Samodejna klasifikacija in prioritizacija Detekcije

Malware

Severe risk (91), Very high confidence, High criticality

Response Wa

New

Summary Analysis Comments Log

Info and above (default)

Quick actions

Isolate affected device

Scan device

Collect forensics package

More response actions

Elevate to WithSecure

Elevate

Company

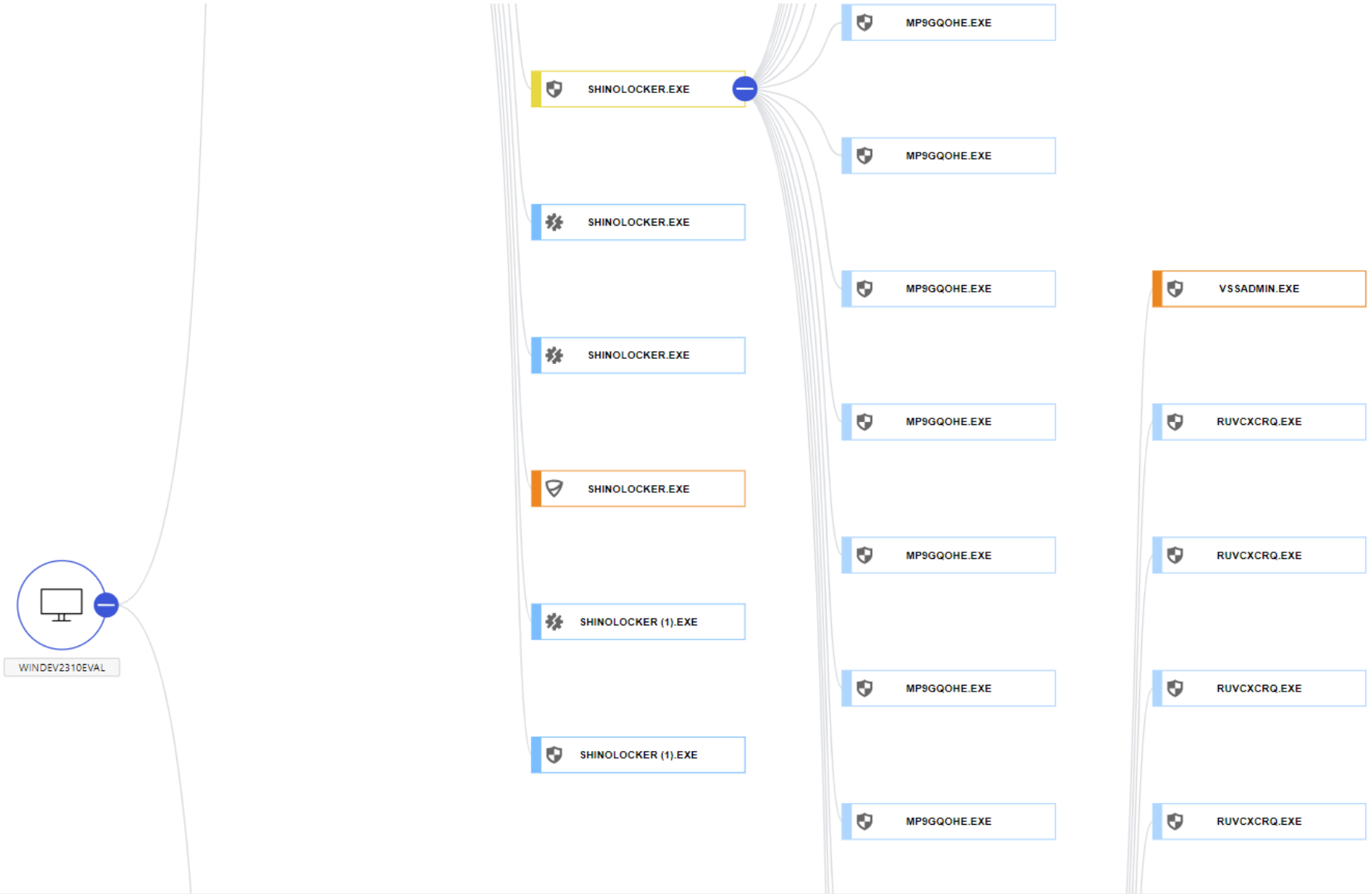
A1 Trainer

Affected devices (1)

WinDev2310Eval

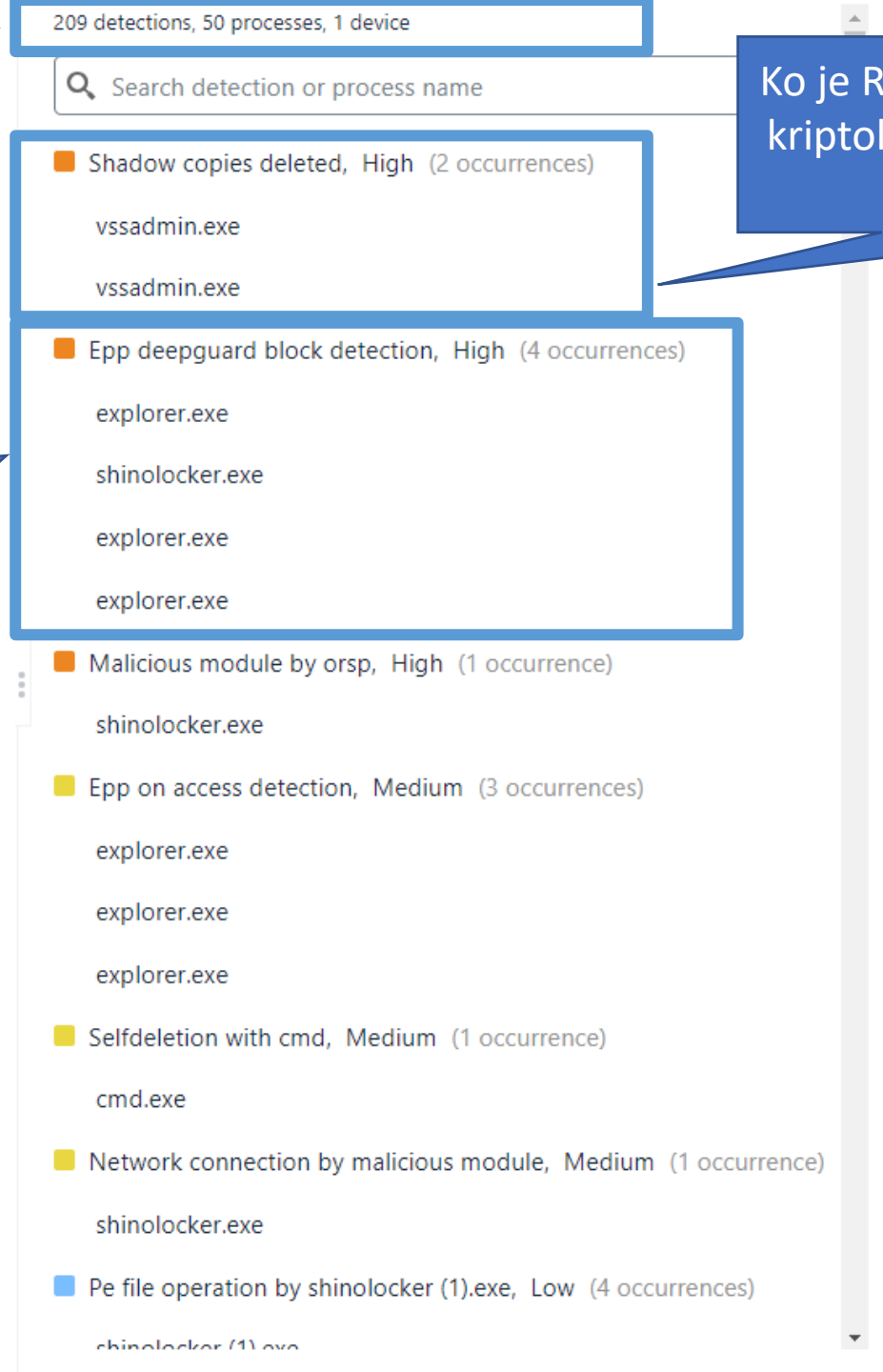
Identical detections (0)

Similar detections (0)



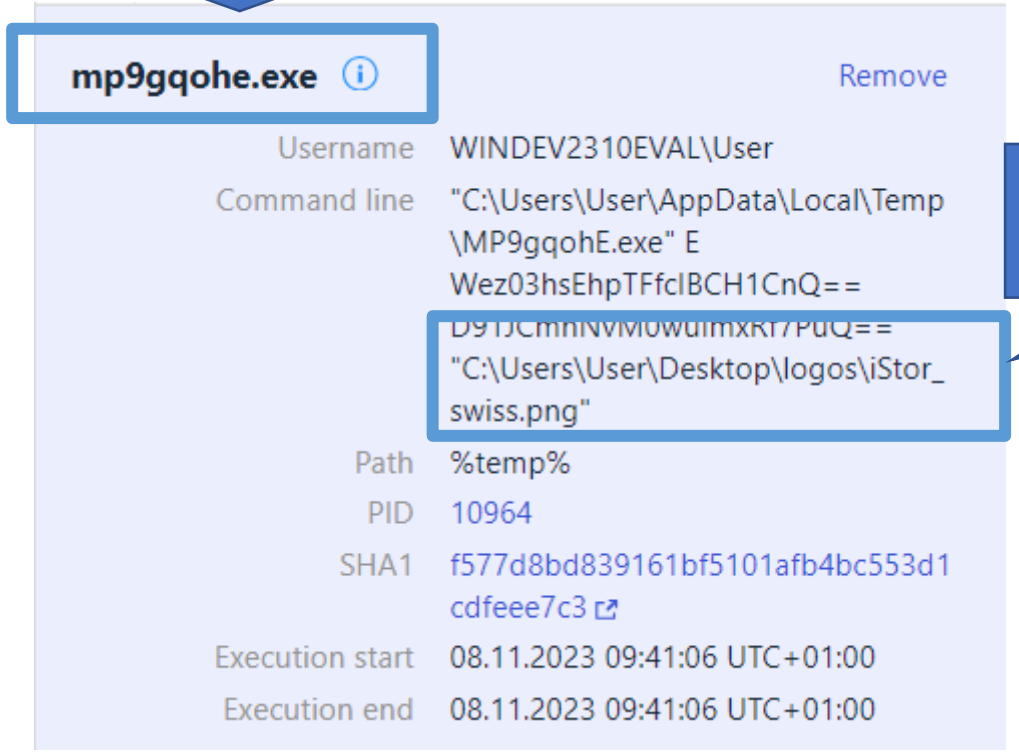
BCD združuje več security eventov v skupen pogled

DeepGuard je pred ugasnitvijo Real-Time Scanninga na EPP delu uspešno blokiral vse kriptoloker poskuse

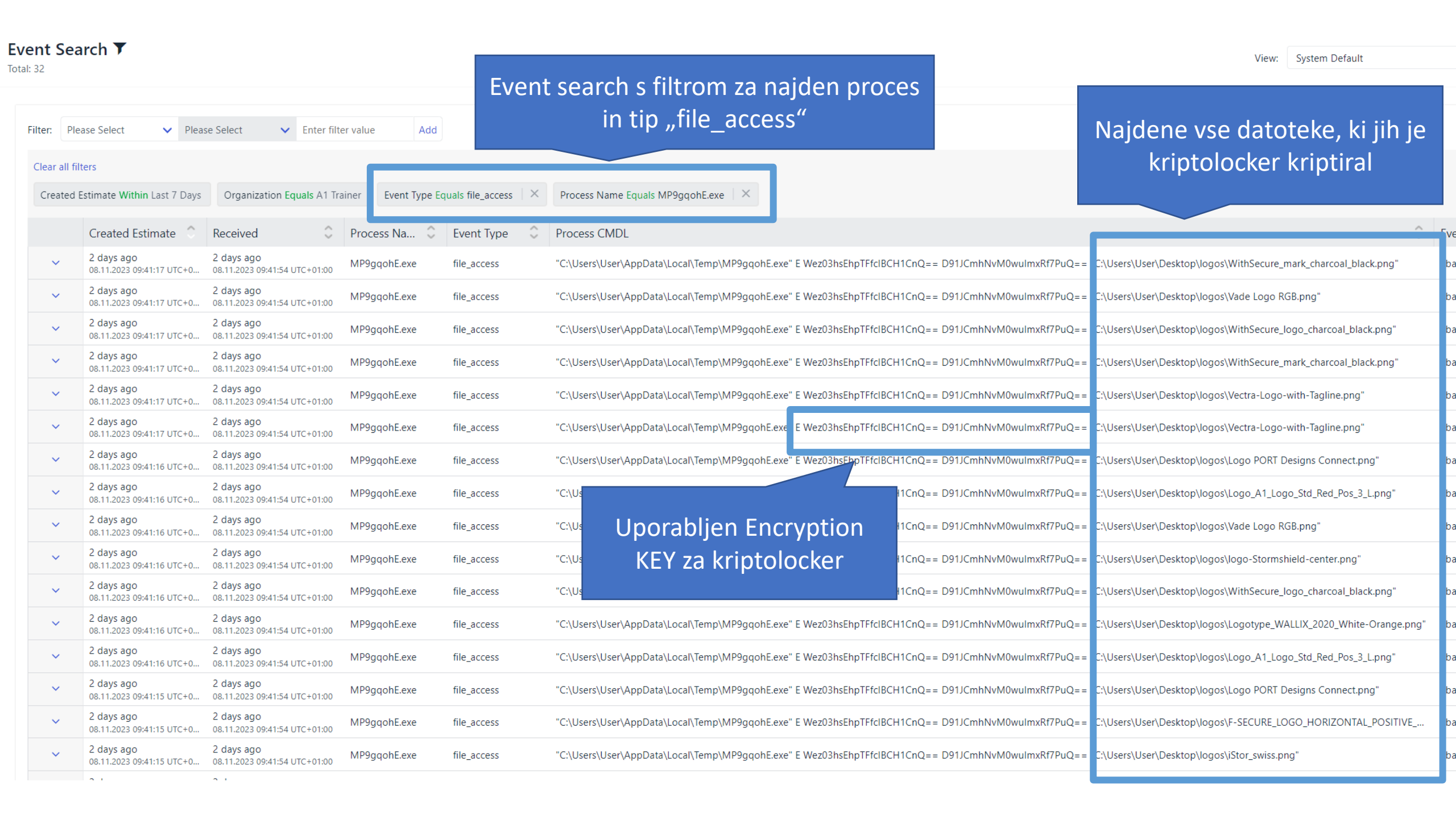


Ko je Real-Time Scan izklopljen, vidimo da je kriptolocker najprej pobrisal shadow copies preko vssadmin

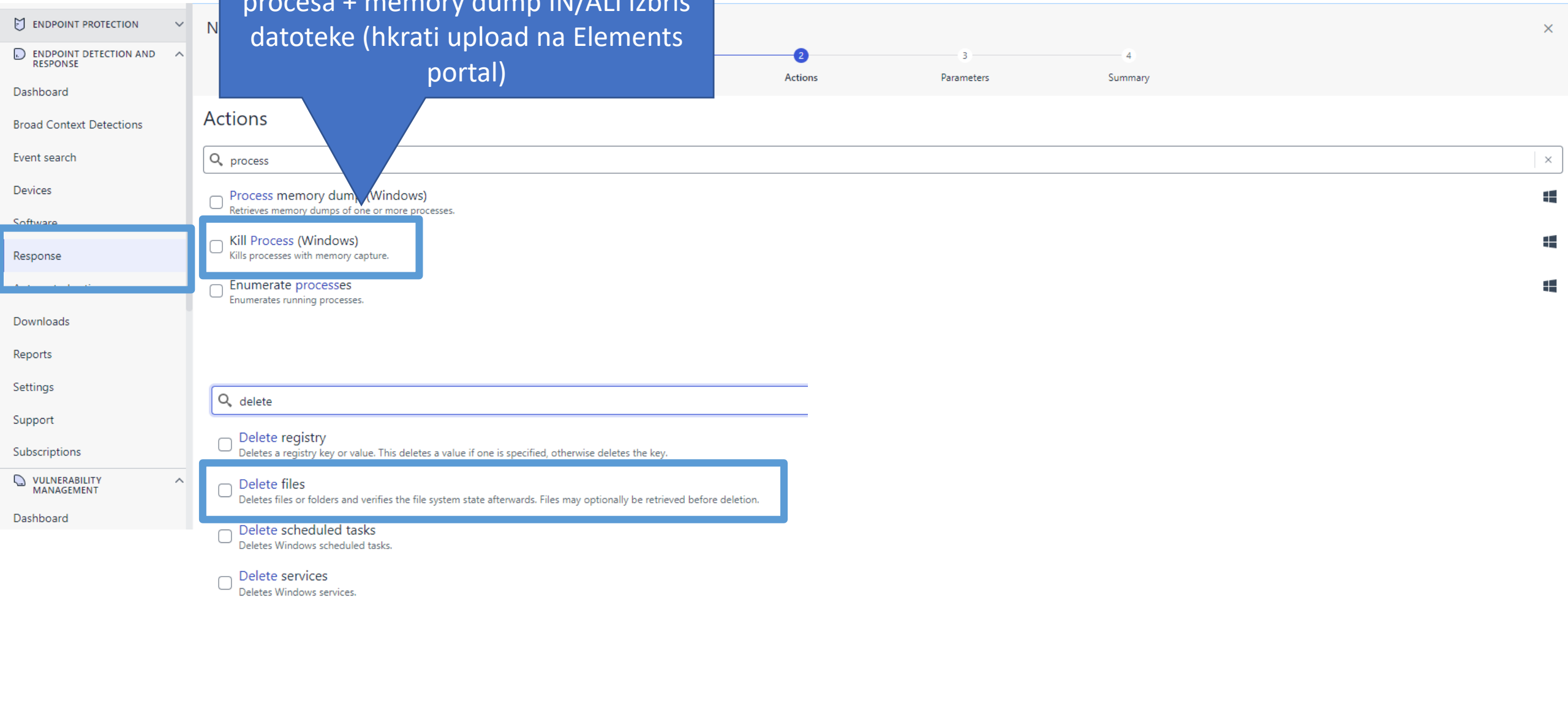
Proces, ki je izvajal kriptiranje

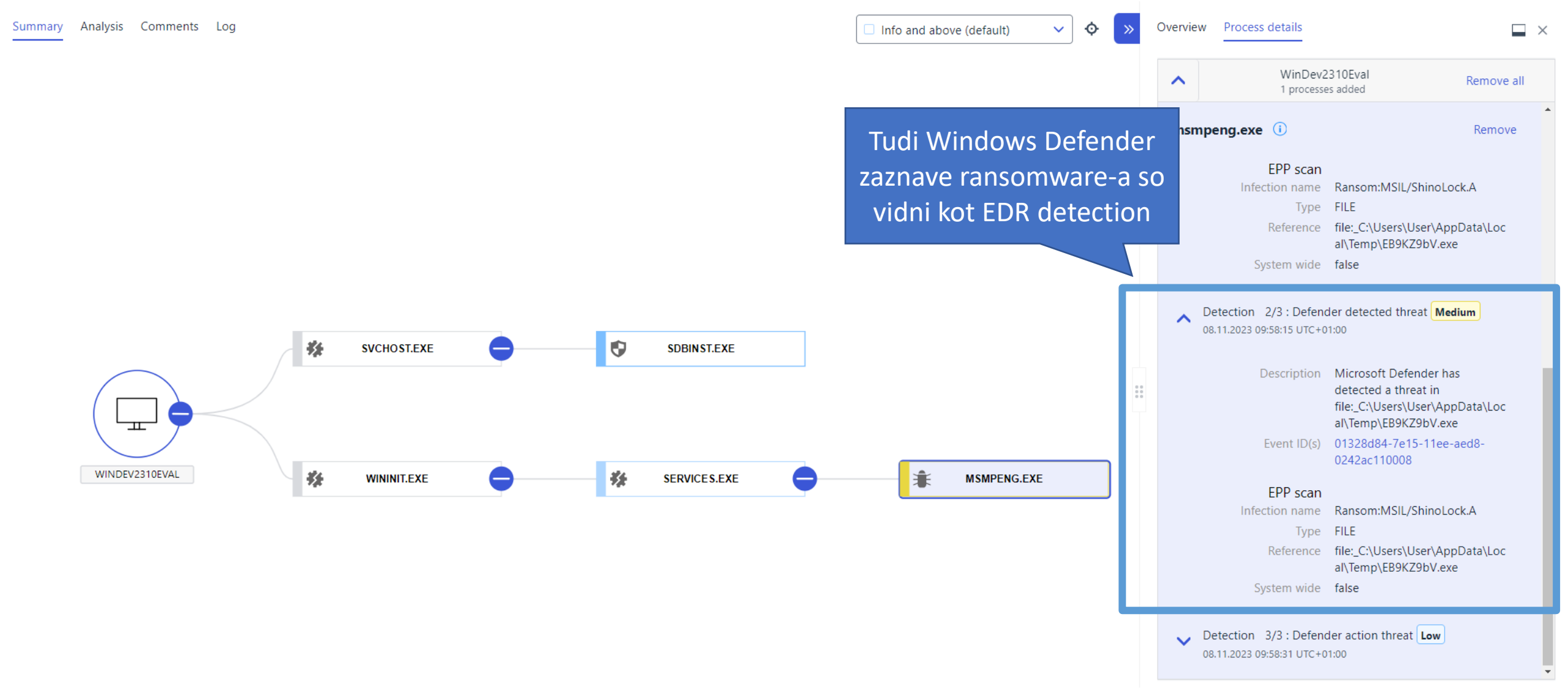


Iz Command line se vidi, katero datoteko je spremenil


Event Search
Total: 32
View: System Default
Event search s filtrom za najden proces in tip „file_access“
Najdene vse datoteke, ki jih je kriptolocker kriptiral
Filter: Please Select Please Select Enter filter value Add
Clear all filters
Created Estimate Within Last 7 Days
Organization Equals A1 Trainer
Event Type Equals file_access
Process Name Equals MP9gqohE.exe
Created Estimate
Received
Process Na...
Event Type
Process CMDL
2 days ago 08.11.2023 09:41:17 UTC+0...
2 days ago 08.11.2023 09:41:54 UTC+01:00
MP9gqohE.exe
file_access
"C:\Users\User\AppData\Local\Temp\MP9gqohE.exe" E Wez03hsEhpTFfcIBCH1CnQ== D91JCmhNvM0wuImxRf7PuQ==
C:\Users\User\Desktop\logos\WithSecure_mark_charcoal_black.png"
C:\Users\User\Desktop\logos\Vade Logo RGB.png"
C:\Users\User\Desktop\logos\WithSecure_logo_charcoal_black.png"
C:\Users\User\Desktop\logos\Vectra-Logo-with-Tagline.png"
C:\Users\User\Desktop\logos\Logo PORT Designs Connect.png"
C:\Users\User\Desktop\logos\Logo_A1_Logo_Std_Red_Pos_3_L.png"
C:\Users\User\Desktop\logos\logo-Stormshield-center.png"
C:\Users\User\Desktop\logos\Logotype_WALLIX_2020_White-Orange.png"
C:\Users\User\Desktop\logos\F-SECURE_LOGO_HORIZONTAL_POSITIVE_...
C:\Users\User\Desktop\logos\iStor_swiss.png"
Uporabljen Encryption KEY za kriptolocker

Ročni odziv na zaznave: zaustavitev procesa + memory dump IN/ALI izbris datoteke (hkrati upload na Elements portal)




Summary
Analysis
Comments
Log
Info and above (default)
Overview
Process details
WinDev2310Eval
1 processes added
Remove all
Tudi Windows Defender zaznave ransomware-a so vidni kot EDR detection
smpeng.exe
Remove
EPP scan
Infection name Ransom:MSIL/ShinoLock.A
Type FILE
Reference file:_C:\Users\User\AppData\Local\Temp\EB9KZ9bV.exe
System wide false
Detection 2/3 : Defender detected threat Medium
08.11.2023 09:58:15 UTC+01:00
Description Microsoft Defender has detected a threat in file:_C:\Users\User\AppData\Local\Temp\EB9KZ9bV.exe
Event ID(s) 01328d84-7e15-11ee-aed8-0242ac110008
EPP scan
Infection name Ransom:MSIL/ShinoLock.A
Type FILE
Reference file:_C:\Users\User\AppData\Local\Temp\EB9KZ9bV.exe
System wide false
Detection 3/3 : Defender action threat Low
08.11.2023 09:58:31 UTC+01:00
WINDEV2310EVAL
SVCHOST.EXE
SDBINST.EXE
WININIT.EXE
SERVICES.EXE
MSMPENG.EXE