

B|ACKNOISE

EFFECTIVENESS OF OPERATIONAL SECURITY

SECOND ANNUAL REPORT
BLACKNOISE 2023

PUBLISHED ON: 01/31/2024

SUMMARY

INTRODUCTION	3
RESULTS 2023	5
Breach & Attack Simulation ^(BAS)	6
Attack simulations performed	7
Assessment of defenses	9
Assessment of risks	11
Focus on sources	13
FINDINGS	15
Improving the defense strategy	16
Optimizing costs	17
Communicating on scoring & risk	18
OUTLOOK 2024	19
Improvement plan for 2024	20

INTRODUCTION

For the 2nd year, BlackNoise publishes its annual operational security effectiveness report.

This report analyzes actual Cyber defense capabilities organized around detection and response observed in 2023. It is based on the analysis of data collected and anonymized during hundreds of attack simulations and security validation tests performed in 2023 .

The context for executing attack simulations in 2023 is centered on **3 topics**.



1 Improve the defense strategy.

Continuous improvement of security conditions is paramount for SecOps. In 2023, this improvement focused on 2 main areas:

- Improve the quality of information on the Cyber threat by optimizing CTI flows.
- Shorten the speed of detection (MTTD)¹ in the event of a security incident by improving the configuration and quality of detection mechanisms (logs, data and alert scenarios and qualification process).



2 Give leaders a picture of the real level of risk. (Cyber Scoring).

Boards require for a regular status on the state of cybersecurity: IRL metrics and dashboards must replace declarative statements. In Europe, it has accelerated in particular with the strengthening of NIS2, CRA, DORA regulations.



3 Optimize the costs of Cyber operations.

In the current context, Cyber leaders and teams are seeking to optimize their investments. This relates to both «offensive» and «defensive» budgets: the former covers audit and control activities such as pentests, Red Team type operations... and the latter covers capacity, tooling, services and staffing. in place. The automation of security detection and validation tests is therefore seen as a lever allowing better use and allocation of:

- Traditional auditing capabilities.
- The technological and human resources in charge of defense.



These 3 issues are still paramount in the strategy and roadmaps of security managers for 2024, with long term perspective.

¹ Mean Time To Detect : Average detection time

RESULTS OF 2023 ATTACK SIMULATIONS

1

1. Breach & Attack Simulation^(BAS)

BAS² solutions enable automation when launching a cyber attack scenario on a targeted infrastructure. The scenario consists is crafted by implementing technical bricks or steps of a malicious activity (also called “Kill Chain”³).

The simulation aims to measure defense capability level over 3 directions:

The overall level of resistance of the infrastructure to different known attack strategies



Detection Capability and Effectiveness (MTTD)⁴



Speed and effectiveness of defensive reaction (MTTR)⁵



A straightforward efficiency rating is established based on the results. It is based on criteria such as the performance of detection in the face of an event (fail, partial, optimal), the precise qualification of the event by the tools and/or analysts, etc.

² Breach & Attack Simulation solution

³ Modelling cyber-attacks by breaking down the modus operandi of attacks into several stages. This principle was imported from the military world and applied for the 1st time to the IT world by Lockheed Martin in 2011. Other models have been proposed since, such as the famous MITRE's ATT&CK model.

⁴ Mean Time To Detect

⁵ Mean Time To React

2. **Attack simulations** performed

The figures for 2023

The attack simulations performed in 2023 targeted the IT infrastructures of mid-sized companies or large groups in all sectors (public, aeronautics, mining, chemicals, finance, services, retail, etc).

+300

**ATTACK
SIMULATION**

13k

**TECHNICAL
EVENTS**

Over 300 Attack Simulations targeting all types of IT environments

- 87% of our attack simulation campaigns took place in (large) IT and IS environments in 2023. No surprise here: these environments are the focal point of security threats and eating up a lion's share in security budgets and spendings.
- Second comes industrial environments with 7% (various factory infrastructures, production site, logistics network). Cyber issues relating to these environments are gaining attention from managers; deployment of security monitoring, services and solutions is fast gaining traction.
- Last but not least with 6% are campaigns launched in cloud environments, mainly IaaS or PaaS. We observed a significant growth in 2023 Q4, and expect to see it increase even more in 2024.

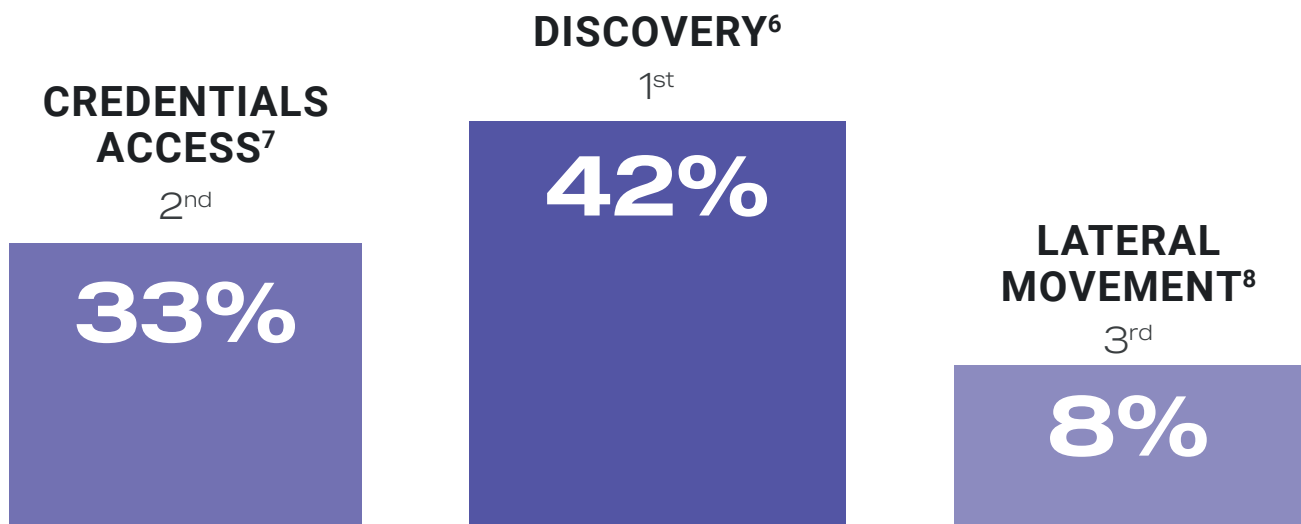
Distribution of **13k** events .

Attack simulations cover the whole Cyber Kill Chain. These simulations made it possible to execute an average of 42 Technical Events per campaign across all categories of the MITRE ATT&CK® framework.

Continuing the findings from 2022, the “Discovery” category is the most represented among the events performed . It brings together the discovery actions performed by an adversary to better understand the internal network and its systems. These actions also make it possible to evaluate the network attack surface, that is to say to identify Cyber targets of interest which would constitute exploitable entry points.

The strong representation of this category in the simulations performed is due to the fact that it brings together many different techniques and a particularly broad field of application. It is also a key step in the operating methods deployed by adversaries. Reproducing this diversity in the form of simulations makes it possible to evaluate the attack detection capacity, before the most impactful actions take place.

The top 3 most executed MITRE ATT&CK® Tactics are as follows:



The expert's gaze

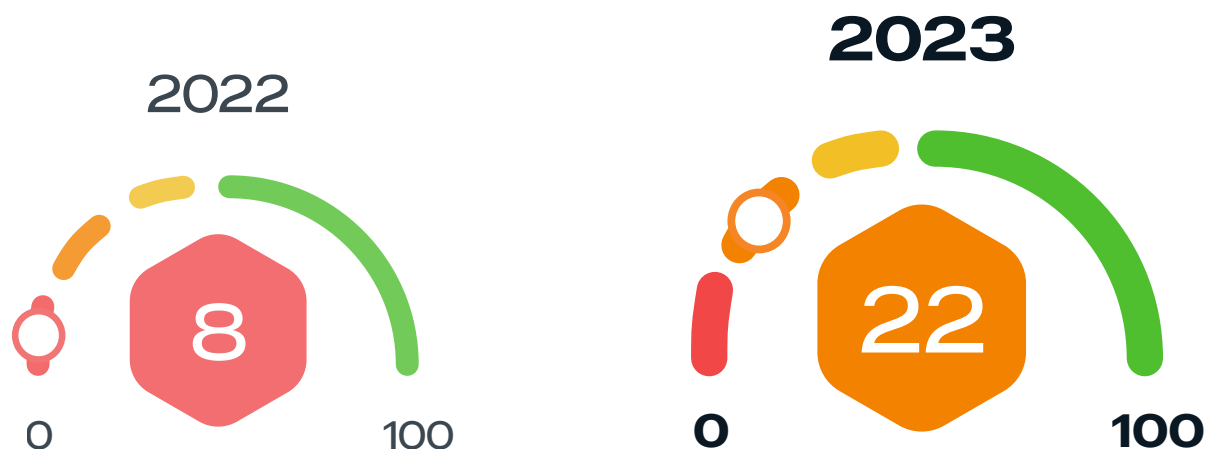
Native operating system tools are often used to achieve this information collection goal. Adversaries massively exploit such tools, thus escaping detection. This method, which is called “living-off-the-land” (LotL), has been strongly present for several years and 2023 has confirmed it.

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

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

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

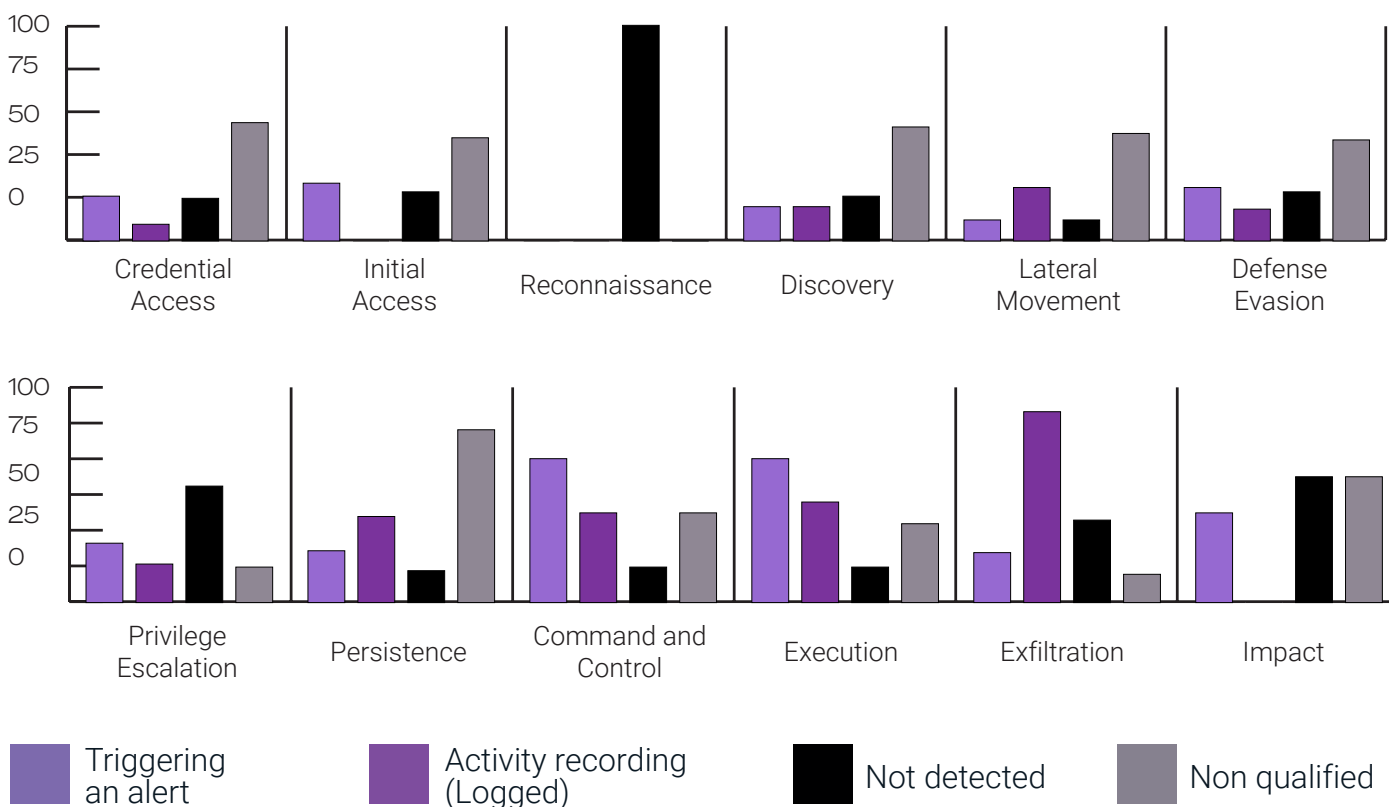
3. **Assessment** of defense capabilities



The average detection rate is increasing compared to last year, although it remains relatively low. The upward trend, even if very relative, reflects a general improvement in defense capabilities.

This can be explained by 2 key factors: the maturity of technologies such as EDR and the competence of SOC teams. But this value, taken in absolute terms, also demonstrates the urgency of advancing the entire defense chain.

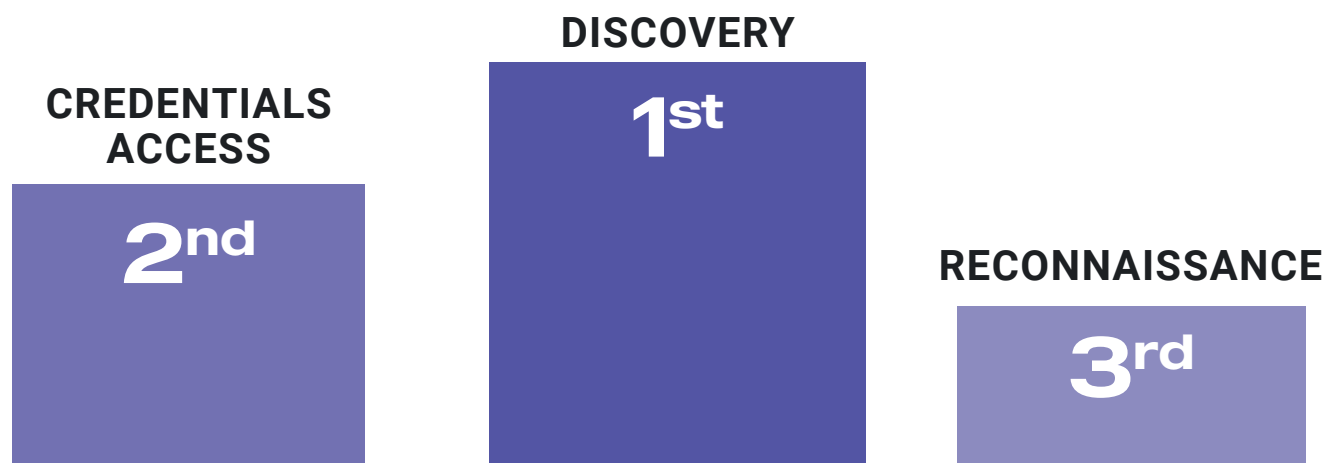
The projection of detection capabilities according to MITRE ATT&CK® tactics is as follows:



BEST DETECTION RATE 2023



WORST DETECTION RATE 2023



The “best” demonstrate that detection is more effective in the advanced phases of the Kill Chain. Adversary activity is mainly detected through sensitive, high-impact actions with a low false positive probability, performed on the systems. Monitoring focuses on the purpose of the attacks, therefore mainly at the endpoint level, and EDR is the major asset of this detection. Exfiltration actions can also be detected by more network-focused tools such as firewalls, IPS/IDS or NDR.

On the contrary, the phases upstream of the Kill Chain are more difficult to detect. Massive and aggressive network scans, brute forces of accounts, and even massive retrievals of technical information on systems or AD which allow better knowledge of the targeted environment are rarely identified⁹. This reality is explained by a multitude of factors already mentioned in 2022:

- The tools deployed do not always have real effective detection capabilities for such actions, or their configuration is not optimal to respond to them. Rather, they are palliative solutions to a little-considered problem.
- The volume of technical data generated by monitoring such behavior (notably network scans) generates several constraints: a prohibitive cost of storing logs, a high complexity of identifying a relevant signal in such a volume of data and an inadequate notification threshold. which leads to an excess of false positives.

Other approaches will be discussed the 2nd section of this report to provide effective and cost-effective responses to this poor detection capacity in the face of such adverse behavior.

“Attacks are **less well detected** upstream than in the middle or downstream of the **Kill Chain**.”

4. **Assessment** of Risk

EXTERNAL ATTACK

First observation: few simulations address the external perimeters exposed on the Internet and the effectiveness of the detection means on these perimeters is very relative. This is explained by the fact that these areas are historically poorly covered by SOCs . The latter mainly concentrate their efforts, technological and human, on the internal perimeter.



⁹ Cf. les techniques de type LotL décrites précédemment

INSIDER THREAT

The risk linked to adversaries without advanced technical skills and having access to the internal network (attackers who have been able to penetrate the IS thanks to phishing for example, employees, subcontractors, etc.) is the one which presents the highest standard deviation. The most mature structures generally detect these scenarios well and know how to neutralize the threat quickly.

Less advanced structures still display an ability to address this risk but within a restricted and well-defined scope (the “management” IS with workstations and AD, a cloud environment with very sensitive applications, etc.).



SPYING / DESTRUCTION

The risk of espionage or targeted destruction concerns operating methods originating from APT attack or equivalent. These attacks are generally targeted and orchestrated by experienced cybercriminal groups, sometimes financed or supported by states. They are often performed over the long term, with initial phases focusing on the discrete execution of preparatory actions before triggering actions linked to the final objective.

These risks can also include supply chain attacks, where cybercriminals deliberately target a less secure supplier or partner to achieve their end goal of more sensitive targets.

The technical complexity of these scenarios combined with the stealth of the operating methods makes detection difficult, which explains the greater level of exposure to risk. It should be noted that only the most mature structures in terms of defensive capabilities are moving towards this type of simulation.



DATA BREACH

The risk of data leaks is better addressed than last year thanks to an improvement noted in the detection and blocking capabilities of data exfiltration. However, the data collection actions which constitute the upstream phase of such scenarios remain undetected.



5. Focus on the main detection sources

The 3 main tools that made it possible to detect the simulations executed are as follows:

EDR **68%**
of simulations detected



Firewall/ IPS/IDS **28%**
of simulations detected



SIEM **24%**
of simulations detected



EDR is once again a major tool in the defensive arsenal this year, as its contribution to the number of detected events demonstrates. The quality of the alerts reported coupled with a low reaction time undeniably makes this type of solution a fundamental asset for detecting the actions of adversaries performed on systems, from the most basic to the most complex.

« EDR, king of detection: **2/3 of adverse actions** are detected thanks to it.»

This strategy focused on the detection of a few types of actions on endpoints, however, presents a risk: in the event of EDR failure, the entire detection and reaction chain may therefore be ineffective. Attackers understand this and often seek to quickly disable EDR or silence it.



EDR

SIEM

Firewall/IPS/IDS

The expert's gaze

Why is SIEM only in 3rd position ?

We note that the management of security incidents (in the sense of detection then triggering of remediation measures) is mainly performed directly from solutions such as EDR, NDR, MDR. Even though SIEM type solutions are older and widely deployed given their maturity, they tend to be used less in the daily performance of detection and remediation operations. data lake type service allowing us to keep traces that can be used retrospectively. But an EDR + SIEM coupling proves even more formidable for defense.

FINDINGS BASED ON THE 2023 RESULTS

A series of thin, light blue wavy lines that originate from the left side of the page and curve towards the right, creating a sense of movement and depth.

2

Improving the defense strategy



1

Hmm... Is something missing here...?

An effective detection strategy is based on 2 fundamentals: the coverage area and access to the data necessary for monitoring (logs). Highlighting blind spots on these two fundamentals through attack simulations is therefore essential.

This strategy must also aim towards defense in depth by means of several complementary detection and reaction devices. This should make it possible to better anticipate attacks by detecting malicious behavior as early as possible; but also to compensate for possible EDR malfunctions.

2

Please hold, we will attend to your call shortly.

Ensure that the detection information is reported correctly and that the people concerned can be reached.

This is one of the most commonly identified SPOFs : the on-call number is not the correct one, no one responds, the alert email falls into spam or is simply not sent, the alert notification is drowned in the flow of false positives, etc.

3

Oh? Normally it should have generated an alert...

Implement permanent monitoring of the most critical surveillance scenarios.

There are many reasons that can cause a detection scenario to fail (logs not generated or transmitted to the monitoring solution, modification of the system configuration which disables controls, modification of the attacker's signature, etc).

Carrying out regular tests to validate this is essential and increasingly systematized.

4

Catching attackers with honey

Place decoys. An ancestral strategy, formidably effective and inexpensive, trapping has made a comeback in detection strategies over the past 2 years and is broken down into several tactics such as positioning of files serving as canaries (honey file) or the deployment of honeypot, honey account, honey email, etc.

5

Go, go, go !

For the most mature structures, efforts are focused on improving the reaction speed. The speed of execution of attacks, and in particular destructive phases (ransomware, wiper), requires an equally rapid reaction capacity which is based on 3 bricks:

- Automation of the reaction with SOAR type solutions or with an EDR, for example. Very little widespread in reality.
- Existence of technical processes, for example: deployment and rapid replication of a strict filtering policy on a firewall chain.
- *Knowledge by analysts of the process applicable to qualify the severity of an incident. "To defend yourself quickly and effectively, you must already qualify gravity at the right level."*

Optimize Costs

6

Do better with what you have

Better use of the tools already in place is reflected in the control of licensing costs. Exploit what is present for better detection, use the automatic remediation functionalities of detection solutions (see previous key learning), rationalize log retention, etc. so many developments observed in 2023.

7

Making do

"low cost" strategies illustrated first and foremost by honeypot, honeyaccount, honneyemail also contributes to cost optimization.



8

Trust does not exclude control, control optimizes costs.

MSSP type services are often entrusted with the strategic function of first responder to Cyber incidents. They are generally responsible for the detection and initial qualification of malicious activities and 2 SPOFs are regularly identified at the initial stages of the incident response process, and have a significant impact on the ROI of these services:

- A severity qualification error, which impacts the rest of the alert process and leads to a significant loss of time in the response.
- A dysfunction in the alert chain which leads to latency in the sharing of information with management and the experts mobilized for support.

Customers of MSSP services wish to ensure the reliability of the incident response process and regularly test the control of the 2 points of fragility above.

9

Review usage, without questioning it.

Rethink the traditional technical audit strategy: assign pentests and redteams to the environments and targets on which the results provided by the BAS are the best, in order to optimize the use and cost of the “human touch”.

Communicate Scoring & Risks



10

KPIs from the battlefield.

Cyber risk awareness is now and permanently anchored in company strategy. But its quantification remains mainly subjective, built on specific, qualitative and declarative analyses.

Managers want to better understand the real level of risk and by extension objectively evaluate the effectiveness of their defense strategy and the effectiveness of the investments made, through concrete, readable indicators constructed on the basis of technical data.

2024 OUTLOOK

3

WHAT FOR 2024?

Building detection capabilities to identify the stealthiest threats is not a top priority. Awareness of the risk is real, but the ability to respond to it globally and effectively depends on resources that are still under construction.

Two arguments stand out regarding the Cyber issues of this strategy:

- On the one hand, it a priori promotes cost rationalization.
- On the other hand, in the medium term, it opens up the prospect of significant efficiency gains with the generalization of defensive AI in cloud infrastructures. Even if the technical reality of these new services is still unclear.

Management bodies have increasingly high expectations regarding the effectiveness of Cyber security. The phenomenon, fueled by awareness of the threat, is reinforced by the weight of future European regulations NIS2, DORA & CRA.
Overall, the effectiveness of operational teams is significantly increasing.

The level of technical knowledge, training and experience of operational teams (SOC, CSIRT, CERT) offers companies response capabilities that are constantly improving. Maintaining this efficiency with operational exercises and regular tests is becoming widespread among the most advanced players

		Trend 2023	trend 2024
TECHNOLOGICAL TRENDS	Deployment of decoys (Honey-x strategy)	➡	↗
	Regular testing of attacks targeting the Active Directory	➡	↗
	Widespread deployment of EDR in desktop environments	↗	↗
	Deployment of EDR in industrial environments		➡
	Utilization of generative AI algorithms to enhance and assist analysts		➡
	Generalization of automatic remediation	➡	↗
ORGANISATIONAL TRENDS	Implementation of Cyber Tech Scoring		↗
	Monitoring of external environments (web apps, APIs, etc.)		➡
	Monitoring of SaaS environments at the application level		➡
	Regular tracking of detection performance (MTTD)		↗
	Regular training of operational teams to optimize response (MTTR)		➡

B↓ACKNO↑SE

DELIVERABLE EDITED BY THE ERIUM GROUP.

erium.fr/blacknoise

contact@erium.fr