BLACKNOISE

# EFFECTIVENESS OF OPERATIONAL CYBERSECURITY

## DEEP PURPLE REPORT 2025

Version 1.0
Published on: 10th April 2025

ERIUM

# TABLE OF CONTENTS

# INTRODUCTION

For the third year running, BlackNoise's **Deep Purple Report** provides a strategic assessment of the effectiveness of cybersecurity systems, based on concrete feedback from simulated attacks in 2024. While detection capabilities are progressing, driven by EDR/XDR solutions, they remain too focused on endpoints and must now evolve towards a global approach, capable of anticipating more complex and targeted attacks.

Faced with a demanding regulatory environment (NIS 2, DORA, TIBER-EU) and increasingly sophisticated threats, organizations need to invest in Security Validation: regular, automated, large-scale tests that optimize existing technologies, boost the responsiveness of operational teams and guarantee business continuity.

More than just a technical challenge, mastering the detection and response to attacks is becoming a key lever for resilience, compliance and business protection in a digital environment under economic and geopolitical strain.

Pierre TEXIER
**CTO**

Arnaud LE MEN
**CEO**

# Context and methodology

BlackNoise's **Deep Purple Report** summarises the technical results of simulations carried out by the BAS[1] solution over the course of 2024. This automated approach makes it possible to assess the level of detection and reaction to different attack scenarios. It highlights key defence indicators such as **MTTD** (Mean Time To Detect) and **MTTR** (Mean Time To React). To facilitate analysis of the results, all the tests run by the solution are linked to the MITRE ATT&CK[2] model.

The solution assigns an effectiveness score based on the results obtained for each attack simulation campaign. This score depends on various criteria, such as the detection performance in the face of an event (non-existent, partial, optimal), the precise qualification of the event by the tools and analysts, the speed of detection, and so on.

## 2024 figures

**+500**
**Simulated attacks**

**18k**
**Technical events**

1 Breach & Attack Simulation solution
2 https://attack.mitre.org/

The simulated attacks carried out in 2024 by BlackNoise and taken into account in this **Deep Purple Report** targeted the IT infrastructures of small, medium or large groups in all sectors (public, telecommunications, aeronautics, transport, finance & insurance, service, distribution, etc.).

The typology of the environments tested is characterised by the following elements:

- Strong representation of office IS (more than 3/4 of campaigns)
- Share of industrial environments stable compared with last year (~6%)
- Growth in cloud environments, with tests targeting SaaS beginning to take off compared with previous years

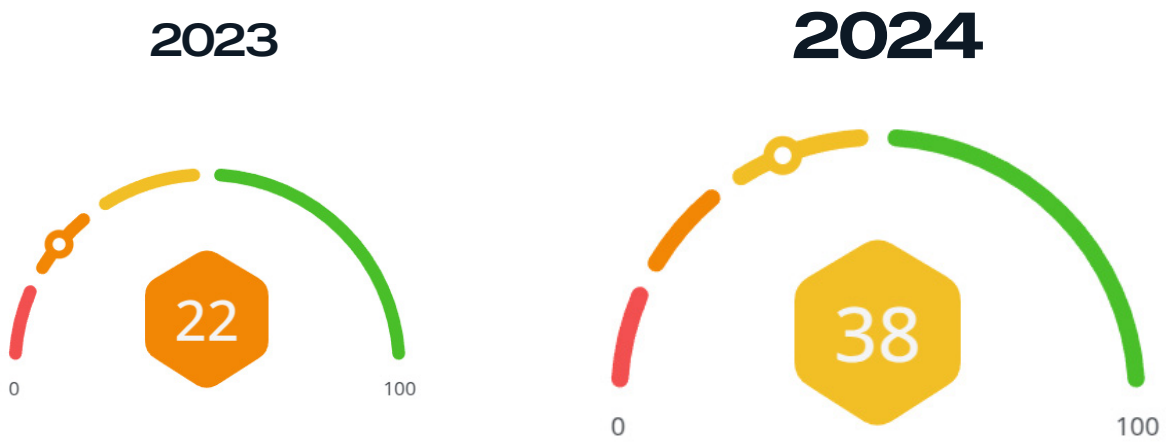
# PART 1

# RESULTS OF THE 2024 ATTACK SIMULATIONS

# 1.1) Defence capabilities assessment

## Synthesis

*Detection capabilities are improving again, both in terms of the coverage of attack techniques and the speed of detection. However, they are still mainly focused on endpoints.*




The average detection rate observed by BlackNoise is **up on last year** (+72%), demonstrating the greater overall maturity of defence systems. This improvement is characterised at a technological level by the maturity and mastery of the tools deployed (EDR, XDR/SIEM, NDR, Honeypots, etc.), as well as the expertise and organisation of the SOC[4] and CSIRT[5] / CERT[6] teams.

It should be pointed out that the figures are fairly similar, regardless of the type of SOC: in-house team, outsourced service (operated by an MSSP) or hybrid model.

The increase in the detection rate shows a significant standard deviation between players who carry out regular attack simulations and those who start this training activity.

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

## THE 2024 TOPS

### CREDENTIAL ACCESS

1st

### DEFENSE EVASION

2nd

### PERSISTENCE

3rd

The 5 techniques with the best detection rates are:

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

## THE 2024 FLOPS

### RECONNAISSANCE

1st

### COMMAND & CONTROL

2nd

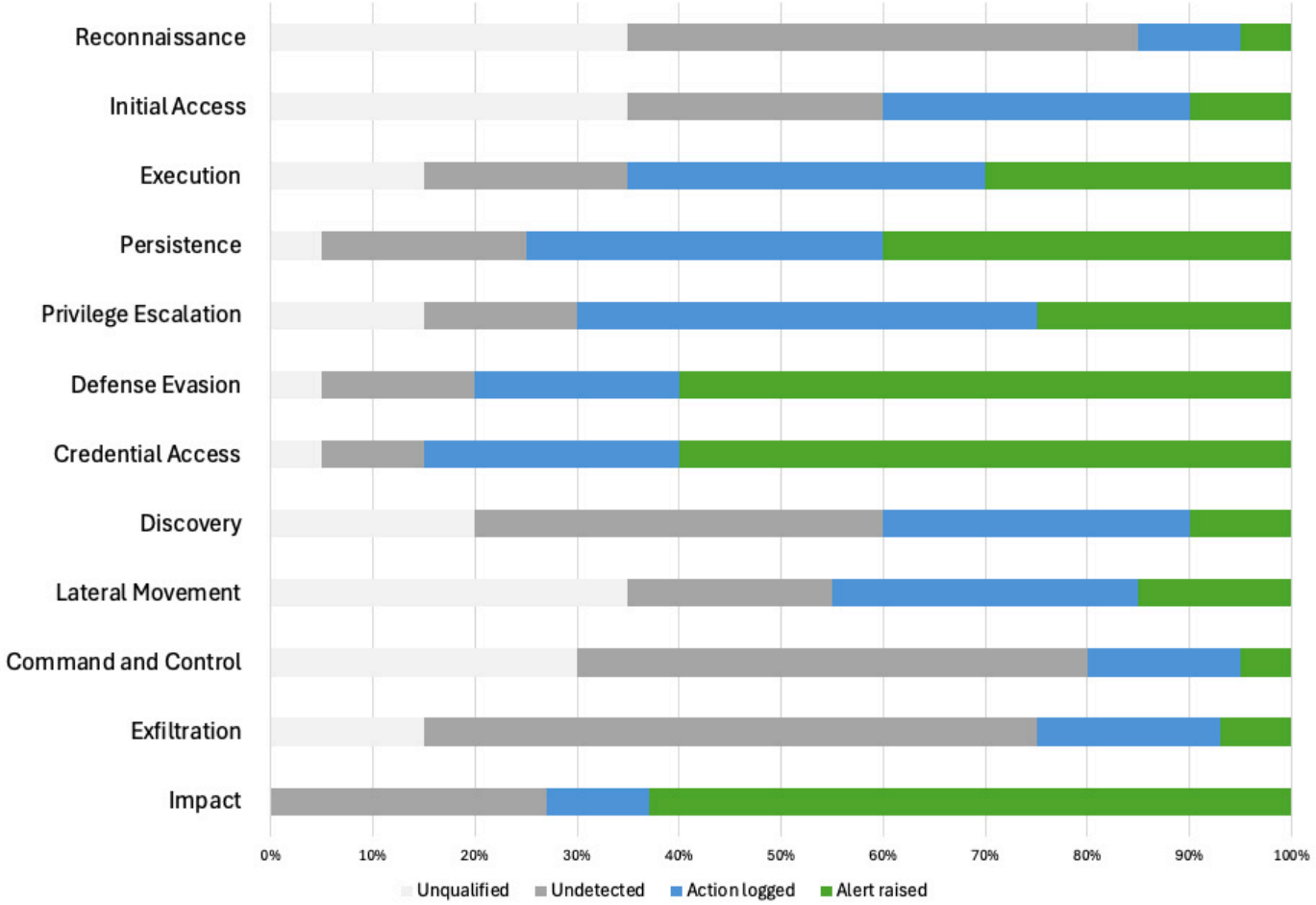
### EXFILTRATION

3rd

The 5 techniques with the lowest detection rates are:

- 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 of detection capabilities observed by BlackNoise according to MITRE ATT&CK® tactics




Firstly, detection measures are more effective in the intermediate phases of the Kill Chain (apart from the final impact). In line with our 2024 report, the behaviour of adversaries is mainly detected through **sensitive, high-impact actions with a low probability of false positives**, carried out technically on operating systems. Surveillance **focuses on the endpoints**, and EDR, coupled with XDR/SIEM, are the major assets of this detection.

Attack techniques associated with the 'Credential Access' and 'Discovery' categories no longer feature among the 'Flops'. However, many execution methods associated with these categories are based on operating modes that exploit so-called 'Living-off-the-land' (LOTL) techniques. This shows that there has been an increase, albeit controlled but real, in the identification of these techniques by defences.

# Details of « Living-off-the-land » (LOTL) techniques

*LOTL techniques use standard tools, applications or processes that are already in place on the system, e.g. powershell, certutil, teams, etc. The following native Windows processes have been observed and tested by BlackNoise: cmd.exe, explorer.exeregsvr32.exe, svchost.exe, taskhost.exe. These software components, used by administrators, are also used by attackers to collect information or execute system commands. This approach complicates the detection of such offensive behaviour because it avoids deploying new software and hides the traces in legitimate 'noise'.*

Finally, as in previous years, the **Deep Purple Report** highlights that it is more difficult to detect the early stages of the Kill Chain. Massive network scans, attempts to hack into accounts and the recovery of technical information about systems or the Active Directory - which help to better understand the target environment - are rarely detected. There are several reasons for this:

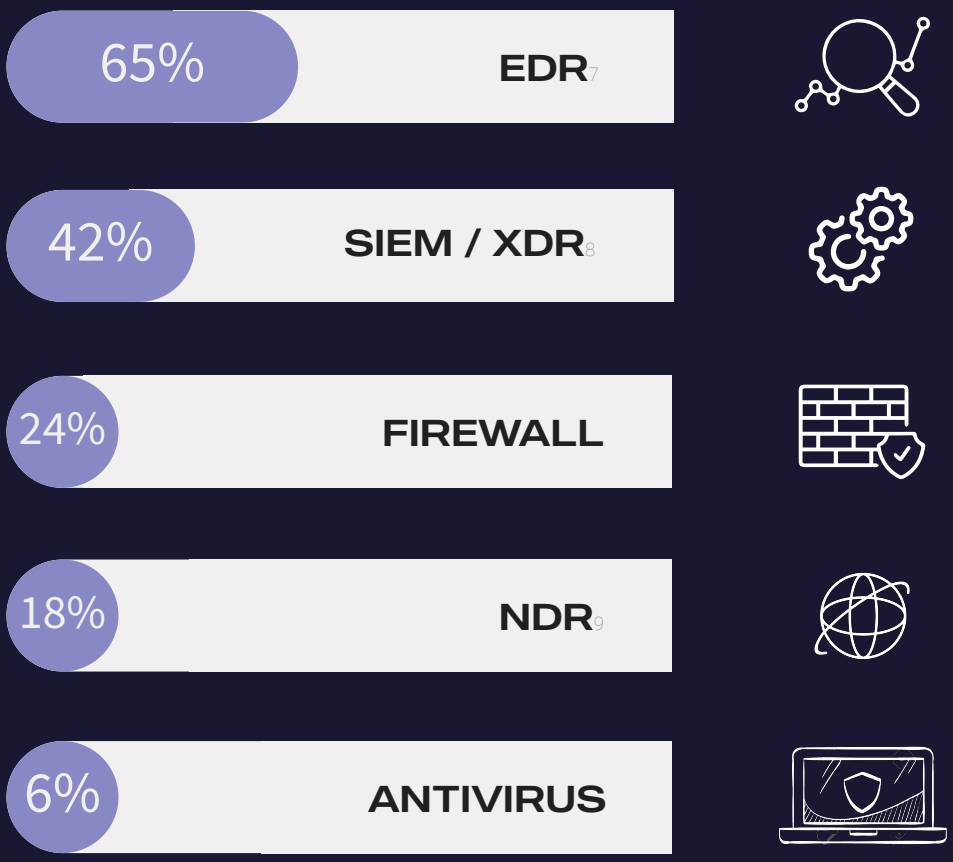
- The ability to detect this type of activity depends on the defence technologies deployed. Monitoring of network environments is often secondary, sometimes ignored or simply deactivated to limit the generation of excessive volumes of data.
- The volume of data generated by monitoring these behaviours (such as network scans) poses a number of problems: high storage costs for logs, great difficulty in finding useful information in this large volume of data, and an ill-adjusted notification threshold that leads to too many false positives.

# 1.2) Focus on the main detection sources

## Synthesis

*The main source of detection is based on the analysis of attacker behaviour detected on endpoints by EDR/XDR/SIEM. Detection is mainly carried out using rules such as Sigma or heuristic approaches.*

**The 5 main technologies used to detect the simulations carried out are as follows:**




7 Endpoint Detection and Response. Detects abnormal or malicious behaviour on terminals.
8 Extended Detection and Response. Platform that correlates and centralises data from several layers of the IT infrastructure to detect malicious behaviour. Aggregates data from different sources, not just endpoints.
9 Network Detection and Response. Monitors network traffic to identify malicious activity. Unlike firewalls, NDRs are able to detect threats by analysing traffic patterns and the behaviour of users and applications, not just signatures.

Once again this year, EDR remains an **essential tool in the defensive arsenal**, enhanced by global solutions such as SIEM/XDR, which combine different sources to capture signals from a variety of sources. The **quality of the alerts** generated, combined with a **reduced reaction time**, means that these solutions are undeniably a fundamental asset in detecting adversaries' actions on systems.

The firewall, which focuses on network layer threats, is now complemented by NDR-type technologies, capable of detecting more sophisticated attack behaviour targeting endpoints too.

Organisations with the right budgets are increasingly turning to the integration of complementary solutions (EDR, SIEM/XDR and NDR) to create a **defence in depth** capable of detecting and responding to a variety of threats. The multi-layered detection and response measures that organisations are moving towards in this way provide redundant, more comprehensive and proactive security coverage. **Increased integration and interconnection of security solutions**, enabling more effective correlation of alerts, is a major contributor to this.

It should be noted that the deployment of UEBA[10] solutions is on BlackNoise's radar this year. These solutions represent a strategic lever for proactively detecting abnormal behaviour, which is a potential indicator of compromise or an internal threat, thanks to a behavioural approach that goes beyond the limits of traditional signature-based mechanisms. The growth in SaaS usage, combined with the increase in attacks on cloud services and the growing maturity of these detection solutions, should see these solutions included in the Top 5 in the near future.

## Recommendations

- *Enhance endpoint detection by enriching the EDR configuration in the face of stealthier techniques*
- *Deploy multi-level detection and response capabilities to identify and block threats at several stages, but also to mitigate the bypassing of one of the devices by attackers (aggregation by an XDR/SIEM, network layer support by an NDR, etc.).*

10 UEBA : User and Entity Behavior Analytics

# PART 2

# TRENDS

# 2.1) Threat detection on endpoints: a combined approach

The detection of threats on endpoints using an EDR or XDR solution is based on 2 components, which can be decoupled from each other:

- The **means of execution** of the malicious action
- The **purpose of the malicious action** (the 'payload')

The data analysed by BlackNoise shows that the effectiveness of this detection varies according to the technical choices made by adversaries.

Significant differences in detection are sometimes observed when the defence tool (Antivirus, EDR or XDR) is based on identifying the means of execution, such as using the cmd or PowerShell vectors, for example. The 1st vector has a better detection rate than the 2nd, with a higher number of malicious behaviours identified, but also with a higher degree of criticality for the same action. The same action can therefore go undetected depending on the execution vector used, because it may not be judged with the same criticality, even if the final effect sought by the attacker remains unchanged.

There are several possible explanations for the lower detection rate for actions using PowerShell:

- *PowerShell* is a richer and more complex tool than *cmd.exe*. It therefore presents a higher risk of false positives, unlike *cmd.exe*, which is more limited and has less ambiguous uses.
- The distinction between legitimate and malicious activity is more complex with *Powershell* because it is part of today's standard administration tools; this would explain why *PowerShell* is increasingly being hijacked by attackers (see LOTL).
- *PowerShell* is a more recent tool than cmd.exe, so it is possible that the signatures and heuristics are better developed to detect abnormal abnormal behaviour in *cmd.exe*.
- PowerShell offers advanced obfuscation and evasion capabilities.

# Feedback

*Cases of variable detection by the same EDR were observed depending on the version of PowerShell installed on the machine. Detection worked well with a version prior to PowerShell 7.1, but was ineffective on more recent versions.*

To avoid unintentional blocking of *PowerShell* usage, detection tools are often configured to be more tolerant. This means that certain actions are ignored or their severity is reduced.

This difficulty is compounded by more **sophisticated techniques**, such as DLL injection execution on Windows, which more easily bypass traditional surveillance mechanisms. Effective detection of threats on endpoints therefore requires a **combined approach**, taking into account not only the means of execution but also the purpose of the actions, in order to identify and neutralise malicious activities more reliably.

# Recommendations

*Enhance endpoint detection by enriching the EDR configuration, whatever the exploitation vector used*

# 2.2) A predominantly manual response

## Less automated remediation

Very few remediation measures are triggered fully automatically, whether by detection tools or orchestration tools such as SOAR[11]. Remediation processes are mainly based on **semi-automated actions**, pre-configured by the tool and subject to validation by a human operator.

This observation is also shared in the SANS 'Detection and response survey 2024' report:

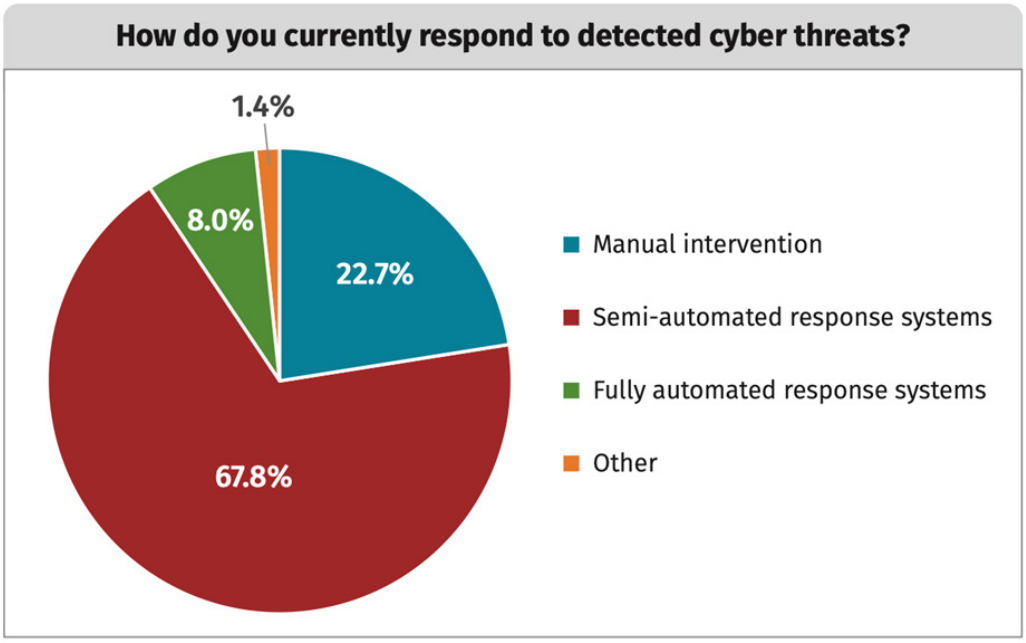



*Figure 5. Threat Response Methods*

[11] SOAR : Security Orchestration, Automation and Response

Although automation is progressing slightly, **human expertise remains essential** to manage false positives, adapt actions to specific business contexts and avoid side effects. The lack of qualified personnel, the complexity of integration and the risks of service interruption limit mass automation. Standards such as OpenC2[12] are emerging to facilitate automation between different solutions.

The most commonly adopted approach, known as semi-automation, involves taking advantage of the power of tools and the interconnection between solutions to **enrich alerts** with precise technical data. The aim of this strategy is to place response teams in optimum conditions, providing them with the information they need to make the best decisions quickly, while retaining ultimate control over the triggering of countermeasures.

The use of AI to enrich these approaches is undeniable and is a key factor that will enhance the value of automation and its benefits.

## Feedback

*Analysis of the results obtained by BlackNoise shows that the technical response actions, when they are triggered, focus mainly on the following measures:*

- *Stopping the incriminating processes*
- *Removing suspicious files*
- *Network isolation of the machine targeted by the attack by activating a local firewall blocking incoming and outgoing flows.*

12 https://openc2.org/

## Focus on the target rather than the source

The measures listed above show that semi-automatic remediation initially focuses on the target in order to **contain the propagation of the attack**. For example, in the case of network isolation, it is the compromised machine that is isolated from the rest of the network, but **the source of the attack is often ignored**. As a result, the attacker can continue his actions and compromise other systems.

To achieve **more proactive remediation aimed at neutralising the source** of the threat, it is necessary to be able to identify the source of the attack precisely in order to deploy targeted and appropriate countermeasures; for example, network isolation of the 'attacking' machine by disabling the Ethernet port to which it is connected or redirecting its flows to a specific environment. This requires advanced detection capabilities, capable of tracing precise technical information (down to the physical port of the switch involved in the case cited), and the ability to rapidly deploy this type of configuration on network equipment.

This illustrates an important point: **detection is not just a matter of speed**. It's true that you have to react quickly, but effective detection, enabling you to react appropriately, requires quality data.

## Lack of training and coordination between teams

Finally, an effective response also depends on **rigorous coordination between the security teams** (SOC, CSIRT/CERT) **and the IT teams** responsible for the infrastructures. The latter must be able to apply defensive countermeasures quickly. This means drawing up detailed procedures tailored to different cyber-attack scenarios, with regular updates based on threat trends and feedback, ideally backed up by playbooks that can be put into action quickly.

Regularly running attack simulations helps to test and improve this coordination:

- Assessing the effectiveness of detection and response processes
- Validating the relevance of available technical data
- Accelerating the correlation of information
- Optimising the implementation of remediation measures

It is essential to regularly train teams on their tools (to familiarise them with the interfaces and advanced analysis queries) and intervention processes to improve their efficiency on D-day. Ongoing training using simulated cyber-attacks, as part of a **Purple Team** approach, helps to strengthen the expertise and commitment of analysts.

## Recommendations

- *Move towards automated remediation, at least through semi-automated responses that enrich the data and suggest playbooks for countermeasures*
- *Train teams in the use of the tools in place and facilitate coordination between SOC, CSIRT/CERT and IT.*
- *Go back to the source of attacks to neutralise the origin, and not just contain the targets impacted*

# 2.3) Tsunami of vulnerabilities

## Identifying and correcting vulnerabilities is a never-ending race

Faced with an ever-increasing number of threats and attack surfaces, the traditional approach is no longer sufficient to guarantee effective protection for information systems. The evolution of IT infrastructures now relies on more and less controlled components. Increased dependence on third-party software libraries - recognised as a **supply chain** risk - is a typical example in recent years.

More broadly, between 2013 and 2023, the number of CVEs identified rose from 5,000 to 28,000, with average annual growth of 20%. In 2024, this trend worsened, with an all-time high of 40,000 VECs, an increase of 38% in one year[13].

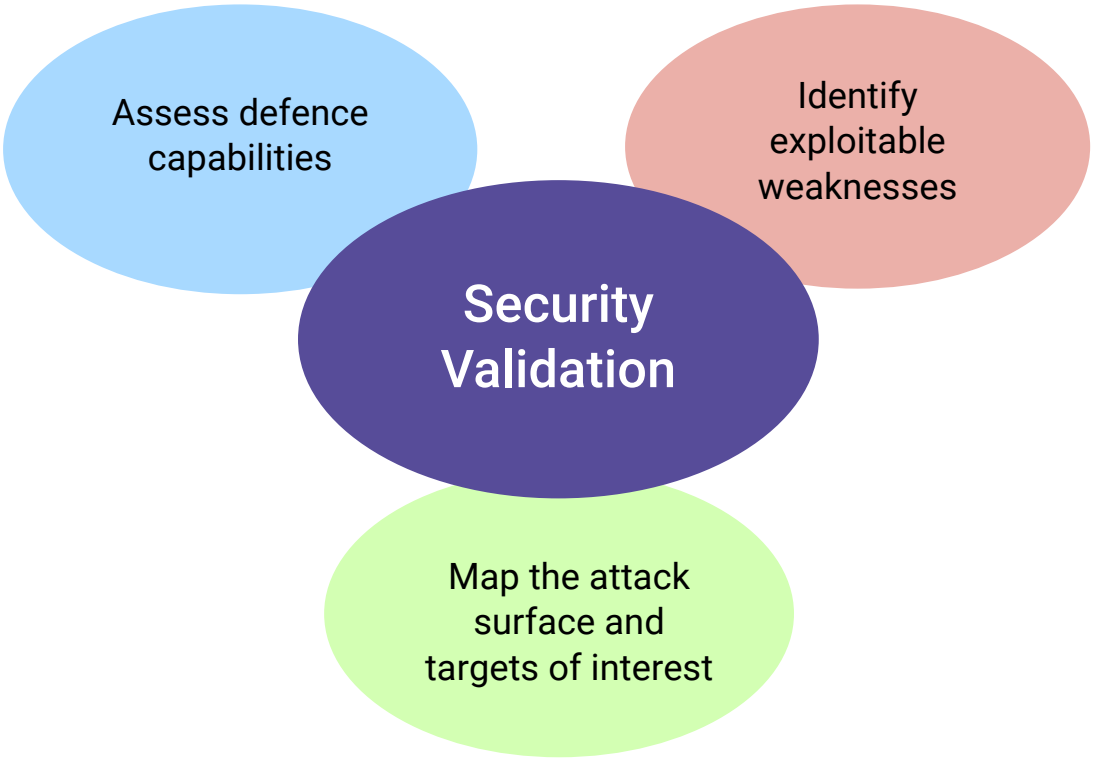
[13] https://www.yeswehack.com/news/cve-surge-record-jump-vulnerabilities

Keeping the CVE system up to date is becoming difficult. NIST can no longer manage this titanic task alone. In April 2024, the organisation announced its intention to create a consortium of private and/or public players to take over management of the NVD (National Vulnerability Database)[14].

CISA maintains an official source of vulnerabilities that have been exploited in the wild: the KEV (Known Exploited Vulnerability) catalogue[15]. The agency strongly recommends that all organisations review and monitor the KEV catalogue and prioritise the remediation of listed vulnerabilities to reduce the likelihood of compromise by known threat actors.

## Limitations of traditional methods

In this context, the usual approaches to identifying vulnerabilities, such as pentests, Red Teams or vulnerability scans, are showing their limitations in the face of an explosion in the number of vulnerabilities to be covered. We need to prepare for the next move by considering that the adversary is in a position to exploit these vulnerabilities. Defence in depth must consider the 2nd level: ensuring detection in order to effectively implement countermeasures to contain the attack.




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

To achieve this, it is not enough to exploit linear attacking patterns. A technical action carried out by an adversary can be executed in multiple ways. So the automation and parallelization of a variety of tests are essential to **test a wide range of scenarios** and strengthen defence against current and future threats.

### Example

*To illustrate this point with a simple example, a port scan performed with Nmap will be easy to spot. Another variant is to use alternative open-source tools that can bypass the detection mechanisms. But manually executing requests via Netcat makes it possible to obtain the result from the attacker's point of view, while using a 'signal' that is more complex to detect.*

## 2.4) Behavioural detection in the cloud

In cloud environments, SOCs focus their efforts on behavioural detection, monitoring unusual user actions that may indicate breaches of security policies. For example, in Microsoft 365, operations such as downloading large numbers of files from SharePoint or OneDrive may indicate an attempt to exfiltrate data, while unauthorised access to mailboxes may reveal espionage activities. Similarly, connections from unusual locations or at atypical times, although sometimes masked by the use of VPNs, are relevant indicators of account compromise.

A notable development in this approach, noted by BlackNoise, is the adoption of **User and Entity Behavior Analytics** (UEBA), which uses machine learning to detect unusual behavior and predict potential threats. UEBA can identify abnormal patterns, such as an unusual connection from a country the user never visits, a suspicious escalation of privileges or repeated attempts to access sensitive resources.

Unlike traditional systems based on fixed rules, UEBA continuously analyses behaviour to establish dynamic baselines and identify significant deviations. UEBA is particularly well-suited to detecting attacks targeting SaaS environments, as it can detect threats that are difficult to spot using traditional rules.

For PaaS and IaaS environments, attack detection still relies on the system and network layers, using the usual mechanisms: heuristics, log correlation, flow analysis, etc. For these cloud models, detection ultimately differs little from the usual environments.

But these environments are also facing attacks designed to exploit technologies and products created specifically for the cloud, such as Microsoft Entra ID. BlackNoise's **Deep Purple Report** highlights the current lower detection capacity to cover the technical components specific to the new cloud environments.

# 2.5) NIS2 and DORA compliance

A significant increase in simulated attacks was observed in the 2nd half of 2024, to the benefit of compliance work towards NIS2 and DORA (but also as part of TIBER-EU).

Compliance with these regulations requires the implementation of incident monitoring measures and clear cyber security governance. The entities concerned must comply with reporting obligations, in particular by rapidly declaring significant incidents to the relevant authorities and by stepping up their cooperation in the event of cyber attacks or operational incidents. These obligations require an effective and constant capacity to detect and react to attacks.

Attack simulations contribute to this in two major ways:

- Testing **technological capabilities** by checking security and detection mechanisms
- Assessing the **organisational set-up** by examining the processes in place

The aim is to ensure **optimum coordination** between the various teams involved, by integrating precise protocols for responding to cyber attacks.

# CONCLUSION

This 2025 edition of BlackNoise's **Deep Purple Report** confirms significant advances in cyber defence resources, particularly in the coverage of attack techniques and speed of detection. The latter is still predominant on endpoints.

However, despite this progress, remediation remains predominantly manual, underlining the urgency of adopting automation solutions. Integrating AI into security processes has become essential for effectively analysing suspicious behaviour and speeding up incident response. These developments should also lead us to step up our strategy for neutralising attacks, going beyond the simple logic of target containment.

Finally, automated attack simulations are increasingly being used to meet European compliance requirements such as NIS 2 and DORA, in order to strengthen organisations' preparedness needs in the face of threats.

BLACKNOISE

www.blacknoise.co

contact@blacknoise.co