kaspersky

Managed Detection and Response Analytics report

H1 2019

www.kaspersky.com

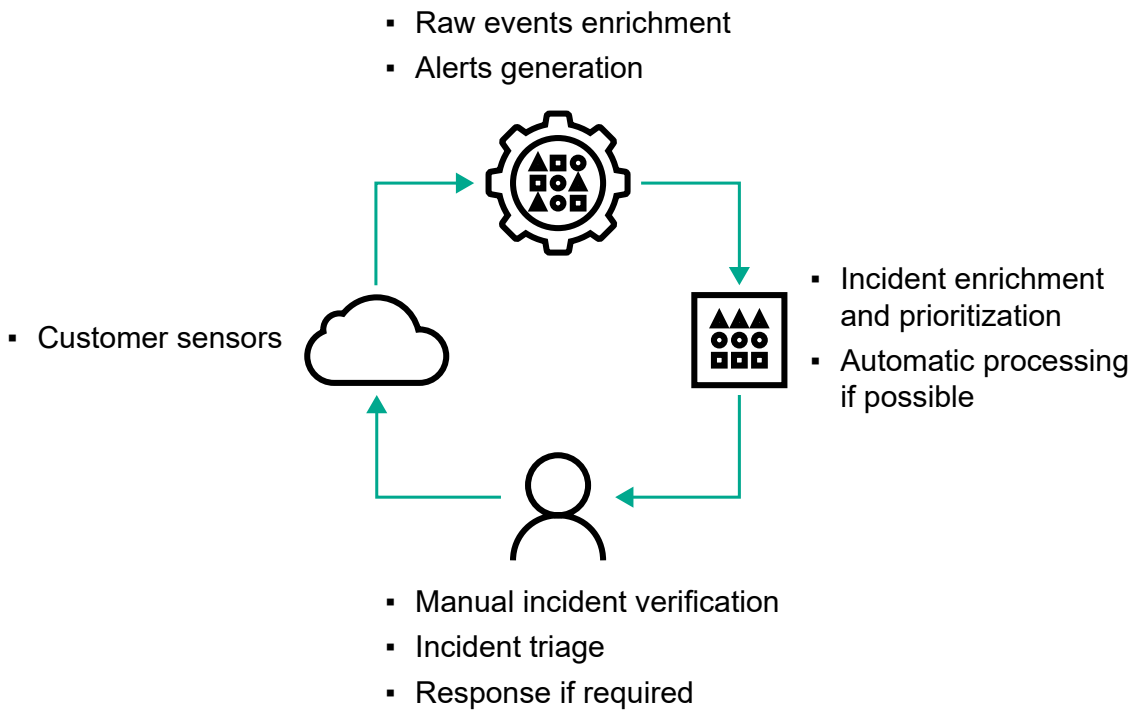
Introduction

This report contains the results of the **M**anaged **D**etection and **R**esponse (**MDR**) service (brand name – Kaspersky Managed Protection[1]). The MDR service provides managed **threat hunting** and **initial incident response**. Threat hunting is the practice of iteratively searching through data collected from sensors (referenced as telemetry or events) in order to detect threats that successfully evade automatic security solutions. A brief description of the service is provided at the end of this document.

The MDR service processes security operations events, focusing on and improving activity performed by professionals in charge of threat hunting projects, their level of expertise and the threat intelligence enabled through the detection process. According to David Bianco's Pyramid of Pain[2], TTP-based threat detection is the most difficult type of indicators of attacks (IoAs) to circumvent for an adversary. **The Kaspersky team is focused on TTP-based threat hunting in its MDR service**, where **humans are heavily involved to ensure the best judgments are made** on collected events, especially advanced threats. This significantly augments automatic detection logic provided by endpoint protection products (EPP) used as sensors during the service delivery.

Report navigation

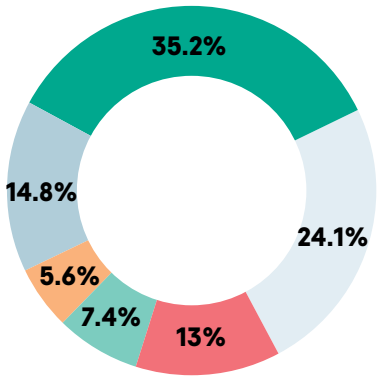
Life cycle of a threat hunting hypothesis



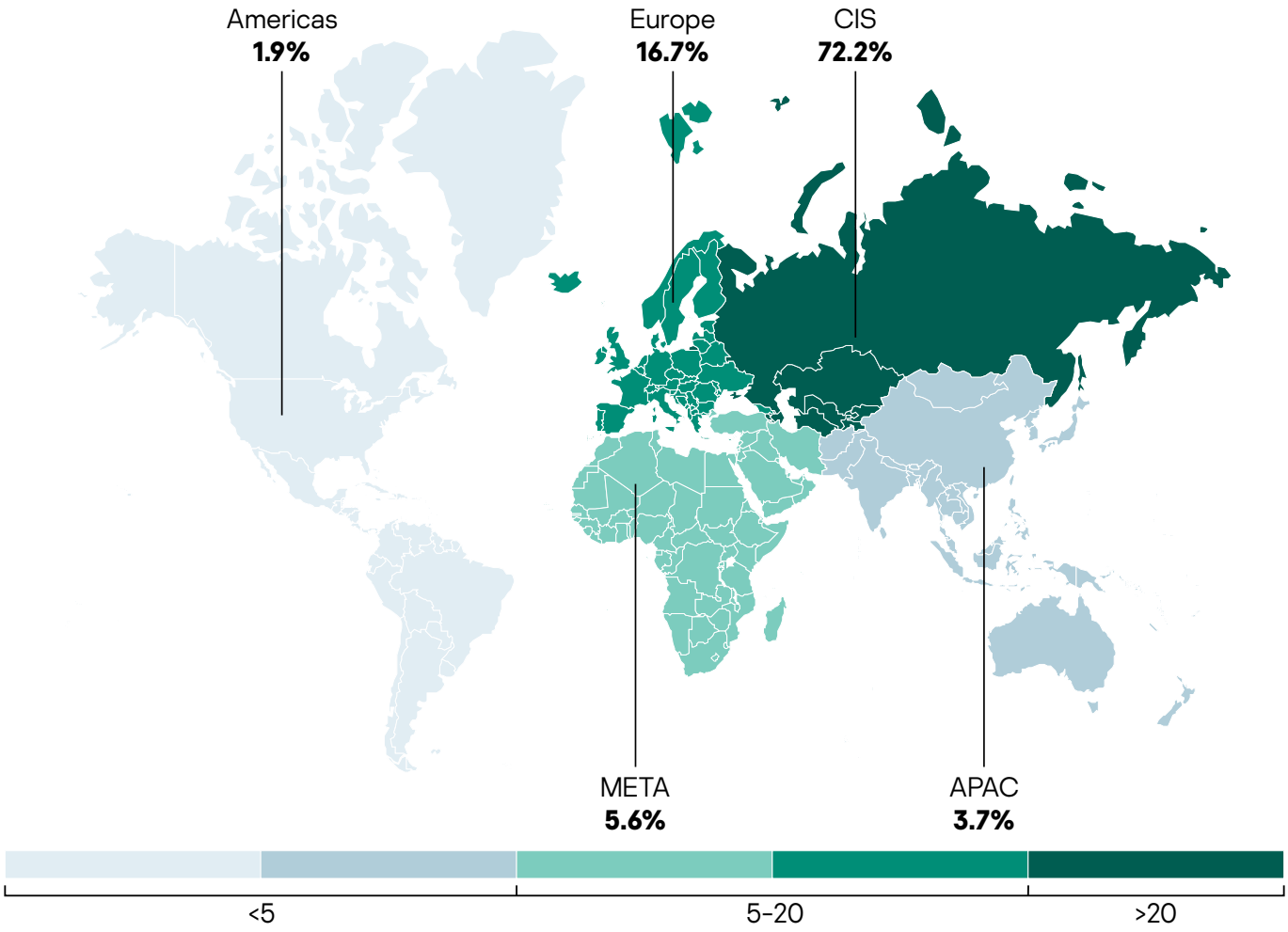
1 https://www.kaspersky.com/enterprise-security/threat-hunting
2 http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Geography and industry verticals of the MDR service delivered by Kaspersky

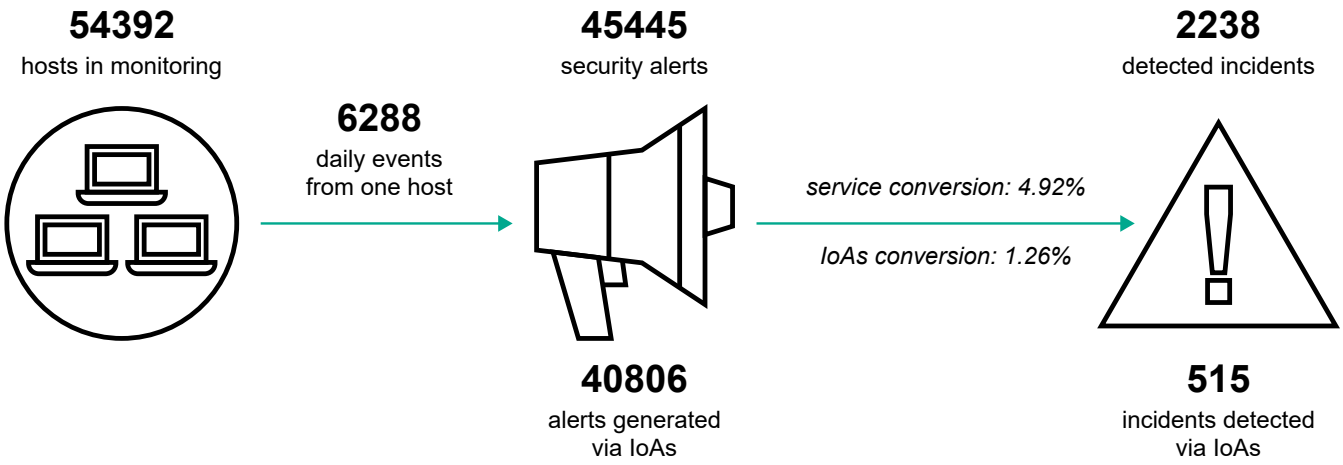
The analysis was conducted based on data from organizations around the world that used our service in the first half of 2019. Government bodies, financial institutions, industrial organizations, telecommunication and IT companies worldwide use our service to protect their IT infrastructure. Data from organizations that used our services for frequent health checks was also included.



- Financial institutions
- Government bodies
- Industrial organizations
- Transport companies
- IT/Telecom companies
- Other



Incident detection operations



Almost all alerts were generated by the analysis of events from endpoint sensors **based on IoAs (TTP-based threat detection logic)** and less than 2% of them were identified as cybersecurity incidents.

The low IoA conversion rate reflects the need to detect advanced threats which use a 'living off the land' approach[3], with behaviors that are very similar to legitimate activity. The more a malicious behavior mimics the normal behavior of users and administrators, the higher the rate of false positives and, consequently, the lower the conversion rate from alerts.

Mean time to response (MTTR)
(or **incident processing time**) is the time from an automatic alert generation as a result of automated analysis of events to its resolution by Kaspersky experts.

~25 mins average MTTR

It is worth noting that incident investigation may include additional work on the customer side or extra expert analysis and it may require more time for resolution – on average, up to 37 minutes in cases of incidents associated with advanced threats or sophisticated attack detection.

MTTR in view of incident severity

The incident processing time can is slightly depend on severity: incidents with a higher degree of severity require more complex and complicated analysis. They require more advanced remediation measures to cure infected systems and to protect against reoccurrence or threat propagation inside the network infrastructure than incidents with medium and low severity levels.

The MTTR values for incidents of different severity are provided below.

Low	Medium	High
20 min	27 min	28 min

Examples of IoAs:

- Start command line (or bat/ PowerShell) script within a browser, office application or server application (such as SQL server, SQL server agent, nginx, JBoss, Tomcat, etc.);
- Suspicious use of certutil for file download (example command: `certutil -verifyctl -f -split https[:]// example.com/wce.exe`);
- File upload with BITS (Background Intelligent Transfer Service);
- `whoami` command from SYSTEM account, and many others.

The main ideas behind IoA-TTP-based detection:

- Applicable for detection of post-exploitation activity.
- Detects standard but suspicious functionality of legitimate utilities: therefore, classification of observed behavior as malicious cannot be accomplished in a fully automated manner.
- Tools used by attackers are not explicitly malicious, but their hostile usage is.

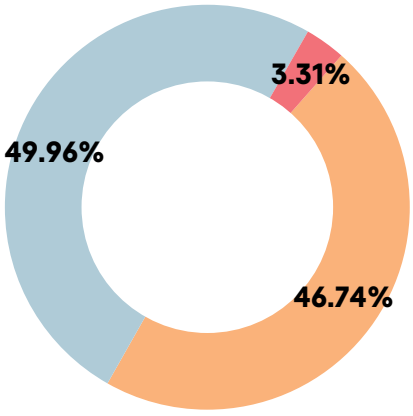
[3] https://medium.com/threat-intel/what-is-living-off-the-land-ca0c2e932931

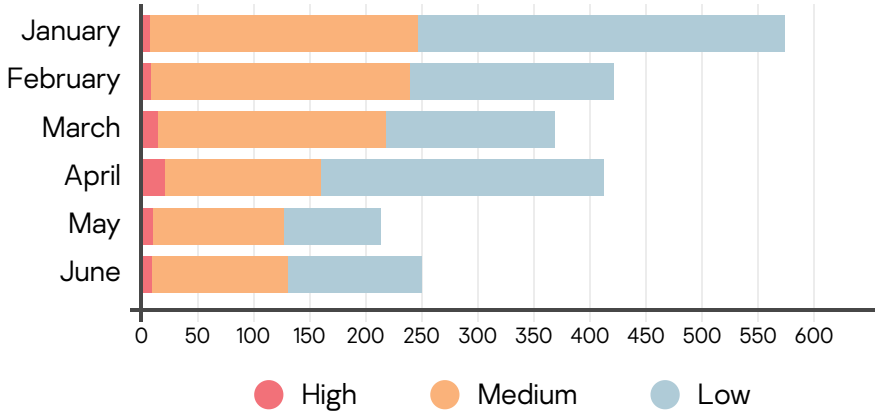
Incident prioritization

Incident severity is evaluated by experts based on a combination of factors, such as threat actor, attack stage at the time of incident detection (e.g. cyber kill chain), the scale of affected infrastructure, details about the threat and how it may be relevant to a customer's business and, with the customer's feedback, the identified impact on infrastructure, complexity of remediation measures and more. The severity levels are described below.

Incident details	Severity level	Typical remediation measures	Action (customer side)
Traces of targeted attack, unknown threat, complex malware or malware with fewer malicious actions.	High	Further investigation using digital forensic methods and manual remediation Incident response	Urgent action from the technical specialists of the targeted organization is required
New malware samples (Trojan, Cryptor, etc.) for which automatic remediation by product is technically possible. Associated with minor damage to the affected systems.	Medium	Malware analysis Removal with EPP	None (affected systems efficiently cured by EPP)
New samples of potential unwanted programs bringing inconvenience (Adware, Riskware, not-a-virus, etc.) for which automatic remediation by product is technically possible. Associated with no damage to the affected systems.	Low	Removal with EPP	

In the first half of 2019, we identified the following severity levels by month.



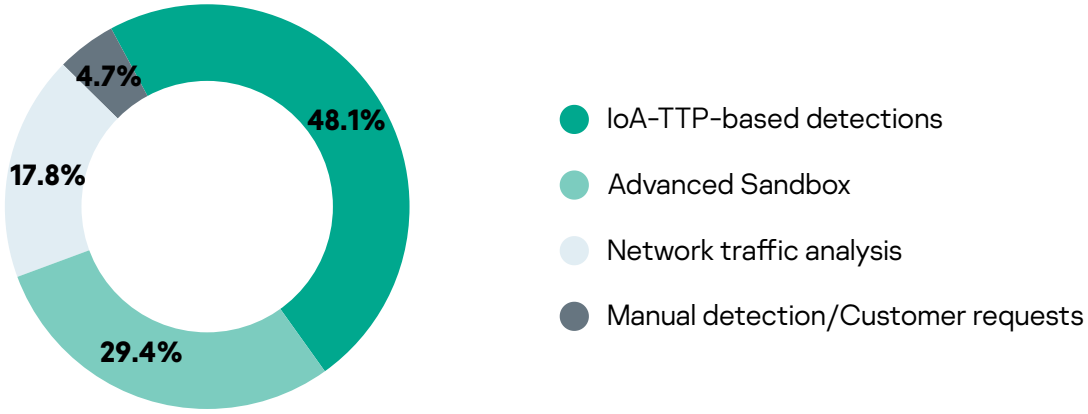


Things to note

Almost all incidents that have medium or low severity are connected to threats that can be efficiently remediated by endpoint protection products (EPP). No action from the side of the victim systems is required except for anti-malware database updates to EPPs to eliminate the risks associated with such incidents. **This shows that an EPP is an effective threat response tool in the case of low and medium severity incidents, but it requires an additional level of TTP-based threat hunting, manual detection, and analysis to find new, unknown, or advanced threats**.

Effectiveness of detection technologies

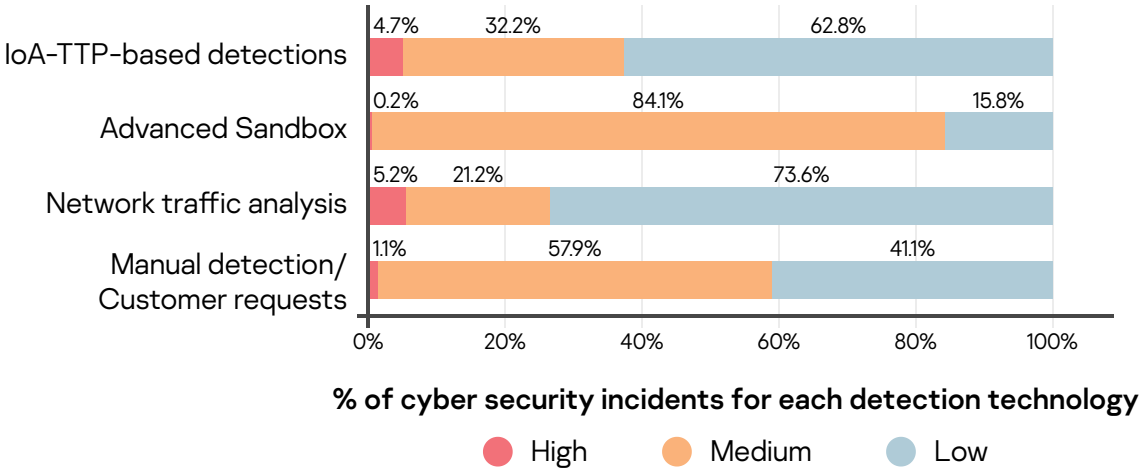
Incident distribution by event source (sensors)



Highlights

- Almost half of all incidents were detected through the analysis of malicious actions or objects detected during the advanced analysis of endpoint behavior using TTP-based threat detection logic (using IoAs). **This demonstrates the general efficiency of the endpoint IoA approach in detecting advanced threats and sophisticated malware-less attacks**.
- About one-third of all incidents were detected through the analysis of suspicious objects by the Advanced Sandbox component, which is usually connected with **fraudulent email attachments that belong to various spam and phishing attacks** targeting organizations all over the world. Detailed information on spam and phishing attacks in Q1 2019 was published on May 15, 2019 on Securelist[4].

Statistics on incident severity level distributed by detection technology



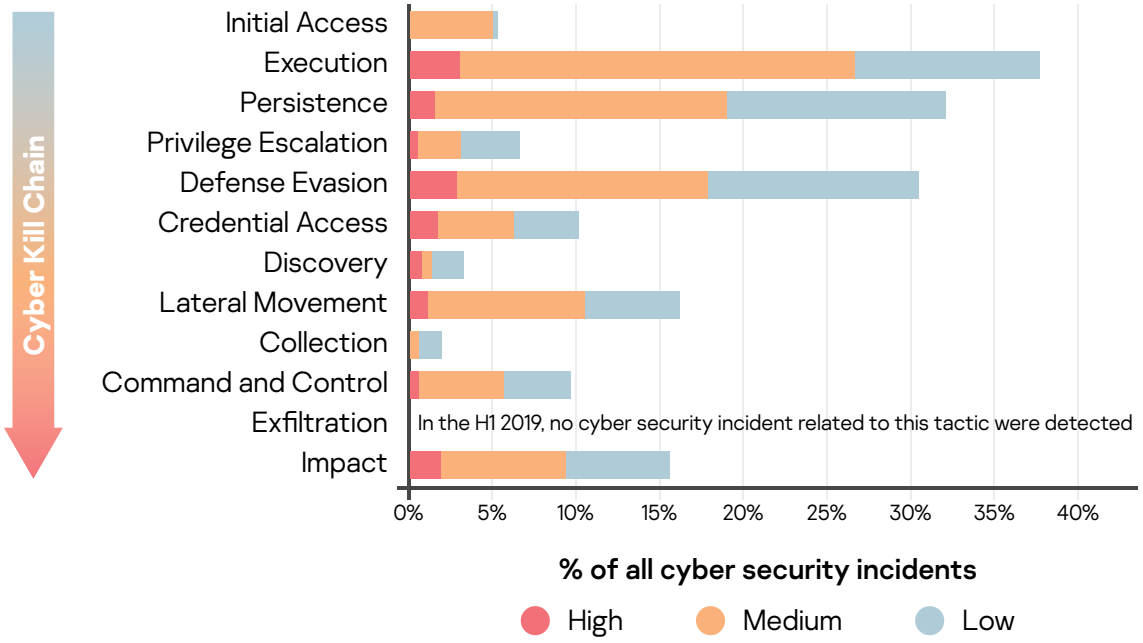
[4] https://securelist.com/spam-and-phishing-in-q1-2019/90795/

Adversary tactics and techniques used in incidents

Kaspersky determines the adversary tactics and techniques related to alerts and cybersecurity incidents detected via TTP-based threat hunting (using IoAs) in accordance with MITRE's globally accepted ATT&CK knowledge base[5].

Statistics on attack tactics used in incidents of different severity (high, medium, low) at the time of detection

The tactics are placed in Cyber Kill Chain order.



Highlights

- Cybersecurity incidents for almost all existing attack tactics were detected, which **indicated the possibility of activity detection at all stages of potential hacker actions** (no incidents with the Exfiltration tactic were implemented in the MDR service detection logic).
- Detection of different ATT&CK tactics shows **the ability to detect threats in the 'post-breach' attack stage** when the intruders had already obtained access to the targeted systems, or even network infrastructure and were in the process of achieving attack objectives.
- The statistics show the **great importance of post-breach scenario detection in threat hunting combined with the classical pre-breach approach mainly implemented in preventive security controls**. The better the threat is able to imitate legitimate activity, the greater its chances of avoiding detection before the actual compromise, which is very common for advanced malware-less threats.

Things to note

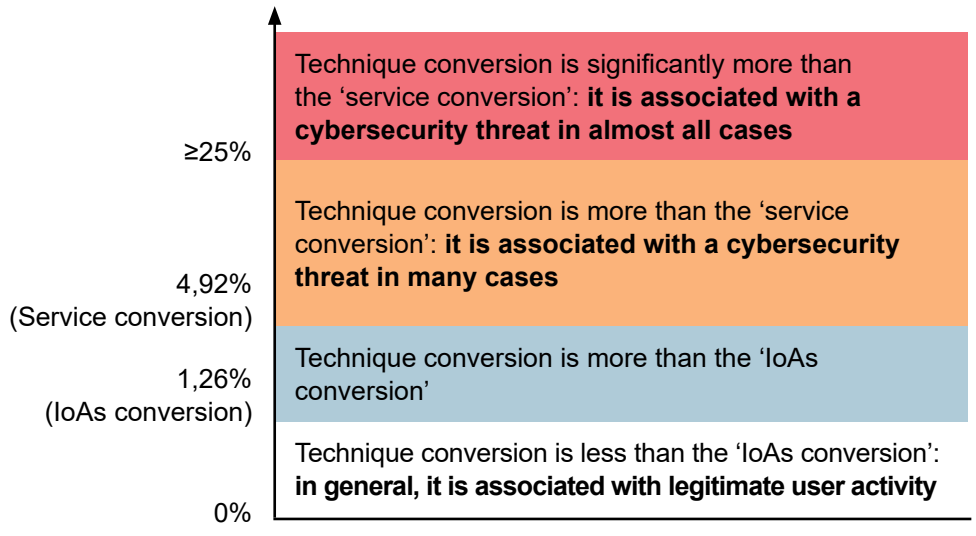
- The greatest number of attacks were found at the **Execution, Defense evasion, Lateral movement and Impact** stages. The tactics used during these stages are often considered the noisiest.
- The significant number of **Persistence** detections demonstrate the importance of being able to detect this tactic's techniques and procedures.

[5] https://attack.mitre.org/

Effectiveness of MITRE ATT&CK in security operations

The technique conversion = # incidents associated with the technique / # alerts associated with the technique

The higher the conversion, the more alerts become cybersecurity incidents after analysis.



Technique frequency (among alerts generated via IoAs)

A large number of alerts associated with an attack technique generally result from its legitimate use in the analyzed infrastructure. This must be controlled properly, because it indicates potentially favorable conditions for conducting corresponding attacks.

- **It is highly important to determine whether behavior is normal for a particular IT infrastructure.**
- Having a baseline for what is normal activity in your IT infrastructure (**efficient situational awareness**) will **help reduce false alerts** for legitimate activity and **raise the effectiveness of threat detection operations**.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Impact
T1189: Drive-by Compromise	**T1059: Command-Line Interface**	T1015: Accessibility Features	**T1134: Access Token Manipulation**	**T1134: Access Token Manipulation**	T1098: Account Manipulation	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1056: Input Capture	T1043: Commonly Used Port	T1485: Data Destruction
T1091: Replication Through Removable Media	**T1203: Exploitation for Client Execution**	T1098: Account Manipulation	T1015: Accessibility Features	T1197: BITS Jobs	**T1003: Credential Dumping**	T1135: Network Share Discovery	**T1175: Distributed Component Object Model**	T1113: Screen Capture	T1090: Connection Proxy	T1486: Data Encrypted for Impact
T1193: Spearphishing Attachment	T1177: LSASS Driver	T1197: BITS Jobs	T1176: Browser Extensions	T1207: DCShadow	T1214: Credentials in Registry	T1040: Network Sniffing	T1076: Remote Desktop Protocol		T1188: Multi-hop Proxy	T1488: Disk Content Wipe
T1192: Spearphishing Link	T1170: Mshta	T1158: Hidden Files and Directories	T1183: Image File Execution Options Injection	T1140: Deobfuscate/ Decode Files or Information	T1056: Input Capture	T1018: Remote System Discovery	**T1105: Remote File Copy**		T1219: Remote Access Tools	T1487: Disk Structure Wipe
T1195: Supply Chain Compromise	**T1086: PowerShell**	T1183: Image File Execution Options Injection	T1050: New Service	T1089: Disabling Security Tools	T1040: Network Sniffing	T1063: Security Software Discovery	**T1021: Remote Services**		**T1105: Remote File Copy**	T1496: Resource Hijacking
T1078: Valid Accounts	T1117: Regsvr32	T1177: LSASS Driver	**T1055: Process Injection**	T1107: File Deletion	T1174: Password Filter DLL	T1016: System Network Configuration Discovery	T1091: Replication Through Removable Media		**T1071: Standard Application Layer Protocol**	T1494: Runtime Data Manipulation
	T1085: Rundll32	T1050: New Service	T1053: Scheduled Task	T1158: Hidden Files and Directories		**T1033: System Owner/User Discovery**	T1077: Windows Admin Shares		T1095: Standard Non-Application Layer Protocol	T1492: Stored Data Manipulation
	T1053: Scheduled Task	**T1060: Registry Run Keys / Startup Folder**	**T1078: Valid Accounts**	T1183: Image File Execution Options Injection		**T1007: System Service Discovery**	**T1028: Windows Remote Management**		T1065: Uncommonly Used Port	T1493: Transmitted Data Manipulation
	T1064: Scripting	T1053: Scheduled Task	T1100: Web Shell	**T1036: Masquerading**		T1124: System Time Discovery			T1102: Web Service	
	T1035: Service Execution	T1101: Security Support Provider		T1170: Mshta						
	T1204: User Execution	**T1078: Valid Accounts**		T1126: Network Share Connection Removal						
	T1047: Windows Management Instrumentation	T1100: Web Shell		T1027: Obfuscated Files or Information						
	T1028: Windows Remote Management	**T1047: Windows Management Instrumentation**		**T1055: Process Injection**						
		T1084: Windows Management Instrumentation Event Subscription		T1117: Regsvr32						
				T1085: Rundll32						
				T1064: Scripting						
				T1078: Valid Accounts						
				T1102: Web Service						

Detailed information on attack technique statistics, including telemetry required for detection of the corresponding cybersecurity incidents, is provided by link.

Kaspersky MDR service description

Detection technologies

Endpoint behavior analysis combined with analysis of metadata gathered via endpoint protection products (used as sensors) is performed by the means of:

- **TTP-based threat hunting** (using IoAs)
- **SIEM rules** for automatic events correlation (if a SIEM system is implemented in the IT infrastructure)

Other detection technologies[6]:

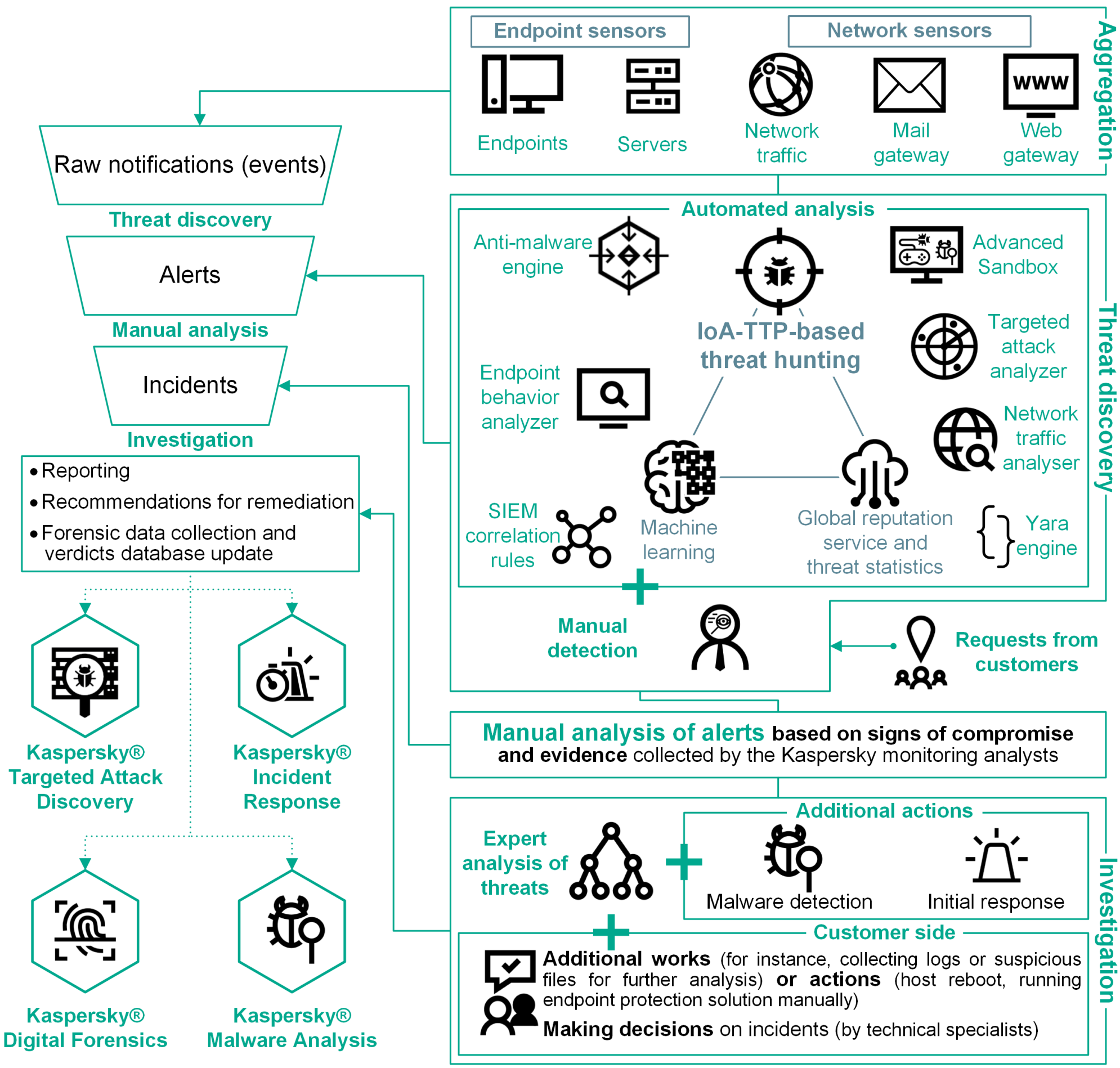
- Advanced Sandbox
- Anti-Malware engine
- Targeted Attack Analyzer
- Network Traffic Analyzer (includes IDS)
- YARA engine

Manual detection

Customer requests

Monitoring process

Real-time monitoring of network traffic combined with object sandboxing and endpoint behavior analysis delivers a detailed insight into what is happening across a business's IT infrastructure. According to the global threat landscape and the use of TTP-based threat detection logic (using IoAs), correlation of events from multiple layers of IT infrastructure, including networks and endpoints, enables "near real-time" detection of complex threats as well as retrospective investigations.



[6] Implemented as Kaspersky Anti-Targeted Attack platform (see https://www.kaspersky.com/enterprise-security/anti-targeted-attack-platform)