



Overview of protection of EDR-XDR solutions

Simulation of offensive security tests
including the visibility of attacks in telemetry

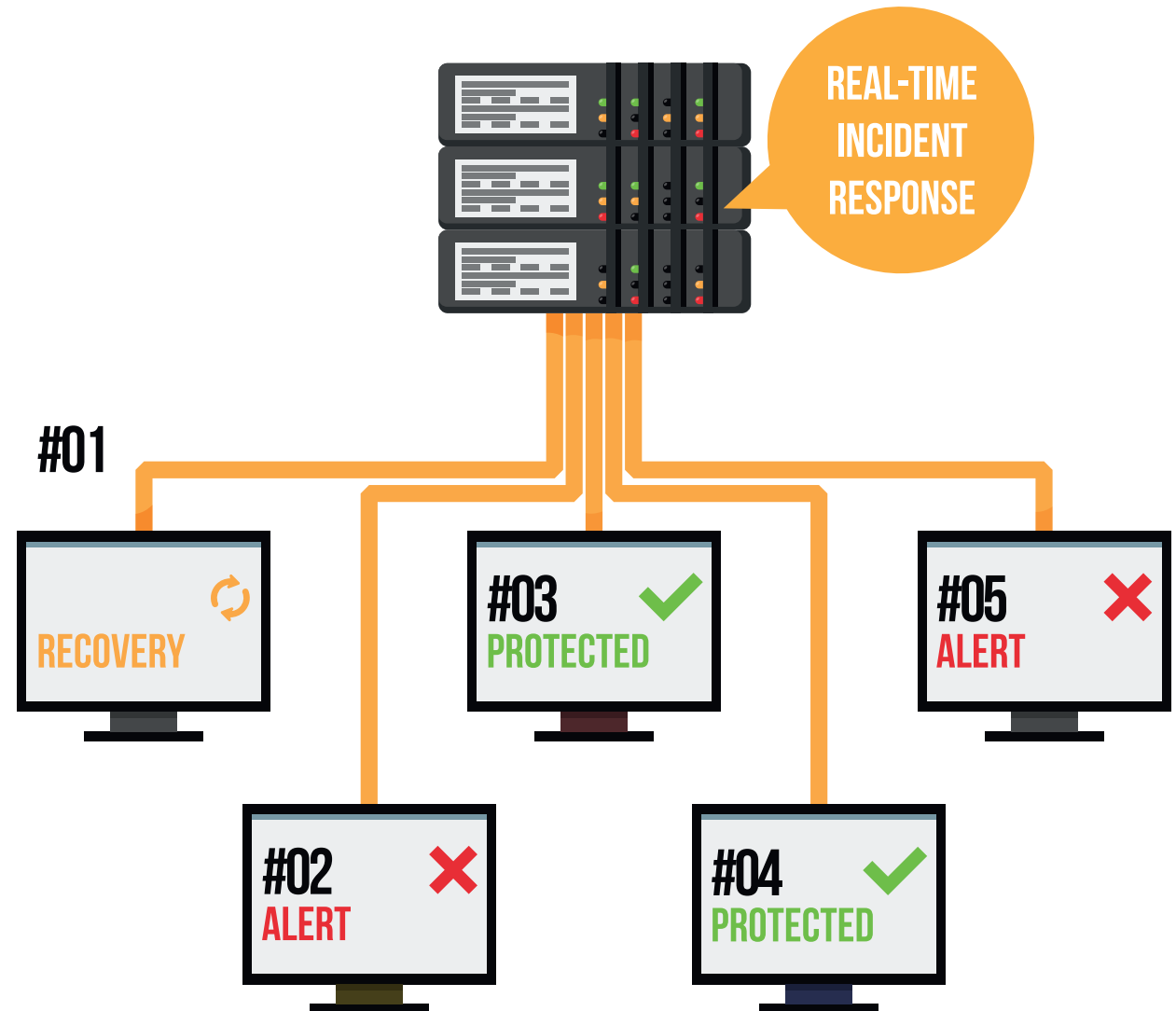
Table of contents

I	Introduction to the test
II	Features of a good EDR-XDR
III	How did we choose the software for the test?
IV	Victim and agent system configuration
V	Comparison of EDR-XDR security features
VI	Results based on simulated attacks
VII	Comparison of developer's results
VIII	Description of simulated attacks
IX	Description of the tools used in the test
X	Conclusions and recommendations
XI	General advices and recommendations
XII	Recommendation cloud

Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) solutions are derived from multi-layered endpoint protection. Their role is to monitor the supported operating systems and applications in the cloud in real time.

They take proactive searching for threats to the next level, including IoC (Indicator of Compromise) artifacts. This may mean that your company will receive more useful feedback from endpoints which will help you better protect the entire network and employees against cyberattacks. Using EDR-XDR improves visibility of information flow from the entire infrastructure.

An insight into Telemetry includes not only endpoints, but also Amazon Web Service, Microsoft Azure, mobile devices, IoT sensors, Web 2.0 applications, and even network edge devices.



EDR-XDR as an ally of Red-Blue Team

In order to compare EDR-XDR solutions, we temporarily step into the shoes of the Red Team, i.e. simulate actions of attackers who already have access to the IT infrastructure, and thus the opportunity to steal data from workstations, and ultimately as defenders of the Blue Team develop conclusions for a better understanding of how EDR-XDR solutions work. The purpose of this test is to justify the investment in a product for active and passive protection of systems by assessing its capabilities in confrontation with targeted APT (Advanced Persistent Threat) attacks.

Tools and protocols we used

We wanted to diversify the ways of bypassing security so we tried to use several network protocols and different tools. For example, in one scenario we use the Telegram API (MTPROTO Mobile Protocol) to try to silently send selected files from a victim's computer to another Telegram account which is controlled by an attacker. According to the MITRE Techniques & Tactics [1], in real attacks on enterprises hackers use system tools such as PowerShell, CMD, MSHTA, WMI, and others which should be covered by the software for monitoring data and information. Threats we use in the test were additionally subjected to the process of obfuscation of malware code. Moreover, we used the Caldera Framework formerly known from the online banking test to obtain basic information about the victim's system. We also used the offensive Metasploit software to check the visibility of attacks in the admin console.

Telemetry and visibility of attacks in the admin console

This is the first edition of the EDR-XDR test so our primary goal was to check the logging of attack traces in the admin console. Some of the attacks will be easy to detect, such as the payload generated in Metasploit software with a reverse TCP connection established immediately after a victim runs a malicious file. **Checking the effectiveness of protection was not even a secondary goal of the test so we focused all our attention on observing the visibility of attacks along with telemetry (the so-called alert attack context). The lack of visibility or telemetry can mean for your company that the product did not work in a real-life situation or detected the threat too late.** This could lead to encrypting a part of the infrastructure before the security agent manages to stop the escalation of a cyberattack on the workstation. In addition, thanks to automation, EDR-XDR is an effective tool for large and small organizations with any level of technical skill.

[1] <https://attack.mitre.org>

Features of a good EDR-XDR

This class of solution must provide multi-layered protection – from supporting a variety of systems to network processes, services and protocols. At the same time, it should be easy to use. We made the following assumptions that guided us in the test:

A

It is important to automatically detect threats as well as fixing issue with malicious software, including an agent and operating system misconfiguration, to quickly and easily support small and medium-sized organizations in the security process.

B

Effective management and visibility of the entire attack chain is an important feature of the product that makes it easier to view events of preventive protection as well as adaptive detection of suspicious activity along with automatic response to incidents.

C

Advanced search for telemetry artifacts must enable identification and remediation of potential issues with security of the organization before the attacker gets what he has planned. That is why EDR-XDR solution must provide detailed visibility of the attack, and quick and easy access to telemetry data in order to assist analysts in detecting threats.

D

An important feature is to avoid "alert spam" by providing the necessary to detect artifacts during suspicious activity. This point can be met by automatically neutralizing cyberattacks without human intervention.

E

EDR-XDR consists of the entire ecosystem of security modules cooperating with each other so in the test we avoid disabling some protection as the goal of EDR-XDR solutions is to detect and stop increasingly complex attacks.

F

Regardless of the operating system, the solution should provide an immediate identification of events from all endpoints using a single dashboard. The so-called holistic view of infected IT resources allows to respond quickly and neutralize any type of attack.



How did we choose the software for the test?

We have taken into account developers of those EDR-XDR solutions which we have easy access to due to previous cooperation in other tests. Generating test accounts and contacting a developer sometimes takes weeks, and because of the 30-day trial version of a product it would be impossible to complete the test. We do not exclude that in next editions we will take into account other solutions. Developers willing to cooperate are invited to contact us.



Bitdefender GravityZone Business
Security Enterprise with XDR



Emsisoft Enterprise Security
with EDR



Microsoft Defender
for Endpoint with EDR



Trend Micro Apex One + Trend
Micro Vision One with XDR



Xcitium Advanced Endpoint
Protection with EDR



Vendor
Private Test

Sophos and ESET refused to participate in the test.

Victim and agent system configuration



Virtual machines with Windows 11 and Windows Server 2019 with agents of the tested solutions were connected to the same network and had full access to the Internet. We used a completely default configuration of Windows.



To simulate attacks we used a virtual machine with Linux Mint as a Command and Control server with the Caldera Framework (with predefined attack types), and a virtual machine with Kali Linux and Metasploit software.



We gave up creating campaigns from scratch. The so-called payload was delivered by the described protocols without any social engineering because the type and purpose of the attack in the simulated scenario was known to testers.

Policy configuration for antivirus agents was the default or included additional settings for more detailed telemetry. We did not disable antivirus protection. In the case of solutions which had to have a predefined policy configuration assigned, e.g. Microsoft Defender for Endpoint, we wanted to assign the best possible protection to have detailed insight into the information on the attack chain and maximum telemetry which was the purpose of our test.



Test preparation schedule

- ▶ Methodology preparation: 3 weeks
- ▶ Start of the test: 3rd November 2022
- ▶ End of the test: 20th December
- ▶ Contact with developers and preparing the report: 40 days.



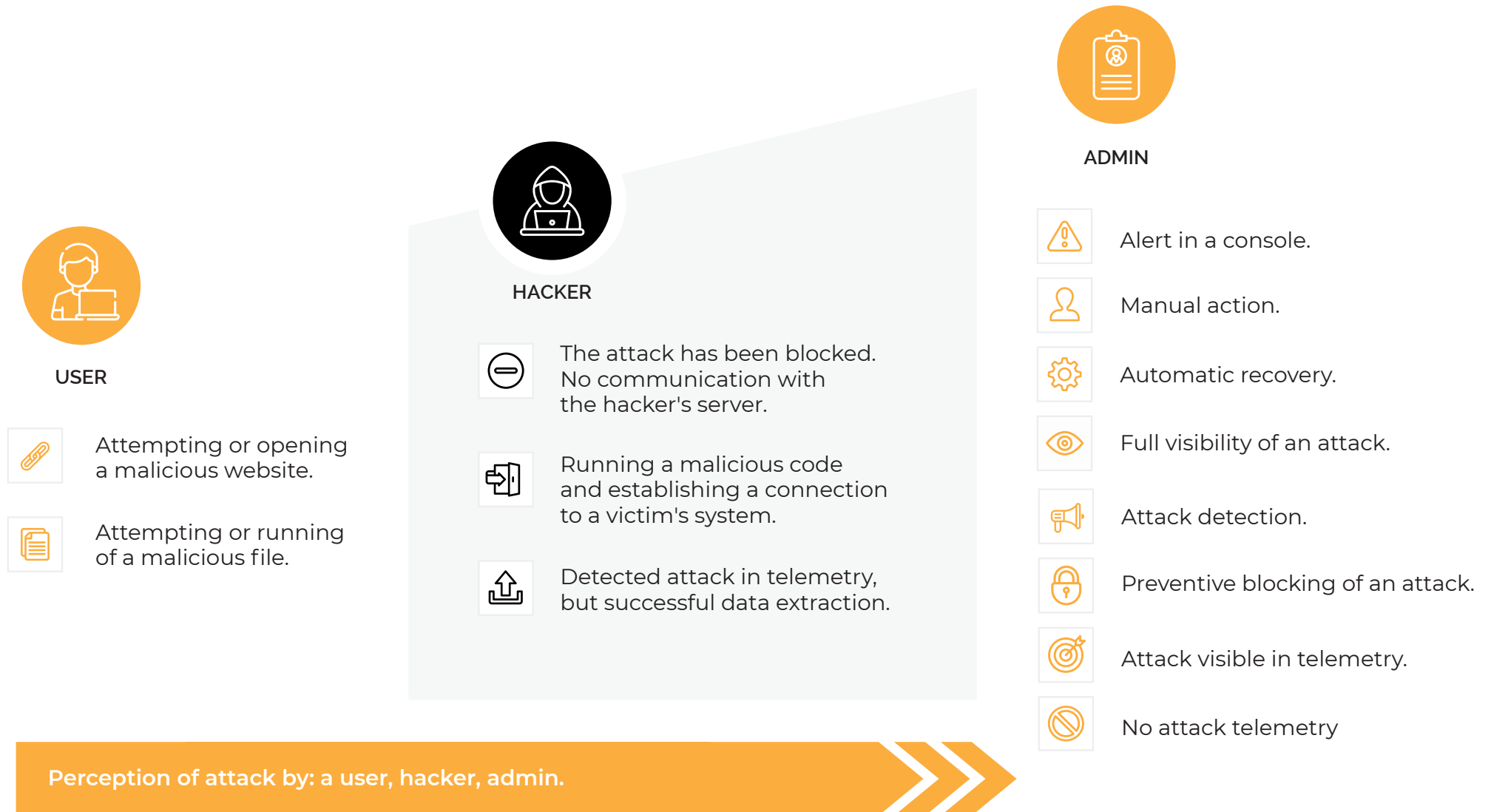
Comparison of EDR-XDR security features

	Bitdefender GravityZone Business Security Enterprise	Emsisoft Enterprise Security	Vendor Private Test	Microsoft Defender for Endpoint	Trend Micro Vision One	Xcitium Advanced Endpoint Protection
Attack visibility	✓	✓	✓	✓	✓	✓
Attack visualization	✓	✓	✓	✓	✓	✓
Attack telemetry	✓	✓	✓	✓	✓	✓
File reputation	✓	✓	✗	✓	✓	✓
Advanced search for attack indicators	✓	✓	✓	✓	✓	✓
Security risk assessment (e.g. vulnerabilities in systems, weak passwords, agent misconfiguration)	✓	✗	✓	✓	✓	✓
Suspicious lists of objects (IP, URL, SHA)	✓	✓	✓	✓	✓	✓
Proposed recovery measures after attack	✓	✓	✓	✓	✗	✗
Additional opinion on threat (sandbox, VirusTotal, file reputation, others)	✓	✓	✓	✓	✓	✓
Isolation of workstation, usage, file	✓	✓	✓	✓	✓	✓
Update management	✓	✗	✓	✓	✓	✓
Restoring data after attack (user files)	✓	✗	✓	✓ *	✓	✓
Secure login to admin panel	✓	✓	✓	✓	✓	✓
Third-party technologies	Bitdefender	Emsisoft, Bitdefender	Vendor - Private	Microsoft	Trend Micro	Xcitium

* Some ransomware also encrypt or delete backups, so Windows Files History may not be a sufficient security. It is important to create backups on external drive or devices that have not been affected by ransomware.

Results based on simulated attacks

The main purpose of the test was to check the visibility attacks in the console of EDR-XDR solution against simulated network activities that should be intercepted by the agent installed on the workstation.

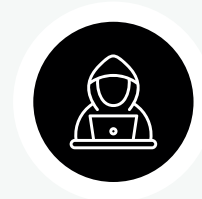


Bitdefender®

GravityZone Business Security Enterprise with XDR



USER



HACKER



ADMIN

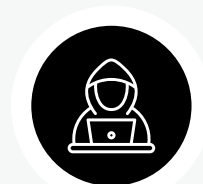
Fake .CPL file of control panel	T1218.002	 	  	       
Microsoft Windows regsvr32.exe	T1218.010	 	  	       
Malicious .ISO file	T1608.005	 	  	       
SVCReady threat	T1204.002	 	  	       
Malicious .HTA file (Metasploit)	T1218.005	 	  	       
Data theft via Telegram API	T1059.003	 	  	       
Ransomware from network drive	T1204.002	 	  	       
Ransomware with SFTP	T1105	 	  	       
Data exfiltration (Caldera)	T1560.001	 	  	       
Adding entry to Task Manager (Caldera)	T1053.005	 	  	       

EMSI

Enterprise Security with EDR



USER



HACKER



ADMIN



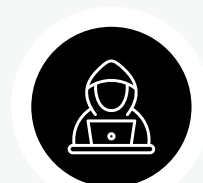
Fake .CPL file of control panel	T1218.002	 	  	       
Microsoft Windows regsvr32.exe	T1218.010	 	  	       
Malicious .ISO file	T1608.005	 	  	       
SVCReady threat	T1204.002	 	  	       
Malicious .HTA file (Metasploit)	T1218.005	 	  	       
Data theft via Telegram API	T1059.003	 	  	       
Ransomware from network drive	T1204.002	 	  	       
Ransomware with SFTP	T1105	 	  	       
Data exfiltration (Caldera)	T1560.001	 	  	       
Adding entry to Task Manager (Caldera)	T1053.005	 	  	       



Vendor - Private Test



USER



HACKER



ADMIN



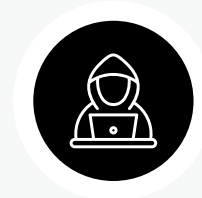
Fake .CPL file of control panel	T1218.002	 	  	       
Microsoft Windows regsvr32.exe	T1218.010	 	  	       
Malicious .ISO file	T1608.005	 	  	       
SVCReady threat	T1204.002	 	  	       
Malicious .HTA file (Metasploit)	T1218.005	 	  	       
Data theft via Telegram API	T1059.003	 	  	       
Ransomware from network drive	T1204.002	 	  	       
Ransomware with SFTP	T1105	 	  	       
Data exfiltration (Caldera)	T1560.001	 	  	       
Adding entry to Task Manager (Caldera)	T1053.005	 	  	       



Microsoft Defender for Endpoint with EDR



USER



HACKER



ADMIN



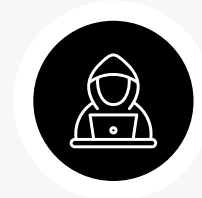
Fake .CPL file of control panel	T1218.002	 	  	       
Microsoft Windows regsvr32.exe	T1218.010	 	  	       
Malicious .ISO file	T1608.005	 	  	       
SVCReady threat	T1204.002	 	  	       
Malicious .HTA file (Metasploit)	T1218.005	 	  	       
Data theft via Telegram API	T1059.003	 	  	       
Ransomware from network drive	T1204.002	 	  	       
Ransomware with SFTP	T1105	 	  	       
Data exfiltration (Caldera)	T1560.001	 	  	       
Adding entry to Task Manager (Caldera)	T1053.005	 	  	       



Advanced Endpoint Protection with EDR



USER



HACKER



ADMIN



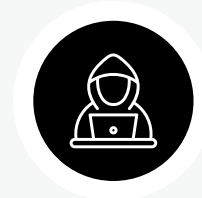
Fake .CPL file of control panel	T1218.002	 	  	       
Microsoft Windows regsvr32.exe	T1218.010	 	  	       
Malicious .ISO file	T1608.005	 	  	       
SVCReady threat	T1204.002	 	  	       
Malicious .HTA file (Metasploit)	T1218.005	 	  	       
Data theft via Telegram API	T1059.003	 	  	       
Ransomware from network drive	T1204.002	 	  	       
Ransomware with SFTP	T1105	 	  	       
Data exfiltration (Caldera)	T1560.001	 	  	       
Adding entry to Task Manager (Caldera)	T1053.005	 	  	       



Trend Micro Apex One + Trend Micro Vision One with XDR



USER



HACKER



ADMIN



Fake .CPL file of control panel	T1218.002	 	  	       
Microsoft Windows regsvr32.exe	T1218.010	 	  	       
Malicious .ISO file	T1608.005	 	  	       
SVCReady threat	T1204.002	 	  	       
Malicious .HTA file (Metasploit)	T1218.005	 	  	       
Data theft via Telegram API	T1059.003	 	  	       
Ransomware from network drive	T1204.002	 	  	       
Ransomware with SFTP	T1105	 	  	       
Data exfiltration (Caldera)	T1560.001	 	  	       
Adding entry to Task Manager (Caldera)	T1053.005	 	  	       

Comparison of developer's results

The final verdict on blocking an attack at the early or late level of detection and telemetry.

PRE

The **PRE-Launch level** applies to detecting malware samples before they are launched in the system.

POST

The **POST-Launch level** applies to concern the analysis when a virus has been launched and blocked by tested products.

FAIL

the failure, i.e. a virus hasn't been blocked and no telemetry.

	MITRE techniques	Bitdefender	Emsisoft	Vendor - Private	Microsoft	Trend Micro	Xcitium
1. Fake .CPL file of control panel	T1218.002	PRE	PRE	PRE	POST	POST	POST
2. Microsoft Windows regsvr32.exe	T1218.010	POST	POST	PRE	POST	PRE	PRE
3. Malicious .ISO file	T1608.005	PRE	PRE	POST	PRE	POST	PRE
4. SVCReady threat	T1204.002	PRE	POST	POST	PRE	PRE	PRE
5. Malicious .HTA file (Metasploit)	T1218.005	PRE	PRE	POST	PRE	POST	PRE
6. Data theft via Telegram API	T1059.003	FAIL	POST	POST	POST	POST	POST
7. Ransomware from network drive	T1204.002	PRE	PRE	POST	PRE	PRE	PRE
8. Ransomware with SFTP	T1105	PRE	PRE	POST	PRE	PRE	PRE
9. Data exfiltration (Caldera)	T1560.001	PRE	POST	PRE	POST	POST	PRE
10. Adding entry to Task Manager (Caldera)	T1053.005	PRE	POST	PRE	POST	POST	PRE

Description of simulated attacks

We have used the following threats carry out an experiment on the visibility of attacks registered in the administrator console:

1

Fake .CPL file of control panel

ATT&CK v12: T1218.002

In order run a potentially dangerous file, we have used a legitimate control.exe application (Windows Control Panel) with a parameter to a file with the .CPL extension which can be automatically run along with the control panel. The calc.exe calculator has been launched in the attack. In a real scenario of cyberattack it could be any malware.

Credentials:

<https://kapitanhack.pl/2020/07/02/nieskategoryzowane/jak-mozna-uruchomic-malware-wykorzystujac-backdoor-w-panelu-sterowania-windows/>

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.002/T1218.002.md#atomic-test-1---control-panel-items>

T1218.002: <https://attack.mitre.org/techniques/T1218/002/>

2

Activating the malicious DLL in Regsvr32.exe

ATT&CK v12: T1218.010

This is the easiest way to load a DLL file. An attacker can use the system tool Regsvr32.exe as a proxy to run malicious code. In theory, using the legitimate regsvr32.exe file with a digital signature from Microsoft, security solution can be tricked.

Credentials:

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.010/T1218.010.md#atomic-test-3---regsvr32-local-dll-execution>

<https://attack.mitre.org/techniques/T1218/010/>

3

Malicious .ISO file

ATT&CK v12: T1608.005

Social engineering attacks using legitimate cloud services for storing and sharing files have become popular. We have used the popular service Mega to privately share an .ISO file. This type of extension and .IMG are used by cybercriminals to send scam messages. This is one of the ways to bypass antispam and antimalware security on email provider servers.

In this way it is possible to bypass system security in the form of the Mark-of-the-Web attribute. This is a security feature that adds Zone.Identifier.* metadata to executable files with a specified value when downloaded from the Internet. MOTW works with the Microsoft SmartScreen technology so tricking the MOTW tag (indicating that a file comes from the Internet) also allows to partially trick the Windows security by using the .ISO, .IMG, .ZIP, and .RAR files. During normal use of a computer the file image is mounted as a driver in which the target malware usually can be found.

Credentials:

<https://attack.mitre.org/techniques/T1608/005/>

4

SVCReady threat

ATT&CK v12: T1204.002

At the beginning of the second quarter of 2022, the SVCReady malware family was distinguished by an unconventional shellcode hidden in the properties of a Microsoft Word document. This type of malware is designed primarily as a downloader for downloading secondary malware after collecting information about the victim's infected system.

Credentials:

<https://threatresearch.ext.hp.com/svcready-a-new-loader-reveals-itself/>

<https://attack.mitre.org/techniques/T1204/002/>

5

Malicious .HTA

ATT&CK v12: T1218.005

.HTA files are used as malware in online attacks. From the point of view of protectors and attackers this is a known attack vector used with the system application mshta.exe – a Windows tool for running Microsoft HTML (HTA), JavaScript, or Visual HTML files. Theoretically, a .HTA file can trick antiviruses, but only to a basic extent.

Credentials:

<https://attack.mitre.org/techniques/T1218/005/>

6

File theft via Telegram API

ATT&CK v12: T1059.003

The Telegram API has been used as a non-standard method of stealing files from the attacked machine. CURL has been run from the command prompt (cmd.exe). The stolen file has been sent to the Telegram bot controlled by the attacker using the POST method. In a real-world scenario a command using the Telegram API can be integrated with any malware without installing Telegram on the victim's system.

Credentials:

<https://core.telegram.org/bots/api#senddocument>

<https://attack.mitre.org/techniques/T1059/003/>

7

Ransomware from network drive

ATT&CK v12: T1204.002

In this scenario we have placed ransomware on a share driver in the form of an application installer waiting for a user to run it.

Credentials:

<https://attack.mitre.org/techniques/T1204/002/>

8

Ransomware from SFTP

ATT&CK v12: T1105

As in the previous point, we have used ransomware saved on a remote server among various types of files that have been downloaded to the victim's system via SFTP, and launched.

Credentials:

<https://attack.mitre.org/techniques/T1105/>

9

Data exfiltration

ATT&CK v12: T1560.001

We have used the Caldera Framework to deliver a malicious payload designed to compress the indicated directories into a single ZIP file, and send it to the attacker's server.

Credentials:

<https://attack.mitre.org/techniques/T1560/001/>

10

Launching malware from task scheduler

ATT&CK v12: T1053.005

Similarly, we have used the Caldera Framework so that malware could be added to the task manager and ran at a scheduled time.

Credentials:

<https://attack.mitre.org/techniques/T1053/005/>

Description of the tools used in the test

Client-server software called Caldera can be used to test endpoint security and to assess the security state of an organization. It will be helpful for Blue and Purple Teams to anticipate some known ways to bypass security. The broad capabilities of the framework allow to check the effectiveness of protection solutions, taking into account specific modules, e.g. protection against file encryption, blocking malicious connections by a firewall, protection against zero-day attacks, reporting suspicious activity using EDR agents on workstations, and much more. The framework emulates ATP attacks of various groups of hackers. It contains configured tactics and techniques that can be run on an infected Windows, Mac, and Linux device.

The Metasploit Framework is one of those tools for security testing, the popularity of which has led to facilitating tedious work of experts during authorized security tests.

In this experiment, we have used several known methods to generate a malicious file and deliver it to the victim's system, but skipping social engineering. Please note that such tools are known to security solution providers. As reports from the revealed incidents show, cybercriminals do not give up using a ready-made tool that is Metasploit.

In subsequent editions, we do not exclude the use of other tools, e.g. Atomic Red Team or Mordor that coincide with the numerous tactics of MITRE, and will allow to check if the EDR agent records telemetry including what malicious activity looks like in systems. These tools are helpful because they show how the product deals with potential attacks, and how it solves security issues with systems and user accounts.



In this year edition of the EDR-XDR solutions test we tested the ability of products to quickly alert, correctly detect attacks, and create a chain of connections. Security software has been confronted with numerous techniques used by hackers.

Please note that the simulated attacks have been previously documented, so the test reflects the protective capabilities of security products against targeted and long-term APT attacks.

Businesses have plenty to choose from. The availability of numerous solutions will be quite challenging for CISO, as it is necessary to make a conscious decision when choosing the right product to protect an organization and employees. The test has evaluated several market leaders of EDR-XDR solutions, including possible vulnerabilities of products in a simulated environment.

The test allowed to learn more about this class of software:



Each product has its advantages and disadvantages which is why its value is a conscious choice of the organization that uses the solution in its environment on a daily basis and has learned its strengths and weaknesses.



EDR-XDR software can report a larger number of general alerts, and this may cause the analyst to be spammed with false positives so a high number of alerts is not always recommended. Collection of such data is good if a dedicated group of experts handles the security of the organization. Detailed telemetry coverage of attacks can provide a lot of information about EDR-XDR, but this approach will not work for a small or inexperienced IT team.



For the same reason as telemetry, information about attacks can be frustrating for IT administrators if it is not accurate. By the visibility of an attack, we mean that attacks can be classified into: opening a malicious file on a network, accessing an application or resource using insecure credentials, logging in using RDP, etc.



An attack usually begins at a single computer in an organization or a group of computers on the same subnet, and can remain unnoticed there for weeks – this is an attack planning cycle. Organizations need to recognize warning signs and respond to alerts faster to avoid falling victim to hackers. It is thus obvious that is better to stop an incident at the beginning of its chain than to implement remediation measures (backups). Without good visibility of attacks, the security team will simply be ineffective.



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



Telemetry is very important information because analysts can use it to search for unknown malware, or create rules based on events logged by an agent, so they can better tailor the product to the needs of the organization.



Telemetry generates a lot of information. They are usually sorted by time, connected 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 logs. In most solutions it is implemented similarly, logs differ on the record structure, but the general principle is similar.



Some EDR-XDR solutions integrate with VirusTotal, so that they allow to quickly search Internet resources for a checksum of a suspicious file, also offering file analysis in the so-called sandbox. It is worth using an additional feedback on a threat.



It will be helpful to use the recommendation proposed in the administrator console regarding incorrect system settings or the lack of operating system updates, as it may reduce the level of security.



Threats detection with EDR-XDR solutions is playing an increasingly important role in an organization's holistic approach to security. The do-called “threat hunting” goes beyond the known spectrum of threats and also analyzes unknown events.



Some EDR-XDR systems do not support other than Windows. Therefore, every company must consider whether it needs to cover all systems with a more expensive solution, and if so, perhaps a SIEM solution will be better.



General advices and recommendations

Building a company's security policy requires knowing your own needs and taking steps to implement it. Here are 3 recommendations resulting from the test, that everyone should consider to start implementing more effective security.

1

The original Zero Trust protection model is based on the principle that organizations do not trust anything outside or inside their network. Access is granted only to authorized users, devices, and data packages, only after trust has been built and a level of threat prevention has been established – without affecting the user experience. The coming years will bring a significant increase in the popularity of this approach.

2

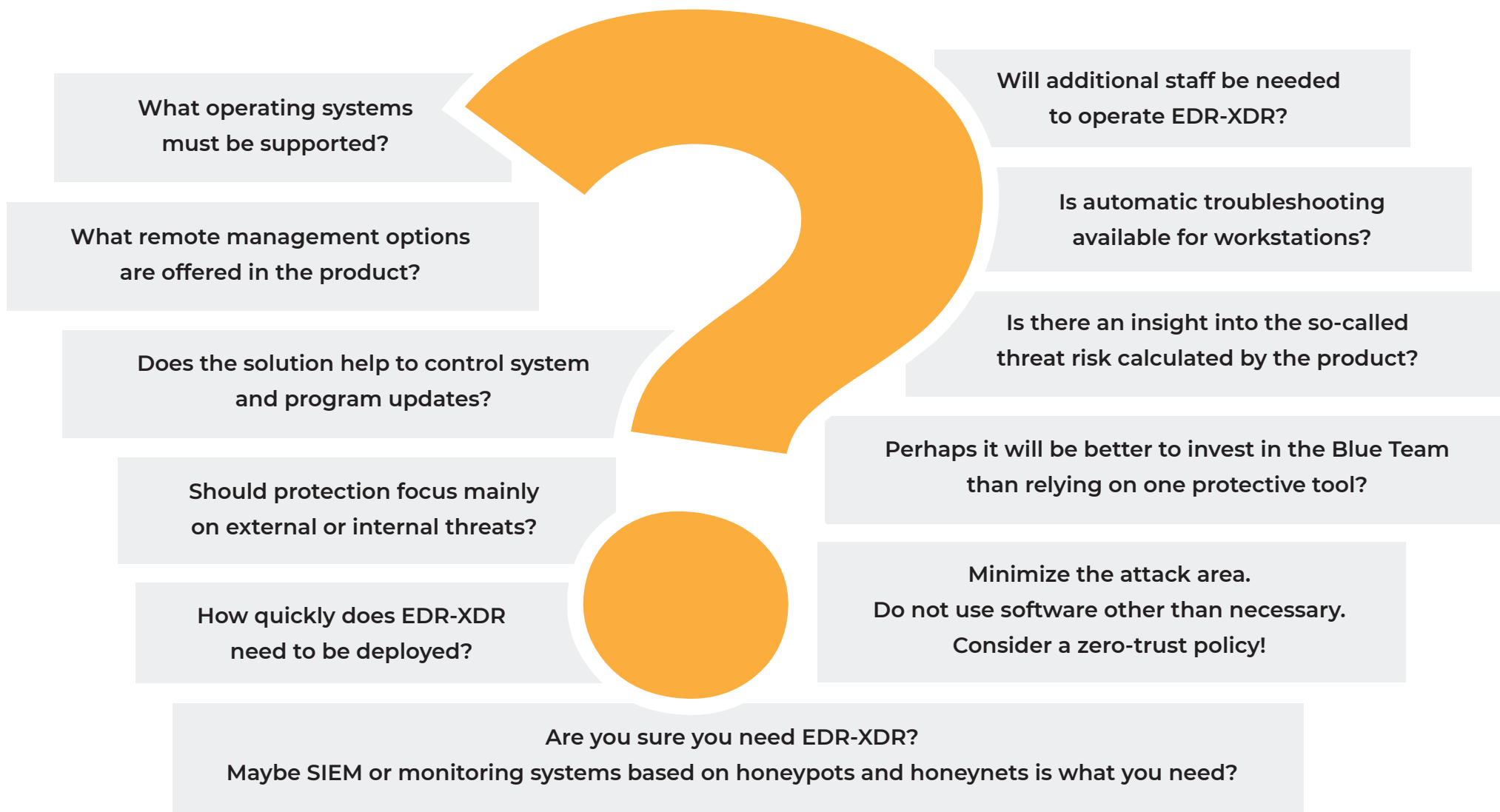
The enemy can attack from the inside, as an employee who has a lot of knowledge about the organization, the structure of data distribution and the applicable security rules. He may also have improper permissions in systems. Therefore, it is reasonable to invest in a comprehensive solution with a DLP module that monitors what an employee can send to the Internet using an encrypted protocol or export using an external storage.

3

PowerShell is a very powerful tool in the hands of an admin and a hacker. It is rarely used by an accountant or user. It is Powershell that allows to remotely manage machines in a larger organization, but also gives almost unlimited possibilities to a hacker. In standard situations, cybercriminals use about 50 of the most executable commands in Powershell, so deactivating Powershell on employee's computers is a good method that prevents from running potentially harmful scripts and files.

Recommendation cloud

When choosing a security solution, companies can be guided by the following criteria:





As an independent organization we are committed to protect privacy and security on the Internet. 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 cyber security. Our strongest asset are 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 popular testing laboratories..

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