



EDR_XDR solutions overview

2ND EDITION



Simulation of offensive fileless attacks
taking into account incident visibility in telemetry

Tools used: Metasploit, Atomic Red Team Framework, Caldera Framework

A background graphic consisting of a network of interconnected nodes and lines, resembling a web or data structure, in a light gray color.

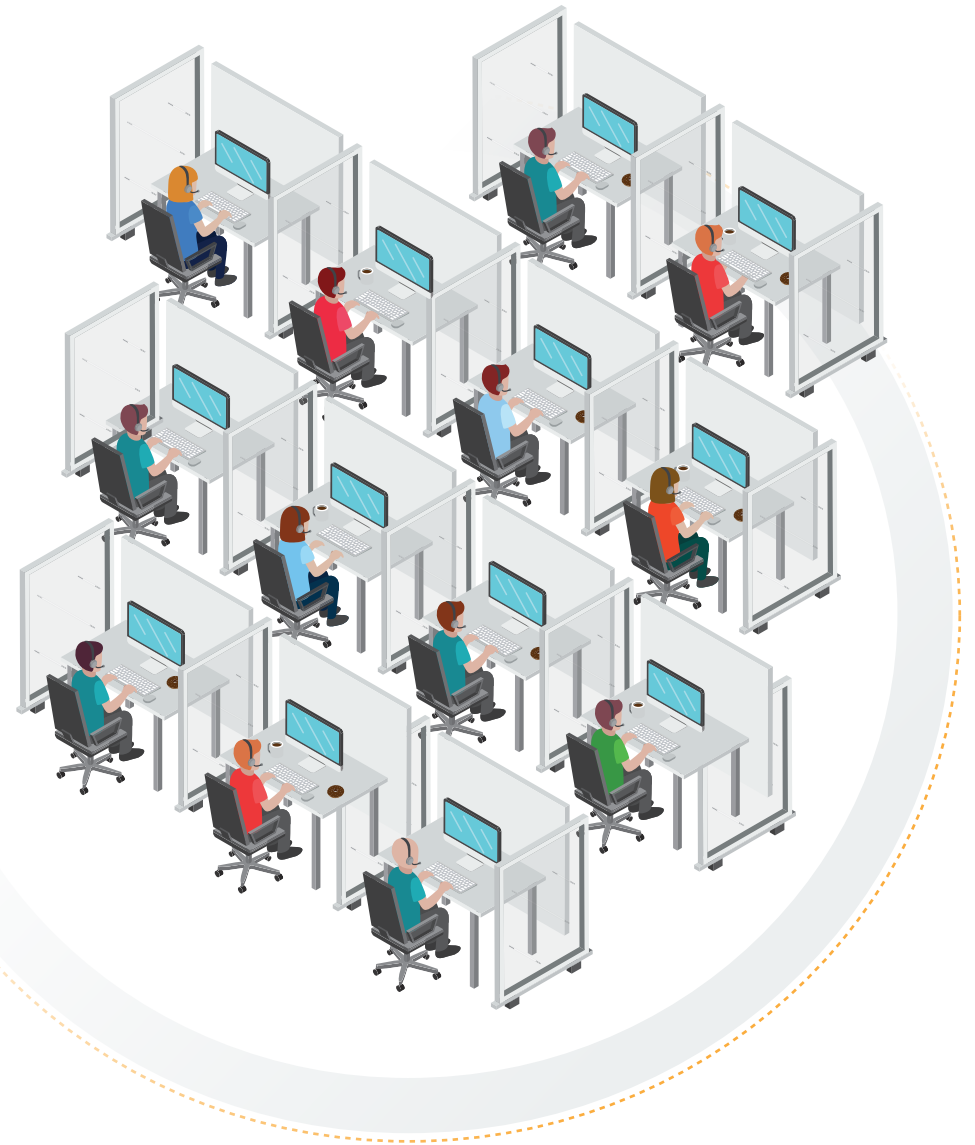
Table of contents

I	Importance of attack visibility in telemetry
II	EDR and XDR - differences
III	Benefits of implementation
IV	Common features of EDR and XDR
V	Tested solutions for business
VI	Configuration of victim system and agent
VII	Comparison of security features
VIII	Results based on attacks
IX	Description of simulated attacks
X	Conclusions and general recommendations

Visibility of attacks in telemetry and incident response from the perspective of SOC (Security Operation Center)

Endpoint Detection and Response (EDR) and eXtended Detection and Response (XDR) are derived from the multi-layered endpoint protection developed over the years. Their main task is to monitor operating systems and applications in the cloud in real time. Properly implemented, they take threat hunting to a higher level, allowing to see indicators of compromise. For any company, this might mean having access to useful information from all endpoints which will certainly contribute to better protection of the entire network as well as employees against cyberattacks.

Using products of this class gives an overview of technical information from the entire infrastructure. In other words, observing telemetry from cyberattacks gives a broader picture of what has happened in the past, and what is currently happening on endpoints. As this test proves, thanks to correlation of incidents from operating systems, EDR-XDR software can provide significant value to large and small organizations with any level of technical skill. At the same time, we would like to point out that the implementation of this class of product needs to be a conscious strategy to protect against cyberattacks.



EDR and XDR – differences

EDR solutions usually focus solely on endpoint security, while XDR covers a wider range of system integration. Both solutions are designed to identify and respond to cyber threats, but XDR supports more data sources, among others, mobile devices, IoT sensors, Web 2.0 applications such as Google Workspace and Microsoft Office, network logs from edge devices, IDS and SIEM systems, etc. The final choice between EDR and XDR should depend on the needs and complexity of the organization's IT environment, but at the same time boundaries between EDR and XDR already start to erase in some security categories.

Basic differences between EPP » EDR » XDR solutions

	EPP	EDR	XDR
INTEGRATION WITH IT INFRASTRUCTURE	Basic elements of IT infrastructure, some business services and applications.	Broader range of security systems, business services and applications.	The widest range of security systems, business services and applications, cloud computing, IoT devices.
SCOPE OF MONITORING	Monitoring of endpoints. Detecting and blocking malware.	Monitoring of endpoints. Detecting and responding to more advanced threats.	Monitoring of endpoints, networks, and cloud applications. Providing a comprehensive view of security.
RESPONDING TO CYBERATTACKS	Quite limited prevention, detection, and automatic response.	Advanced prevention, detection, response, isolation, and automation.	Detection and prevention of attacks from the most diverse areas. Availability of the so called Threat Hunting.

* The table above contains many simplifications. Not all features can be assigned to a single product category. For example, EPP solutions have evolved to EDR, and the differences between EDR and XDR are no longer as big as they used to be. The common core has been retained, i.e. an advanced protection of workstations against threats and cyberattacks, but it is EDR and XDR that can better correlate logs from different endpoints. In addition, they provide the most detailed data visibility and enable the so called Threat Hunting, effectively securing endpoints.



Why you should

Why should you consider implementing EDR?

Thanks to EDR, IT security officers can monitor and analyze incidents that will correlate with system processes, files, network connections, registry key modifications, etc. Here, automation, as it is based on machine learning, allows to quickly identify suspicious or clearly malicious activity on devices. This is crucial in detecting advanced ATP attacks, including 0-day ones.

Solutions equipped with EDR offer very precise visibility of events from end devices. Some developers implement features known so far only from XDR. We are talking about the so-called Threat Hunting, thanks to which EDR works perfectly in the hands of malware analysts. It is also necessary to mention effective defense mechanisms, such as: isolating infected devices, searching for traces of intrusions, obtaining information about the course of the attack, revealing the initial attack vector, methods of spreading malware.

Why should you consider implementing XDR?

XDR combines the features of EPP and EDR. It uses telemetry from all endpoints, even from systems and applications in the cloud. It provides a comprehensive and holistic view of security of the entire infrastructure. With XDR, it is possible to identify attacks quickly and effectively. SOC teams can take appropriate remedial action just as quickly.

Products of this class make it easier to track not only suspicious activity at all levels of the IT infrastructure, but also seemingly trusted events, where the attacker's malicious code may be among the so-called "system noise". The solution takes security of the organization to a higher level by reducing the response time to threats and automatic repair of systems after a reported incident.

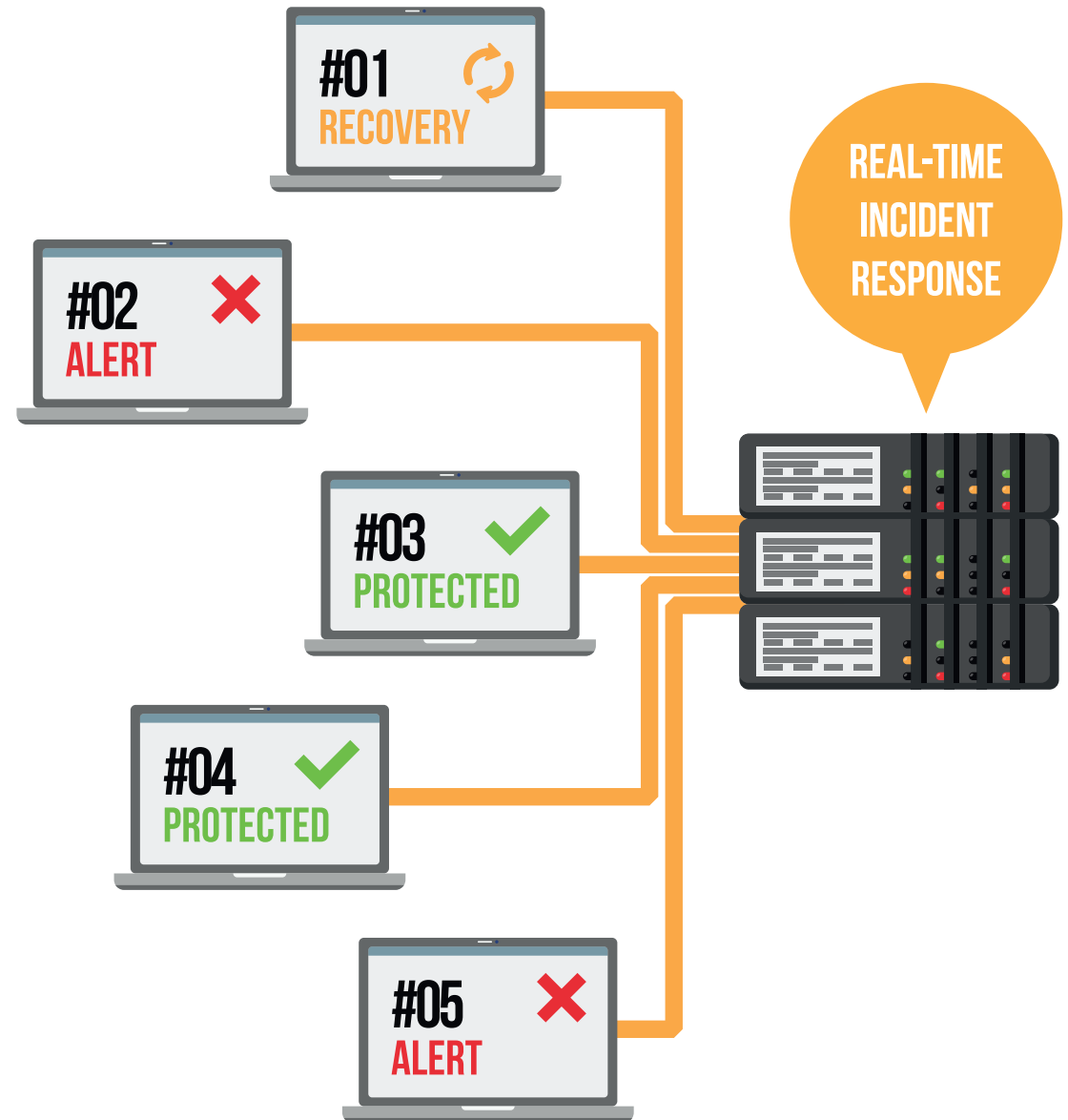


Telemetry and visibility of attacks – common features of EDR and XDR

We conducted an analysis of the EDR and XDR modules to justify the investment in a given product designed to protect systems against cyberattacks. As the Red Team, we simulated the actions of attackers who had gained access to the IT infrastructure. As Blue Team, we analyzed data from these attacks to assess the capabilities of the tested product to detect and respond to a threat.

Based on the data collected, we believe that the most important thing is that the product records traces of attacks in the administrator console. It does not matter if these events are processed automatically or manually by a team of qualified employees. The product must provide visibility into system events along with telemetry that allows to understand the context of the attack and capture the necessary technical details.

In this test, we did not test the effectiveness of protection against cyberattacks. Rather, we focused on ensuring that the solution guarantees visibility of incidents through attack telemetry. Lack of visibility of the incident or telemetry may mean that the product's protection did not work or it detected a threat too late.



Testing solutions for business

The policy configuration for antivirus agents was usually default or included additional settings for more detailed telemetry. Importantly, we did not disable antivirus protection or any other features. Solutions that had to be assigned a predefined agent configuration after installation were configured with the most hardened settings possible to achieve detailed visibility into the attack chain and telemetry which was the goal of this test. At the request of the developers, we assigned the proposed settings.



Emsisoft Enterprise Security + EDR
default settings

emsisoft.com



Eset Protect Elite + XDR
default settings
+ all rules for EDR enabled

eset.com



Microsoft Defender for Business + EDR
default settings

microsoft.com



Metras + EDR
default settings

site.sa



Xcitium Advanced + EDR
predefined policy 8.1

xcitium.com

Configuration of victim system and agent



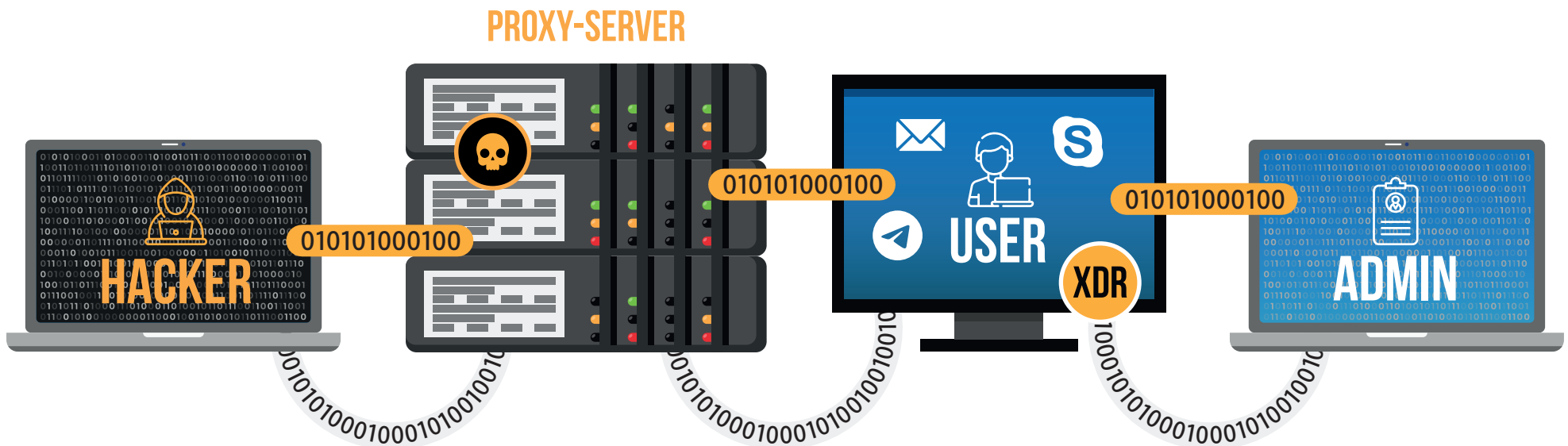
To simulate the attacks, we used a virtual machine running Kali Linux as a Command and Control server with Metasploit software. In addition, the Atomic Red Team tool with predefined types of attacks, as well as the Caldera Framework and several of our own methods to deliver the malicious payload, and run on the operating system.



Virtual machines with Windows 11 Pro with the agent installed of a given solution had full access to the Internet. We have applied the default Windows configuration.



We have given up creating campaigns from start to finish. The so-called payload has been delivered using the described protocols without any social engineering because the type and purpose of the attack in the simulated scenario was known to the testers.



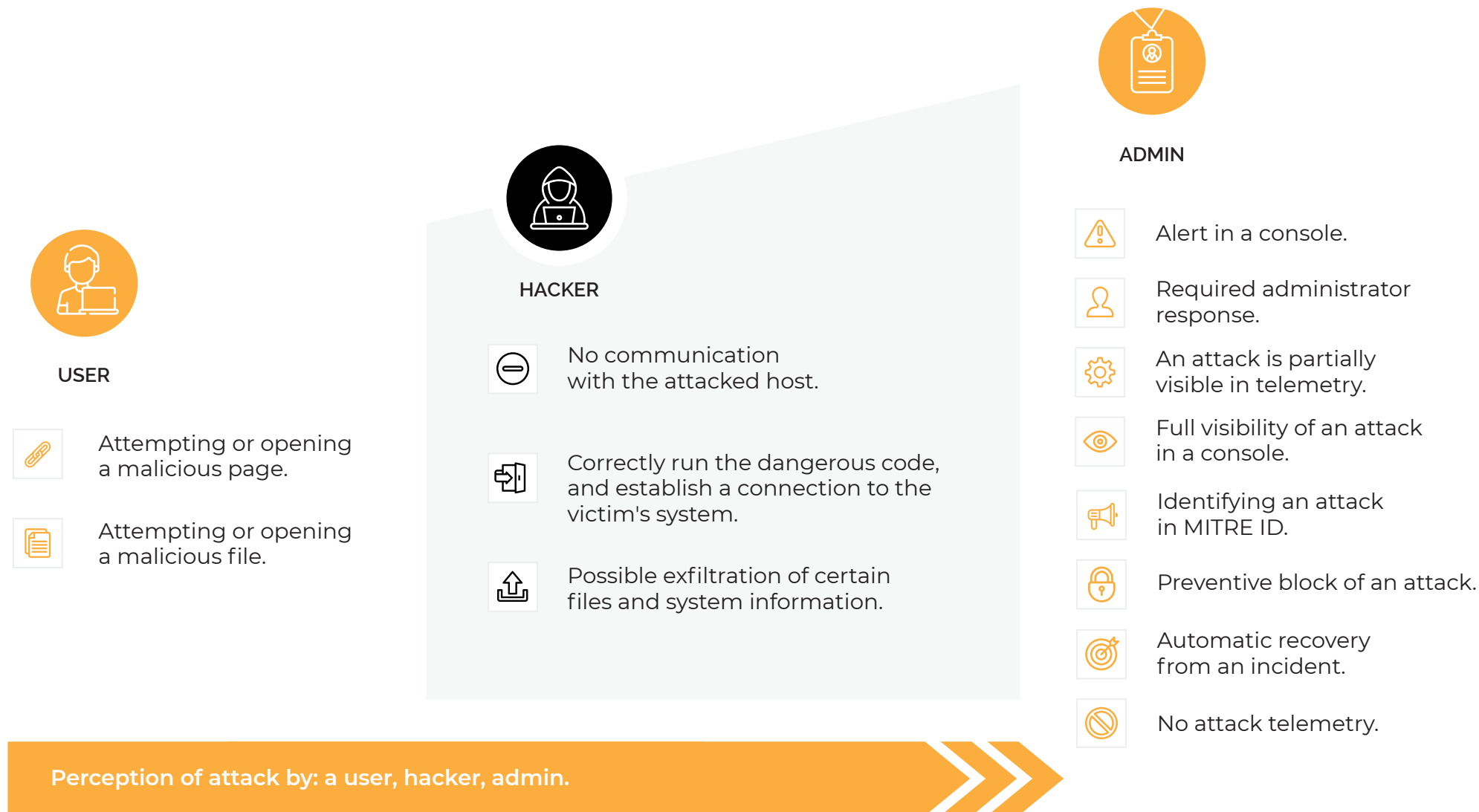
Comparison of security features of EDR-XDR solutions

	Emsisoft Enterprise Security	ESET Protect Elite	Metras	Microsoft Defender for Business	Xcitium Advanced
Attack visibility	✓	✓	✓	✓	✓
Graphical visualization of an attack (event correlation)	✓	✓	✓	✓	✓
Full telemetry of an attack	✓	✓	✓	✓	✓
Estimated reputation of malicious file	✓	✓	✓	✓	✓
Possibility to search for traces of intrusion (Search Query)	✓	✓	✓	✓	✓
Graphical security simulation (e.g. system vulnerabilities, weak passwords, incorrect agent configuration)	✗	✓	✗	✓	✓
Insight into suspicious lists of objects (IP addresses, URL, SHA)	✓	✓	✓	✓	✓
Proposed measures for recovery after an attack	✓	✓	✗	✓	✗
Second opinion of a threat (sandbox, VirusTotal, file reputation, others)	✓	✓	✓	✓	✓
Isolation of a workstation, user, and file after detected attack	✓	✓	✓	✓	✓
Update management	✗	✓	✗	✓	✓
Restoring data after an attack (user files)	✓	✗	✗	✗	✗
Securing the logging into administration panel	✓	✓	✓	✓	✓
Used third-party technologies	Emsisoft, Bitdefender	Eset	Metras	Microsoft	Xcitium, Comodo
Supported operation systems for EDR/XDR*	Windows, Windows Server	Windows, Windows Server, macOS, Linux	Windows, Windows Server, Linux	Windows, Windows Server, macOS, Linux	Windows, Windows Server

* Due to technological limitations, features for EDR-XDR may vary for operating systems.

Results based on simulated attacks

The primary objective of the test was to verify the visibility of attacks in the EDR-XDR console against simulated file-network activities that should be logged by an agent installed on a workstation.

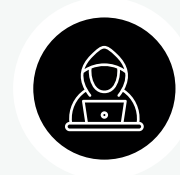


EMSIOSOFT

Enterprise Security with EDR



USER

































HACKER



ADMIN

PRIMARY TTP

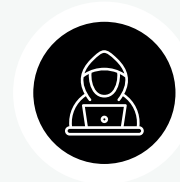
	PRIMARY TTP	USER	HACKER	ADMIN
Software Discovery Attack by PowerShell	T1518			
Software Discovery Attack by Malicious Executable	T1204.002			
Malicious .CPL file by Control Panel (control.exe)	T1218.002			
Signed Binary Proxy Execution by regsvr32.exe	T1218.010			
Malicious .LNK file by .ISO Image Mounting	T1204.003			
Data Theft via Telegram API	T1059.003			
Data Theft via Malicious File Execution	T1048			
Malicious Macro in Word & Metasploit	T1105			
PsExec & Launching Malware via certutil.exe	T1570			
Clearing the history of PowerShell commands by Malicious File	T1070.003			



ESET Protect Elite



USER



HACKER



ADMIN

PRIMARY TTP

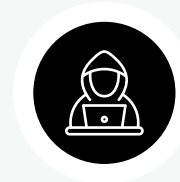
	PRIMARY TTP	USER	HACKER	ADMIN
Software Discovery Attack by PowerShell	T1518			
Software Discovery Attack by Malicious Executable	T1204.002			
Malicious .CPL file by Control Panel (control.exe)	T1218.002			
Signed Binary Proxy Execution by regsvr32.exe	T1218.010			
Malicious .LNK file by .ISO Image Mounting	T1204.003			
Data Theft via Telegram API	T1059.003			
Data Theft via Malicious File Execution	T1048			
Malicious Macro in Word & Metasploit	T1105			
PsExec & Launching Malware via certutil.exe	T1570			
Clearing the history of PowerShell commands by Malicious File	T1070.003			

SITE METRAS

METRAS



USER



HACKER



ADMIN

PRIMARY TTP

	PRIMARY TTP	USER	HACKER	ADMIN
Software Discovery Attack by PowerShell	T1518			
Software Discovery Attack by Malicious Executable	T1204.002			
Malicious .CPL file by Control Panel (control.exe)	T1218.002			
Signed Binary Proxy Execution by regsvr32.exe	T1218.010			
Malicious .LNK file by .ISO Image Mounting	T1204.003			
Data Theft via Telegram API	T1059.003			
Data Theft via Malicious File Execution	T1048			
Malicious Macro in Word & Metasploit	T1105			
Psexec & Launching Malware via certutil.exe	T1570			
Clearing the history of PowerShell commands by Malicious File	T1070.003			



MICROSOFT Defender for Business

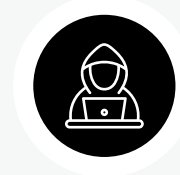
	PRIMARY TTP	USER	HACKER	ADMIN
Software Discovery Attack by PowerShell	T1518			
Software Discovery Attack by Malicious Executable	T1204.002			
Malicious .CPL file by Control Panel (control.exe)	T1218.002			
Signed Binary Proxy Execution by regsvr32.exe	T1218.010			
Malicious .LNK file by .ISO Image Mounting	T1204.003			
Data Theft via Telegram API	T1059.003			
Data Theft via Malicious File Execution	T1048			
Malicious Macro in Word & Metasploit	T1105			
Psexec & Launching Malware via certutil.exe	T1570			
Clearing the history of PowerShell commands by Malicious File	T1070.003			



XCITIUM Advanced



USER



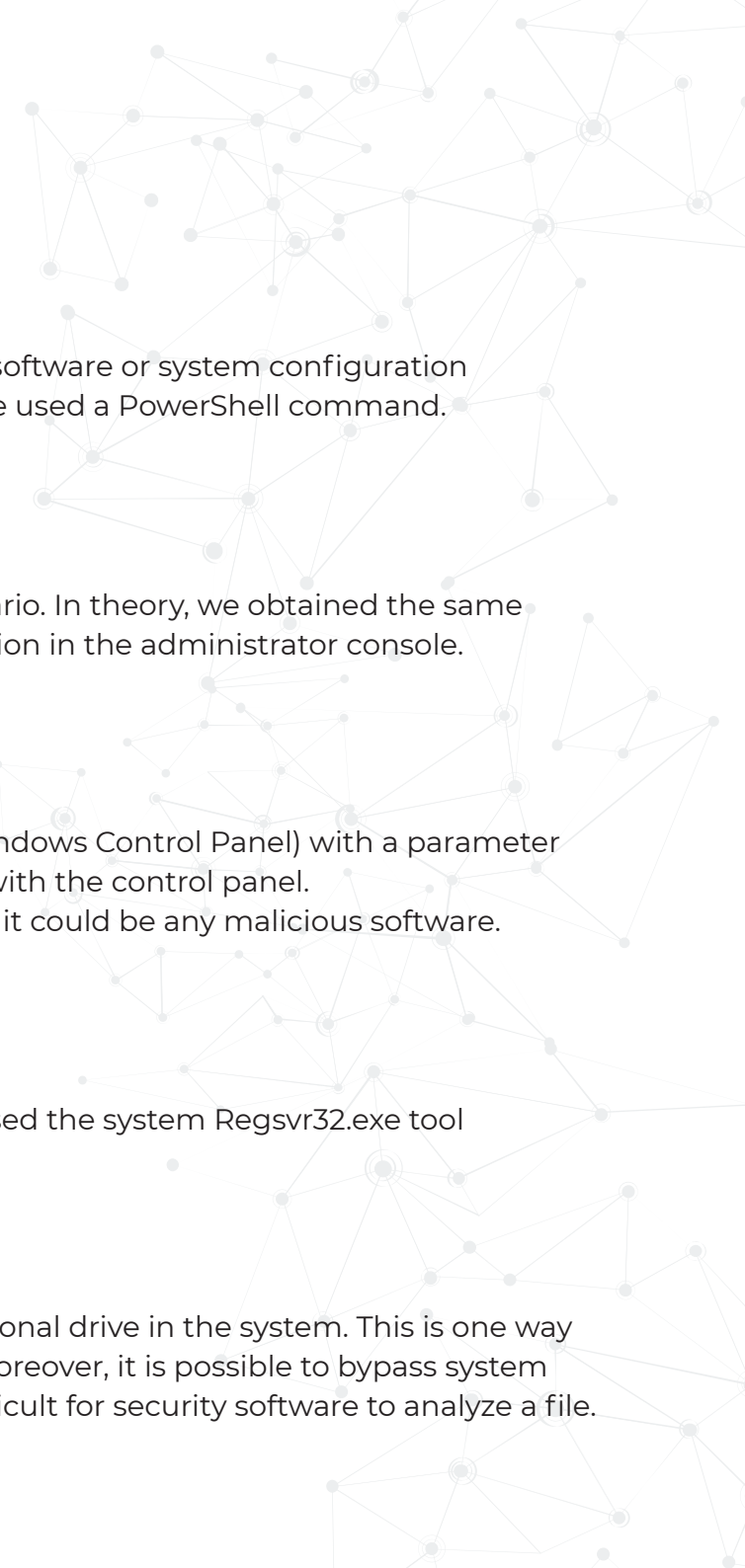
HACKER



ADMIN

PRIMARY TTP

	PRIMARY TTP	USER	HACKER	ADMIN
Software Discovery Attack by PowerShell	T1518			
Software Discovery Attack by Malicious Executable	T1204.002			
Malicious .CPL file by Control Panel (control.exe)	T1218.002			
Signed Binary Proxy Execution by regsvr32.exe	T1218.010			
Malicious .LNK file by .ISO Image Mounting	T1204.003			
Data Theft via Telegram API	T1059.003			
Data Theft via Malicious File Execution	T1048			
Malicious Macro in Word & Metasploit	T1105			
Psexec & Launching Malware via certutil.exe	T1570			
Clearing the history of PowerShell commands by Malicious File	T1070.003			



1

T1518 - Software Discovery

In the initial phase of the attack, cybercriminals may try to obtain a list of installed software or system configuration to proceed to the next step. To extract basic information from the attacked host, we used a PowerShell command.

2

T1204.002 - Software Discovery

In this method, we used a script containing a similar command as in the first scenario. In theory, we obtained the same output, but in practice, the attack can be interpreted differently by the tested solution in the administrator console.

3

T1218.002 - Signed Binary Proxy Execution: Control Panel

To run a potentially dangerous file, we used the trusted application control.exe (Windows Control Panel) with a parameter to a file with the .CPL extension which allows to automatically run the code along with the control panel. Although in the attack the calculator calc.exe has been launched, in a real scenario it could be any malicious software.

4

T1218.010 - Signed Binary Proxy Execution: Regsvr32

To execute code from DLL in Windows, we need a process that will run a file. We used the system Regsvr32.exe tool as a proxy which is a popular method of loading a DLL file into memory.

5

T1204.003 - User Execution: Malicious Image

We used the technique of downloading an image file, and mounting it as an additional drive in the system. This is one way to bypass anti-spam and anti-malware protections on servers of email providers. Moreover, it is possible to bypass system security by removing the Mark-of-the-Web attribute for a file – this can make it difficult for security software to analyze a file.

**6**

T1059.003 – Data Theft via Telegram API

We used the Telegram API as a non-standard method of stealing files from the targeted machine. The stolen file was sent to a Telegram bot controlled by an attacker using the HTTP POST method. In a real-life scenario, a command that uses the Telegram API can be integrated with any malware. Telegram application does not need to be installed on the victim's system.

7

T1048 - Data Theft via Malicious File Execution

We used the same command for stealing files from the attacked host, but compiled into an executable file (EXE). The file can be delivered to the victim's system in various ways.

8

T1105 - Malicious Macro in Word & Metasploit

Using Word documents in social engineering attacks is a very old technique. However, the methods of embedding malicious code are evolving. The prepared macro uses a popular method of downloading a file from a remote location, and runs the file without interacting with the victim. In this scenario, there can be many techniques and tactics according to MITRE.

9

T1570 - PsExec & Launching Malware via certutil.exe

Once again we use legitimate software to run malicious code. This time it is PsExec which is part of SysInternals. We used it to remotely log into the attacked host, download a file from a remote location using the certutil.exe file, and execute malware in the system from the command line.

10

T1070.003 - Clearing the history of PowerShell commands by Malicious File

In this scenario, we used the Caldera tool to install remote access malware, then we tried to clear the PowerShell command history.

Test conclusions and general recommendations

In this year's edition of the test, we tested the ability of products to quickly alert, correctly detect attacks, and create a chain of suspicious events. Please note that some simulated attacks have already been well documented, and are known to developers and the community of experts. Nevertheless, the test reflects the protective capabilities of security products against targeted and long-lasting APT attacks.

The test evaluated several EDR-XDR solution leaders, including considering possible product vulnerabilities in a simulated environment. The test allowed to learn more about software of this class:



Each product has its advantages and disadvantages, so its value is determined by the conscious choice of the organization that uses the solution on a daily basis, and has learned about its strengths and weaknesses.



Without EDR-XDR modules, some attacks can be completely undetectable by anti-malware software. The lack of any telemetry can indicate to the security team that there is no information about an incident. And this is an open way to a partial or complete breach of the organization's security.



An attack usually starts with one computer in an organization or a group of computers on the same subnet, and can stay unnoticed for many weeks – this is known as the attack planning cycle. Thanks to products of this class, organizations can recognize warning signals faster, and respond to alerts to avoid falling victim to hackers.



EDR-XDR should not send false positives to analysts, so a high number of alerts is not always advisable. Collecting such data is good if security is handled by a dedicated group of experts. Detailed telemetry coverage of attacks can tell a lot about the product, but this approach will not work where there is a competence gap.



For the same reason as telemetry, attack information can be frustrating for administrators if it is not accurate. Attacks can be divided into, for example: opening a malicious file in the network, accessing an application or resource using unprotected credentials, logging in using the RDP protocol, etc. Without proper visibility of attacks, the security team will be ineffective.



Alerts in the admin panel can depend greatly on policy settings. For example, low-risk events (on a scale of 0 to 10) may not generate a warning alert when running a file from the %TEMP% directory to avoid driving analysts crazy. The lack of alert is not a bad thing, unlike the lack of telemetry from an attack.



Telemetry is a very important piece of information because it can be used by analysts to search for unknown malware or create rules based on events recorded by the agent, so that it becomes possible to adjust the product to the needs of the organization.



Telemetry generates a lot of information. They are usually sorted by time, related to processes in the form of trees and graphs. The most important thing is to know what to look for, and learn how to read the logs. In most solutions it is done similarly, the logs differ in the record structure, but the general principle is similar.



Some EDR-XDR solutions integrate with VirusTotal which allows to quickly search the Internet for the checksum of a suspicious file. They also offer file analysis in the so-called sandbox or manual analysis by a qualified team of the developer. It is worth using an additional opinion about the threat, if such a service is provided free of charge.



It is helpful to use recommendations regarding incorrect system settings or lack of operating system updates, as those reduce the level of security.



When considering the implementation of a given solution, make sure that systems other than Windows are supported, if necessary.



Cybercriminals use legitimate and trusted software, as well as built-in Windows components, to hide malicious activity. Living off the Land Binaries (LOLBins) files are crucial for the proper functioning of the operating system. During a cyberattack, it can be difficult or even impossible to block them which makes them very attractive to malware developers. For this reason, attack telemetry and the threat hunting module are often necessary to obtain information about events.



Fundacja AVLab dla Cyberbezpieczeństwa as an independent organization, we are committed to protecting your privacy and security online. We build user awareness of digital protection. We issue opinions, technical analyses and tests of IT solutions in the field of cybersecurity. We also have a security blog where we post articles about IT security news, vulnerabilities and IT solutions.

We conduct regular tests of various protection programs and publish the results on our website. These tests cover a wide range of malware samples, including both known and unknown threats, and evaluate each software effectiveness in detecting and removing them. This helps users compare the effectiveness of different security programs and make an informed decision when choosing a PC protection solution.

Our strongest asset is insightful and detailed reviews, preparation of reports related to privacy and protection of end devices, and in particular security tests, thanks to which we are recognized all over the world as one of the most popular testing laboratories.

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

