AV LAB
CYBERSECURITY FOUNDATION



Detailed EDR_XDR Solutions Overview

2025, Edition 3rd

Simulate offensive cyberattacks with telemetry event visibility

Environment: Windows 11, Windows Server 2025

2025

Table of contents

01 Introduction

02 Attacks visibility in telemetry

03 Understand the differences

04 Two-level certification

05 Which solutions have we tested?

06 Victim and agent system configuration

07 Comparison of security features

08 Comparative results

09 Simulated attacks description

10 Test conclusions

01 A word of introduction

The growing number of network-connected devices and widespread access to AI language models make organizations constantly vulnerable to cyberattacks and the consequences of careless employees. What's more, cybercriminals' access to widely popular AI technologies means that even the sophisticated protection methods implemented by defenders are not always sufficient to fend off timely threats that exploit the ignorance of insufficiently trained employees, weaknesses and vulnerabilities in operating systems and the configuration of cloud application environments.

EDR and XDR-class solutions require systematic testing to assess their real-world applicability in sub-criminal situations. Simulations of offensive cyberattacks will give a more complete picture of what security management experts in an organization can expect from a product when it clashes with real-world threats.



The importance of using EDR-XDR

EDR (Endpoint Detection and Response) and XDR (eXtended Detection and Response) solutions are derived from multi-layered endpoint protection. Their role is to monitor operating systems and cloud applications in real time. They take real-time and past threat searches to the next level, allowing you to spot the subtle signs of infected workstations. For any company, using this type of product can mean that it will receive more useful information from all endpoints, helping to contribute to better protection of the entire business from the aftermath of cyberattacks. Using EDR-XDR improves access to technical information from across the infrastructure. Insight into detailed telemetry from cyberattacks gives a broader perspective of what is happening in real time at endpoints.

02 Attacks visibility in telemetry



Having recorded at least residual information from potential cyber security incidents, it is possible to reconstruct the events that took place in the analyzed environment. Solutions for monitoring systems and applications, thanks to information correlation and automation functions, can clearly support IT employees who are responsible for security execution. With this, a team of experts can verify what and when the attacker did in the system, what processes and applications were referenced, what user accounts were used, and so on. All of this together will create an incident graph and reveal what the attacker targeted. The broader the scope of data and system monitoring, the easier it is to recreate the intentions of the hacker, in addition, the easier it is to configure the security product for the specific requirements of the organization, which can better respond to incidents and minimize their detrimental impact on business operations. The importance of using these defensive technologies also stems from their ability to integrate deeply with the IT infrastructure, which also makes it possible to more than adequately separate so-called system noise from real security incident indicators.

03 Understand the differences

EDR solutions focus on endpoint security, while XDRs cover a wider range of systems from which data is collected. Both solutions are designed to identify and respond to cyber threats, but XDRs cover more sources, among others, mobile devices, IoT sensors, Web 2.0 applications such as Google Workspace or Microsoft Office, network logs from edge devices, IDS, SIEM, etc. The final choice between EDR and XDR should depend on the needs and complexity of the environment of the organization that will use it, but the line between EDR and XDR is already starting to blur in some aspects of security.

Basic differences between EPP » EDR » XDR solutions

	INTEGRATION WITH IT INFRASTRUCTURE	SCOPE OF MONITORING	RESPONDING TO CYBERATTACKS
EPP	Integration with core IT infrastructure components: workstations, servers, business applications (e.g. SaaS).	Endpoint monitoring to detect and block malware.	Blocks malware, provides basic prevention and automatic responses.
EDR	Integration with a wider range of components: servers, workstations, SaaS, networked systems.	Advanced endpoint monitoring, analysis of more complex threats such as ransomware, fileless attacks, exploits, using advanced detection technologies.	Detects and isolates infected devices, analyzes incidents, and automates responses.
XDR	The broadest integration: servers, edge devices, cloud infrastructure, SaaS, IoT devices.	Comprehensive monitoring including endpoints, network traffic (e.g., anomalies, attack attempts), cloud applications (e.g., event logs) and IoT devices.	Offers advanced threat analytics, Threat Hunting and comprehensive protection for various environments.

* The table above contains many simplifications. Not all features can be assigned to one product category. For example, EPP solutions have evolved to EDR, and the differences between EDR and XDR are not as great as they used to be. The prototypes of EPP-EDR-XDR solutions have retained their core, i.e. advanced protection of workstations against threats and cyberattacks, but it is EDR and XDR that can correlate logs from different endpoints, provide visibility of the most detailed logs with the option of threat hunting, and what is related to it – more effective protection of the entire IT environment.

04 Two-level certification

Advances in workstation monitoring and protection technologies allow for more sophisticated analysis and detailed visibility of incidents. Solutions are tested and certified based on attack visibility in telemetry.



Attacks Visibility in Telemetry GOLD AWARD 2025

Solutions that have achieved full visibility of attacks in telemetry.



Attacks Visibility in Telemetry CERTIFIED 2025

Solutions that featured at least partial visibility of each attack in telemetry.

05 Which solutions have we tested?

Most EDR-XDR solutions come with an antivirus agent. We've kept this enabled so that the tests are the same as what the administrator can see in the production. The configuration of policies for antivirus agents was usually the default or included additional settings for more detailed telemetry. For solutions that needed a predefined agent policy configuration, we chose the most hardened settings to understand the attack chain and telemetry. This was also the goal of the test.

Vendor's Tested

Bitdefender

CHECK POINT

CISCO

elastic

METRAS part of Site

SOPHOS

ThreatDown Powered by Malwarebytes

WITH secure

xcitium

Vendor's Tested List and a specific agent configuration

BITDEFENDER GravityZone Extended Detection and Response (XDR)
Configuration: Policy Default + Ransomware Mitigation Enabled ◆ Sandbox Analyzer Enabled (Automatic sample submission from managed endpoints – Monitoring Mode) + Scripts scanning ◆ Intrusion Detection System (IDS) Enabled (Normal Mode) ◆ Risk Management Enabled ◆ Live Search Enabled

CHECK POINT Harmony Endpoint Advanced + EDR
Web & Files Protection all settings on Prevent mode ◆ Behavioral Protection all settings on Prevent mode ◆ All remediation security alerts enabled ◆ Analysis & Remediation - Protection mode as “Always” ◆ Enable Threat Hunting as “On” ◆ Attack Remediation as “Always” ◆ Windows agent version - 88.70.0326

CISCO AMP + XDR
Security Policy Default (Quarantine Threats) for all features

ELASTIC Security XDR
Default Policy + Complete XDR configuration

METRAS
Default + Agent Version 1.2.1

SOPHOS Intercept X Advanced + XDR
Policy Default + Complete XDR

THREATDOWN + EDR
Default + EDR + Enable Event Tracing for Windows

WITHSECURE Elements Endpoint Detection and Response
Policy Default + XDR

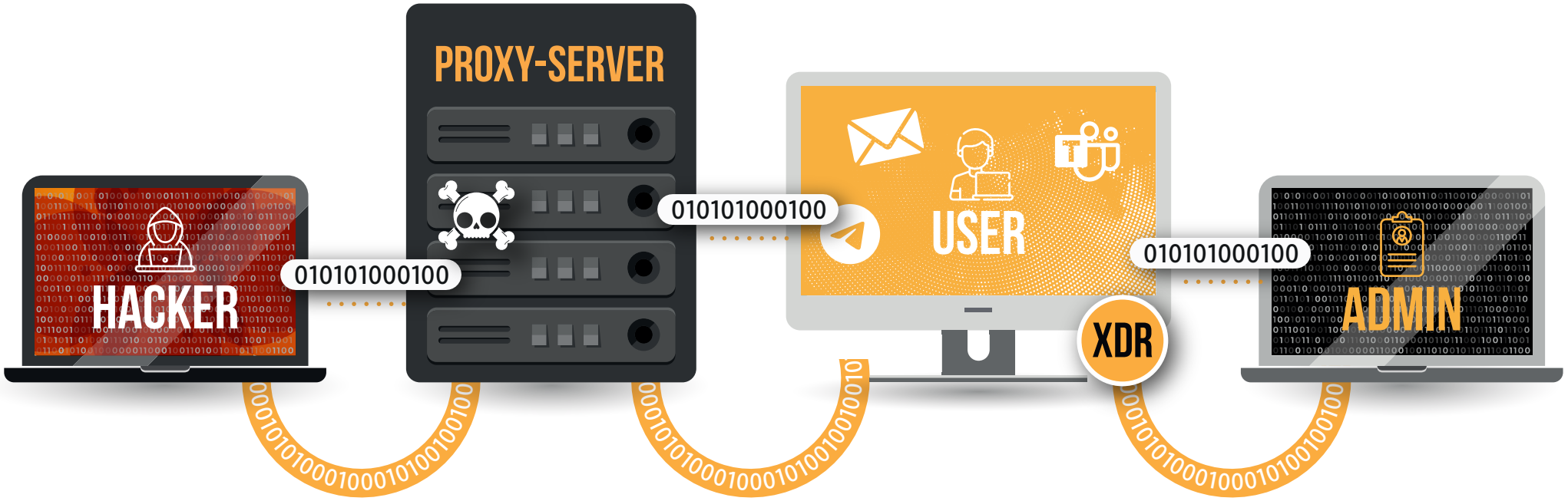
XCITIUM XDR
Policy MDR Policy + agent configuration Windows 8.1 Default for all features

06 Victim and agent system configuration

To test the attacks, we used a virtual machine running Kali Linux as a Command-and-Control server. We also used the Atomic Red Team tool, which has predefined types of attacks and other several methods to deliver the malicious payload and run it on the operating system.

We connected virtual machines running Windows 11 Pro with the solution agent installed to the same network. These machines had full Internet access. We used the standard Windows configuration that comes with the software.

We stopped creating campaigns from start to finish. The attack plan was carried out using the described protocols without any social engineering, because the type and purpose of the attack in the test scenario was known to the testers.



07 Comparison of security features

✱ Available as additional integration with external service

	BITDEFENDER	CHECK POINT	CISCO	ELASTIC	METRAS	SOPHOS	THREATDOWN	WITHSECURE	XCITIUM
Attack visibility	✓	✓	✓	✓	✓	✓	✓	✓	✓
Graphical visualization of an attack (event correlation)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Full attack telemetry	✓	✓	✓	✓	✓	✓	✓	✓	✓
Approximate reputation of a malicious file	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ability to search for intrusion traces (Search Query)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Graphical security simulation (e.g. vulnerabilities in systems, weak passwords, incorrect agent configuration)	✓	✓	✓	✓	✗	✓	✓	✓	✓
Insight into suspicious object lists (IP addresses, URL, SHA)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Proposed measures to recover from an attack	✓	✓	✓	✓	✗	✓	✓	✓	✗
Additional feedback about threat (Sandbox, VirusTotal, file reputation, other)	✓	✓	✓	✗	✓	✓	✓	✓	✓
Isolation of workstation, user, file after detecting an attack	✓	✓	✓	✓	✓	✓	✓	✓	✓
Updates management	✓	✗	✗	✗	✗	✓	✓	✓	✓
Data recovery after attack (user files)	✓	✗	✗	✗	✗	✓ ✱	✓	✗	✗
Securing login to an admin panel	✓	✓	✓	✓	✓	✓	✓	✓	✓
AI availability for admin in the console	✓	✓	✓	✓	✗	✓	✓	✓	✗

08 Assessing effectiveness in responding to attacks



USER

An employee using a Windows workstation is not always an expert and is not required to be. He must use business applications, communicate through various sources, upload and run files that can sometimes be malicious.

In this perspective, we evaluated what an employee might see after a hacker delivers a malicious payload to the system.



HACKER

Initially, a hacker may not have information on what security technologies an organization uses. His primary goal is to deliver the payload to the system or provoke the user to do it for him. As a result, he can gain access to resources in the organization.

In the context of this analysis, we evaluate what the hacker might see on his side in the event of success in authorizing instructions or launching a malicious application by the user.



ADMIN

The administrator's job is to monitor, manage security with the tools at his disposal. The user and the hacker, by performing certain actions, trigger certain alerts, which must flow down to the console of the EDR-XDR solution in question. Ideally, they should get all the data about the attack - the so-called full visibility of the incident with automatic remediation. If this fails every residual information from the attack is important to at least be able to notice the incident and respond to it sooner or later.

From an administrator's perspective, we evaluated the usefulness of information from attacks and user activity (clicking on links, software, running scripts, etc.) that flows down to the security solution console.

We evaluated the effectiveness of a given EDR-XDR solution from the perspective of three people who have different roles to play.



USER

- Attempting or opening a malicious page.
- Attempting or opening a malicious file.



HACKER

- No communication with the attacked host.
- Correctly run the dangerous code, and establish a connection to the victim's system.
- Possible exfiltration of certain files and system information.



ADMIN

- Important console alert.
- Preventive block of an attack.
- Automatic repair of the incident.
- Attack partially visible in the telemetry.
- Full visibility of the attack in the console.
- Administrator response required.
- Identification of the attack in MITRE ID.
- No telemetry of the attack - negative result.

Each attack includes a corresponding description with attribution to observed events from different perspectives:

	PRIMARY TTP	USER	HACKER	ADMIN	DEFENSE
Defensive Evasion Recon	T1518				DYNAMIC

08 Comparative results

It is characteristic of the solutions tested to detect attacks and anomalies automatically or manually if an alert about an attack is not reported in the console. The combination of both methods produces the best results. We can divide incident recognition into:

ACTIVE

Active Detection

Refers to proactive threat analysis through manual or automated analytical activities. In this model, analysts manually look for threats instead of waiting for the system to report them. Threat hunting techniques - that is, analyzing logs, processes and memory to look for unusual patterns - can be used.

DYNAMIC

Dynamic Detection

Refers to automatic and adaptive real-time threat detection. EDR systems use behavioral analysis - recognizing abnormal process and user actions, machine learning and AI, sandboxing and emulation of suspicious files or scripts in an isolated environment.

NO EVID.

No evidence of the attack

We did not detect any significant attack indicators in the administrator console during the analysis.

ACTIVE **Active Detection** DYNAMIC **Dynamic Detection** NO EVID. **No evidence of the attack**

	BITDEFENDER	CHECK POINT	CISCO	ELASTIC	METRAS	SOPHOS	THREATDOWN	WITHSECURE	XCITIUM
Defensive Evasion Recon	ACTIVE	ACTIVE	ACTIVE	ACTIVE	DYNAMIC	ACTIVE	ACTIVE	ACTIVE	DYNAMIC
Parent Process Spoofing	DYNAMIC	ACTIVE	ACTIVE	DYNAMIC	ACTIVE	DYNAMIC	DYNAMIC	DYNAMIC	ACTIVE
DLL Side-Loading via CPL	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC	ACTIVE	ACTIVE	ACTIVE	DYNAMIC
Masquerading: Rename System Utilities	ACTIVE	ACTIVE	ACTIVE	DYNAMIC	ACTIVE	ACTIVE	ACTIVE	DYNAMIC	ACTIVE
GhostLoader: Regsvr32 Evasion	ACTIVE	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC
Silent ISO - Hidden Payload	ACTIVE	ACTIVE	ACTIVE	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC	ACTIVE	ACTIVE
Windows Management Instrumentation Abuse	ACTIVE	ACTIVE	ACTIVE	ACTIVE	ACTIVE	ACTIVE	ACTIVE	NO EVID.	DYNAMIC
TG-Leak - File steal via Telegram API	NO EVID.	ACTIVE	ACTIVE	DYNAMIC	DYNAMIC	DYNAMIC	ACTIVE	ACTIVE	ACTIVE
URL Triggered Exploits via FTP	DYNAMIC	ACTIVE	DYNAMIC	DYNAMIC	ACTIVE	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC
Exploit of Legitimate Tools for Fileless Malware	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC	ACTIVE	DYNAMIC	DYNAMIC	DYNAMIC	DYNAMIC
DNS-based Fileless Attack	ACTIVE	ACTIVE	ACTIVE	ACTIVE	ACTIVE	ACTIVE	DYNAMIC	NO EVID.	ACTIVE
Stealthy Exfiltration via Encrypted Channels	ACTIVE	ACTIVE	ACTIVE	ACTIVE	ACTIVE	ACTIVE	ACTIVE	NO EVID.	ACTIVE
Attacks Passed	11/12	12/12	12/12	12/12	12/12	12/12	12/12	9/12	12/12
Certification									

09 Simulated attacks description

Type	Attack short description	Primary TTP
Defensive Evasion Recon	A technique used by attackers to identify installed software on a victim's system. It can be used to detect potential vulnerabilities, security (e.g. EDR, AV) or other applications that may facilitate further privilege escalation or data exfiltration.	T1518
Parent Process Spoofing	This technique involves running an application under the context of another process to evade detection and analyze how an EDR system reacts. We used LOLBIN to execute payloads stealthily.	T1202
DLL Side-Loading via CPL	Using Control Panel (.cpl) as a proxy to run malicious code - an attempt to bypass security mechanisms.	T1036.003
Masquerading: Rename System Utilities	Renaming Windows system tools to hide the hacker's intentions from security software and attempting to use them to perform malicious actions.	T1036.003
GhostLoader: Regsvr32 Evasion	Regsvr32.exe is a Windows system utility that is used to register and unregister DLL libraries. Attackers can exploit this utility to execute code and bypass security measures.	T1218.010
Silent ISO - Hidden Payload	This is a technique in which the opening or running of a malicious image initiates an attack without the user's awareness. This phenomenon can result in the compromise of the system through malware infiltration or other malicious activities.	T1204.003
Windows Management Instrumentation Abuse	The WMI attack uses Windows Management Instrumentation (WMI) to execute malicious commands and scripts both locally and remotely. It allows adversaries to covertly gather information and execute code on Windows systems.	T1047
TG-Leak - File steal via Telegram API	Telegram messenger API as an unusual channel for exfiltrating files from an attacked system. In this simulated attack and a real scenario, a command using the Telegram API can be integrated into any malware without installing Telegram messenger on the victim's system.	T1567.002
URL Triggered Exploits via FTP	Using FTP to deliver a malicious script, which is then run in the default browser	T1071.002
Exploit of Legitimate Tools for Fileless Malware	Using LOLBIN to launch a malicious code attack that leaves no permanent trace on the system.	T1197
DNS-based Fileless Attack	The DNS zone is exploited to retrieve the payload from the TXT record, which may contain an encrypted malicious code that is designed to run on the system in a fileless attack.	T1071.004
Stealthy Exfiltration via Encrypted Channels	An attacker can use SFTP to exfiltrate data from the system without leaving visible traces.	T1041

Bitdefender

GravityZone Extended Detection and Response (XDR)







	PRIMARY TTP	USER	HACKER	ADMIN	DEFENSE
Defensive Evasion Recon	T1518				ACTIVE
Parent Process Spoofing	T1202				DYNAMIC
DLL Side-Loading via CPL	T1036.003				DYNAMIC
Masquerading: Rename System Utilities	T1036.003				ACTIVE
GhostLoader: Regsvr32 Evasion	T1218.010				ACTIVE
Silent ISO - Hidden Payload	T1204.003				ACTIVE
Windows Management Instrumentation Abuse	T1047				ACTIVE
TG-Leak - File steal via Telegram API	T1567.002				NO EVID.
URL Triggered Exploits via FTP	T1071.002				DYNAMIC
Exploit of Legitimate Tools for Fileless Malware	T1197				DYNAMIC
DNS-based Fileless Attack	T1071.004				ACTIVE
Stealthy Exfiltration via Encrypted Channels	T1041				ACTIVE

CHECK POINT™

Harmony Endpoint Advanced + EDR



	PRIMARY TTP	USER	HACKER	ADMIN	DEFENSE
Defensive Evasion Recon	T1518				ACTIVE
Parent Process Spoofing	T1202				ACTIVE
DLL Side-Loading via CPL	T1036.003				DYNAMIC
Masquerading: Rename System Utilities	T1036.003				ACTIVE
GhostLoader: Regsvr32 Evasion	T1218.010				DYNAMIC
Silent ISO - Hidden Payload	T1204.003				ACTIVE
Windows Management Instrumentation Abuse	T1047				ACTIVE
TG-Leak - File steal via Telegram API	T1567.002				ACTIVE
URL Triggered Exploits via FTP	T1071.002				ACTIVE
Exploit of Legitimate Tools for Fileless Malware	T1197				DYNAMIC
DNS-based Fileless Attack	T1071.004				ACTIVE
Stealthy Exfiltration via Encrypted Channels	T1041				ACTIVE

Advanced Malware Protection (AMP) + XDR



	PRIMARY TTP	USER	HACKER	ADMIN	DEFENSE
Defensive Evasion Recon	T1518				ACTIVE
Parent Process Spoofing	T1202				ACTIVE
DLL Side-Loading via CPL	T1036.003				DYNAMIC
Masquerading: Rename System Utilities	T1036.003				ACTIVE
GhostLoader: Regsvr32 Evasion	T1218.010				DYNAMIC
Silent ISO - Hidden Payload	T1204.003				ACTIVE
Windows Management Instrumentation Abuse	T1047				ACTIVE
TG-Leak - File steal via Telegram API	T1567.002				ACTIVE
URL Triggered Exploits via FTP	T1071.002				DYNAMIC
Exploit of Legitimate Tools for Fileless Malware	T1197				DYNAMIC
DNS-based Fileless Attack	T1071.004				ACTIVE
Stealthy Exfiltration via Encrypted Channels	T1041				ACTIVE

Elastic Security XDR



	PRIMARY TTP	USER	HACKER	ADMIN	DEFENSE
Defensive Evasion Recon	T1518				ACTIVE
Parent Process Spoofing	T1202				DYNAMIC
DLL Side-Loading via CPL	T1036.003				DYNAMIC
Masquerading: Rename System Utilities	T1036.003				DYNAMIC
GhostLoader: Regsvr32 Evasion	T1218.010				DYNAMIC
Silent ISO - Hidden Payload	T1204.003				DYNAMIC
Windows Management Instrumentation Abuse	T1047				ACTIVE
TG-Leak - File steal via Telegram API	T1567.002				DYNAMIC
URL Triggered Exploits via FTP	T1071.002				DYNAMIC
Exploit of Legitimate Tools for Fileless Malware	T1197				DYNAMIC
DNS-based Fileless Attack	T1071.004				ACTIVE
Stealthy Exfiltration via Encrypted Channels	T1041				ACTIVE

METRAS
part of Site

METRAS



	PRIMARY TTP	USER	HACKER	ADMIN	DEFENSE
Defensive Evasion Recon	T1518				DYNAMIC
Parent Process Spoofing	T1202				ACTIVE
DLL Side-Loading via CPL	T1036.003				DYNAMIC
Masquerading: Rename System Utilities	T1036.003				ACTIVE
GhostLoader: Regsvr32 Evasion	T1218.010				DYNAMIC
Silent ISO - Hidden Payload	T1204.003				DYNAMIC
Windows Management Instrumentation Abuse	T1047				ACTIVE
TG-Leak - File steal via Telegram API	T1567.002				DYNAMIC
URL Triggered Exploits via FTP	T1071.002				ACTIVE
Exploit of Legitimate Tools for Fileless Malware	T1197				ACTIVE
DNS-based Fileless Attack	T1071.004				ACTIVE
Stealthy Exfiltration via Encrypted Channels	T1041				ACTIVE

SOPHOS

Intercept X Advanced + XDR



	PRIMARY TTP	USER	HACKER	ADMIN	DEFENSE
Defensive Evasion Recon	T1518				ACTIVE
Parent Process Spoofing	T1202				DYNAMIC
DLL Side-Loading via CPL	T1036.003				ACTIVE
Masquerading: Rename System Utilities	T1036.003				ACTIVE
GhostLoader: Regsvr32 Evasion	T1218.010				DYNAMIC
Silent ISO - Hidden Payload	T1204.003				DYNAMIC
Windows Management Instrumentation Abuse	T1047				ACTIVE
TG-Leak - File steal via Telegram API	T1567.002				DYNAMIC
URL Triggered Exploits via FTP	T1071.002				DYNAMIC
Exploit of Legitimate Tools for Fileless Malware	T1197				DYNAMIC
DNS-based Fileless Attack	T1071.004				ACTIVE
Stealthy Exfiltration via Encrypted Channels	T1041				ACTIVE

ThreatDown
Powered by Malwarebytes

ThreatDown + EDR



	PRIMARY TTP	USER	HACKER	ADMIN	DEFENSE
Defensive Evasion Recon	T1518				ACTIVE
Parent Process Spoofing	T1202				DYNAMIC
DLL Side-Loading via CPL	T1036.003				ACTIVE
Masquerading: Rename System Utilities	T1036.003				ACTIVE
GhostLoader: Regsvr32 Evasion	T1218.010				DYNAMIC
Silent ISO - Hidden Payload	T1204.003				DYNAMIC
Windows Management Instrumentation Abuse	T1047				ACTIVE
TG-Leak - File steal via Telegram API	T1567.002				ACTIVE
URL Triggered Exploits via FTP	T1071.002				DYNAMIC
Exploit of Legitimate Tools for Fileless Malware	T1197				DYNAMIC
DNS-based Fileless Attack	T1071.004				DYNAMIC
Stealthy Exfiltration via Encrypted Channels	T1041				ACTIVE

WithSecure + EDR







	PRIMARY TTP	USER	HACKER	ADMIN	DEFENSE
Defensive Evasion Recon	T1518				ACTIVE
Parent Process Spoofing	T1202				DYNAMIC
DLL Side-Loading via CPL	T1036.003				ACTIVE
Masquerading: Rename System Utilities	T1036.003				DYNAMIC
GhostLoader: Regsvr32 Evasion	T1218.010				DYNAMIC
Silent ISO - Hidden Payload	T1204.003				ACTIVE
Windows Management Instrumentation Abuse	T1047				NO EVID.
TG-Leak - File steal via Telegram API	T1567.002				ACTIVE
URL Triggered Exploits via FTP	T1071.002				DYNAMIC
Exploit of Legitimate Tools for Fileless Malware	T1197				DYNAMIC
DNS-based Fileless Attack	T1071.004				NO EVID.
Stealthy Exfiltration via Encrypted Channels	T1041				NO EVID.

xcitium

Advanced Endpoint Protection + XDR



	PRIMARY TTP	USER	HACKER	ADMIN	DEFENSE
Defensive Evasion Recon	T1518				DYNAMIC
Parent Process Spoofing	T1202				ACTIVE
DLL Side-Loading via CPL	T1036.003				DYNAMIC
Masquerading: Rename System Utilities	T1036.003				ACTIVE
GhostLoader: Regsvr32 Evasion	T1218.010				DYNAMIC
Silent ISO - Hidden Payload	T1204.003				ACTIVE
Windows Management Instrumentation Abuse	T1047				DYNAMIC
TG-Leak - File steal via Telegram API	T1567.002				ACTIVE
URL Triggered Exploits via FTP	T1071.002				DYNAMIC
Exploit of Legitimate Tools for Fileless Malware	T1197				DYNAMIC
DNS-based Fileless Attack	T1071.004				ACTIVE
Stealthy Exfiltration via Encrypted Channels	T1041				ACTIVE

10 Test conclusions

High effectiveness of threat detection

Most of the solutions tested in this edition achieve very high efficiency in neutralizing threats, which can confirm their effectiveness in real-world attack scenarios.

Incident visibility as a priority

Organizations should pay special attention to recording and presenting complete incident data. The choice of the right solution should be based not only on the effectiveness of protection, but also on the detail of available telemetry, which is essential for an effective response. Lack of adequate data in the administrator's console could mean that the product failed to register the attack or did so too late, which could result in serious consequences.

Differences between EDR and XDR

XDR solutions will work better for large organizations, with multiple locations, with cloud systems, where correlation of events from different sources is required, sometimes as SOAR. While EDR may fit better into the requirements of small and medium-sized companies with their own IT/SOC department, with a large number of end devices, but without distributed infrastructure. The broader EDR can also be delegated to remote incident management by a third-party service provider as part of MDR (Managed Detection and Response).

Configuration and settings

Tests have shown that the default settings do not always provide optimal protection and event visibility. For fully effective protection and detailed telemetry, it is recommended to activate additional features, such as automatic PUP repair, rollback, isolation of devices with detected incidents, enabling an additional level of log detail, etc.

Simulating attacks

Before making a choice, it's a good idea to use free tools such as Metasploit, Atomic Red Team and Caldera Framework to conduct your own experiments on how to represent the full context of an attack and how to respond to incidents.

What do we look out for during this test?



Through an independent evaluation of solutions equipped with EDR-XDR modules, we confirm their effectiveness in detecting and responding to advanced attacks (APTs). The test is conducted in a simulated environment. The goal of the test is to provide as much detail as possible about the solution when responding to attacks and threats. The feedback can be used to improve software and better secure endpoints.

The test covers the following areas:

Attack Detection

The test evaluates whether the solution is capable of detecting a wide range of APT attacks, including 0-day attacks.

Responding to Attacks

The tested solution should effectively respond to attacks in real time, including isolating infected devices, and limiting damage.

Visibility of Artifacts

We verify that the solution provides sufficient visibility of attacks in the admin console which is necessary to trace the event from the initiation of the attack to the remediation phase.

Who are these tests for?

The evaluation of the tested solutions is addressed to developers and companies that are looking for comprehensive protection of all devices in the network. The test ends with a certificate, and the results and conclusions can help you choose the solution that best meets the needs of your organization.

The final report can indicate the strengths of the product, and additionally shows whether the solution meets certain standards. This will have a positive impact on customer decisions related to product selection.

How do we test in details?



- Initial preparation of Windows security breach scenarios.
- Setting up the test environment and verifying that the simulated attacks are working correctly.
- Conduct a targeted investigation taking into account the visibility of attacks and threats in telemetry.
- The test examines the ability to automatically respond to threats, such as isolation of infected devices, blocking communication, and automatic repair.
- We verify the correct operation of manual incident management.
- We provide and discuss technical details.

Why is it worth having the certificate?

- Join the developers certificated by the independent organization.
- Use the certificate for marketing purposes, e.g. place it on your website, promote your company in a magazine, allow potential customers to see that you own a reputable solution.
- Safely test out your solution in a controlled environment.
- Receive feedback and improve the effectiveness of your security product.





To learn more about the collaboration, please visit the Attack Visibility in EDR-XDR Telemetry page, where you can also track the results of recent editions.

CHECK OUR WEBSITE



We also conduct tests of other types:

Test of modules to protect online banking

Antivirus solutions are subjected to scenarios of payment details theft, information manipulation by banking Trojans and other malware.

Advanced In-The-Wild Malware Test

We evaluate the effectiveness of protection software against threats in the wild, and reveal the true ability of the product to neutralize threats.

Cyber Transparency Audit

We verify information from Endpoint Protection software vendors for compliance with specific standards and the idea of transparency.

For more information, please visit our website...

AVLab CYBERSECURITY FOUNDATION

The AVLab Cybersecurity Foundation is an independent organization dedicated to protecting privacy and security on the Internet.
We are part of the CTF (Cyber Transparency Forum) and provide independent assessments of cybersecurity vendors' systems. We are a member of AMTSO (Anti-Malware Testing Standards Organization), which works to improve the transparency, objectivity and quality of testing. Also, we are a member of MVI (Microsoft Virus Initiative) in this matter as well.

We build awareness of users in the field of digital protection.
We issue opinions, technical analyzes and tests of IT solutions in the field of cybersecurity. Our strongest assets include thorough and detailed reviews, preparation of reports related to privacy and endpoint protection, and in particular, security tests that make us recognizable all over the world as one of the most trusted and popular testing laboratories.

To learn more about other opportunities for cooperation, please refer to our full offer and contact us: kontakt@avlab.pl

amtso
The cybersecurity industry's testing standard community
MEMBER

www.avlab.pl