SECURITY DAYS

ČELIŤ POKROČILÝM ÚTOKOM "LEN" S ANTIMALVÉROVOU OCHRANOU NEMUSÍ VŽDY STAČIŤ

Július Selecký

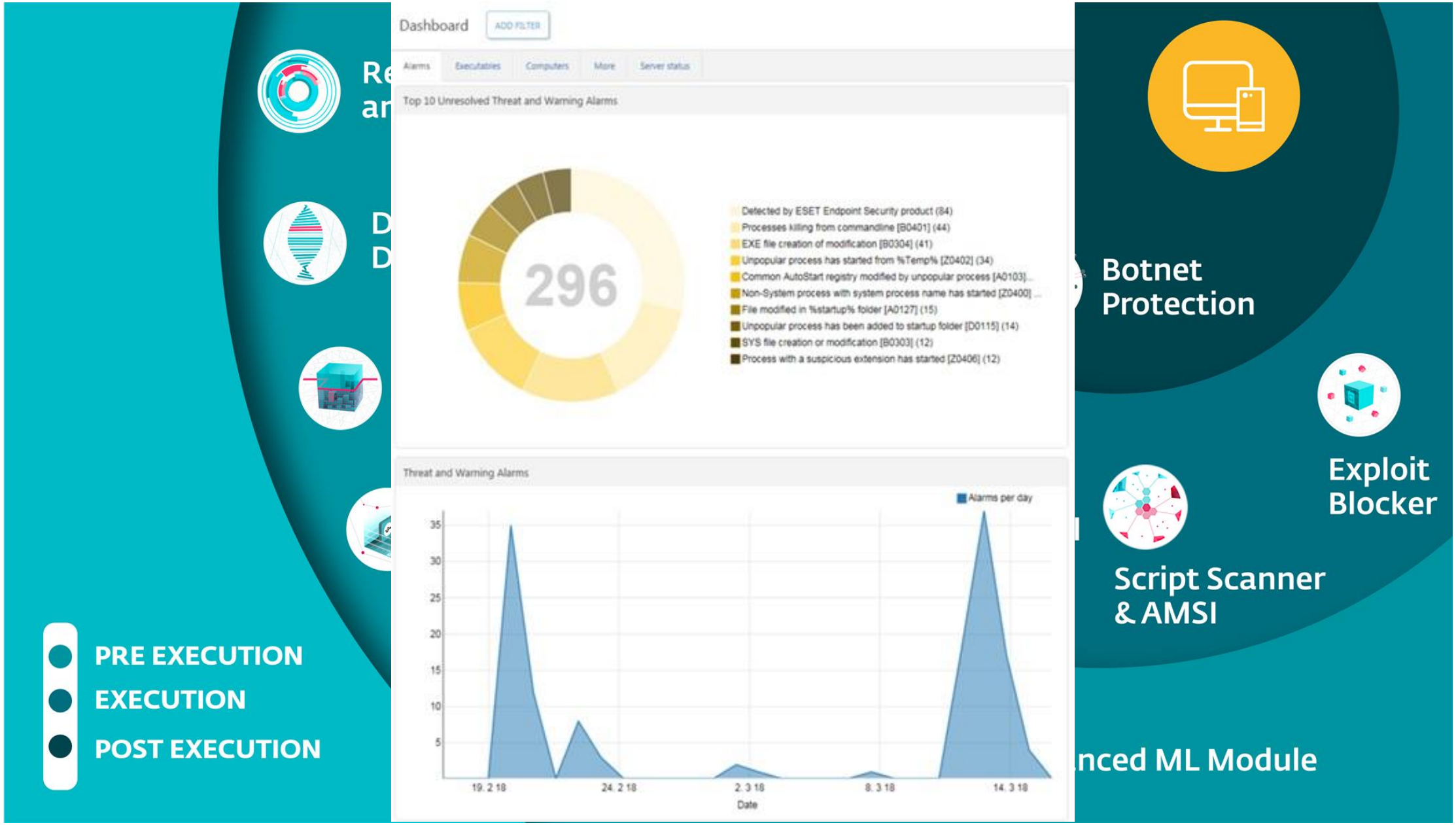
UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™ & SME KONFERENCIE

ESET Enterprise Inspector

Prečo EDR? (Endpoint Detection and Response)

- Evolúcia ransomware
- Komplexnosť útokov sa zvyšuje
  - Presnejšie cielenie

- Útočníci nepoužívajú len spustiteľné súbory
- Pretrvávajúce hrozby v systéme
- 69/2018 Z. z. o kybernetickej bezpečnosti


Dashboard
ADD FILTER
Alarms
Executables
Computers
More
Server status
Top 10 Unresolved Threat and Warning Alarms
296
Detected by ESET Endpoint Security product (84)
Processes killing from commandline [B0401] (44)
EXE file creation of modification [B0304] (41)
Unpopular process has started from %Temp% [Z0402] (34)
Common AutoStart registry modified by unpopular process [A0103]...
Non-System process with system process name has started [Z0400] ...
File modified in %startup% folder [A0127] (15)
Unpopular process has been added to startup folder [D0115] (14)
SYS file creation or modification [B0303] (12)
Process with a suspicious extension has started [Z0406] (12)
Threat and Warning Alarms
Alarms per day
35
30
25
20
15
10
5
19. 2 18
24. 2 18
2. 3 18
8. 3 18
14. 3 18
Date
Botnet Protection
Exploit Blocker
Script Scanner & AMSI
nced ML Module
PRE EXECUTION
EXECUTION
POST EXECUTION

Phishing správy s malvérom

Bezpečná sieť

Začiatok

Koniec

Ukradnuté alebo zašifrované dáta

Phishing správy s malvérom

Bezpečná sieť

Koniec

Začiatok

Malvér cez USB alebo sociálne inžinierstvo

Ukradnuté alebo zašifrované dáta

Phishing správy s malvérom

Sofistikované útoky

Bezpečná sieť

Začiatok

Malvér cez USB alebo sociálne inžinierstvo

Koniec

Ukradnuté alebo zašifrované dáta

ESET Enterprise Inspector

- Detekcia pokročilých pretrvávajúcich hrozieb
- Zastavenie bezsúborových útokov
- Blokovanie zero-day hrozieb
- Ochrana pred ransomware
- Zachytenie porušovania bezpečnostných politík
- Detekcia incidentov (analýza príčin vzniku)
- Úplná sieťová izolácia

EPR CyberRisk Quadrant™

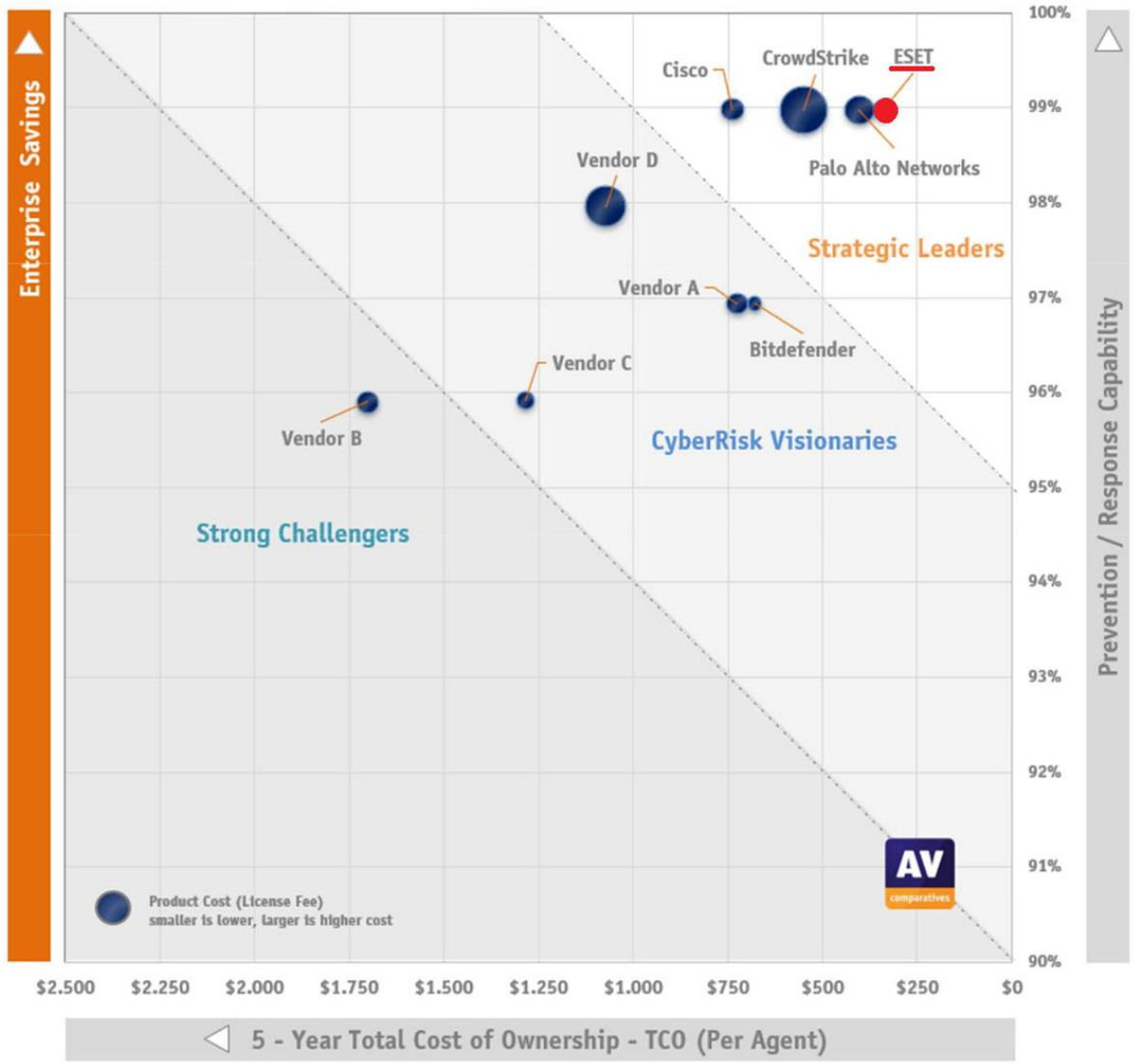


Figure 1 – Endpoint Prevention and Response (EPR) – ECRQ – Enterprise CyberRisk Quadrant™

Endpoint Prevention and Response October 2020

ESET

AV comparatives Certified EPR 2020 Strategic Leader

ESET Enterprise Inspector

Detekcia

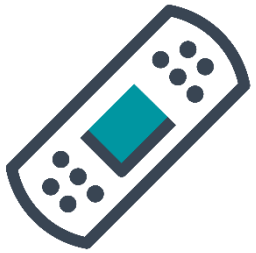
Hľadanie anomálií

Viditeľnosť

Čo sa stalo?

Kedy sa to stalo?

Ako sa to stalo?



Reakcia

Blokovanie

Odstránenie

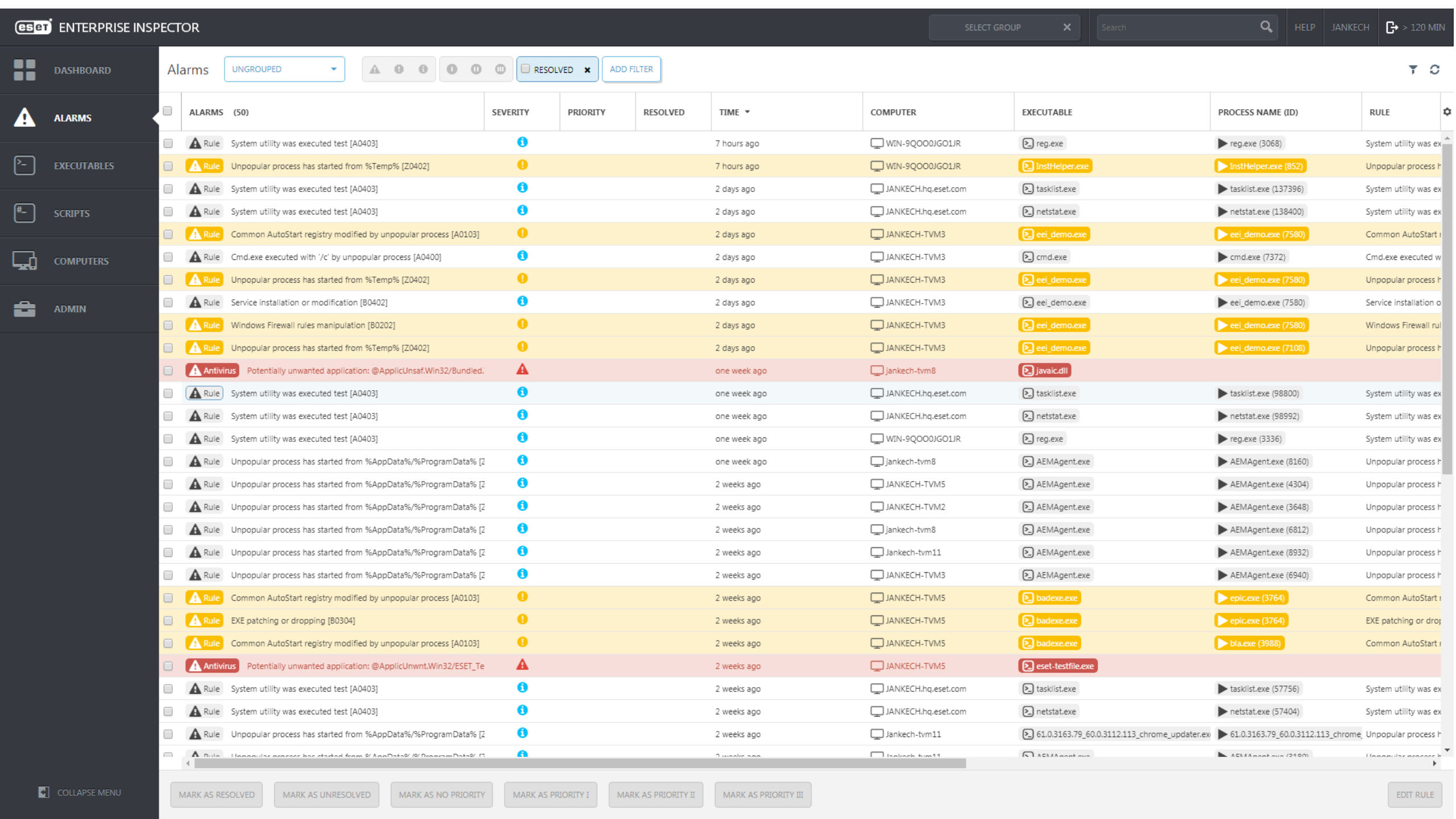
69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

§24 Hlásenie kybernetických bezpečnostných incidentov

- povinnosť hlásiť každý závažný kybernetický bezpečnostný incident
- kategória závažnosti
- dĺžka trvania kybernetického bezpečnostného incidentu
- geografické rošírenie kybernetického bezpečnostného incidentu

CSIRT.SK

- typ závažného incidentu (nežiadúci obsah, škodlivý kód, získavanie informácií, pokus o prienik do systému, nedostupnosť, neoprávnený prístup, podvod, zraniteľnosť...)
- časové údaje zistenia a vzniku incidentu
- detailný opis a priebeh incidentu
- rozsah škôd
- prvotné zasiahnuté aktíva
- stav riešenia závažného kybernetického incidentu


ENTERPRISE INSPECTOR
SELECT GROUP
Search
HELP
JANKECH
> 120 MIN
DASHBOARD
ALARMS
EXECUTABLES
SCRIPTS
COMPUTERS
ADMIN
COLLAPSE MENU
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
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 badexe.exe epic.exe (3764) Common AutoStart
Rule EXE patching or dropping [B0304] 2 weeks ago JANKECH-TVM5 badexe.exe epic.exe (3764) EXE patching or drop
Rule Common AutoStart registry modified by unpopular process [A0103] 2 weeks ago JANKECH-TVM5 badexe.exe bla.exe (3988) Common AutoStart
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
MARK AS RESOLVED
MARK AS UNRESOLVED
MARK AS NO PRIORITY
MARK AS PRIORITY I
MARK AS PRIORITY II
MARK AS PRIORITY III
EDIT RULE

< 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

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

ESET LiveGrid®

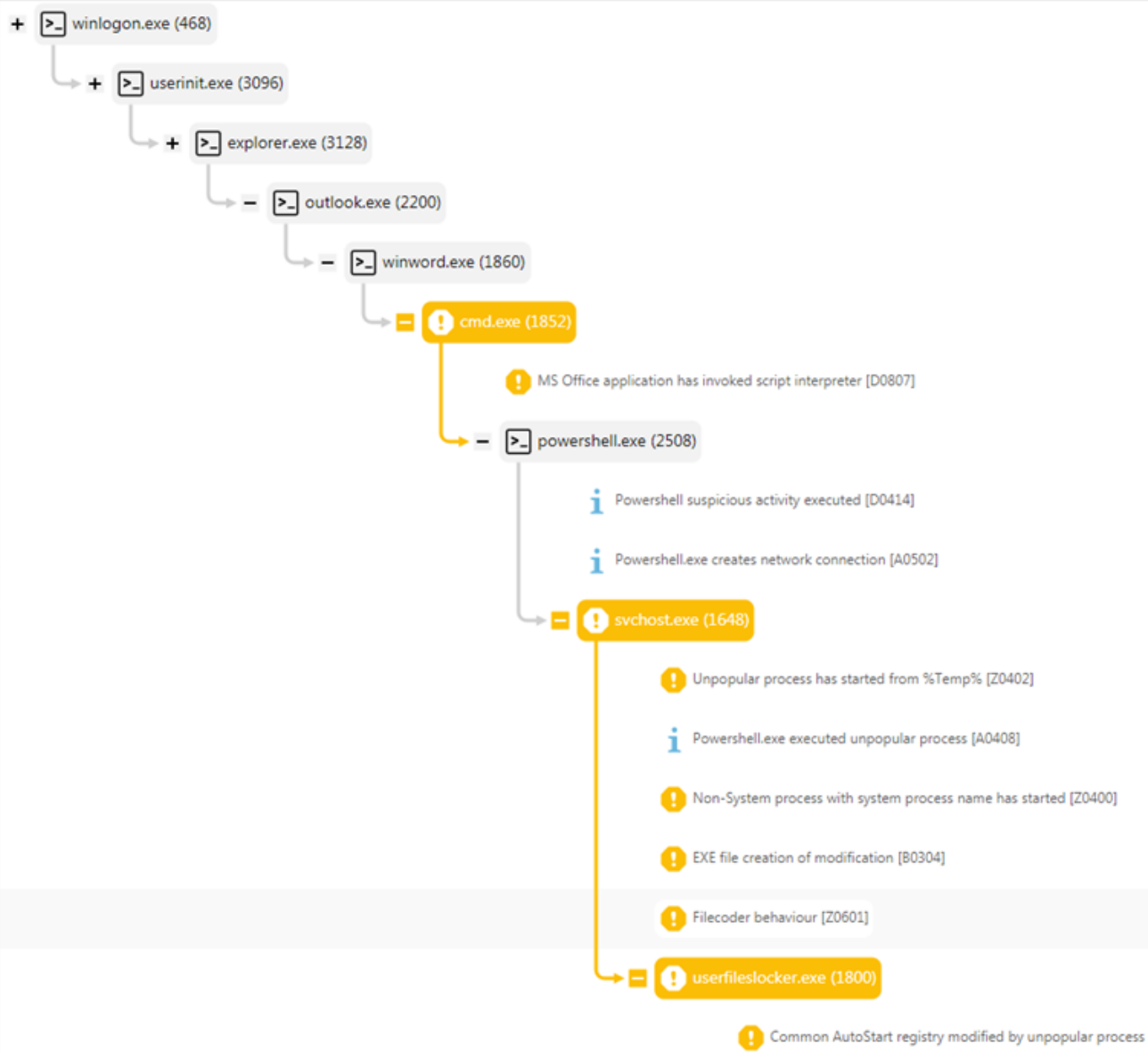
REPUTATION	
POPULARITY	
FIRST SEEN	one year ago

findeppc-128

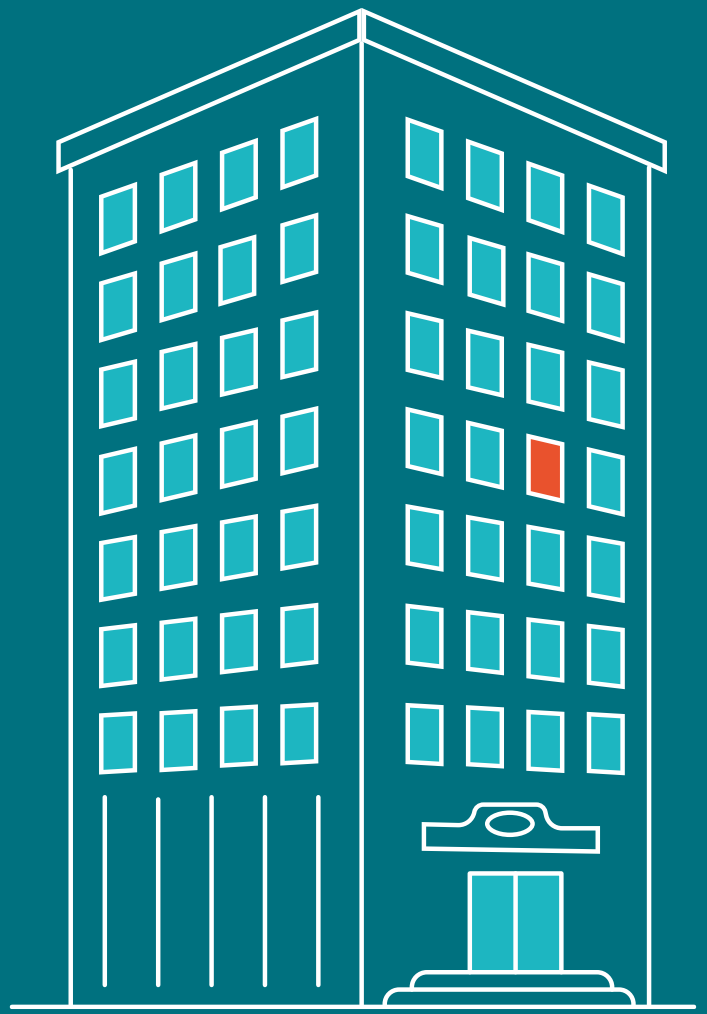
PARENT GROUP	Finance Department
LAST CONNECTED	3 minutes ago - Mar 7, 2018, 5:05:32 PM
LAST EVENT	4 minutes ago - Mar 7, 2018, 5:05:02 PM
AGENT VERSION	1.2.649
OS	Windows 7

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

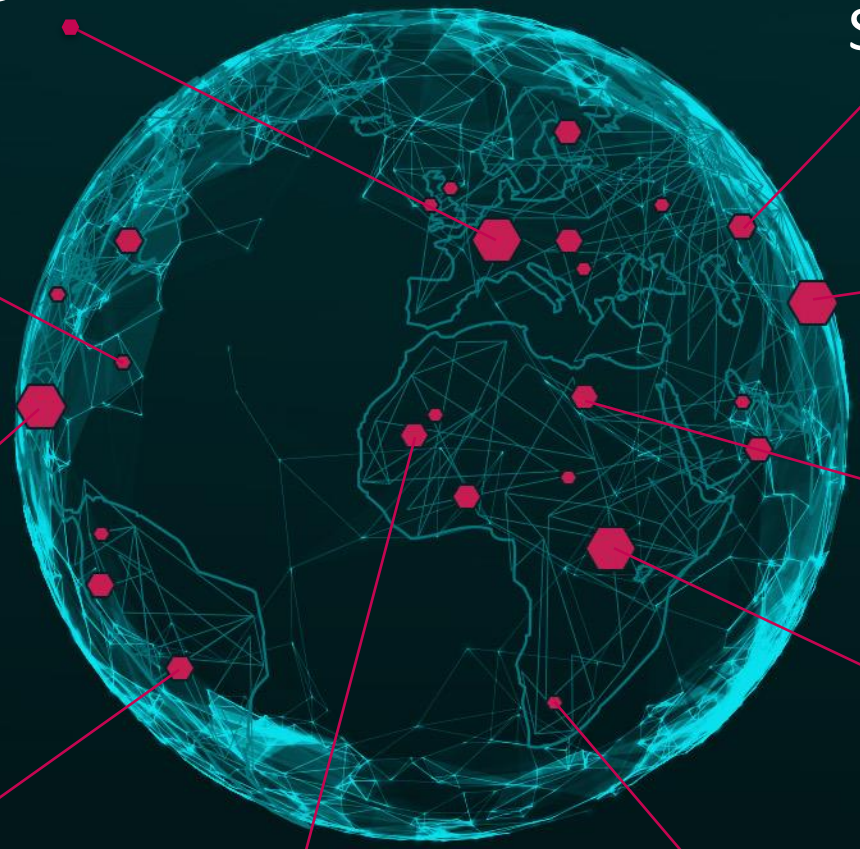


Bezpečnostní špecialisti potrebujú chrániť kompletne **celý perimeter**



Útočníkom stačí nájsť **jedno slabé miesto**

Svet sa mení a rovnako aj ESET



Cielené útoky

Súlad

Analýza hrozieb

Detekcia správania

Strojové učenie

Ransomware

Bezsúborové útoky

UEFI

IoT

Kybernetická vojna

ESET Enterprise Inspector v produktových balíkoch

Cloudové produktové balíky *

PROTECT ENTERPRISE

On-prem produktové balíky

PROTECT ENTERPRISE ON-PREM

Služby pri EDR:

- implementácia
- optimalizácia, konfigurácia pravidiel/výnimiek
- integrácia so SIEM

* očakávame Q4-21

Obráťte sa na nás

V prípade otázok kontaktujte:

- ESET obchodný kontakt
- obchod@eset.sk

SECURITY DAYS

Ďakujem za pozornosť

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™ & SME KONFERENCIE