack of detection, or thresholds unrelated to the context
- **Insufficient use of logging and reporting with some logs** not getting exploited beyond the system where they are generated, with the lack of log aggregation and proper log analysis by a SIEM. For instance, firewall logs are often excluded from global management: log storage cost and bandwidth constraints used to be an issue, but log reduction technologies have become increasingly efficient. As a consequence, too few relevant alerts are triggered, hence lower capability to identify relevant events
- **Uneven quality and completeness of SOC playbooks and reaction processes**

Analysis of organisation's detection strategies

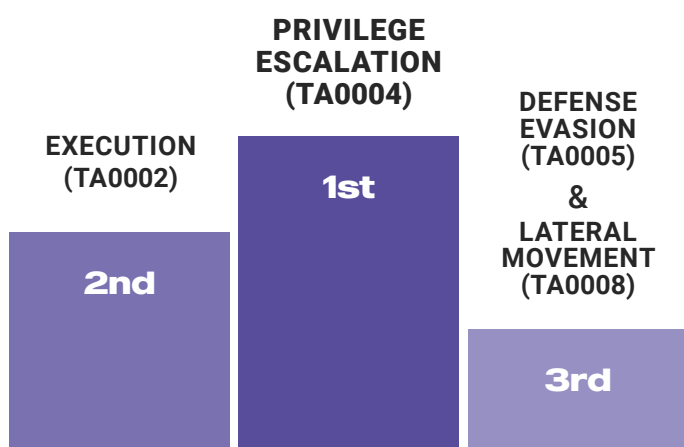


Danger ahead! over the course of the kill chain, detection ability ranges from 7% upstream, to 12% in the middle of the kill chain, and 11% downstream. Globally, this study shows that malicious activities affecting endpoints (servers, workstations, applications) are generally better detected (12% detection) than those affecting network infrastructures (7% detection). This can be explained in part by the increasingly widespread use of EDR-type solutions.

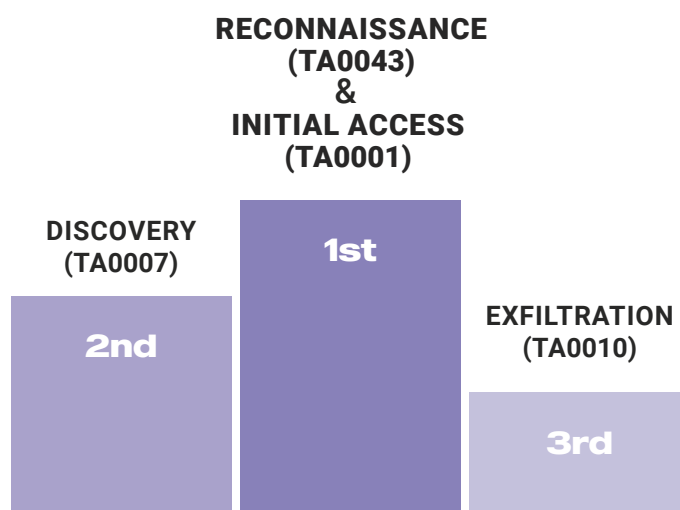
- In most cases, attacks aims at servers connected to a target network; Therefore monitoring should focus on these environments.
- Detecting malicious activity on a system has a lower false positive rate: an alert on a system has a higher probability of being real malicious activity.

Detection performance according to the MITRE ATT&CK® Tactics

BEST DETECTION RATE



WORST DETECTION RATE



SHOULD DETECTION RATE BE BETTER, OPSEC OPERATIONS WOULD BE MORE EFFICIENT

The low detection rate of Discovery (TA0007) tactics at system level can be explained by the increasingly widespread use of the Living Off The Land (LOTL) technique, as mentioned by ANSSI - the French national security agency - in its 'Cyber Threat Overview' for 2022 .

Events related to persistence (TA0003) are the most difficult to detect within the «Lateral Movement» (TA0008) tactic category. Such events are most often detected at the time of their «creation» (modification of registry keys, creation of scheduled tasks, configuration of a rootkit, positioning of files...). Attackers can remain under the radar for long period of time, and keep on performing their malicious activities. 

To lower the risks of being detected, attackers take benefit of existing legitimate tools readily available present on the victims' environments, thus escaping detection by using the Living-Off-The-Land (LOTL) technique. Commonly found examples of such LOTL tools are administration tools or utilities, such as PsExec and PowerShell.

These findings lead the way to new approaches to improve attack detection

1

EDR can be used as a primary source for port scanning detection and compensate for the lack of a dedicated solution. However this usage is complex to configure as alert thresholds must be carefully defined and tuned.

2

Honeypots set-up to remediate the lack of detection tools on the upstream part of the kill chain. A very rewarding technique is to spread such carefully tuned decoys at several locations on the network. Suspicious network activity on these prime targets will quickly generate alerts at an early stage of an attack.

THE FAILURE OF THE MULTI-LAYERED CYBER TECHNOLOGICAL ENVIRONMENT

Despite a growth in investment in cyber (9% to 14% growth of the market in the world according to various studies), the operational results are not up to expectations.

The results of this study do not show a lack of technological capacity, but it highlights a lack of optimisation and efficiency in their usages. It is high time to start rethinking operational security by integrating effectiveness and non-regression controls. Security solutions and services must be challenged, on a regular basis, on all their capabilities, with simulated attacks. What is best than performing tests in «in real life» conditions, and Breach and Attack Simulation (BAS) are an enabler.

BAS is how organisations will be able to check and validate that their cybersecurity meets expectations, are fully operational and functional in a simple and straightforward way.

FOR MORE EFFECTIVE CYBER DETECTION IN 2023

4

An effective cyber defence strategy must detect attacks as early as possible to limit the attacker's ability to affect critical systems.

As new vulnerabilities are constantly being discovered and attack techniques evolve, the defence must adapt constantly and quickly to deter the attacker.

The defence system is based on three pillars:



Complexity

Making the techniques that the attacker must deploy complex



Cost

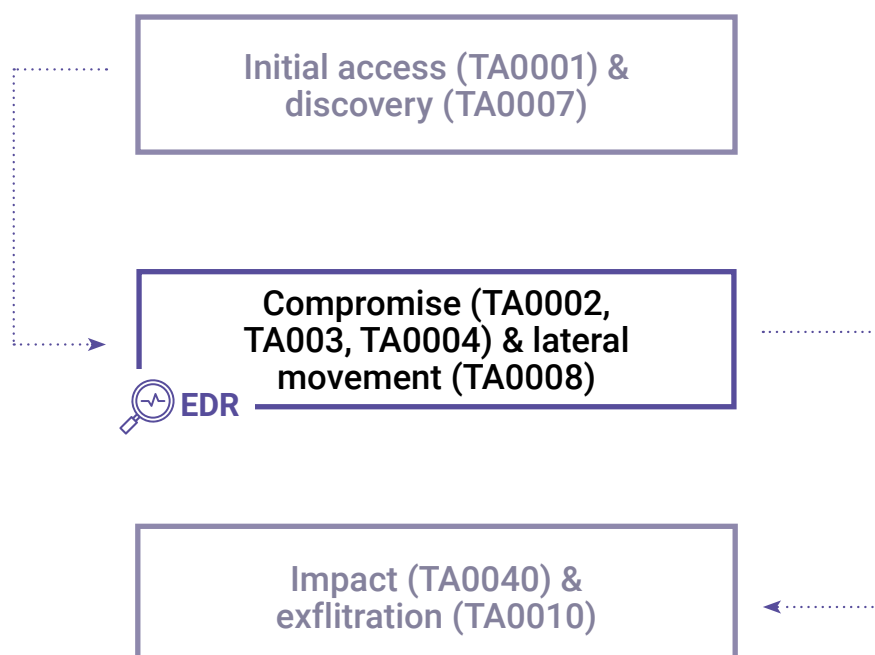
Making the attack costly in terms of resources, skills and time



Non-standard

Making more complex - or even impossible to follow common attacking schemes

Detection capability is currently focused on the central area of the Kill Chain, and relates to malicious activity on systems. With EDR, organisations keep focusing on actions performed at the endpoints as the core component of their defence. EDR is seen as the new silver bullet.



Other types of actions from the attackers' modus operandi are not sufficiently detected.

MAJOR DANGER: Excessive reliance on the EDR means accepting to be in blind mode in case of EDR malfunction. Attackers have understood this perfectly.

Is EDR their best enemy?

What to look out for in 2023 ?

Years ago, a defence in depth strategy was carried out by deploying complementary security measures at different technical levels. Nowadays, a detection capacity must integrate sources able of pick up low signals and to react adequately at multiple levels.

More globally, as mentioned by various security organisations and agencies, improving detection is key to move towards a Zero Trust model.

In order to strengthen detection capabilities and ultimately enable an effective defence, 3 key measures are required:

- 1 Stronger ability to detect the initial phase of an attack at an early stage, and to interact with network environments with a Honeypot strategy.
- 2 Better detection of reconnaissance activities which enable attackers to get a better cartography of the target assets, such as systems, and Active Directory. Many identifiable activities based on native tools - e.g., LOLT attack, dual-use tools - are typical of a hostile behaviour, but have a low detection rate.
- 3 Faster containment and eradication of a threat in case of a detection of such hostile behaviour. This is not just a technological dimension. Experience shows that reaction is often hampered by a lack of organisation and collaboration between cybersecurity and IT/IS operations teams. Improvement often comes from a clear threat qualification process, well set and validated roles and responsibilities, and SLAs.

FEEDBACK FROM THE TRENCHES

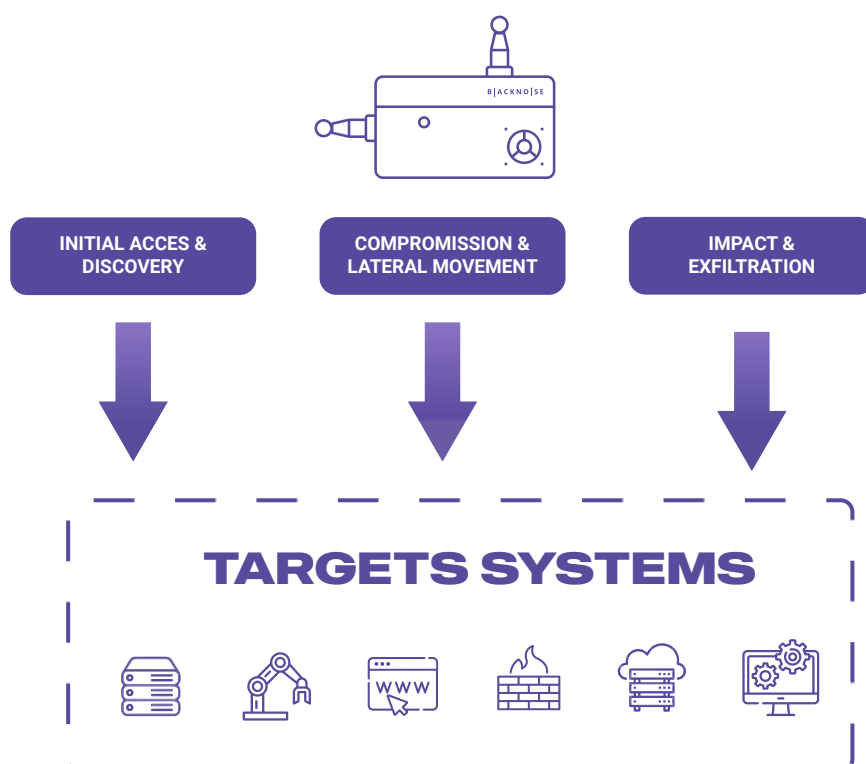
This is a case where simulated attacks generated a huge amount of alerts in a SIEM with rules which was improperly configured. Alerts were converted into notification emails, and the SIEM became blacklisted by the internal email platform. As a result, the SOC stopped receiving messages, and analysts became happy that the day was better from a workload perspective... Therefore an attacker can disable the SIEM's alerting process by saturating it with useless and noisy events against secondary targets. He can then concentrate on his final objective with a decreased risk of detection.

Breach and attack simulation :

UNDER THE HOOD

A «Breach & Attack Simulation» (BAS) solution simulate attackers' modus operandi to measure the effectiveness of detection and response to cyber attacks. The objective is to put the defence system under stress to check the effectiveness of its reactions.

BAS solutions are based on the principle of generating cyber noise - let's call it some nice noise - by reproducing realistic attack patterns at all stages of the cyber kill chain. Best of breed BAS solutions allow for the testing of multiple operating modes for each attack technique considered, aligne with the MITRE ATT&CK® framework.



B|ACKNOISE

DOCUMENT WITTEN BY THE ERIUM
CYBERSECURITY TEAM

WWW.ERIUM.FR/EN/SOLUTION/BLACKNOISE-EN

CONTACT@ERIUM.FR

EFFICIENCY OF ATTACK DETECTION:
BLACKNOISE 2022 BAROMETER