



BEZPEČNOSTNÍ IT EXPERTI
NA VAŠEJ STRANĚ

Ochrana pred pokročilými hrozbami a súvisiace služby



Július Selecký

Senior Technical Pre-Sales Representative

julius.selecky@eset.com



20. októbra 2020 15:24 [Hakeri a kyberbezpečnosť](#) [Ruskí špióni](#)

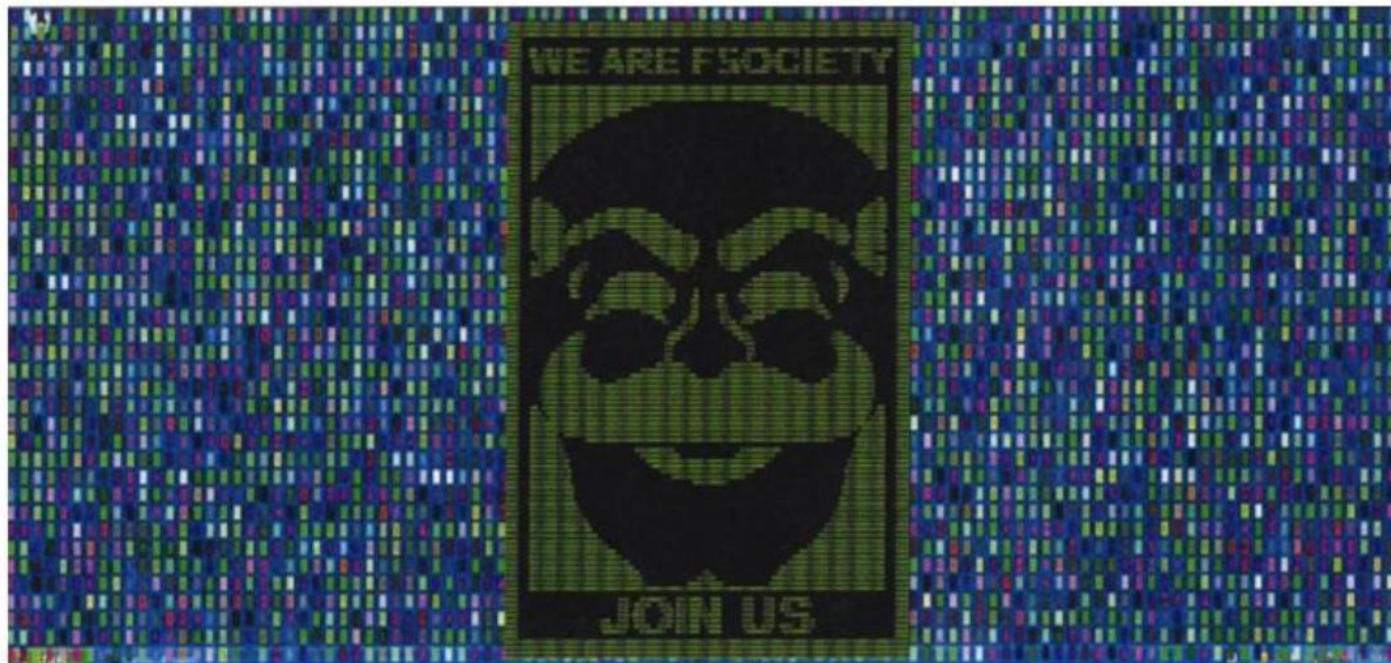
Útočili ako zo sci-fi knihy: vypli elektrinu, zasiahli voľby aj olympiádu. Ruskí hekeri z jednotky 74455



MIREK TÓDA



Zapnúť články e-mailom



Hakeri z ruskej rozviedky GRU sa ukázali ako fanúšikovia seriálu Mr. Robot. Pri útokoch použili obrázok masky fsociety – fiktívnej anarchistickej hekerskej skupiny. Foto – americké ministerstvo spravodlivosti

Prehľad najdesivejších útokov obáwanej hekerskej skupiny z Moskvy.

welivesecurity™ BY **eset**

Lazarus supply-chain attack in South Korea

How the Lazarus supply-chain attack leveraging WIZVERA VeraPort

welivesecurity™ BY **eset**

Operation NightScout: Supply-chain attack targets online gaming in

cyberespionage operation targeting

welivesecurity™ BY **eset**

Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia

ESET researchers have uncovered a supply-chain attack on the website of a government in Southeast Asia.



Ignacio Sanmillan



Matthieu Fauriol

welivesecurity™ BY **eset**

Operation StealthyTrident: corporate software under attack

LuckyMouse, TA428, HyperBro, Tmanger and ShadowPad linked in Mongolian supply-chain attack



Mathieu Tartare



Čo s tým?





Recycle Bin



Microsoft
Edge



ENDPOINT SECURITY

Threat removed

A threat (**Eicar**) was found in a [file](#) that **Notepad** tried to access.

The file has been deleted.

[Learn more about this message](#)

Čo je EDR?

Čo sa deje?

Ako sa to začalo?

Kde sa to začalo?

Kedy sa to začalo?

Čo to obsahuje?

Ako tomu vieme predísť?

Asi ide o kybernetický útok.

Nie sme si istí.

Nie sme si istí.

Nie sme si istí.

Nie sme si istí.

Nie sme si istí.

EDR Vám umožňuje
odpovedať na tieto otázky

Čo robí ESET EDR technológia?

- Priebežne monitoruje všetky aktivity na **ESET Endpoint**
- Analyzuje systémové aktivity
- Deteguje potenciálne hrozby a problémy so zabezpečením
- Upozorňuje administrátorov systému
- Upozorňuje na nápravné opatrenia
- Udržiava históriu aktivít na koncových bodoch - Threat Hunting

Ktoré lokálne aktivity sú monitorované?

- Veľmi dlhý zoznam
- Dôležité:
 - PowerShell
 - WMI
 - Komunikácia s externými servermi
 - DNS Requests
 - Brute-Force a Pass-The-Hash útoky

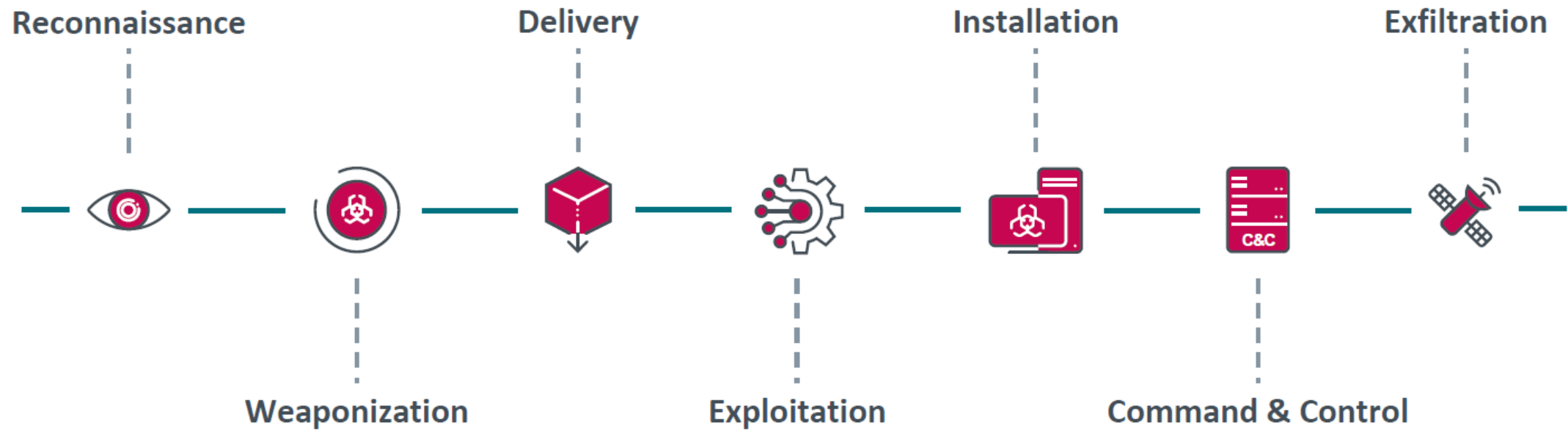
Aké typy hrozieb?

- Endpoint **Malware** Detections
- Indicators of Compromise (**IOC**)
- Techniques Tactics Procedures (**TTP**)
- Advanced Persistent Threats (**APT**)



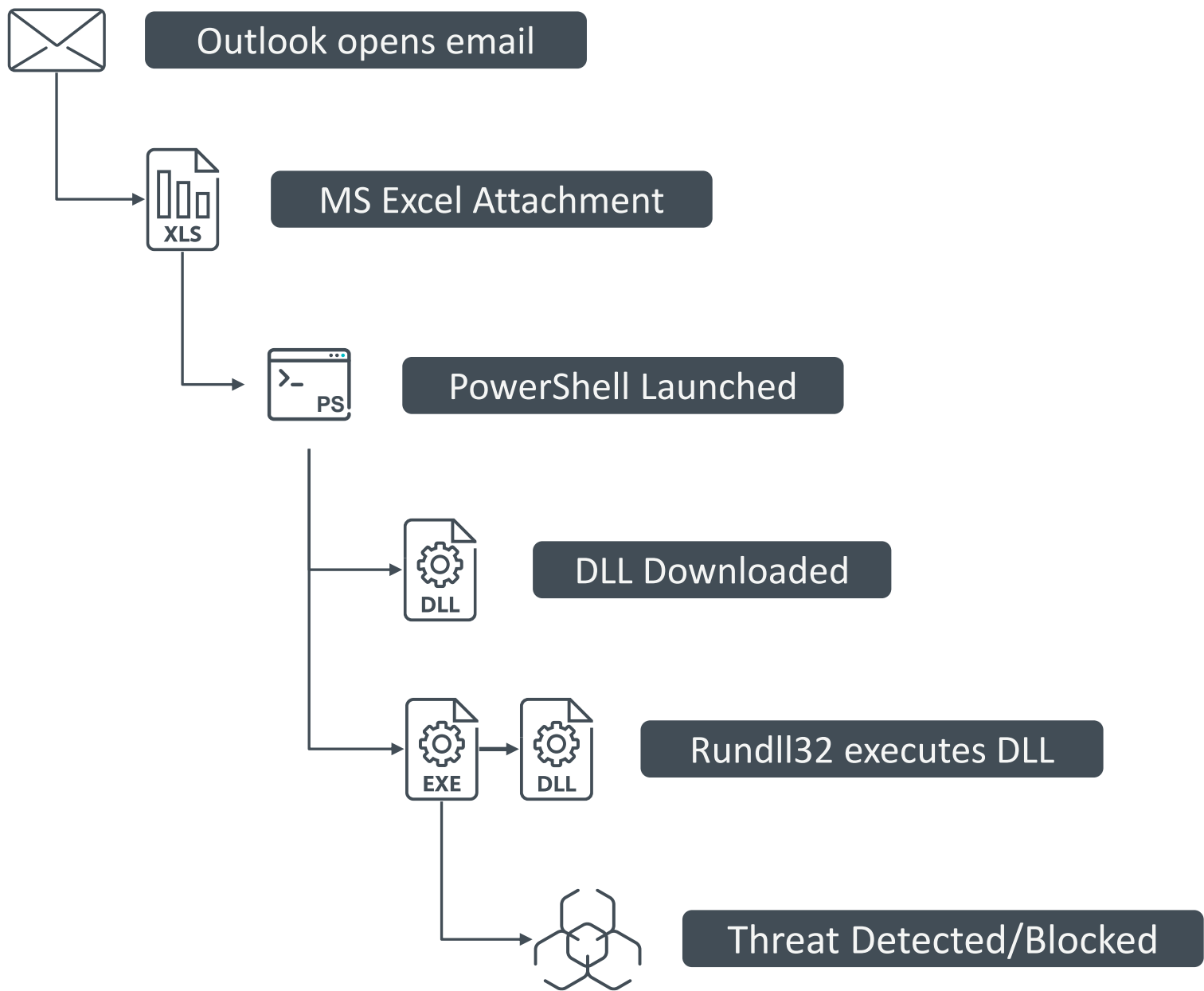
APT útoky

Cyber Kill Chain



The background image shows a laboratory setting. A person wearing a white lab coat and a face mask is using a pipette to transfer liquid into small vials. In the foreground, a microscope is visible on a lab bench. The entire image has a blue color overlay.

Endpoint Detection & Response



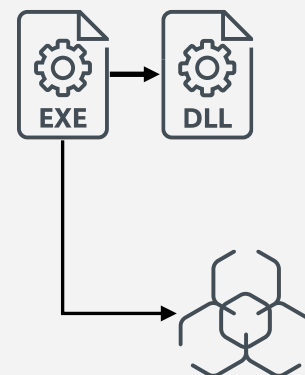
Without ESET Enterprise inspector:



Minimal Visibility



Uncertainty



Rundll32 executes DLL

Threat Detected/Blocked

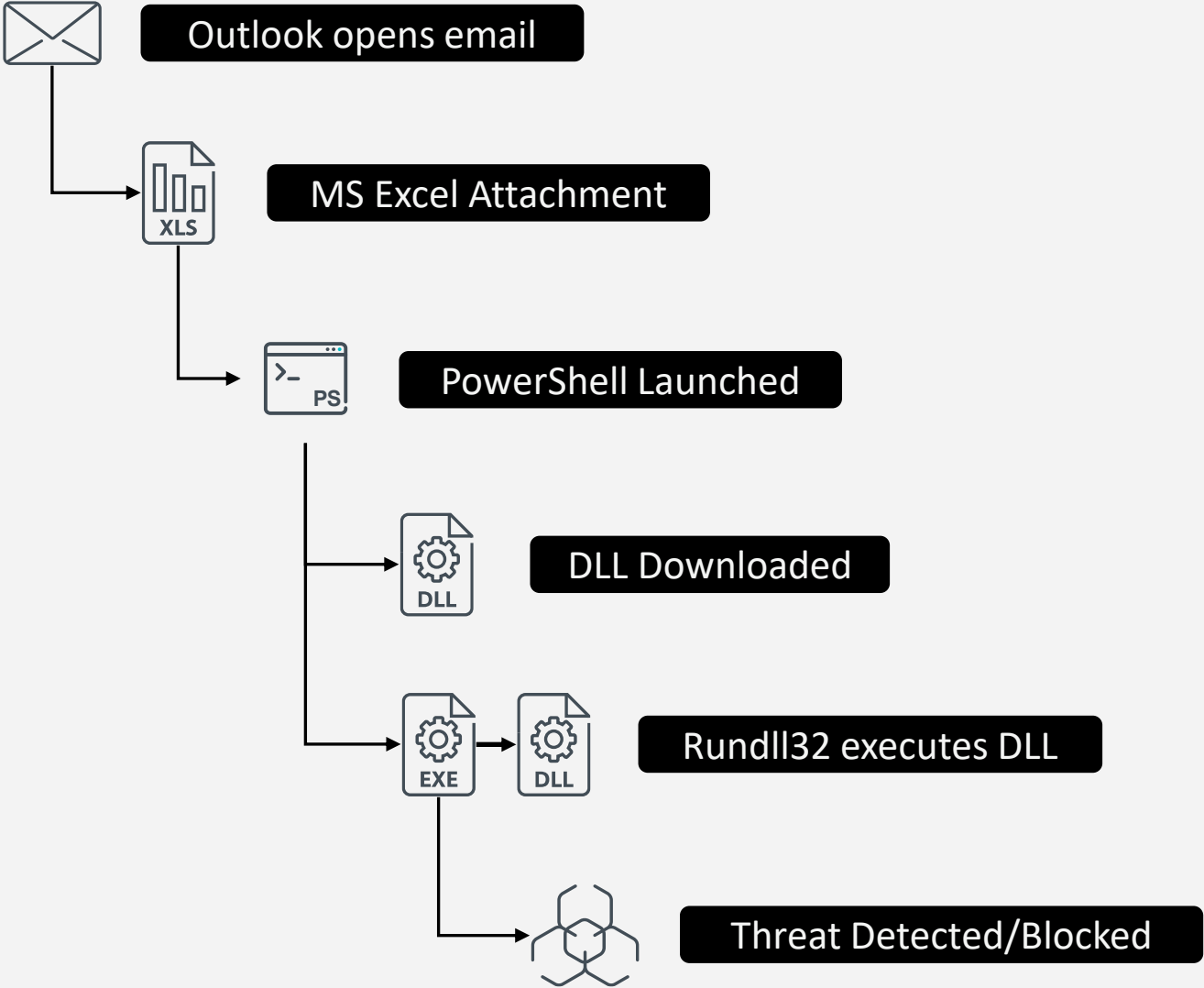
With Enterprise Inspector you gain:



Increased Visibility



Peace of mind





< BACK

Alarm details



Filecoder behaviour [Z0601]

SOURCE	Filecoder behaviour [Z0601]
CATEGORY	Filecoders
OCCURED	11 minutes ago - Mar 7, 2018, 4:57:39 PM
PRIORITY	0

ESET LiveGrid®

REPUTATION	●●●●●●●●
POPULARITY	●●●●●●●●
FIRST SEEN	one year ago

svchost.exe

SIGNATURE TYPE	None
SIGNER NAME	None
SEEN ON	2 computers
FIRST SEEN	one day ago - Mar 6, 2018, 2:55:50 PM
LAST EXECUTED	11 minutes ago - Mar 7, 2018, 4:57:38 PM

findepcc-128

PARENT GROUP	Finance Department
LAST CONNECTED	3 minutes ago - Mar 7, 2018, 5:05:32 PM
LAST EVENT	4 minutes ago - Mar 7, 2018, 5:05:02 PM
AGENT VERSION	1.2.649
OS	Windows 7

CATEGORY	Filecoders
EXPLANATION	File with a duplicate extension created on top of a popular file extension (such as .jpg.lock) has been created. That may indicate activity of ransomware encrypting files.
MALICIOUS CAUSES	Generated by ransomware when encrypting files.
BENIGN CAUSES	Sometimes used by legitimate program to "lock"/ensure exclusive access to some file. Usually used only on one or few files.
RECOMMENDED ACTIONS	Check the count of files with changed extension and content of such changed files. Are they encrypted? Is there any reason for adding a duplicate extension? Scan the reported program by AV. If not detected then submit the executable for analysis. Locate encrypted files (find out extent of damage). Shares on network may be affected. Investigate how the program reached your company and how was it was executed.
ALARM TYPE	Rule was activated
SOURCE RULE	Filecoder behaviour [Z0601]
OCCURRED	11 minutes ago - Mar 7, 2018, 4:57:39 PM
TRIGGERED	10 minutes ago - Mar 7, 2018, 4:58:31 PM

MARK AS RESOLVED

MARK AS PRIORITY ▾

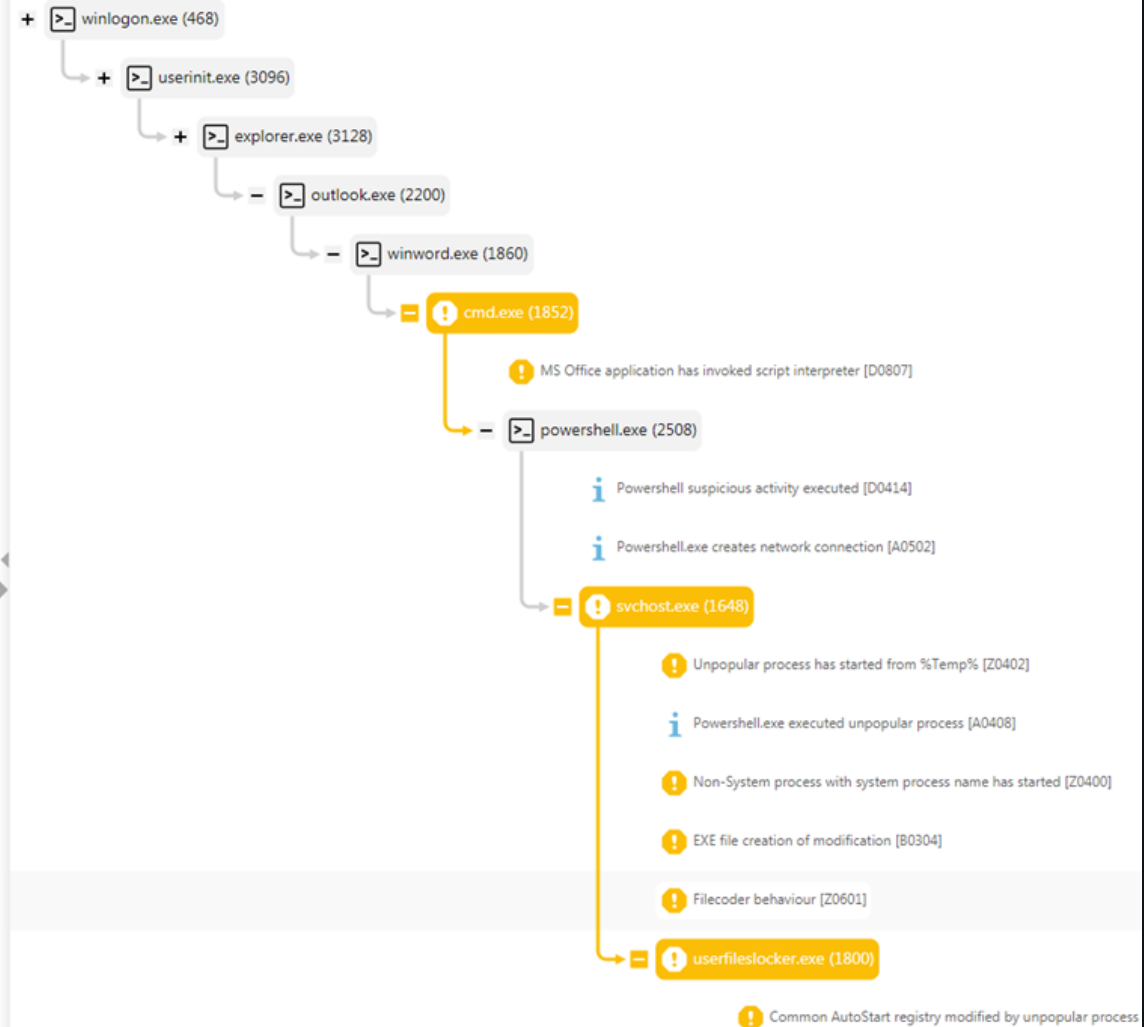
COMPUTER ▾

KILL PROCESS

EXECUTABLE ▾

CREATE EXCLUSION

EDIT RULE



Prečo EDR?

- **pokročilé pretrvávajúce útoky (APT)**
- **phishingové útoky**
- **hrozba ransomware**
- **hrozby priamo zvnútra organizácie**
- **prevádzkovateľ základnej služby**
- **zákon č.69/2018 Z.z. o kybernetickej bezpečnosti**



ESET je podľa Radicati "popredným hráčom" v oblasti ochrany pred APT

Kľúčové hodnotené funkcionality

- detekcia a reakcia na útoky (EDR)
- možnosti nasadenia
- podpora rôznych platforiem
- detekcia malvéru
- sandboxing a karanténa
- forenzná analýza
- rozbor zero-day a pokročilých hrozieb





Endpoint Detection & Response

EDR – “R” for Response



Block Hash
Kill Process



Run Scan
Download File



Restart
Shutdown



Network
Isolation



Terminal
(remote
PowerShell)

DASHBOARD

ALARMS

EXECUTABLES

SCRIPTS

COMPUTERS

ADMIN

Alarms

UNGROUPED

RESOLVED

ADD FILTER

ALARMS (50)	SEVERITY	PRIORITY	RESOLVED	TIME	COMPUTER	EXECUTABLE	PROCESS NAME (ID)	RULE
Rule System utility was executed test [A0403]				7 hours ago	WIN-9QOO0JGO1JR	reg.exe	reg.exe (3068)	System utility was ex
Rule Unpopular process has started from %Temp% [Z0402]				7 hours ago	WIN-9QOO0JGO1JR	InstHelper.exe	InstHelper.exe (852)	Unpopular process h
Rule System utility was executed test [A0403]				2 days ago	JANKECH.hq.eset.com	tasklist.exe	tasklist.exe (137396)	System utility was ex
Rule System utility was executed test [A0403]				2 days ago	JANKECH.hq.eset.com	netstat.exe	netstat.exe (138400)	System utility was ex
Rule Common AutoStart registry modified by unpopular process [A0103]				2 days ago	JANKECH-TVM3	eei_demo.exe	eei_demo.exe (7580)	Common AutoStart i
Rule Cmd.exe executed with '/c' by unpopular process [A0400]				2 days ago	JANKECH-TVM3	cmd.exe	cmd.exe (7372)	Cmd.exe executed w
Rule Unpopular process has started from %Temp% [Z0402]				2 days ago	JANKECH-TVM3	eei_demo.exe	eei_demo.exe (7580)	Unpopular process h
Rule Service installation or modification [B0402]				2 days ago	JANKECH-TVM3	eei_demo.exe	eei_demo.exe (7580)	Service installation o
Rule Windows Firewall rules manipulation [B0202]				2 days ago	JANKECH-TVM3	eei_demo.exe	eei_demo.exe (7580)	Windows Firewall rul
Rule Unpopular process has started from %Temp% [Z0402]				2 days ago	JANKECH-TVM3	eei_demo.exe	eei_demo.exe (7108)	Unpopular process h
Antivirus Potentially unwanted application: @ApplicUnsaf.Win32/Bundled:				one week ago	jankech-tvm8	javaic.dll		
Rule System utility was executed test [A0403]				one week ago	JANKECH.hq.eset.com	tasklist.exe	tasklist.exe (98800)	System utility was ex
Rule System utility was executed test [A0403]				one week ago	JANKECH.hq.eset.com	netstat.exe	netstat.exe (98992)	System utility was ex
Rule System utility was executed test [A0403]				one week ago	WIN-9QOO0JGO1JR	reg.exe	reg.exe (3336)	System utility was ex
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				one week ago	Jankech-tvm8	AEMAgent.exe	AEMAgent.exe (8160)	Unpopular process h
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	JANKECH-TVM5	AEMAgent.exe	AEMAgent.exe (4304)	Unpopular process h
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	JANKECH-TVM2	AEMAgent.exe	AEMAgent.exe (3648)	Unpopular process h
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	Jankech-tvm8	AEMAgent.exe	AEMAgent.exe (6812)	Unpopular process h
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	Jankech-tvm11	AEMAgent.exe	AEMAgent.exe (8932)	Unpopular process h
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	JANKECH-TVM3	AEMAgent.exe	AEMAgent.exe (6940)	Unpopular process h
Rule Common AutoStart registry modified by unpopular process [A0103]				2 weeks ago	JANKECH-TVM5	bad.exe	epic.exe (3764)	Common AutoStart i
Rule EXE patching or dropping [B0304]				2 weeks ago	JANKECH-TVM5	bad.exe	epic.exe (3764)	EXE patching or dro
Rule Common AutoStart registry modified by unpopular process [A0103]				2 weeks ago	JANKECH-TVM5	bad.exe	bla.exe (3988)	Common AutoStart i
Antivirus Potentially unwanted application: @ApplicUnwnt.Win32/ESET_Te				2 weeks ago	JANKECH-TVM5	eset-testfile.exe		
Rule System utility was executed test [A0403]				2 weeks ago	JANKECH.hq.eset.com	tasklist.exe	tasklist.exe (57756)	System utility was ex
Rule System utility was executed test [A0403]				2 weeks ago	JANKECH.hq.eset.com	netstat.exe	netstat.exe (57404)	System utility was ex
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	Jankech-tvm11	61.0.3163.79_60.0.3112.113_chrome_updater.ex	61.0.3163.79_60.0.3112.113_chrome	Unpopular process h
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	Jankech-tvm11	AEMAgent.exe	AEMAgent.exe (2180)	Unpopular process h

COLLAPSE MENU

MARK AS RESOLVED

MARK AS UNRESOLVED

MARK AS NO PRIORITY

MARK AS PRIORITY I

MARK AS PRIORITY II

MARK AS PRIORITY III

EDIT RULE

DASHBOARD

COMPUTERS

DETECTIONS

SEARCH

Executables

Scripts

Admin

COLLAPSE

Executables

☐	NAME (98)	STATUS	REPUTATION (LIVEGRID®)	POPULARITY (LIVEGRID®)	EXECUTED ON COMP	SIGNER NAME	FILE DESCRIPTION
☐	lsass.exe	⚠	●●●●●●●●	●●●●●●●●	19	Microsoft Windows	Local Security Authority Proc...
☐	compattelrunner.exe	⚠	●●●●●●●●	●●●●●●●●	19	Microsoft Windows	Microsoft Compatibility Tele...
☐	msiexec.exe	⚠	●●●●●●●●	●●●●●●●●	19	Microsoft Windows	Windows® installer
☐	cmd.exe	⚠	●●●●●●●●	●●●●●●●●	19	None	Windows Command Processor
☐	sc.exe	i	●●●●●●●●	●●●●●●●●	19	Microsoft Windows	A tool to aid in developing s...
☐	wininit.exe	⚠	●●●●●●●●	●●●●●●●●	19	Microsoft Windows	Windows Start-Up Application
☐	lsim.exe	⚠	●●●●●●●●	●●●●●●●●	19	Microsoft Windows	Local Session Manager Service
☐	spoolsv.exe	⚠	●●●●●●●●	●●●●●●●●	19	Microsoft Windows	Spooler SubSystem App
☐	vsrv.exe	⚠	●●●●●●●●	●●●●●●●●	19	None	Microsoft® Volume Shadow ...
☐	rundll32.exe	i	●●●●●●●●	●●●●●●●●	19	Microsoft Windows	Windows host process (Run...
☐	csrss.exe	⚠	●●●●●●●●	●●●●●●●●	19	Microsoft Windows	Client Server Runtime Process
☐	svchost.exe	⚠	●●●●●●●●	●●●●●●●●	19	Microsoft Windows	Host Process for Windows S...
☐	winlogon.exe	⚠	●●●●●●●●	●●●●●●●●	16	Microsoft Windows	Windows Logon Application
☐	services.exe	⚠	●●●●●●●●	●●●●●●●●	16	Microsoft Windows	Services and Controller app
☐	explorer.exe	i	●●●●●●●●	●●●●●●●●	14	Microsoft Windows	Windows Explorer
☐	searchindexer.exe	⚠	●●●●●●●●	●●●●●●●●	14	None	Microsoft Windows Search I...
☐	lsass.exe	⚠	●●●●●●●●	●●●●●●●●	13	Microsoft Windows	Local Security Authority Proc...
☐	wermgr.exe	⚠	●●●●●●●●	●●●●●●●●	13	Microsoft Windows	Windows Problem Reporting
☐	netsh.exe	i	●●●●●●●●	●●●●●●●●	8	Microsoft Windows	Network Command Shell
☐	windows-kb890830-v5.82.exe	i	●●●●●●●●	●●●●●●●●	6	Microsoft Windows	Microsoft Windows Maliciou...
☐	sc.exe	i	●●●●●●●●	●●●●●●●●	5	Microsoft Windows	Service Control Manager Co...
☐	services.exe	⚠	●●●●●●●●	●●●●●●●●	5	Microsoft Windows Publisher	Services and Controller app
☐	svchost.exe	⚠	●●●●●●●●	●●●●●●●●	5	Microsoft Windows Publisher	Host Process for Windows S...
☐	drwtsn32.exe	⚠	●●●●●●●●	●●●●●●●●	5	None	DrWatson Postmortem Debu...
☐	python.exe	⚠	●●●●●●●●	●●●●●●●●	3	None	None
☐	lsass.exe	⚠	●●●●●●●●	●●●●●●●●	3	Microsoft Windows	Local Security Authority Proc...
☐	netstat.exe	i	●●●●●●●●	●●●●●●●●	3	Microsoft Windows	TCP/IP Netstat Command
☐	efds.exe	⚠	●●●●●●●●	●●●●●●●●	3	"ESET, spol. s r.o."	Agent Interface Service
☐	efdsrv.exe	⚠	●●●●●●●●	●●●●●●●●	3	"ESET, spol. s r.o."	ESET FDE Service

MARK AS SAFE

MARK AS UNSAFE

BLOCK

UNBLOCK

MARK AS INSPECTED

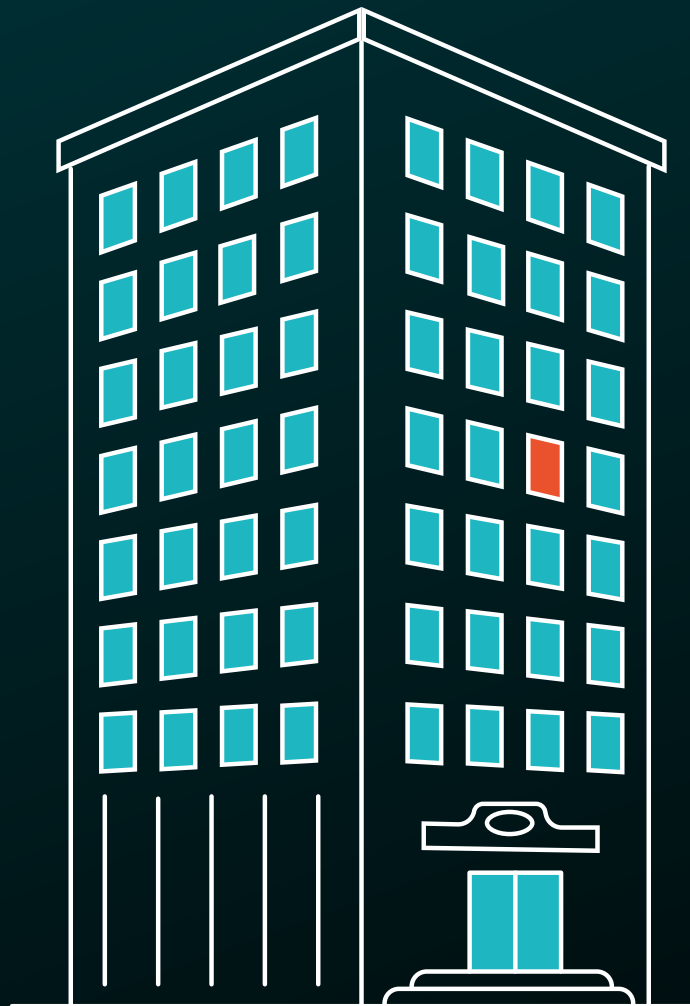
MARK AS UNINSPECTED

TAGS

SEEN ON

FILTER EVENTS

Bezpečností špecialisti
potrebujú chrániť
kompletne **celý perimeter**



Útočníkom stačí nájsť
jedno slabé miesto

KATEGÓRIE SLUŽIEB

PROFESIONÁLNE SLUŽBY

- ✓ Riešenie problémov s ESET produktami
- ✓ Prioritná a garantovaná technická podpora (SLA)
- ✓ Inštalácia a konfigurácia ESET produktov
- ✓ Kontrola nastavení a odporúčania

BEZPEČNOSTNÉ SLUŽBY

- ✓ Analýza podozrivých súborov
- ✓ Pomoc pri reakcii na malvérové incidenty
- ✓ Bezpečnostná podpora pre EDR
- ✓ Threat monitoring / Threat hunting

ESET DETECTION AND RESPONSE ESSENTIAL

KATEGÓRIA AKTIVÍT	AKTIVITA	ŠTANDARDNÁ BEZPEČNOSTNÁ PODPORA	DETECTION AND RESPONSE ESSENTIAL
Bezpečnostná podpora pre koncové zariadenia	Malvér: nezachytená detekcia	áno	áno
	Malvér: problém s liečením	áno	áno
	Malvér: infekcia ransomvérom	áno	áno
	Nesprávna detekcia	áno	áno
	Všeobecné: preskúvanie podozrivého správania	áno	áno
Vyšetrenie incidentov a reakcia na ne	Základná analýza súborov	X	áno
	Podrobná analýza súborov	X	áno
	Digitálna forenzná analýza	X	áno
	Digitálna forenzná pomoc pri reakcii na incidenty	X	áno

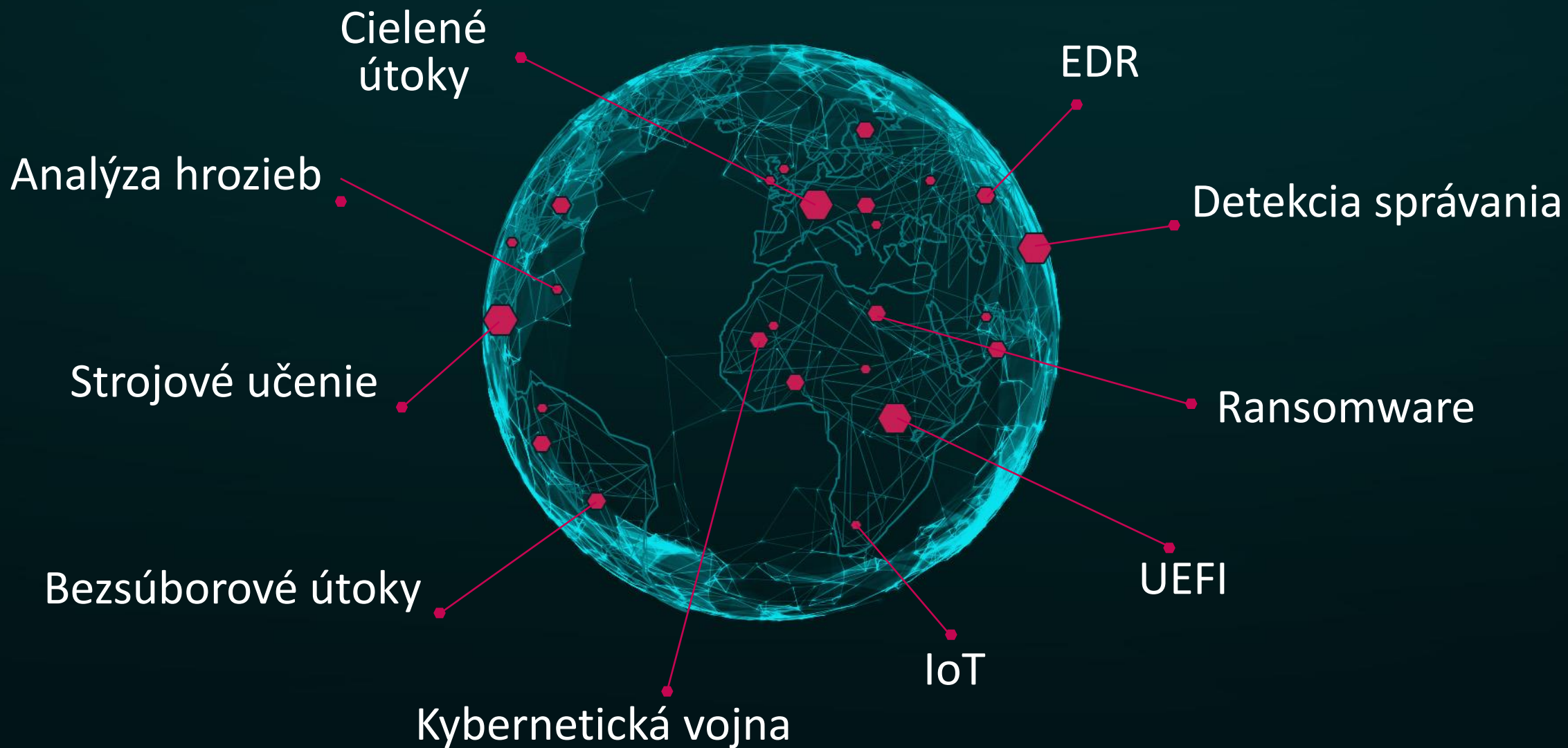
ESET DETECTION AND RESPONSE **ADVANCED**

KATEGÓRIA AKTIVÍT	AKTIVITA	ŠTANDARDNÁ BEZPEČNOSTNÁ PODPORA	DETECTION AND RESPONSE ESSENTIAL	DETECTION AND RESPONSE ADVANCED
Bezpečnostná podpora pre koncové zariadenia	Malvér: nezachytená detekcia	áno	áno	áno
	Malvér: problém s liečením	áno	áno	áno
	Malvér: infekcia ransomvérom	áno	áno	áno
	Nesprávna detekcia	áno	áno	áno
	Všeobecné: preskúmanie podozrivého správania	áno	áno	áno
Vyšetrenie incidentov a reakcia na ne	Základná analýza súborov	X	áno	áno
	Podrobná analýza súborov	X	áno	áno
	Digitálna forenzná analýza	X	áno	áno
	Digitálna forenzná pomoc pri reakcii na incidenty	X	áno	áno
Bezpečnostná podpora pre EDR	Technická podpora – pravidlá	X	X	áno
	Technická podpora – vylúčenia	X	X	áno
	Všeobecné: otázky týkajúce sa nástroja EDR	X	X	áno
	EDR: počiatočná optimalizácia	X	X	áno
	EDR: ESET Threat Hunting (vyhľadávanie hrozieb na vyžiadanie)	X	X	áno

ESET DETECTION AND RESPONSE **ULTIMATE**

KATEGÓRIA AKTIVÍT	AKTIVITA	ŠTANDARDNÁ BEZPEČNOSTNÁ PODPORA	DETECTION AND RESPONSE ESSENTIAL	DETECTION AND RESPONSE ADVANCED	DETECTION AND RESPONSE ULTIMATE
Bezpečnostná podpora pre koncové zariadenia	Malvér: nezachytená detekcia	áno	áno	áno	áno
	Malvér: problém s liečením	áno	áno	áno	áno
	Malvér: infekcia ransomvérom	áno	áno	áno	áno
	Nesprávna detekcia	áno	áno	áno	áno
	Všeobecné: preskúvanie podozrivého správania	áno	áno	áno	áno
Vyšetrenie incidentov a reakcia na ne	Základná analýza súborov	✗	áno	áno	áno
	Podrobná analýza súborov	✗	áno	áno	áno
	Digitálna forenzná analýza	✗	áno	áno	áno
	Digitálna forenzná pomoc pri reakcii na incidenty	✗	áno	áno	áno
Bezpečnostná podpora pre EDR	Technická podpora – pravidlá	✗	✗	áno	áno
	Technická podpora – vylúčenia	✗	✗	áno	áno
	Všeobecné: otázky týkajúce sa bezpečnostného nástroja EDR	✗	✗	áno	áno
	EDR: počiatočná optimalizácia	✗	✗	áno	áno
	EDR: ESET Threat Hunting (vyhľadávanie hrozieb na vyžiadanie)	✗	✗	áno	áno
Bezpečnostné služby pre EDR	EDR: ESET Threat Monitoring (monitorovanie hrozieb)	✗	✗	✗	áno
	EDR: ESET Threat Hunting (proaktívne vyhľadávanie hrozieb)	✗	✗	✗	áno
Profesionálne služby	ESET Deployment & Upgrade	✗	✗	✗	áno

Svet sa mení a rovnako aj ESET





BEZPEČNOSTNÍ IT EXPERTI
NA VAŠEJ STRANĚ

Ďakujeme za pozornost.

