

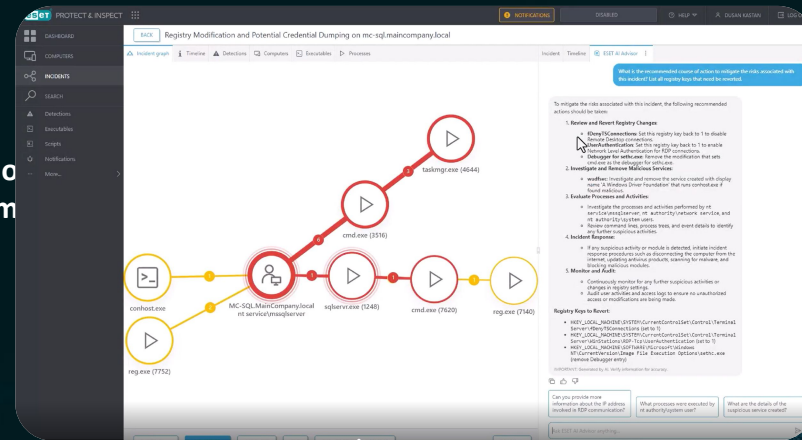
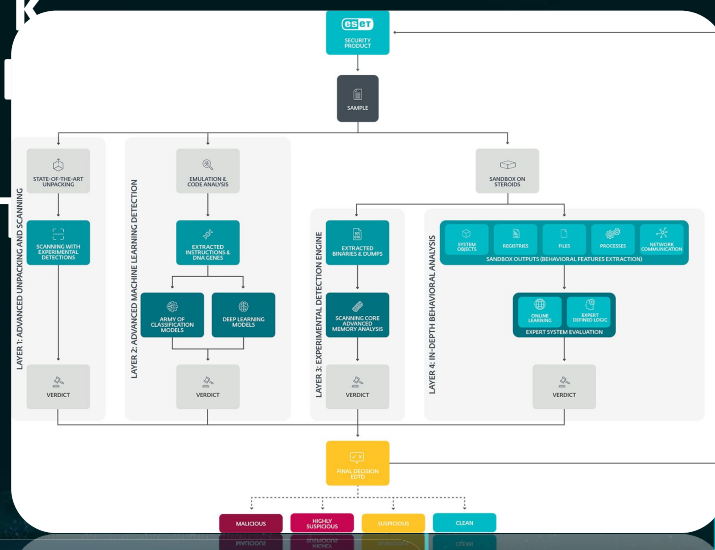
Od incidentu k obnoveniu: moderné trendy v detekcii a reakcii

Július Selecký
Solution Architect



Digital Security
Progress. Protected.

ESET UŽ DESAŤROČIA PATRÍ K LÍDROM V POUŽÍVANÍ UMELEJ INTELEGENCIE V OBLASTI KYBERNETICKEJ BEZPEČNOSTI



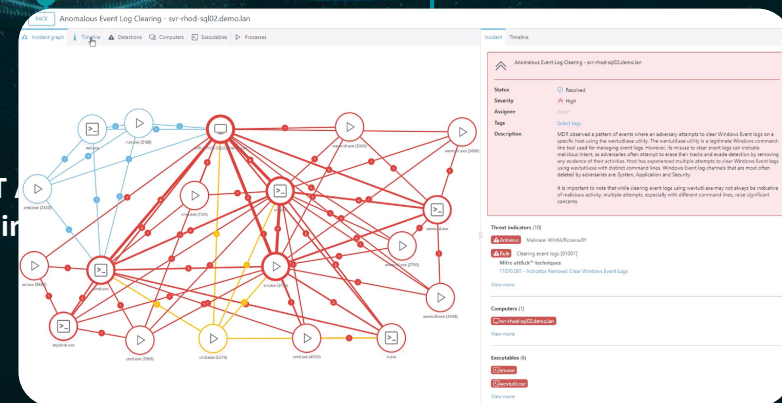
```

text: 00403960 89 9D 94 FE FF FF
text: 00403973 C7 03 07 00 01 00
text: 00403979 FF 05 A4 FE FF FF
text: 0040397F FF 15 A8 E0 42 00
text: 00403985 85 C0
text: 00403987 0F 84 58 01 00 00
text: 0040398D 5A 00
text: 0040398F 6A 0A
text: 00403991 80 85 06 FE FF FF
text: 00403997 50
text: 00403999 48 0C 3F 43 00
text: 0040399D FF 85 A0 FE FF FF
text: 004039A3 FF 15 54 E0 42 00
text: 004039A5 80 47 34
text: 004039AC 39 85 06 FE FF FF
text: 004039B2 75 28
text: 004039B4 68 10 3F 43 00
text: 004039B6 68 28 3F 43 00
text: 004039B8 FF 15 88 E0 42 00
text: 004039C4 50
text: 004039C6 FF 15 44 E0 42 00
text: 004039C8 FF 85 06 FE FF FF
text: 004039D1 FF 85 A0 FE FF FF
text: 004039D3 FF 00
mov     dword ptr [ebx], 1000h
push   [ebp+ProcessInformation.hThread] ; hThread
call   ds!GetThreadContext
test   eax, eax
je      loc_4B3AE5
push   0 ; lpNumberOfBytesRead
push   4 ; nSize
lea     eax, [ebp+Buffer]
push   eax ; lpBuffer
push   433F0C ; lpSourceAddress
push   [ebp+ProcessInformation.hProcess] ; hProcess
call   ds!ReadProcessMemory
mov     eax, [edi+34h]
mov     [ebp+Buffer], eax
cmp     short loc_4B39DC
jnz     offset ProcName ; "ntmapviewoffsection"
push   offset ModuleName ; "ntdll.dll"
call   ds!GetModuleHandleA
push   eax ; hModule
call   ds!GetProcAddress
push   [ebp+Buffer]
push   [ebp+ProcessInformation.hProcess]
call   eax
mov     [ebp+ProcessInformation.hProcess]
mov     [ebp+Buffer]
call   ds!GetProcAddress
mov     eax

```

2019

18

ESET
Machin

2023

2024



ČAS VENUJTE
REÁLNYM
HROZBÁM, NIE
ZBYTOČNÉMU
ŠUMU.





Sila riešenia
ESET Inspect

Hlboký prehľad o tom
Čo, Kde a **Ako**
prebiehajú hrozby a útoky



Poznatky
ESET odborníkov

Špičkoví bezpečnostní
výskumníci ESET zabezpečujú
nepretržitú **24/7**
reakciu na hrozby



ESET MDR

Najlepšie hodnotená
spravovaná bezpečnosť, **ktorá**
vás chráni

**Čas na detekciu a reakciu je
rozhodujúci**

Čas na detekciu a reakciu (MTTR)



Ďakujem za pozornosť



Digital Security
Progress. Protected.