kaspersky

2022

ANALYST REPORT | MDR | SOC

MANAGED DETECTION AND RESPONSE

by Kaspersky Security Operations Center

Contents

Introduction

The Managed Detection and Response Analyst Report 2022 presents the results of analysis of incidents detected by Kaspersky's Security Operations Center (SOC) team. The report is published annually.

The report provides information about the most common attack tactics, techniques and tools, as well as the nature of detected incidents, their geography and distribution by vertical.

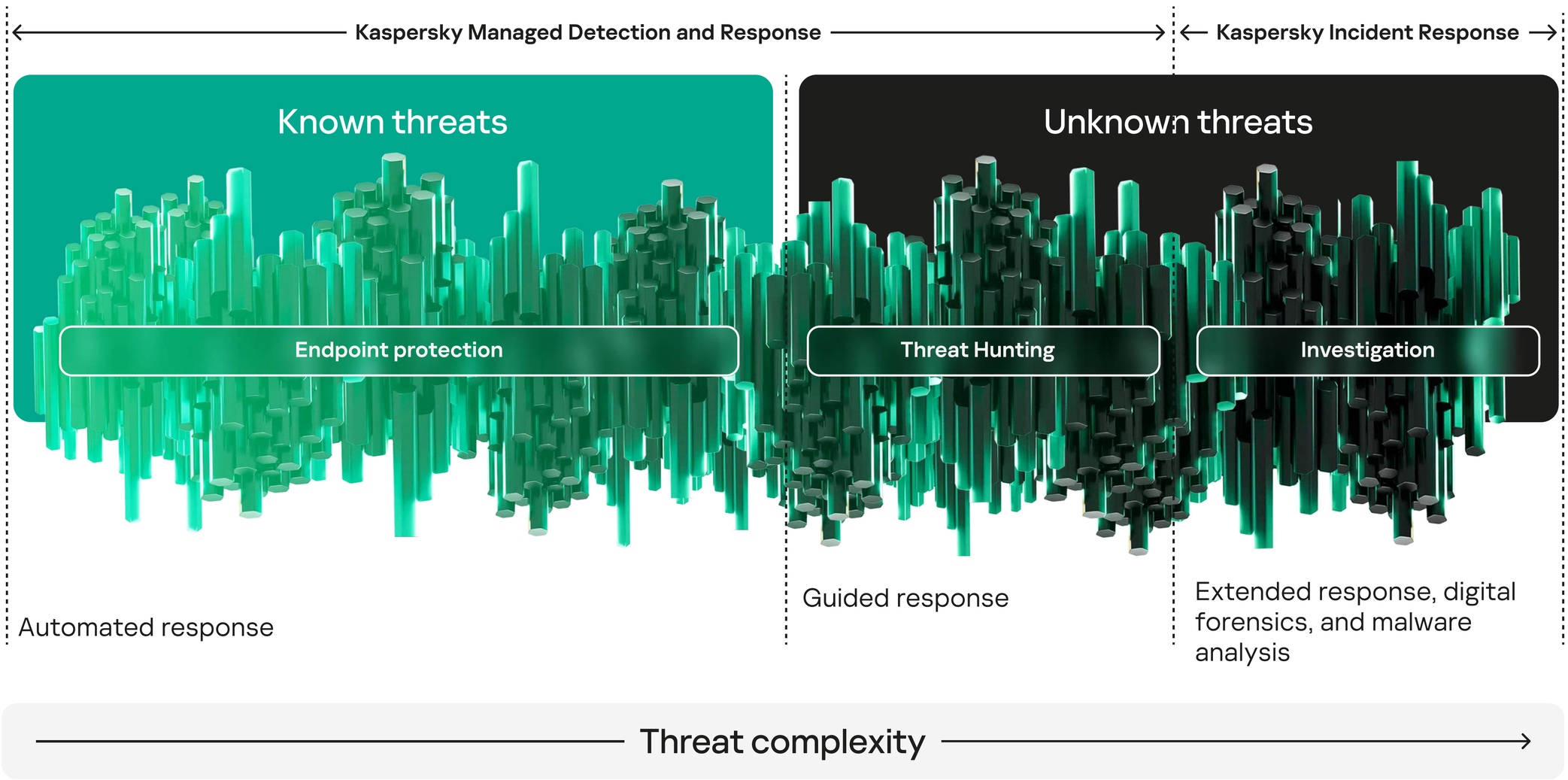
The report answers the following key questions:

- Who are your potential attackers?
- What are their current methods?
- How can you discover their activities?

Kaspersky's approach to incident detection and response

Kaspersky Managed Detection and Response (MDR) and Kaspersky Incident Response (IR) services cover the entire incident management cycle - from threat detection to post-attack recovery.

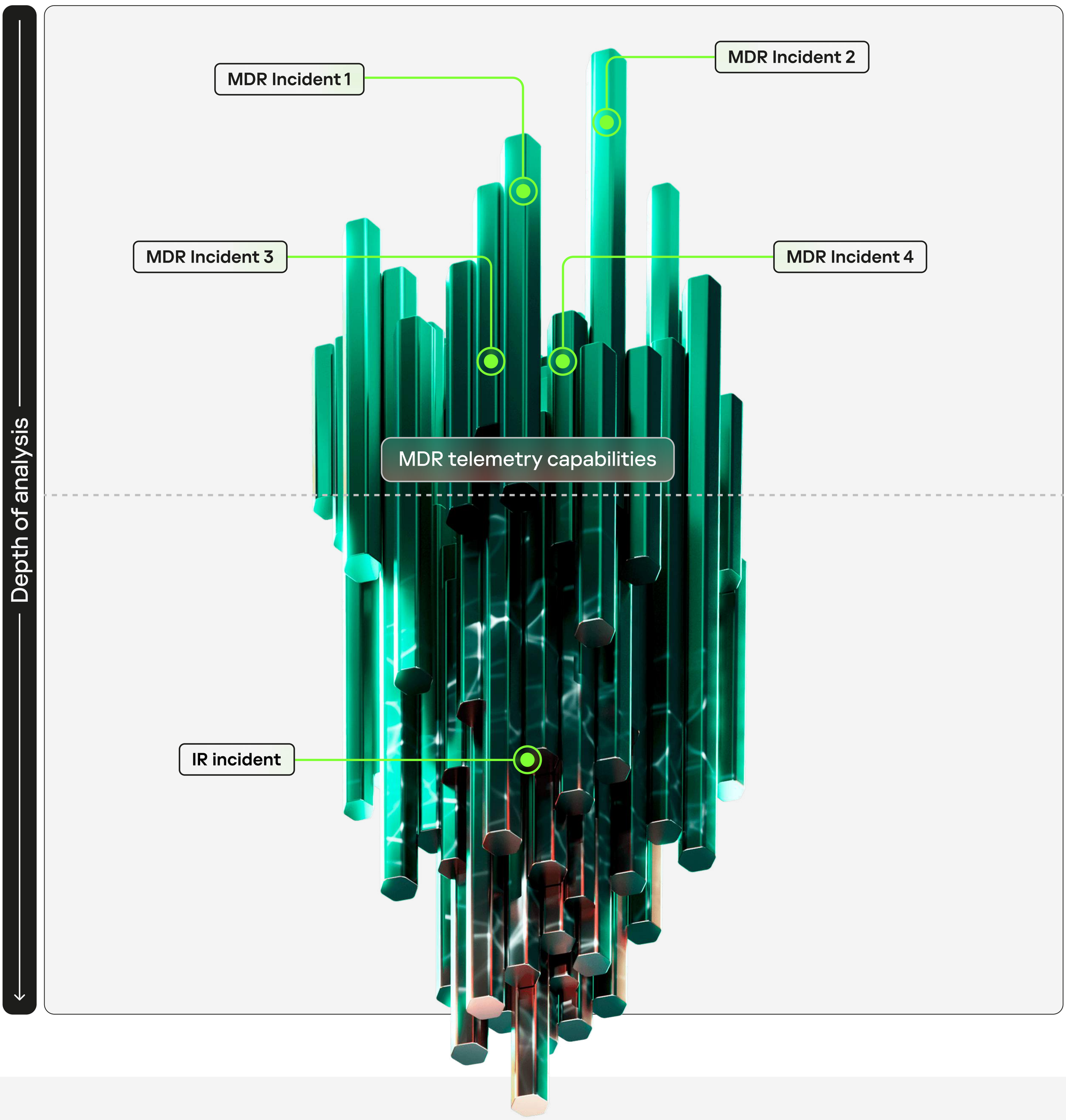
The main purpose of the MDR service is to detect threats at every stage of a cyberattack, both prior to actual compromise and after malicious actors have penetrated the corporate infrastructure. This is achieved through the use of preventative security systems and threat hunting, both integral components of MDR.



MDR also includes incident investigation and response, but depth is limited by the capabilities of the technology stack. If the situation calls for in-depth analysis of artifacts and advanced response capabilities beyond a fixed set of tools, we can engage the Incident Response team. They use an adaptive approach to design an optimal plan as part of the investigation effort.*

* MDR and IR can be purchased together. Each detected MDR incident may be forwarded to the IR team at the customer's discretion if advanced response that is outside of the MDR scope is required. These are typically high-severity incidents with direct attacker involvement.

Attacker activity during incident

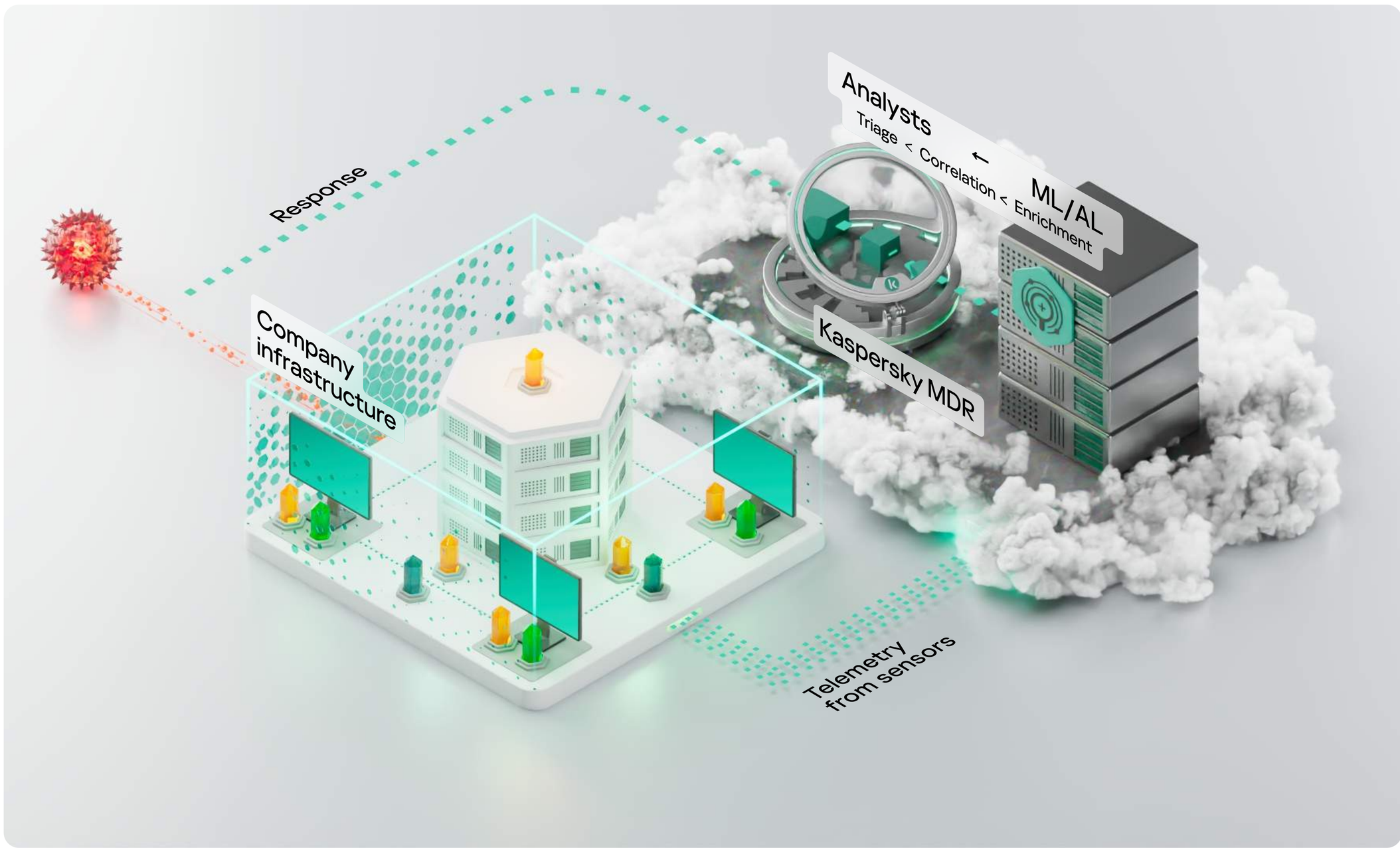


About Kaspersky Managed Detection and Response (MDR)

Kaspersky MDR is a 24/7 incident monitoring and response service powered by Kaspersky SOC technology and expertise.*

Endpoint security systems installed on the customer's premises capture and forward telemetry data which is then analyzed by machine learning tools, with the direct involvement of the Kaspersky SOC's attack detection experts. Response is provided by endpoint security sensors.

SOC analysts investigate alerts and notify the customer about the malicious activity, providing tool-based response and advice.



Sensors NIDS EPP/EDR Sandbox

* Supports all endpoint security products and Kaspersky Anti Targeted Attack Platform.

Key takeaways from 2022

Key incident statistics

3+ critical incidents per day

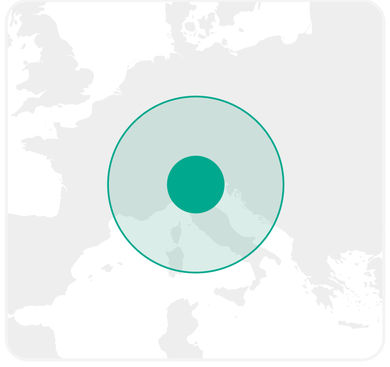
43.8 min mean time to detect a high severity incident

72% of incidents were successfully remediated following one alert

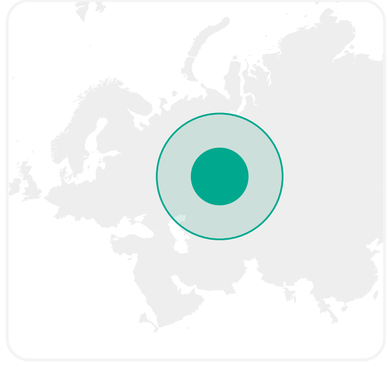
Verticals with the greatest number of recorded incidents

Industrial	22%
Government	15%
IT	16%

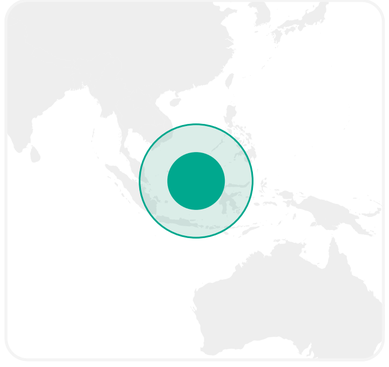
Key regions



Europe 44%



Russia and the CIS 25%



APAC 15%

Incident severity distribution

High	8.1%
Medium	71.8%
Low	20.1%

Most frequent attack profiles

[3] Malware attack conducted without visible human involvement

APT	30%
Penetration testing	19%
Crime[3]	26%

Most popular techniques and tactics as classified by MITRE ATT&CK

T1210	Exploitation of Remote Services
T1078	Valid Accounts
T1098	Account Manipulation

Attackers' tools of choice

powershell.exe	1.29%
rundll32.exe	1.02%
msiexec.exe	0.44%

General recommendations

Multi-layered information security

More than 25% of high-severity incidents are linked to malware, which proves the need for a multi-layered approach to information security.

Threat Hunting

The number of targeted attacks with direct human involvement continues to grow from year to year. Efficient detection of these requires threat hunting combined with classic alert monitoring.

To provide technological support for threat hunting, it is recommended to use professional tools such as threat intelligence platforms, specialized sandbox environments, and threat attribution systems to identify the correct defensive measures.

Threat Intelligence

Any targeted attack involves thorough preparation, and at this stage, traditional security systems are powerless against the actions of attackers since there is no active impact on the infrastructure.

Special attention should be paid to tactical, operational, and strategic threat data related directly to your organization. It is also important to analyze the techniques and tools used by known APT campaigns and cybercriminal groups.

Incident Response

The success of incident management largely depends on the correct response to identified threats, including how effectively suspicious objects are analyzed, whether all artifacts are correctly interpreted, and if the response process is properly organized.

Red Teaming

Targeted attacks are simulated as close to reality as possible during cyber-exercises involving Red Teaming. This is a productive way to train attack detection and security assessment teams.

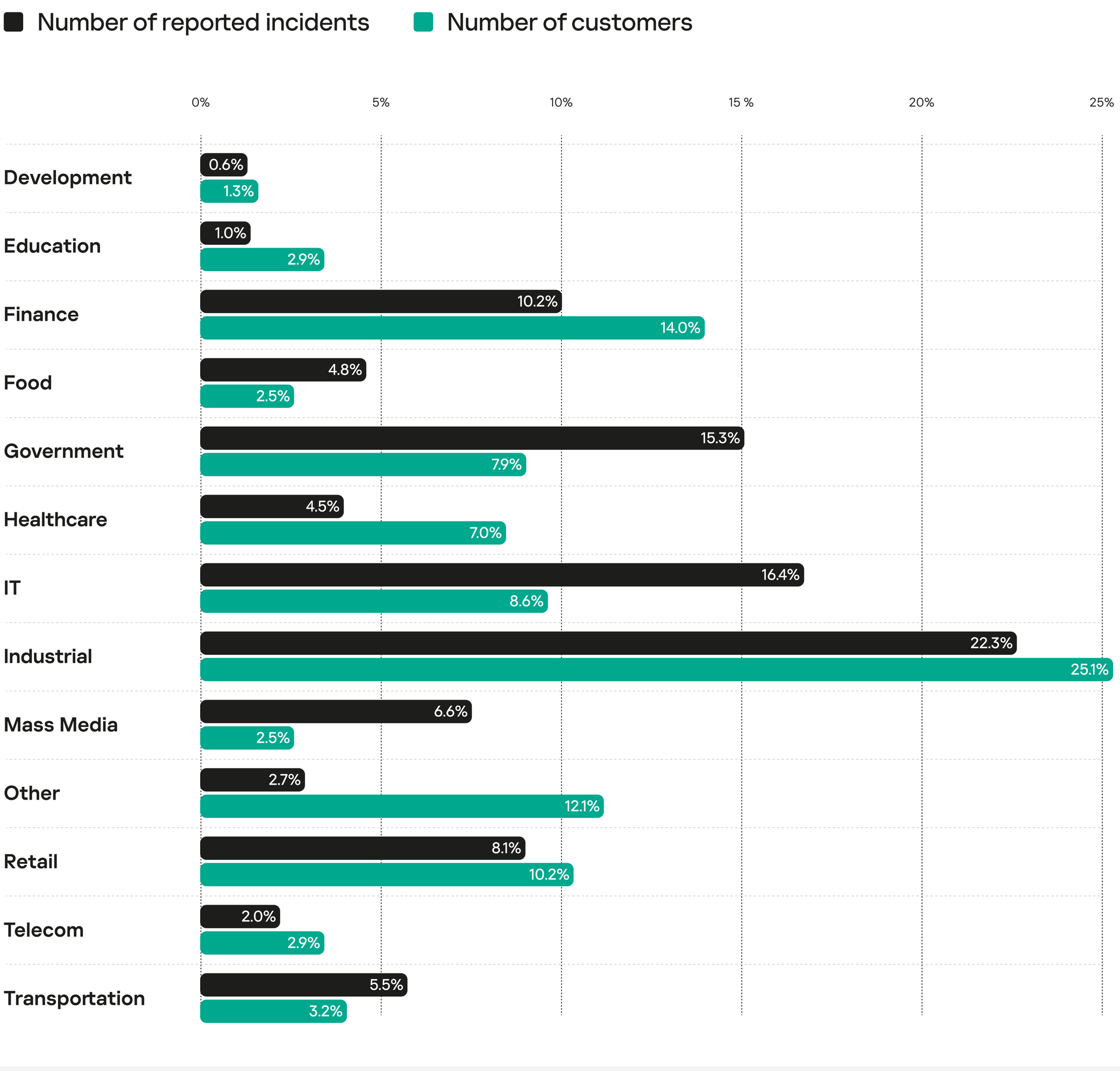
MITRE ATT&CK®

Using the MITRE ATT&CK® knowledge base boosts detection performance. The most complex attacks consist of simple steps and techniques. Detecting one step can help to expose the entire attack sequence.

MDR incident landscape

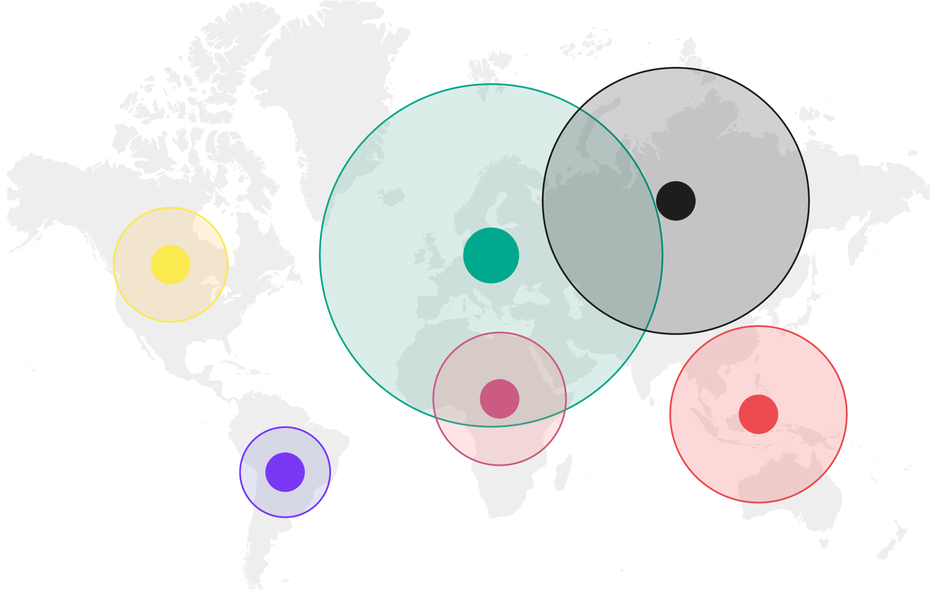
Most-attacked verticals

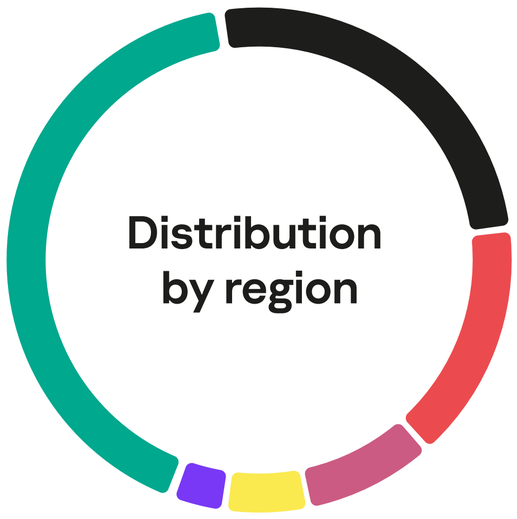
The greatest number of MDR incidents in 2022 was discovered in the industrial sector (22.3%), in government institutions (15.3%), in IT (16.4%), financial institutions (10.2%), retail (8.1%) and mass media (6.6%) companies.



MDR incident geography

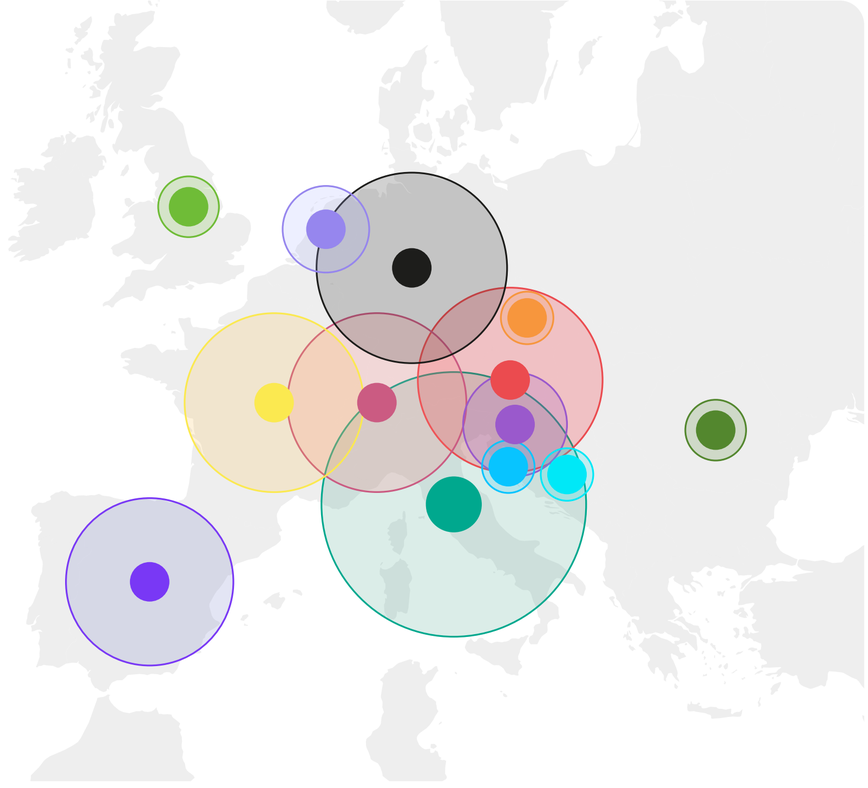
If you’re looking for a complete grasp of threats, you need to gather information from various regions, as threat actors' motivations, tactics and techniques are location-specific.



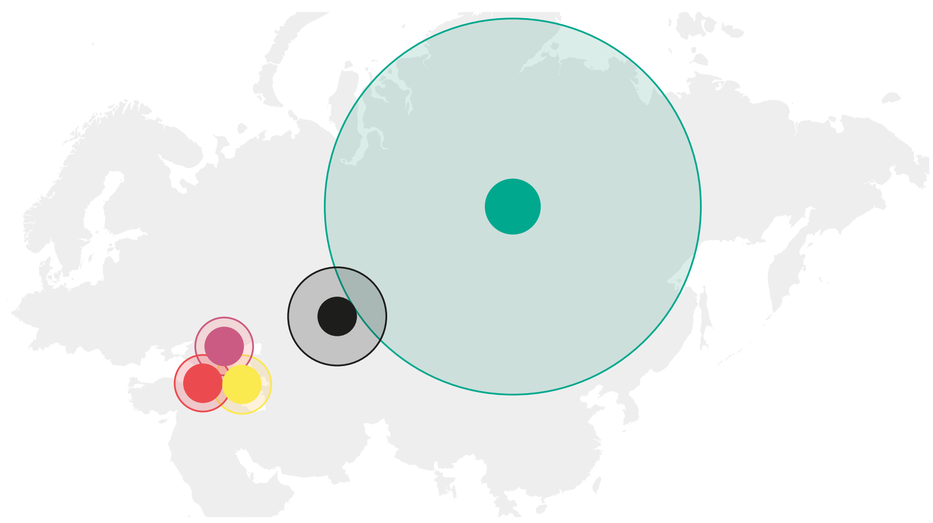


Region	%
Europe	44
Russia and the CIS	25
APAC	15
Middle East	8
North America	5
Latin America	3

In Europe, MDR provides the best coverage for Italy, Germany, and Austria.

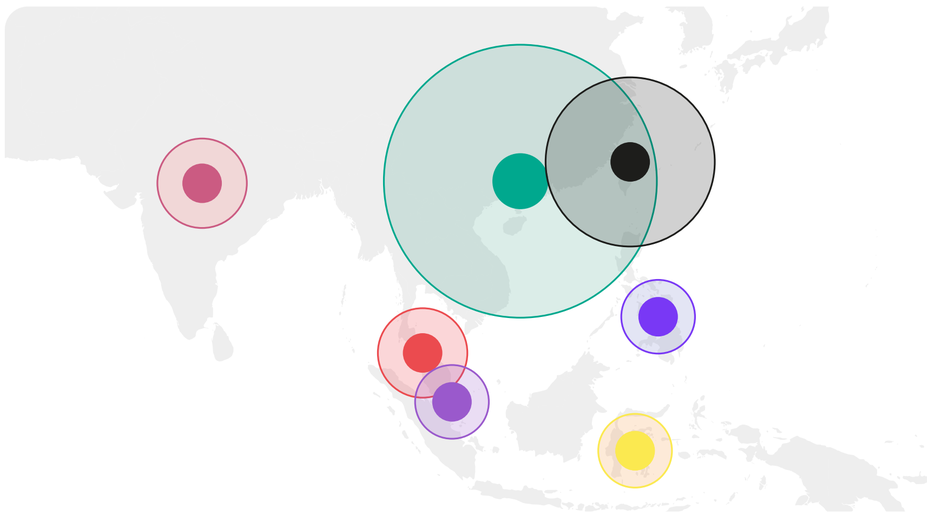


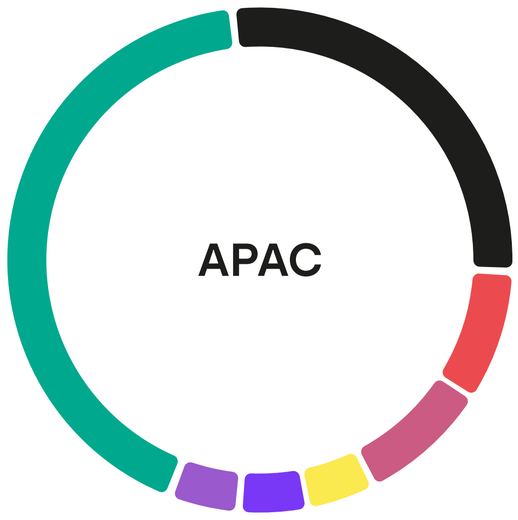
Country	%
Italy	28
Germany	15
Austria	12
Switzerland	10
France	10
Spain	9
Slovenia	5
The Netherlands	4
Great Britain	2
Romania	2
Czech Republic	1
Bosnia and Herzegovina	1
Croatia	1



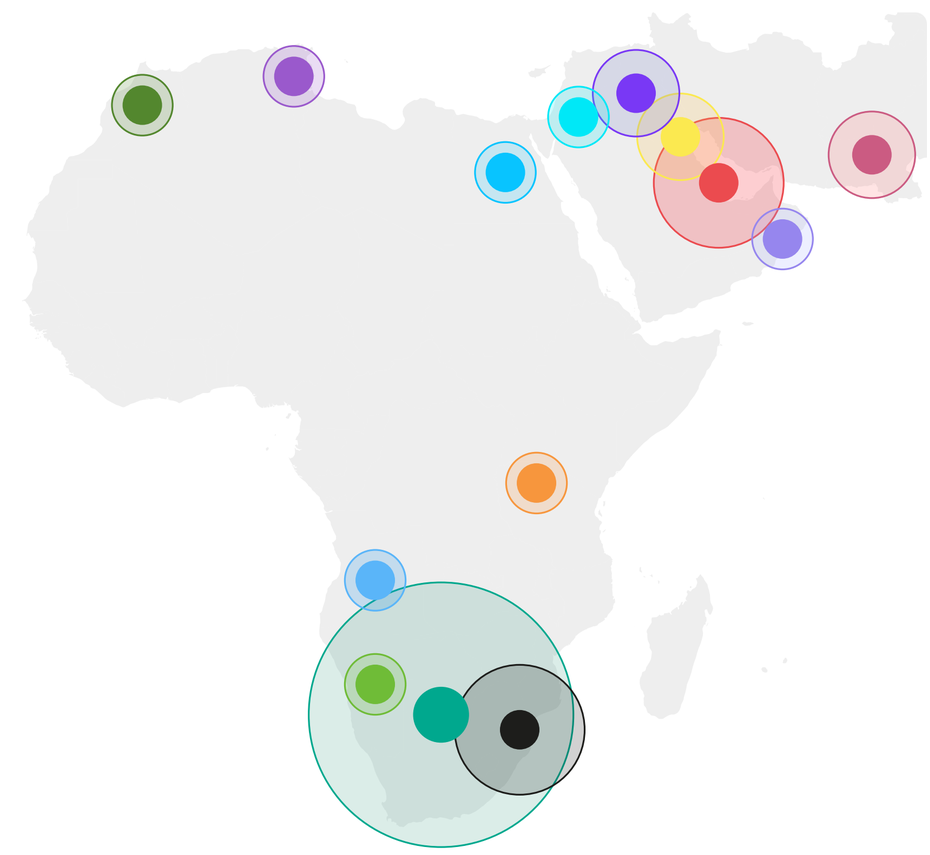
Страна	%
Russia	90
Kazakhstan	7
Armenia	1
Georgia	1
Azerbaijan	1

In APAC, MDR is most active in Hong Kong and Malaysia, in META, it's South Africa, Eswatini and Qatar, and in LATAM, it's most prominent in Brazil.

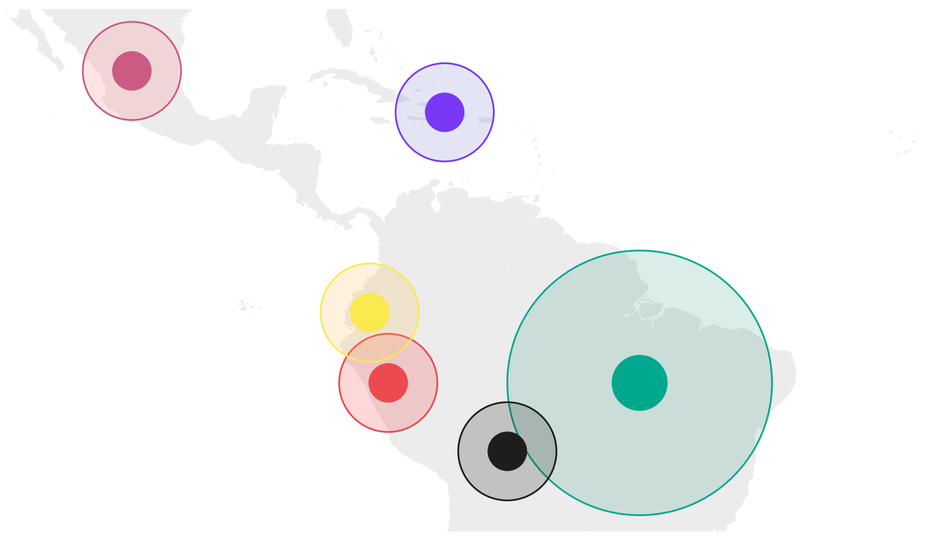




Country	%
Hong Kong	44
Taiwan	27
Malaysia	8
India	8
Indonesia	4
Philippines	4
Singapore	4



Country	%
South Africa	23
Eswatini	12
Qatar	12
Pakistan	8
Kuwait	8
Iraq	8
Tunisia	4
Oman	4
Namibia	4
Morocco	4
Kenia	4
Jordan	4
Egypt	4
Angola	4



Country	%
Brazil	50
Bolivia	10
Peru	10
Mexico	10
Ecuador	10
Dominican Republic	10

Actual MDR incidents in 2022

In 2022, the MDR infrastructure received huge volumes of telemetry data daily, which generated alerts when processed.

Roughly 33% of the alerts were run through machine learning algorithms. A further 11% were analyzed by SOC experts and found to be the consequence of real incidents, which customers were notified about via the MDR portal.

433 000+

security alerts

292 000+

alerts were processed by SOC analysts

141 000+

alerts were processed automatically by AI-powered technology

33 000+

alerts were categorized as the consequence of real incidents

12 000+

incidents were identified in 2022

~14 000

telemetry events per host daily. The figure may vary significantly with the level of host activity and sensor type.

89%

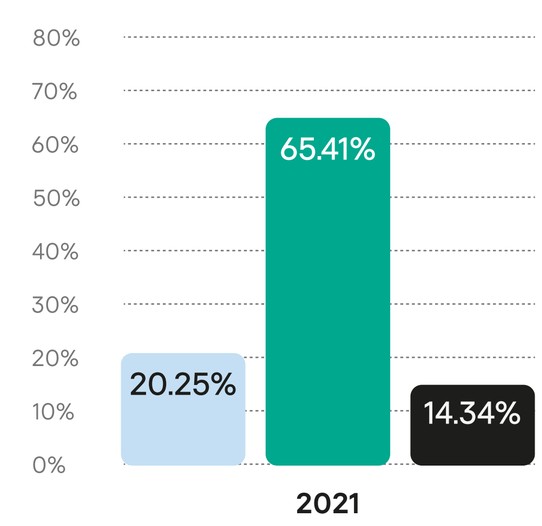
of alerts were rejected by the SOC team as false positives

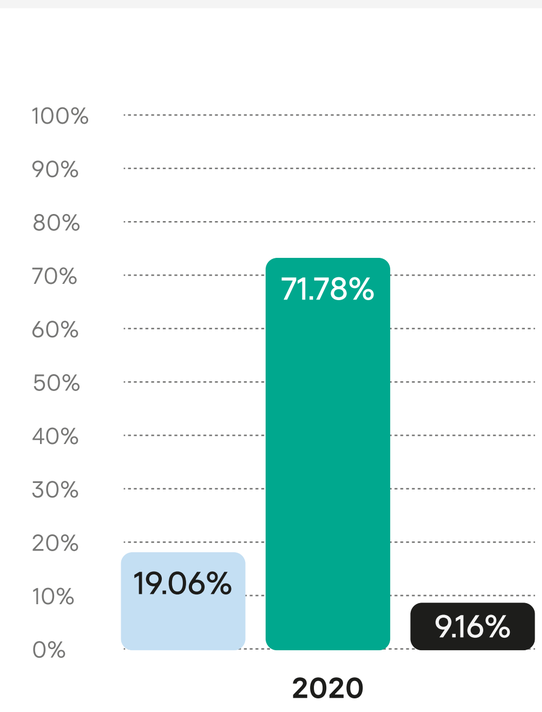
Incident severity levels

In 2022, SOC analysts discovered more than three high-severity incidents every day. Compared to previous years, the share of these incidents remained at or below 10%. The year 2021 was a notable exception with 14%.

We only provide notifications of incidents to which customers can respond effectively.*

High → 8.13%	Human-driven attacks or a malware infection that has a serious impact on business.
Medium → 71.82%	No confirmed human involvement and any potential impact is not severe.
Low → 20.05%	No substantial impact on business, but some security improvements are required.





* For example, if a portable computer connects to a public WLAN, and the intrusion prevention system detects attempts to use the EternalBlue exploit, this definitely constitutes an incident. However, it doesn't require a response as some compromised computers can connect to a public WLAN, but they can't be disinfected because public networks are beyond customer control. In this case, there will be no incident notification from MDR.

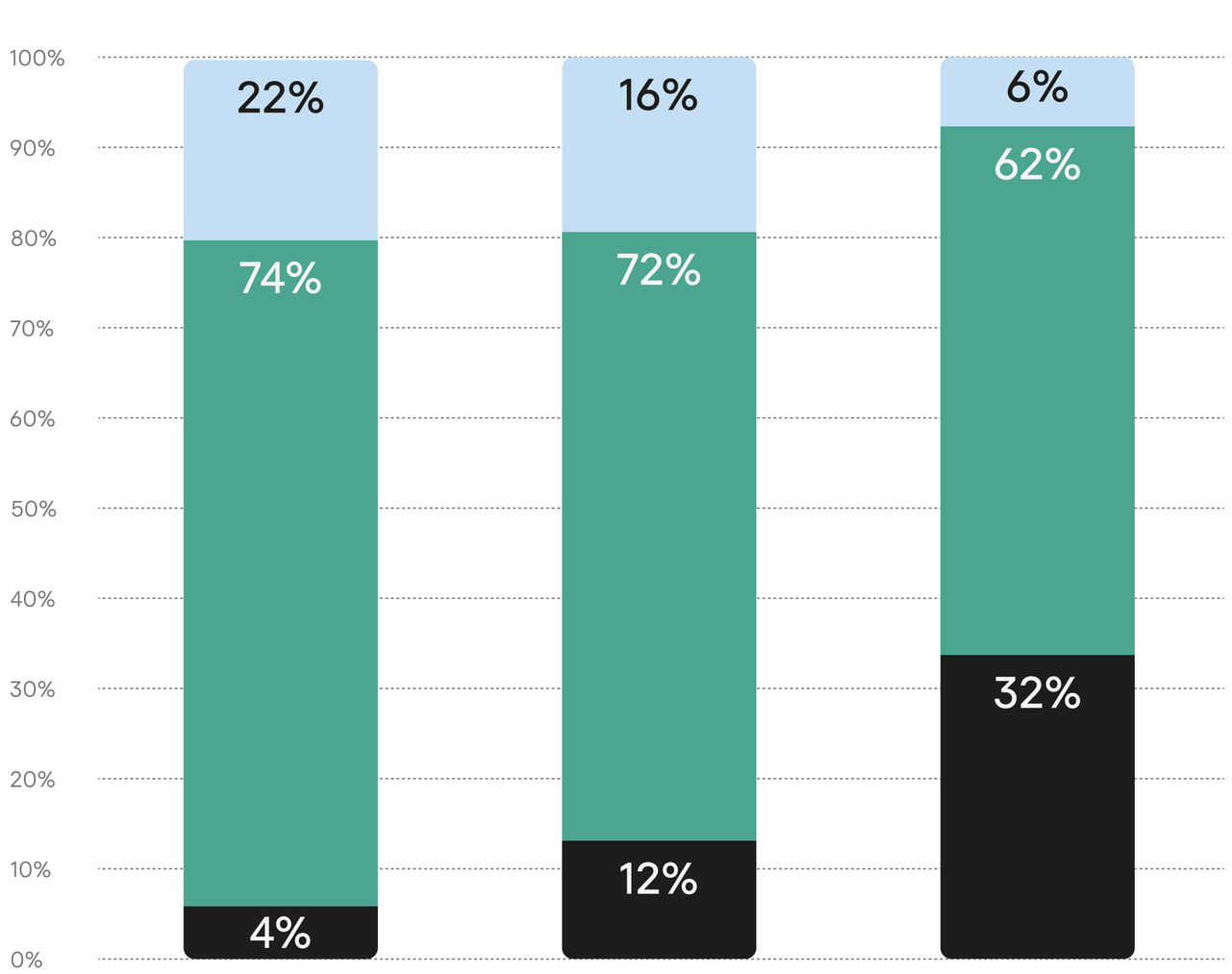
Let's consider a similar incident discovered on a corporate network involving a compromised PC that is not protected with MDR but fully managed and controlled by the customer. This type of incident would be published on the MDR portal, along with response recommendations.

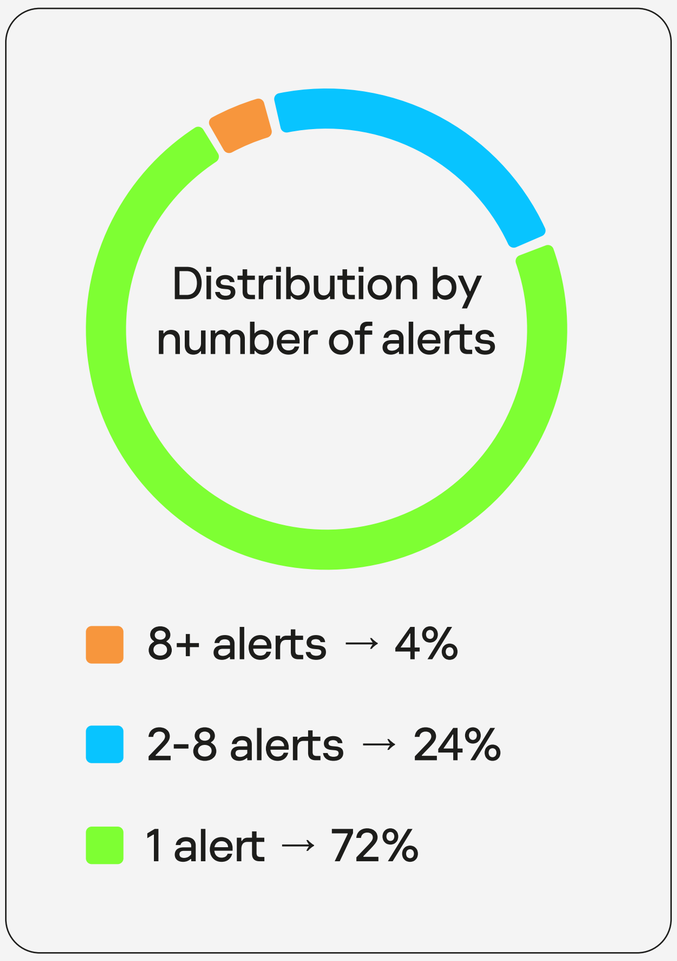
The chart below illustrates the expected number of incidents of particular severity per 10,000 monitored endpoints, by vertical.

The chart demonstrates how an increase in the number of monitored systems drives the number of incidents, by severity level and industry.

- The data suggests that in 2022, media companies saw the highest volume of incidents. But most of them had medium or low severity, i.e. APTs directly controlled by attackers were rare.
- Interestingly, it was relatively calm in telecom, the industry that saw the highest level of high-severity incidents in the previous year.

Response efficiency





Seventy-two percent of incidents were detected following a single security alert, leading to the attack being stopped - demonstrating very high response efficiency. This category includes typical incidents with well-defined response scenarios.* The share of high-severity incidents is the lowest (4%), with the bulk composed of medium- (74%) and low-severity (22%) incidents.

Twenty-four percent of incidents were detected after two to eight alerts. To make bypassing detection for the same threat more difficult, we use a set of technologies that generates different types of alerts. The category includes incidents that were not automatically detected after the initial alert - the response involved a human specialist or the incident was not adequately classified after the first relevant alert.

Four percent of incidents were associated with eight or more alerts. These are cases where the response was rejected by the customer, or was inefficient. This could be a new type of APT that called for in-depth investigation prior to responding, or the customer requested the attack to be monitored but not actively countered — for example, in a red teaming scenario. The percentage of high-severity incidents in this category is the highest (32%), while the share of low-severity incidents is the lowest (just 6%).

* Examples include replacement of Windows accessibility feature binaries (T1546.008), brute force (T1110), detection by a Kaspersky Anti Targeted Attack Platform sandbox (T1566.001) not followed by further development on endpoints, etc.

Incident detection time

Severity

High

Time to process, in minutes

The most complex incidents requiring more time to add data enrichment and establish a timeline.

The processing time here increased by approximately 6% compared to preceding periods due to an increase in human-driven incidents in 2022 (see below), investigation of which takes up more of SOC analyst time and lends itself to automation to a lesser degree.

Severity

Medium

Time to process, in minutes

This severity level dominates the statistics. Most medium-severity incidents are caused by malware. Compared to previous periods, processing time was reduced through a higher level of automation when processing new types of incidents.

Severity

Low

Time to process, in minutes

The incidents with the lowest level of severity, mostly associated with unwanted software, spent the longest time in the queue. A large number of available automation tools have reduced the need for SOC analyst involvement, as well as processing time.

The process of detecting an incident involves several steps:

1. Alert triage

A specialized algorithm transfers an alert from the common list into the queue for an available SOC analyst.

2. Alert analysis

The analyst processes the alert with the severity level and guaranteed SLA in mind.*

3. False positives analysis

If the analysis suggests a false positive**, the alert is ignored and appropriate client or global filters are created.***

4. Incident creation

Unless one of these filters is applied, the alert will be imported into a new or existing incident, which may then be closed as a false positive or forwarded to the customer's MDR portal along with a note with recommended response actions.

5. Recommendations execution

If the customer approves the response recommendations, these will be automatically executed on the endpoints.

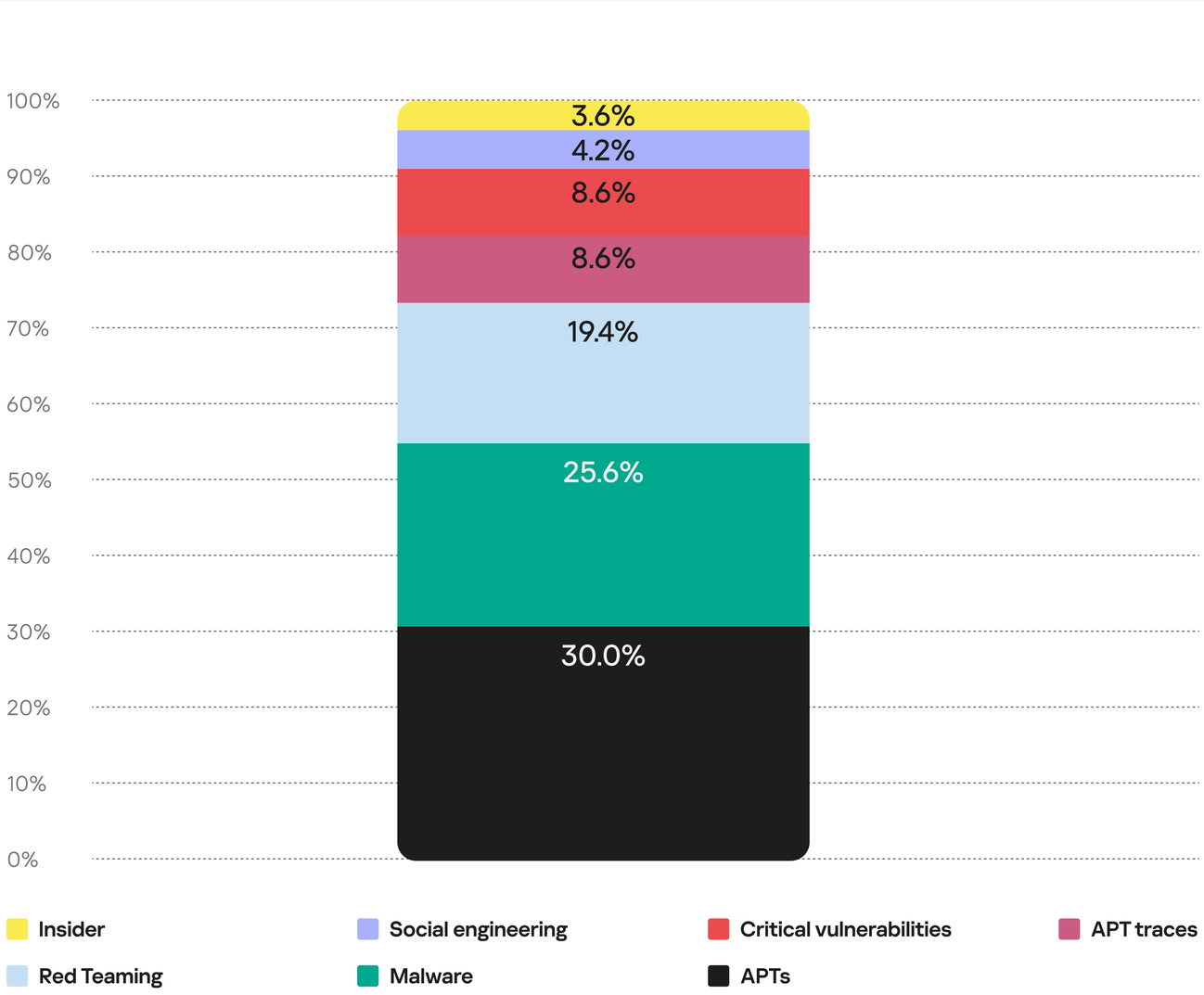
* SLA – Service Level Agreement

** We distinguish two main types of false positives: infrastructural false positives, where the alerting logic is correct, but the alert is due to certain features of the customer infrastructure and not the consequence of an incident; and technological false positives, where the alerting logic is incorrect and needs adjusting.

*** A client filter is a detection logic configuration tailored to the client's particular infrastructure; these filters are created to address infrastructural false positives. A global filter is a global detection logic adjustment across all clients to address technological false positives.

Nature of high-severity incidents

Key causes of high-severity incidents



30% of all high-severity incidents detected in 2022 were associated with human-driven APTs.

A large number of these incidents may also be linked to various kinds of ethical hacking, as both training and real scenarios involve the active efforts of an attacker. We classify these incidents as APTs by default and only change their types to Red Teaming if we receive explicit confirmation from the customer.

Malware attacks with major impact accounted for slightly less than 26% of incidents.

Ethical hacking (pentests, red teaming, etc.) accounted for more than 19%.

The proportion of incidents linked to publicly available critical vulnerabilities and discoveries of traces of prior human-driven attacks (APTs and red teaming) was around 9%.

Roughly 4% resulted from successful use of social engineering techniques and were subsequently developed, causing severe impact.

Slightly less than 4% of incidents were linked to insiders.*

The distribution by number of companies largely follows the same pattern as the number of incidents.

The causes show a similar pattern:

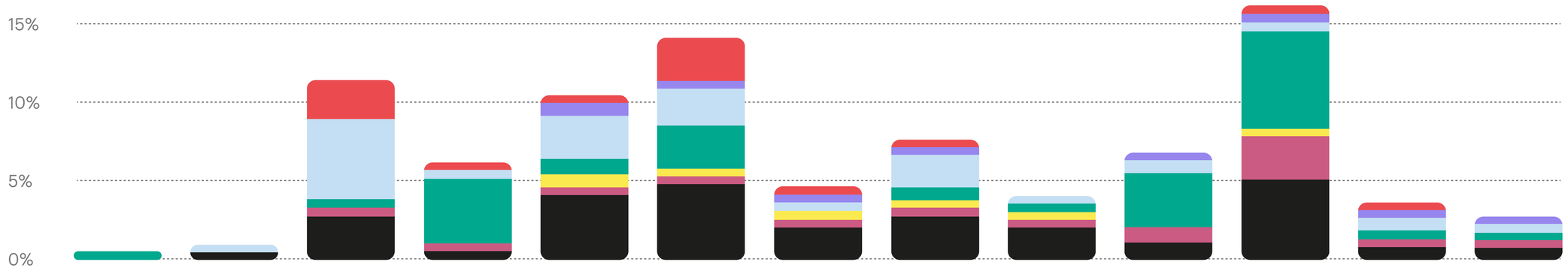
31% of companies experienced APTs

19% of customers were engaged into different types of red teaming

18% of organizations experienced malware attacks with significant impact on business

* We were unable to detect any traces of external malicious actors. All suspicious actions were performed on behalf of legitimate privileged accounts. We have no reason to classify these incidents as false positive ones due to a lack of client feedback as to whether the activities were legitimate. For all we know, these might have been attempts at probing MDR's readiness to respond or actual illegal activities by IT team members that the customers preferred not to disclose. Starting in 2023, we introduced a new incident type, Security Policy Violation, for this small but persistent percentage. We will use this to label high-severity incidents caused by legitimate accounts that showed no signs of compromise. The Insider label will only be applied where an insider's involvement is confirmed.

Number of high-severity incidents by vertical



Red Teaming	%
Finance	5.00
IT	3.20
Industrial	2.20
Healthcare	2.20
Retail	1.40
Transportation	1.20
Other	1.00
Food	0.80
Mass Media	0.80
Education	0.60
Government	0.60
Telecom	0.40

APT	%
Government	5.00
Industrial	4.80
IT	4.20
Healthcare	3.60
Finance	3.40
Telecom	2.20
Mass Media	2.00
Retail	1.60
Transportation	1.40
Other	1.00
Food	0.60
Education	0.20

APT Traces	%
Government	3.40
Retail	1.40
IT	0.40
Healthcare	0.80
Finance	0.60
Industrial	0.60
Food	0.40
Transportation	0.40
Mass Media	0.20
Telecom	0.20
Other	0.20

Malware	%
Government	8.00
Food	4.20
Retail	4.00
Industrial	3.60
IT	1.80
Healthcare	1.40
Telecom	0.80
Transportation	0.60
Finance	0.20
Development	0.20
Other	0.14

Social engineering	%
IT	1.40
Industrial	0.60
Government	0.40
Retail	0.40
Other	0.20
Mass Media	0.20
Healthcare	0.20
Transportation	0.14

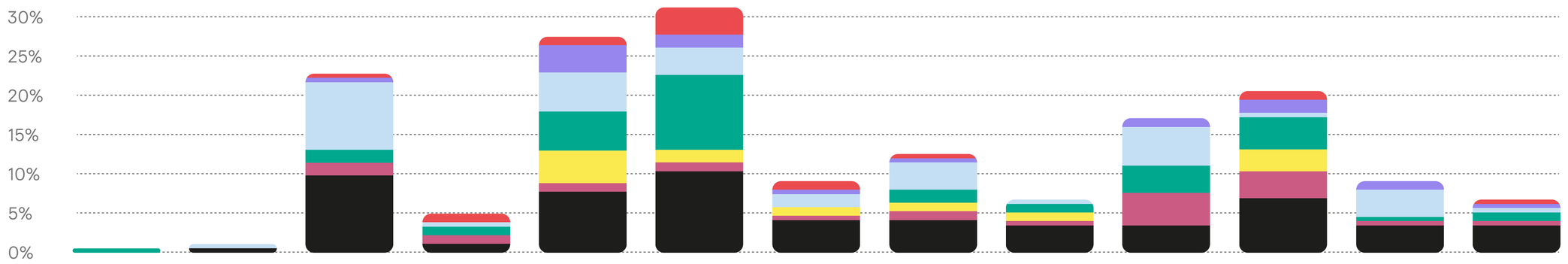
Critical vulnerabilities	%
Industrial	3.40
Finance	2.80
IT	0.60
Government	0.60
Food	0.40
Mass Media	0.40
Healthcare	0.20
Transportation	0.20

Insider	%
IT	1.20
Mass Media	0.80
Industrial	0.60
Healthcare	0.40
Government	0.40
Telecom	0.20

Key takeaways:

1. All of the high-severity incidents observed during the period were recorded in Government, IT, Industrial and Healthcare verticals.
2. All companies where human-driven (APT) incidents were recorded also saw incidents associated with traces of past APTs — with the exception of Education, which showed active attacks but no traces of past hacks in 2022. This shows that malicious actors tend to return to the scene of the crime.
3. The APT statistics follow the same pattern as Red Teaming, the only exception being Development. This may suggest that most companies adequately assess their information security risks.
4. Virtually every industry experienced malware-related incidents without visible human involvement, the exceptions being Education and Mass Media.
5. The APT statistics are in many ways similar to the distribution of malware-related incidents, with the exception of Education and Mass Media again. This supports a recent trend of severely damaging malware attacks starting out as human-driven APTs - initial access and launch are done manually, but further spread of the malware happens without human involvement.
   Due to monitoring coverage being incomplete, attacks are detected at the stage where the system is not able to form a link between the malicious activity and previously discovered human actions by looking at the MDR telemetry data, so two unrelated incidents are registered: an APT and a malware attack.

Number of organizations with high-severity incidents by vertical



Red Teaming	%
Finance	4.09
IT	2.73
Retail	2.73
Healthcare	1.82
Industrial	1.82
Other	1.82
Mass Media	1.36
Education	0.45
Food	0.45
Telecom	0.45
Government	0.45
Transportation	0.45

APT	%
Industrial	6.36
Finance	4.55
IT	3.64
Government	3.18
Mass Media	2.27
Healthcare	2.27
Telecom	1.82
Retail	1.82
Transportation	0.91
Food	0.91
Other	0.45
Education	0.45

APT traces	%
Retail	2.27
Government	1.82
Finance	1.36
Food	0.91
IT	0.91
Industrial	0.91
Healthcare	0.91
Mass Media	0.45
Telecom	0.45
Transportation	0.45
Other	0.45

Malware	%
Industrial	5.00
IT	2.73
Government	2.27
Retail	1.82
Healthcare	1.36
Finance	1.36
Food	0.91
Telecom	0.91
Transportation	0.91
Development	0.45
Other	0.45

Social engineering	%
IT	1.82
Industrial	1.36
Government	1.36
Retail	0.91
Other	0.91
Finance	0.45
Mass Media	0.45
Healthcare	0.45
Transportation	0.45

Critical vulnerabilities	%
Industrial	1.82
Food	0.91
IT	0.91
Mass Media	0.91
Government	0.91
Finance	0.45
Healthcare	0.45
Transportation	0.45

Insider	%
IT	2.27
Industrial	1.36
Mass Media	0.91
Healthcare	0.91
Telecom	0.45
Government	0.45

Key takeaways:

1. The largest number of attacked organizations were from the industrial sector, where all types of critical incidents took place. APTs were identified in 34% of organizations and 27% fell victim to malware.
2. The financial sector is no less interesting for attackers, where all types of critical incidents were observed in 2022, except for insider activity. APTs were detected in 37% of organizations in this vertical.
3. The number of attacked mass media organizations grew substantially in 2022 compared to 2021: high-severity incidents were detected with every customer, and more than third of these incidents were APTs*.
4. IT companies remain a popular target. The vertical saw every type of incident in 2022, but the situation improved slightly in comparison to the previous year. Quarter experienced only APTs, and just 18% were hit by malware that caused serious damage.
5. The development sector was least affected in 2022: only malware-related high-severity incidents were recorded.
6. In telecom APTs were detected in more than 40% of organizations, 20% saw malware attacks that caused damage, and red teaming was detected in just 11% of cases.

* Here, and below in this section, we give percentages of total organizations in the vertical, while the chart shows percentages of total MDR customers in 2022.

Detection technology

The largest number of high-severity incidents

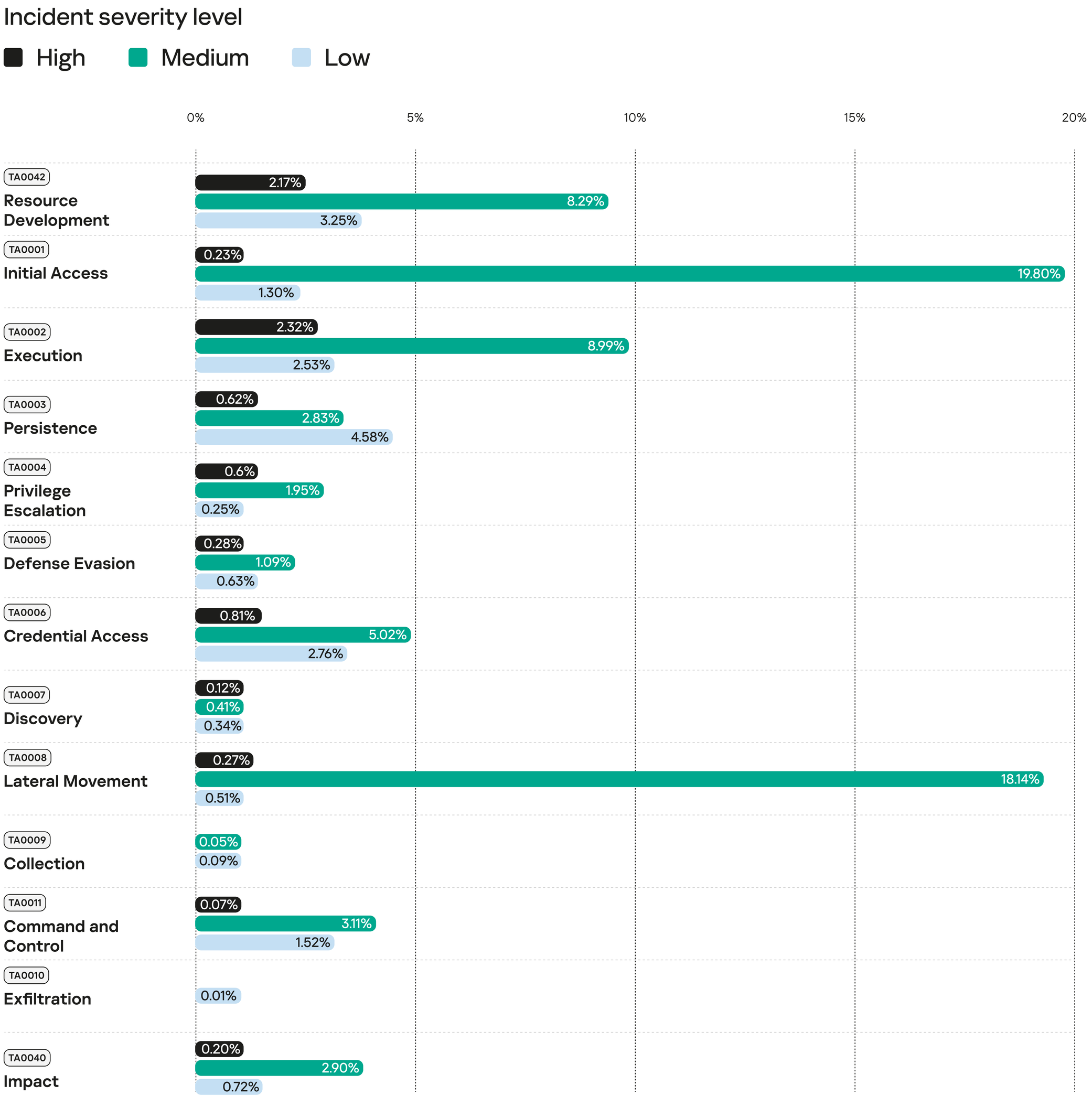
TA0002
Execution
2.32%

The largest number of medium-severity incidents

TA0001
Initial Access
19.80%

Adversarial tactics

MDR can detect incidents at various stages of the attack kill chain. A typical incident passes every stage (MITRE ATT&CK® tactics), but the diagram below displays only the tactic that was detected first.



Key tactics used to detect incidents:

Resource Development	These were "suspicious file detected" incidents, where a potentially offensive tool was observed without any signs of execution. This is often related to red teaming, but is sometimes linked to a real attacker's foothold.
Initial Access	Mainly covered by the Kaspersky Anti Targeted Attack platform on the perimeter by detecting phishing and social engineering
Execution	Detection at this stage was very similar to the one before it, except here we observed tool execution. Execution is always noisy, which is why this is the stage where most high-severity incidents were detected. This proves that tool-based detection remains efficient, as most actors use off-the-shelf attack frameworks.
Persistence	All kinds of malware and unwanted software are always detected at the Persistence stage, so the percentage of low-severity incidents is small.
Credential Access	This tactic led to detection fairly often. A large percentage of incidents detected at this stage was linked to probing of MDR operational readiness, but the small number of published incidents was due to detection of active attacks that began before connecting to MDR.
Lateral Movement	This stage accounts for a large share of detected incidents, but they have a medium severity level. For instance, when a worm is exploiting **SMB** with no visible attacker involvement, while telemetry data suggests that the OS is up to date and patched, and endpoint security is successfully thwarting spread attempts.
Collection	Not every incident includes collection of data, so chances are that these were human-driven APTs detected and forestalled at earlier stages — this stage was well covered with MDR detection rules
Command and Control	This stage often leads to detection, but the percentage of high-severity incidents was less than 0.1%. Nearly all detected incidents were associated with the hosts where MDR was not enabled, so the only reason was suspicious traffic attributed to malware or unwanted software.
Exfiltration	Exfiltration cannot always be reliably distinguished from Command and Control, so when in doubt, analysts tend to choose the latter as the more frequent case.
Impact	Not that many incidents were detected at this stage. Bear in mind that it may be too late to avoid major damage if an attack is detected at the Impact stage.

Attack tactics and detection technology

Although an IDS that analyzes network traffic is also a part of the endpoint sensor, in this report, we consider IDS verdicts as the endpoint sensor's alerts.

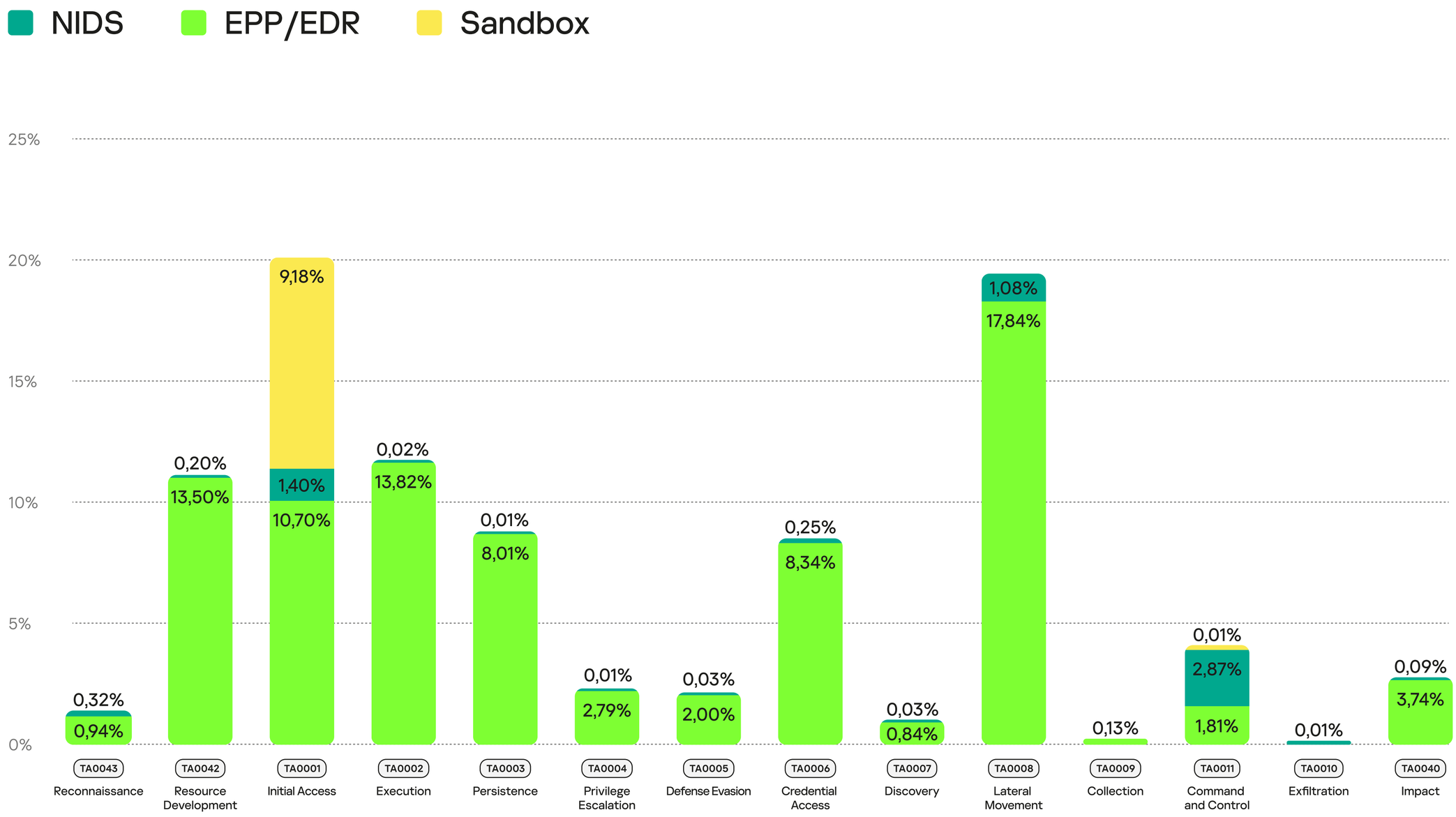
The diagram below illustrates the percentage of incidents detected by the various types of sensors.

MDR analyzes telemetry data from various types of sensors:

- endpoints

- network Intrusion Detection Systems (IDS)
- sandboxes

Components of the Kaspersky Anti Targeted Attack (KATA) platform



The sandbox and network IDSs owe their high performance at the **Initial Access** stage to the popular approach of using KATA to detect phishing attacks on the perimeter. A network IDS also works well for the **Lateral Movement** and **Command and Control** stages.

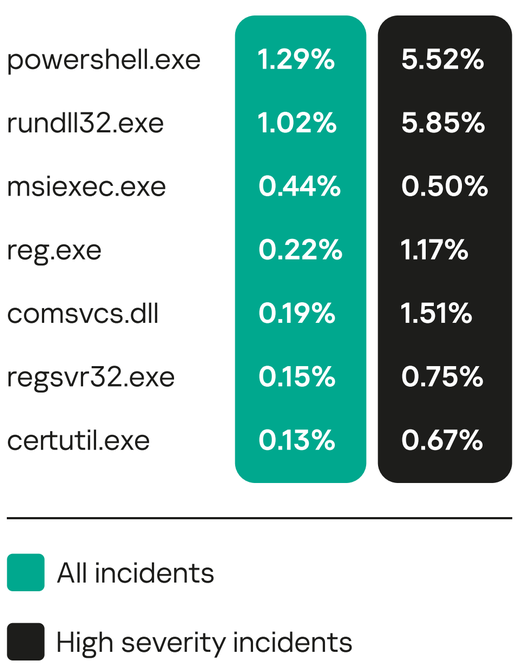
The endpoint sensor acts as the key sensor at the **Execution, Persistence, Privilege Escalation, Defense Evasion, Collection** and **Impact** stages. Interestingly, it also works very well for the **Lateral Movement**, tactic as it uses built-in OS interfaces, which are well covered by detection rules. As can be seen from the chart, endpoint sensors also show good performance at the **Command and Control** stage, which is covered by the built-in IDS.

The **Reconnaissance** tactic was detected by the endpoint sensor and the network IDS, picking up various incidents relating to network scanning and inventory.

The network IDS being triggered by the **Credential Access** tactic can be explained by the system's ability to detect the use of standard tools, for password cracking, for example, when analyzing network traffic.

Adversarial techniques

The most popular LOL-binaries



* For instance, MSF Meterpreter or CobaltStrike beacon

** Conversion is the ratio of security events classified as incidents to total security events based on a particular MITRE ATT&CK® technique. Contribution is the ratio of incidents based on a particular technique to total incidents.

*** To keep the statistics meaningful, we considered only techniques with a contribution exceeding five percent, those that were identified in five percent of incidents.

Attack tools

Malicious actors tend to use built-in OS tools to minimize the chances of being detected while delivering custom tools to a system they previously hacked.

The most popular **LOL-binaries**, observed in almost any incident, were **powershell.exe**, **rundll32.exe** and **reg.exe**. Last year saw high-severity incidents use **comsvcs.dll**: despite this being nothing new, the technique had never been detected this frequently before.

The **certutil.exe** utility, hard to miss at this point, is nonetheless still popular among attackers.

The malicious payloads* for the stages that follow Initial Access take the form of MSI files, which is why **msiexec.exe** was popular overall and for high-severity incidents in particular.

Incident mapping to MITRE ATT&CK®

Our detection logic is mapped to MITRE ATT&CK® techniques. We calculate conversion and contribution** for each rule, so we can evaluate these for MITRE ATT&CK® techniques as well. The nine techniques listed below produced the highest conversion.*** The heatmap below displays the contribution percentages for the techniques we detected in 2022. The somewhat low percentages are explained by the fact that some of attackers' attempts at implementing the detected techniques were stopped in their tracks by preventative security before they could result in an attack and an incident requiring a response.

MITRE ATT&CK®

MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge — is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

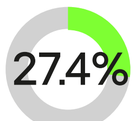
RECONNAISSANCE	RESOURCE DEVELOPMENT	INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques
Active Scanning T1595	Acquire Infrastructure T1583	Drive-by Compromise T1189	Command and Scripting Interpreter T1059	Account Manipulation T1098	Abuse Elevation Control Mechanism T1548	Abuse Elevation Control Mechanism T1548	Adversary-in-the-Middle T1557	Account Discovery T1087	Exploitation of Remote Services T1210
Gather Victim Host Information T1592	Compromise Accounts T1586	Exploit Public-Facing Application T1190	Container Administration Command T1609	BITS Jobs T1197	Access Token Manipulation T1134	Access Token Manipulation T1134	Brute Force T1110	Application Window Discovery T1010	Internal Spearphishing T1534
Gather Victim Identity Information T1589	Compromise Infrastructure T1584	External Remote Services T1133	Deploy Container T1610	Boot or Logon Autostart Execution T1547	Boot or Logon Autostart Execution T1547	BITS Jobs T1197	Credentials from Password Stores T1555	Browser Bookmark Discovery T1217	Lateral Tool Transfer T1570
Gather Victim Network Information T1590	Develop Capabilities T1587	Hardware Additions T1200	Exploitation for Client Execution T1203	Boot or Logon Initialization Scripts T1037	Boot or Logon Initialization Scripts T1037	Build Image on Host T1612	Exploitation for Credential Access T1212	Cloud Infrastructure Discovery T1580	Remote Service Session Hijacking T1563
Gather Victim Org	Establish Accounts	Phishing	Inter-Process	Browser Extensions	Gather Victim Org	Debugger Evasion	Forced	Cloud Service	Remote Services

Techniques with the highest conversions

Exploitation of Remote Services

Many types of ransomware continue to exploit **SMB** buffer overflow for lateral movement, often with some success.

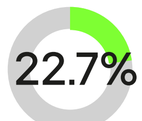
T1210



Valid Accounts

Adversaries abused domain and local accounts as a means of gaining initial access and subsequently, persistence.

T1078



Account Manipulation

Despite the fact that privileged accounts and groups are typically monitored, adversaries often activate disabled accounts and/or add accounts to groups.

T1098

Malware

Attack stages that preceded active exploitation were often detected as a potentially malicious code with no signs of being run.

T1587.001

Malicious File

One of the two of the most widely used scenarios for initial compromise through successful use of social engineering techniques.

T1204.002

Exploit Public-Facing Application

As in 2021, not all organizations installed updates in a timely manner, which is why penetration through the network perimeter was successful in almost 12% of cases.

T1190

Malicious Link

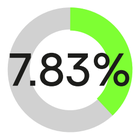
One of the two of the most widely used scenarios for initiating compromise through successful use of social engineering techniques.

T1204.001

Application Layer Protocol

Adversaries may communicate with their C2 centers by using standard application layer protocols, as custom ones could become a reliable indicator of compromise.

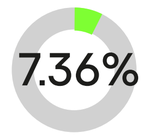
T1071



Spearphishing Attachment

Spearphishing retains its leading position as an initial access method, but in 2022, as in 2021, it lost ground to exploits of public-facing applications at the network perimeter.

T1566

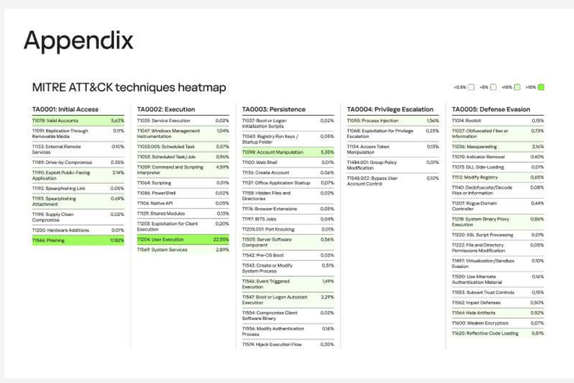


Most-used detection scenarios

A total of 550 unique scenarios with a non-zero conversion percentage provided detects for our customers in 2022. This section looks at the most frequent detection scenarios with a total contribution exceeding 70%.

For convenience, we divided these into two groups: product detect-based scenarios and OS event-based scenarios.

The number of productive scenarios based on "classic" **EDR** events, such as process run or network connection, was certainly large, but their combined contribution in 2022 amounted to less than a third, so they are omitted from this report.



Appendix

MITRE ATT&CK techniques heatmap

See MITRE ATT&CK tactics & techniques heatmap in Appendix on page 26.

Detection based on a verdict by an XDR system or endpoint security product

MDR does not register an incident for each product detection, but extra context enrichment, combined with a product verdict, may prompt an investigation.

The use of advanced telemetry providers means that these verdicts still remain the most frequent and fairly certain security events resulting in detection of major incidents.

Total contribution	61%
Average conversion	26%

The most-used scenarios

Requisite telemetry Enrichment

IDS triggered

Network IDS (KATA or endpoint security component) detect. A likely false positive could not be confirmed, because the monitoring data lacked an attack source.

IDS verdict

Network settings of monitored hosts

Malicious email attachment received

Endpoint product detect triggered by an email attachment.

Product verdict

Email attachment received

Persistence in memory

Product detect triggered by memory area.

Product verdict

Sandbox triggered

KATA sandbox triggered. No exact endpoint security verdict available for object.

Sandbox verdict

Other product verdicts for object

Malicious URL access attempt

Attempt to access bad URL.

DNS request

Product verdict

URL reputation

HTTP connection

APT-related product verdict

List of relevant certain and uncertain verdicts.*

Product verdict

Certain verdict by server product

Response from server-based endpoint security product. For example, product detect on domain controller, mission-critical server.

· Product verdict

List of critical servers

· Product configuration

Malicious URL in command line

A URL is extracted from any field — most frequently, the command line which gives the scenario its name — and searched against the reputation database.

· URL reputation

Known tool created

A tool classified by the product as a hack tool was created in the file system.

Product verdict

File created in file system

Product verdict description

* A certain verdict means that the activity detected by the product is definitely to be malicious. The product typically responds automatically. An uncertain verdict or suspicious activity means the product has detected an anomaly, but the likelihood of a false positive is high, so the product does not give an active response, yet still notifies the MDR team.

Detections based on OS events

Operating system events, however easily observed and accessible, also provide ample material for attack detection. Enriched with threat data and correlated with other EDR events, they yield a high level of conversion while serving as virtually the only detection method for a number of scenarios.

Total contribution 10%

Average conversion 28%

The most used scenarios

Requisite telemetry

Built-in account enabled

Built-in accounts (Administrator and/or Guest) enabled

OS events: account enabled

Network login by known tool

Network login by known hacking tool (kali, nmap, etc.) detected

OS events: login, logout

User added to privileged group

User added to privileged group (Domain Admins, Enterprise Admins, Cert Publishers, etc.) detected

OS event: group member added

Successful login by nonexistent user

A successful login was registered, but an account search returned the error: "1332 (0x534) No mapping between account names and security IDs was done"

OS event: login

Obfuscated PowerShell script run

ML-powered analysis detected obfuscation in a scenario.

OS events: PowerShell command log

Suspicious incoming AD replication request

A Domain-DNS object was requested with the DS-Replication-Get-Changes and DS-Replication-Get-Changes-All privileges

OS events: operation on directory object

Suspected DCShadow attack

SPNs required for DCShadow installed for computer account

OS events: computer account edited

System process service run

Running a service with cmd.exe, wmic.exe, bash.exe, mshta, etc. stated as the executable

OS events: service run and install

Suspicious service installed

A service with a suspicious name that contains "winexesvc", "dumpsvc", "paexec", "comspec", etc. was installed in the operating system.

OS events: service install

Appendix

MITRE ATT&CK techniques heatmap

<0.5% <5% <10% >10%

TA0001: Initial Access

T1078: Valid Accounts	5,63%
T1091: Replication Through Removable Media	0.11%
T1133: External Remote Services	0.10%
T1189: Drive-by Compromise	0.35%
T1190: Exploit Public-Facing Application	2.14%
T1192: Spearphishing Link	0.05%
T1193: Spearphishing Attachment	0.69%
T1195: Supply Chain Compromise	0.02%
T1200: Hardware Additions	0.01%
T1566: Phishing	17.82%

TA0002: Execution

T1035: Service Execution	0,02%
T1047: Windows Management Instrumentation	1,04%
T1053.005: Scheduled Task	0,57%
T1053: Scheduled Task/Job	0,96%
T1059: Command and Scripting Interpreter	4,59%
T1064: Scripting	0,01%
T1086: PowerShell	0,02%
T1106: Native API	0,05%
T1129: Shared Modules	0,13%
T1203: Exploitation for Client Execution	0,20%
T1204: User Execution	22,55%
T1569: System Services	2,89%

TA0003: Persistence

T1037: Boot or Logon Initialization Scripts	0,02%
T1060: Registry Run Keys / Startup Folder	0,05%
T1098: Account Manipulation	5,35%
T1100: Web Shell	0,01%
T1136: Create Account	0,06%
T1137: Office Application Startup	0,07%
T1158: Hidden Files and Directories	0,02%
T1176: Browser Extensions	0,05%
T1197: BITS Jobs	0,04%
T1205.001: Port Knocking	0,01%
T1505: Server Software Component	0,56%
T1542: Pre-OS Boot	0,03%
T1543: Create or Modify System Process	0,31%
T1546: Event Triggered Execution	1,49%
T1547: Boot or Logon Autostart Execution	2,29%
T1554: Compromise Client Software Binary	0,02%
T1556: Modify Authentication Process	0,16%
T1574: Hijack Execution Flow	0,20%

TA0004: Privilege Escalation

T1055: Process Injection	1,56%
T1068: Exploitation for Privilege Escalation	0,23%
T1134: Access Token Manipulation	0,13%
T1484.001: Group Policy Modification	0,01%
T1548.002: Bypass User Account Control	0,10%

TA0005: Defense Evasion

T1014: Rootkit	0,15%
T1027: Obfuscated Files or Information	0,73%
T1036: Masquerading	2,16%
T1070: Indicator Removal	0,40%
T1073: DLL Side-Loading	0,01%
T1112: Modify Registry	0,65%
T1140: Deobfuscate/Decode Files or Information	0,08%
T1207: Rogue Domain Controller	0,44%
T1218: System Binary Proxy Execution	0,86%
T1220: XSL Script Processing	0,01%
T1222: File and Directory Permissions Modification	0,05%
T1497: Virtualization/Sandbox Evasion	0,10%
T1550: Use Alternate Authentication Material	0,16%
T1553: Subvert Trust Controls	0,15%
T1562: Impair Defenses	0,50%
T1564: Hide Artifacts	0,52%
T1600: Weaken Encryption	0,07%
T1620: Reflective Code Loading	0,81%

TA0006: Credential Access

T1003: OS Credential Dumping	7,04%
T1040: Network Sniffing	0,10%
T1056: Input Capture	0,31%
T1110: Brute Force	1,78%
T1187: Forced Authentication	0,01%
T1212: Exploitation for Credential Access	0,10%
T1539: Steal Web Session Cookie	0,02%
T1552: Unsecured Credentials	0,71%
T1555: Credentials from Password Stores	0,52%
T1557: Adversary-in-the-Middle	0,06%
T1558: Steal or Forge Kerberos Tickets	1,73%
T1606: Forge Web Credentials	0,01%
T1649: Steal or Forge Authentication Certificates	0,01%

TA0007: Discovery

T1007: System Service Discovery	0,35%
T1012: Query Registry	0,31%
T1016: System Network Configuration Discovery	0,30%
T1018: Remote System Discovery	0,52%
T1033: System Owner/User Discovery	0,68%
T1046: Network Service Discovery	0,52%
T1049: System Network Connections Discovery	0,30%
T1057: Process Discovery	0.02%
T1069: Permission Groups Discovery	0,48%
T1082: System Information Discovery	0,05%
T1083: File and Directory Discovery	0,07%
T1087: Account Discovery	0,72%
T1135: Network Share Discovery	0,06%
T1201: Password Policy Discovery	0,01%
T1482: Domain Trust Discovery	0,51%
T1482: Domain Trust Discovery	0,05%
T1615: Group Policy Discovery	0,35%

TA0008: Lateral Movement

T1021: Remote Services	6,81%
T1076: Remote Desktop Protocol	0,02%
T1080: Taint Shared Content	0,01%
T1210: Exploitation of Remote Services	16,22%
T1534: Internal Spearphishing	2,63%
T1563: Remote Service Session Hijacking	0,06%
T1570: Lateral Tool Transfer	0,30%

TA0009: Collection

T1005: Data from Local System	0,07%
T1039: Data from Network Shared Drive	0,04%
T1113: Screen Capture	0,10%
T1119: Automated Collection	0,09%
T1125: Video Capture	0,06%
T1560: Archive Collected Data	0,06%

TA0010: Exfiltration

T1020: Automated Exfiltration	0,06%
T1029: Scheduled Transfer	0,01%
T1030: Data Transfer Size Limits	0,01%
T1041: Exfiltration Over C2 Channel	0,03%
T1048: Exfiltration Over Alternative Protocol	0,02%
T1567: Exfiltration Over Web Service	0,04%

TA0011: Command and Control

T1001: Data Obfuscation	0,01%
T1071: Application Layer Protocol	8,55%
T1090: Proxy	0,22%
T1095: Non-Application Layer Protocol	0,90%
T1102: Web Service	0,06%
T1104: Multi-Stage Channels	0,01%
T1105: Ingress Tool Transfer	1,15%
T1219: Remote Access Software	0,13%
T1568: Dynamic Resolution	0,13%
T1571: Non-Standard Port	0,07%
T1572: Protocol Tunneling	0,17%
T1573: Encrypted Channel	0,01%

TA0040: Impact

T1485: Data Destruction	1,12%
T1486: Data Encrypted for Impact	1,20%
T1487: Disk Structure Wipe	0,01%
T1489: Service Stop	0,07%
T1490: Inhibit System Recovery	0,01%
T1492: Stored Data Manipulation	0,01%
T1493: Transmitted Data Manipulation	0,01%
T1496: Resource Hijacking	1,86%
T1498: Network Denial of Service	0,02%
T1499: Endpoint Denial of Service	0,04%
T1561: Disk Wipe	2,16%
T1565: Data Manipulation	9,65%

TA0042: Resource Development

T1583: Acquire Infrastructure	0,17%
T1584: Compromise Infrastructure	0,06%
T1586: Compromise Accounts	0,01%
T1587: Develop Capabilities	9,36%
T1588: Obtain Capabilities	7,48%
T1608: Stage Capabilities	0,96%

TA0043: Reconnaissance

T1589: Gather Victim Identity Information	0,02%
T1590: Gather Victim Network Information	0,20%
T1592: Gather Victim Host Information	0,01%
T1595: Active Scanning	0,85%
T1598: Phishing for Information	0,85%

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 240,000 corporate clients protect what matters most to them.

Cybersecurity services

- Kaspersky Managed Detection and Response
- Kaspersky Incident Response
- Kaspersky Digital Forensics and Malware Analysis
- Kaspersky Targeted Attack Discovery
- Kaspersky Security Assessment
- Kaspersky SOC Consulting
- Kaspersky Cybersecurity Training

Global recognition

Kaspersky products and solutions undergo constant independent testing and reviews, routinely achieving top results, recognition and awards.

Our technologies and processes are regularly assessed and verified by the world's most respected analyst organizations.

Most tested. Most awarded.

MITRE | ATT&CK®

AV comparatives

Quadrant Knowledge Solutions

FORRESTER®

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

5000+
professionals work at Kaspersky

50%
of employees are R&D specialists

35
35 world-leading security experts in Kaspersky GReaT

9
transparency centers across the world

400 000+
new malicious files detected by Kaspersky every day

240 000+
corporate clients worldwide

650+ mln
cyberattacks stopped by Kaspersky solutions in 2022

#kaspersky
#bringonthefuture

Contact us

For inquiries about Kaspersky cybersecurity services and for emergency assistance:

services@kaspersky.com

www.kaspersky.com