

Ochrana kyberpriestoru a moderné trendy

Ondrej Krajč

Senior Technical Pre-Sales
Representative

Populárne hrozby a vektory

- ☐ Phishing
- ☐ Zraniteľnosti
- ☐ Malware / Ransomware
- ☐ DDoS útoky
- ☐ Útoky typu man-in-the-middle
- ☐ AI generované deepfake
- ☐



Zero-Days a
APT's

69/2018 Z.z., Zákon o kybernetickej bezpečnosti

(transpozícia smernice NIS 2)

Riadenie udalostí a kyber incidentov

- Čo a ako riadiť?

- procesne
- technicky

- Technické opatrenia:

- XDR
- zber a korelácia dát
- multiplatformovosť
- vizualizácia incidentov
- štandardizovaný framework (MITRE ATT&CK)

The screenshot displays the ESET PROTECT & INSPECT cloud interface. The main content area shows a blocked process: "Blocked by Anti-Phishing blacklist" detected by ESET Endpoint Security product. The process is "chrome.exe" (PE: Google Chrome) with SHA-1 87C41FD9D56D838FBA5C934... and is trusted. The command line is "--type=utility --field-trial-handle=1552,1504401125157094 3637,6223533554436846995,131 072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1824 /prefetch:8". The process was first seen 6 days ago at 4:58:29 PM and last executed at 6:24:18 PM. The user is "hb-c-ep01\john" with an unknown role.

Below this, the "ESET LiveGrid" section shows a reputation of 5 stars, popularity of 5 stars, and first seen a year ago. The "Detections" section shows 1 threat, 5 warnings, and 0 informational messages.

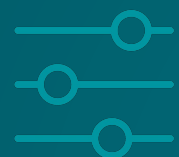
On the right, a process tree shows "userinit.exe (5008)" spawning "explorer.exe (5068)", which in turn spawns "7zg.exe (7524)", "7zg.exe (2964)", "7zg.exe (5080)", and "chrome.exe (8092)". The "7zg.exe (2964)" process is blocked by "Malware: Win32/Injector.RVT" and "Malware: Win32/Duqu.A". The "chrome.exe (8092)" process is blocked by "Blocked by Anti-Phishing blacklist: h...".



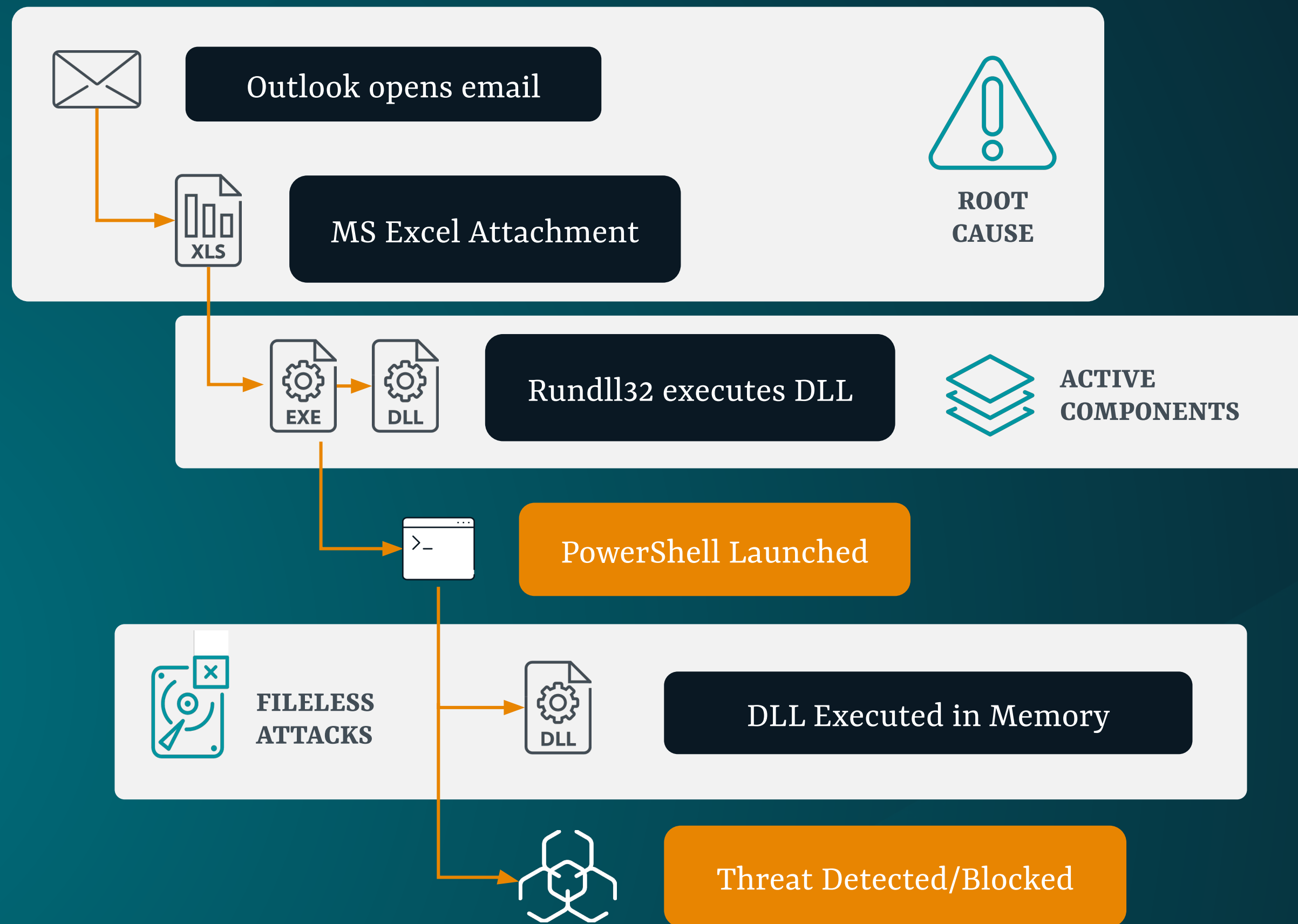
S XDR ESET Inspect riešením:



zvýšená viditeľnosť



dodatočná kontrola



eset PROTECT & INSPECT

QUESTIONS DISABLED HELP LOG OUT

BACK Suspected Malware Execution and Botnet Activity on ei- -mgr-test-endpoint-1

Incident graph Timeline Detections Computers Executables Processes Incident Timeline Assistant

What data or information was accessed or exfiltrated?

The data accessed or exfiltrated includes a dropped executable named make-nearmiss.exe, which was flagged as similar to known malware but not confirmed as malware yet. Additionally, suspected botnet activity with the threat name Win32/BotnetProtectionTest was detected from source IP 127.0.0.1 to destination IP 127.0.0.1, initiated by the user ei- -mgr-t\administrator through httpclnttester.exe, which was blocked due to its unknown reputation and lack of signature.

IMPORTANT: Generated by AI. Verify information for accuracy.

What is the reputation of the dropped executable make-nearmiss.exe?

The dropped executable make-nearmiss.exe has a reputation of "trusted."

IMPORTANT: Generated by AI. Verify information for accuracy.

any more suggestions?

1. Can you provide more details about the source IP 127.0.0.1 and the destination IP 127.0.0.1 in the suspected botnet activity?
2. What action was taken in response to the suspected botnet activity with the threat name Win32/BotnetProtectionTest?
3. Can you provide information about the process httpclnttester.exe and its reputation?

IMPORTANT: Generated by AI. Verify information for accuracy.

Ask ESET AI Advisor anything...

Responses are generated by AI. Verify information for accuracy.

INCIDENT REMEDIATION COMMENT EDIT ASSIGN PROGRESS GRAPH

COLLAPSE

Monitorovanie, zaznamenávanie, hlásenie udalostí

Ako si pomôcť?

- MDR (služby manažovanej bezpečnosti)

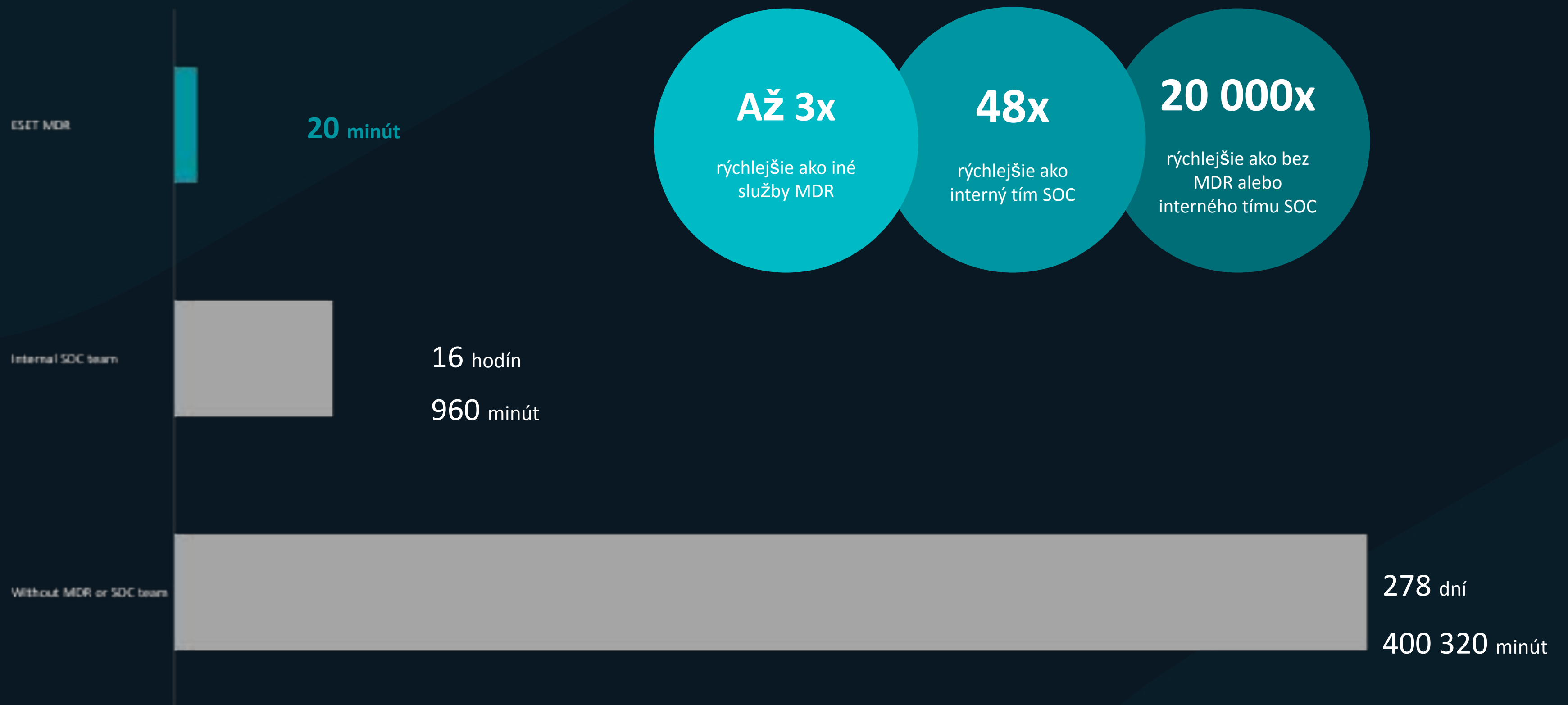
Čo to obsahuje:

- nepretržité monitorovanie, triedenie a reakcie na hrozby
- reakcia na aktívne prebiehajúce kampane útočníkov
- knižnica príznakov podozrivého správania
- optimalizácia príznakov podozrivého správania a výnimiek
- expertíza dodávateľa
- ...

ESET PROTECT MDR



Rýchlosť detekcie a reakcie



{Logická hádanka}

- $8-6=2$
- $8+6=2$
- $8+11=?$

?=c

{Odpoveď AI}

ChatGPT:

- Vzhľadom na neštandardné pravidlá v úlohe môžeme predpokladať, že sa používa operácia modulo. Pre príklad:
- $8 + 6 = 2$ naznačuje, že používame operáciu modulo 6.
- Pre $8 + 11$:
- - $8 + 11 = 19$
 - $19 \bmod 6 = 1$
- **Takže najpravdepodobnejší výsledok pre $8 + 11 = ?$ je 1.**

Spôsobilosť ľudských zdrojov

Čo je to spôsobilosť?

- schopnosť alebo možnosť vykonávať určité činnosti alebo plniť určité úlohy

Ako ju budovať?

- metodické vzdelávanie
- opakované testovanie vedomostí a skúseností

Katalóg balíka PLATINUM

Vyberte si školenia zamerané na konkrétne témy podľa potrieb vašej spoločnosti.



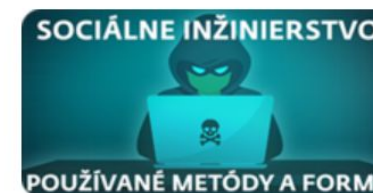
Phishing

V tomto školení sa zamestnanci naučia rozpoznávať phishingové správy vďaka praktickým cvičeniam a videám, ktoré vysvetľujú problematiku podvodných e-mailov.



Silné heslá

Vďaka tomuto školeniu si zamestnanci osvoja správne návyky pri vytváraní a používaní silných hesiel a dozvedia sa ako predchádzať tomu, aby útočníci ich heslá prelomili.



Sociálne inžinierstvo: Používané metódy a formy

Úvodné z troch našich školení zameraných na sociálne inžinierstvo približuje, aké metódy využíva útočník na dosiahnutie svojich cieľov a aké formy môžu nadobúdať jeho útoky.



Sociálne inžinierstvo: Hrozby v online priestore

Sociálne inžinierstvo sa využíva pri útokoch, v online priestore, či už je to phishing, podvodné webstránky, alebo aj telefonáty, na ktoré vás toto školenie pripraví.



Sociálne inžinierstvo: Hrozby v priestoroch firmy

S útokmi, ktoré využívajú metódy sociálneho inžinierstva, sa môžeme stretnúť aj v reálnom svete. Naučíte sa, ako môže útočník prekonať vašu fyzickú bezpečnosť.

Ďakujem za pozornosť

Ondrej Krajč

