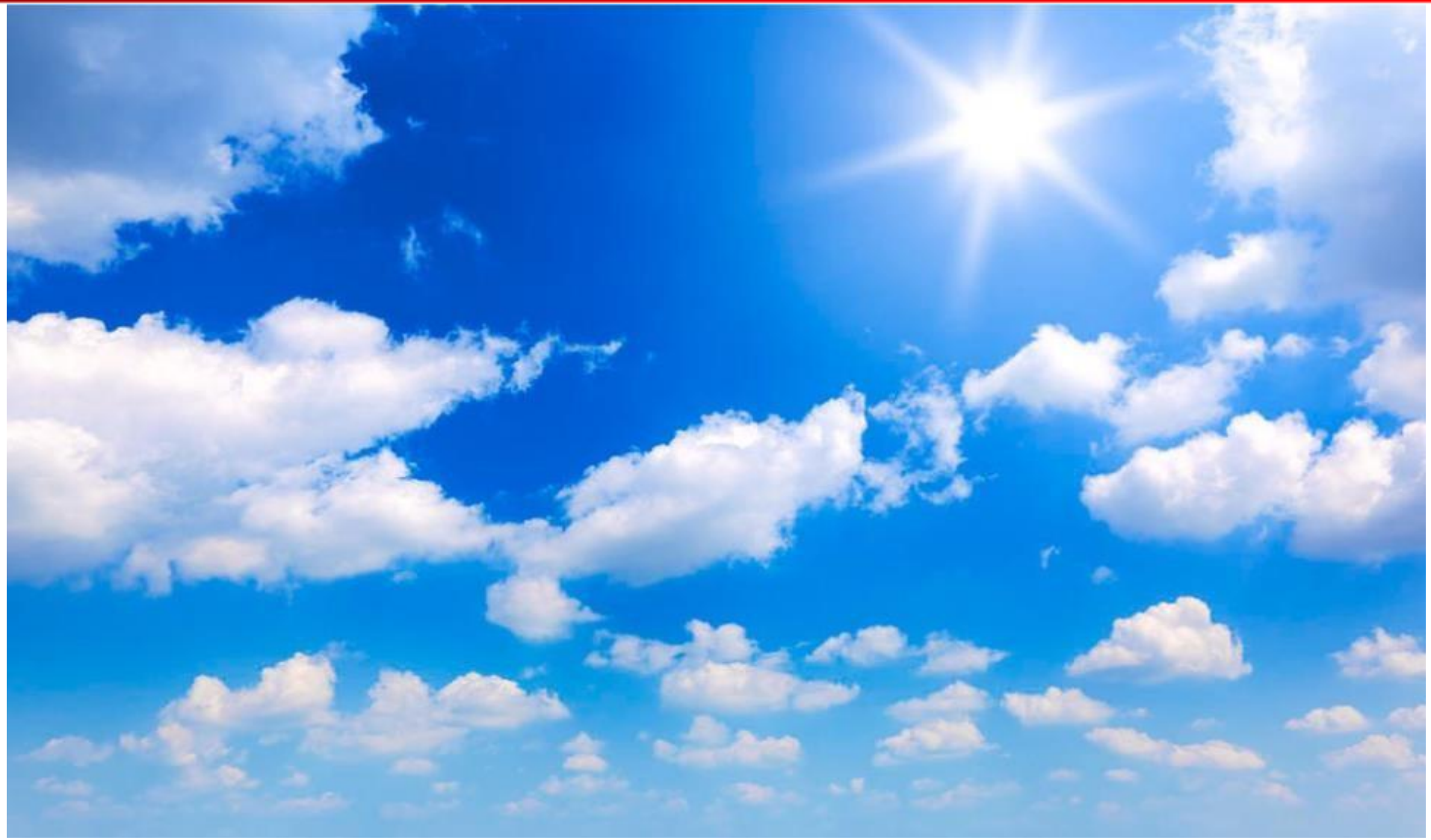
Cyber Security
Lession 4



Labs

Assignments

Užduotis - Create Risk register

Due today at 5:30 PM

Points
10 points possible

Instructions

Remiantis Teorines paskaitos Nr.02 medžiaga, sukurti Rizikų registrą su ne mažiau kaip 10 skirtingų rizikų (teigiamų ir neigiamų - santykis nesvarbus). Rizikas įvertinti kokybiniu analizės metodu. Bonus taškai (respect), jeigu ir kiekybiniu bus pvz.

Rizikų registre, kiekvienai rizikai, turi būti pateikta tokia informacija:
1. Cause/priežastis.
2. Event (Risk)/įvykis (rizika).
3. Effect / padariniai (efektas).
4. Probability/tikimybė (1-8).
5. Impact/poveikis (1-10).
6. Value (Probability x impact) / Vertė (tikimybė x poveikis).
7. Risk Tolerance / Rizikos tolerancija.

Praktinį darbą atlikti remiantis pateiktu rizikų registro šablonu ir pavyzdžiu.

Turite laiko iki 2025-04-04.

Įkelti failus, dokumentus, reikia, paspaudus apačioje:
"Užduotis - Create Risk register (25 03 26 Kiber NF OV)"

Rekomenduojama PDF formatu.

11 Students – Turned in

Labs

Assignments

Sukurto rizikų registro papildymas veiksmais/priemonėmis

Due April 7, 2025 5:30 PM

Instructions

Remiantis Teorinės paskaitos Nr. 3 medžaga, papildyti Rizikų registrą prevenciniais ir atgrasymo veiksmais ar priemonėmis.

Praktinį darbą atlikti remiantis pateiktu papildytu rizikų registro šablonu ir pavyzdžiu.

Cause	Event (risk)	Effect	Probability (1-8)	Impact (1-10)	Value (probability x impact)	Preventative actions (tools)	Deterrent actions (tools)
Because there are no team lead	Module will be developed poorly with many security issues	More time for testing and bug fixing, more possibilities and time to use for hacking	2	7	14		

Student work

Untitled quiz (25 03 26 Kiber NF OV) ...

3 Students – Turned in
8 Students – Viewed
x Students – Not turned in

Labs

Cause	Event (risk)	Effect	Probability (1-8)	Impact (1-10)	Value (probability x impact)	Preventative actions (tools)	Deterrent actions (tools)
Because there are no team lead	Module will be developed poorly with many security issues	More time for testing and bug fixing, more possibilities and time to use for hacking	2	7	14		

Preventative Actions: Regular Cybersecurity Trainings, Phishing simulations, Password change policy, Security Audits, Policies renew, OS and Software updates, Allow only VPN connection

Deterrent: Firewall, 2FA activation, Trainings about sensitive data, Monetary losses, Penalties, Activity Monitoring

Tools: Firewall, Antivirus>Security, VPN client, CTV, DLP, IPS, IDS, Access Control System, PAM

Labs

Assignments

Cause/priežastis	Event (Risk)/įvykis (rizika)	Effect / padariniai (efektas)	Probability/tikimybė (1-8)	Impact/poveikis (1-10)	Value (Probability x impact) / Vertė (tikimybė x poveikis)	Risk Tolerance / Rizikos tolerancija	Preventative actions (tools) / Prevenciniai veiksmai (priemonės)	Deterrent actions (tools) / atgrasantys veiksmai (priemonės)

Labs

Assignments

Effect / padariniai (efektas)	Probability/tikimybė (1-8)	Impact/poveikis (1-10)	Value (Probability x impact) / Vertė (tikimybė x poveikis)	Risk Tolerance / Rizikos tolerancija	Preventative actions (tools) / Prevenciniai veiksmai (priemonės)	Deterrent actions (tools) / atgrasantys veiksmai (priemonės)
Įsilaužimas į serverius ir kompiuterius	4	7	28	25	Įdarbinti Cyber Security specialistą arba samdyti MDR/SOC paslaugas teikiančią įmonę	Informacinių grėsmių valdymas su XDR ir SIEM įrankiais
Finansiniai nuostoliai, įmonės veiklą ribojančios kardomosios priemonės	3	5	15		Samdyti teisės paslaugas teikiančią įmonę	Parengti/atnaujinti pagal galiojančius teisės aktus aktualią teisinę dokumentaciją
Darbo prastovos ir finansiniai nuostoliai	5	8	40		Serverinės patalpos duryse įmontuoti užraktą	Prie serverinės patalpos įrengti vaizdo stebėjimo kamerą
Užšifruoti įmonės dokumentai	3	4	12		Inventorizuoti turtą	Nesaugius kompiuterius pakeisti į naujus
Nuolatinės pajamos ir klientų lojalumas	3	3	9		Atlikti rinkos tyrimą	Pagal tyrimo išvadas priimti sprendimus
Išauga pardavimai, didesnis pelnas	2	5	10		Sandėliavimo patalpų paieška	Surasti potencialius didmenos pirkėjus

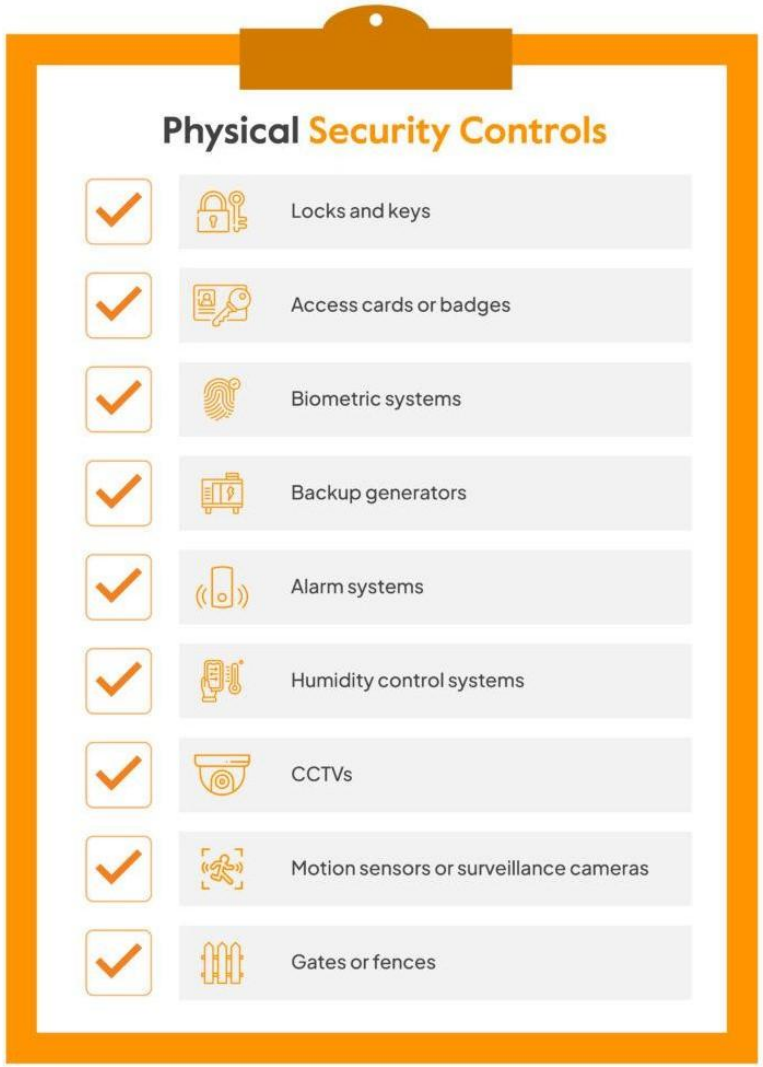
In the previous lession…

Understanding Security Controls

Understanding Security Controls

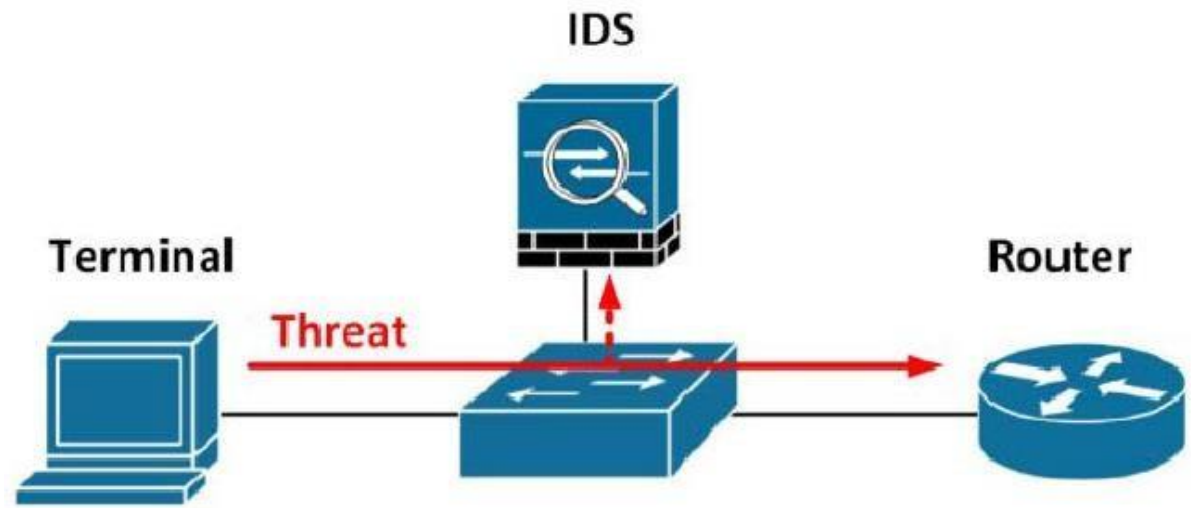
Understanding Security Controls

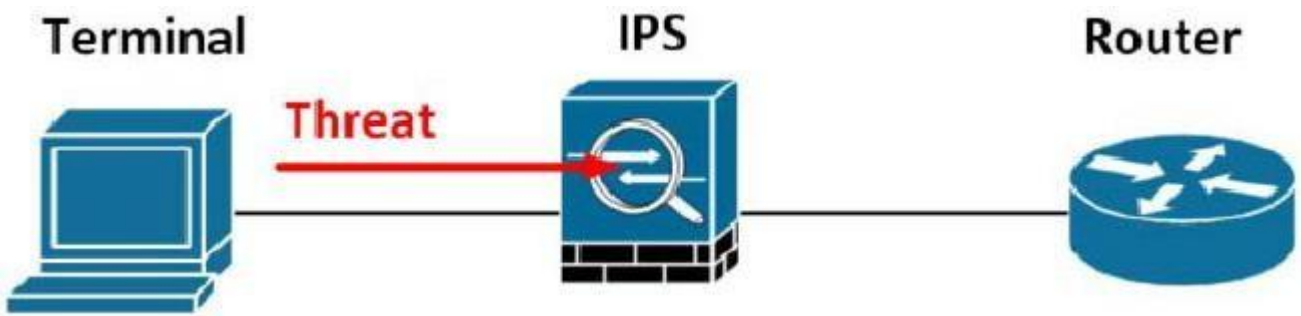
Understanding Security Controls



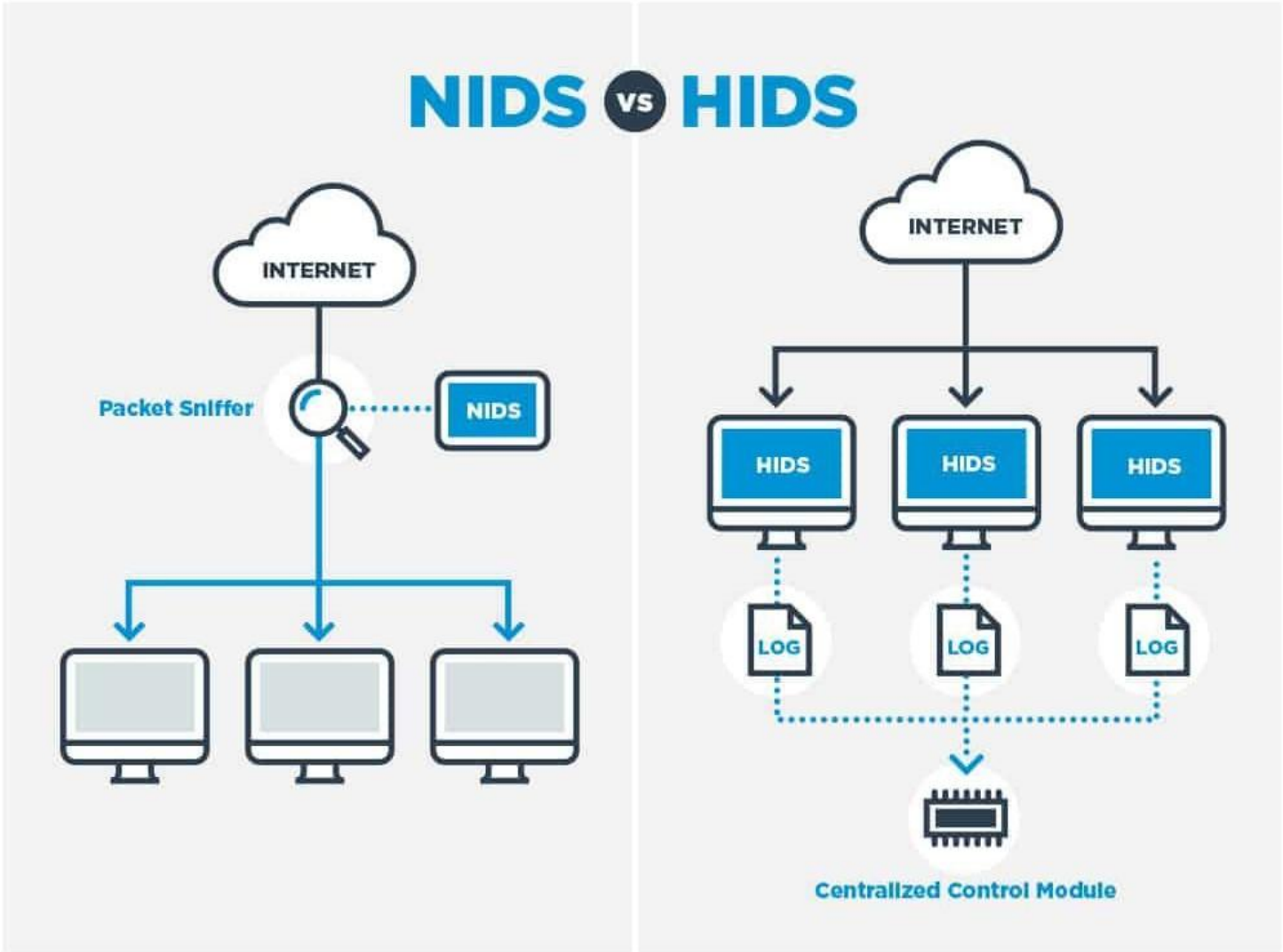
Understanding Security Controls

IDS vs IPS

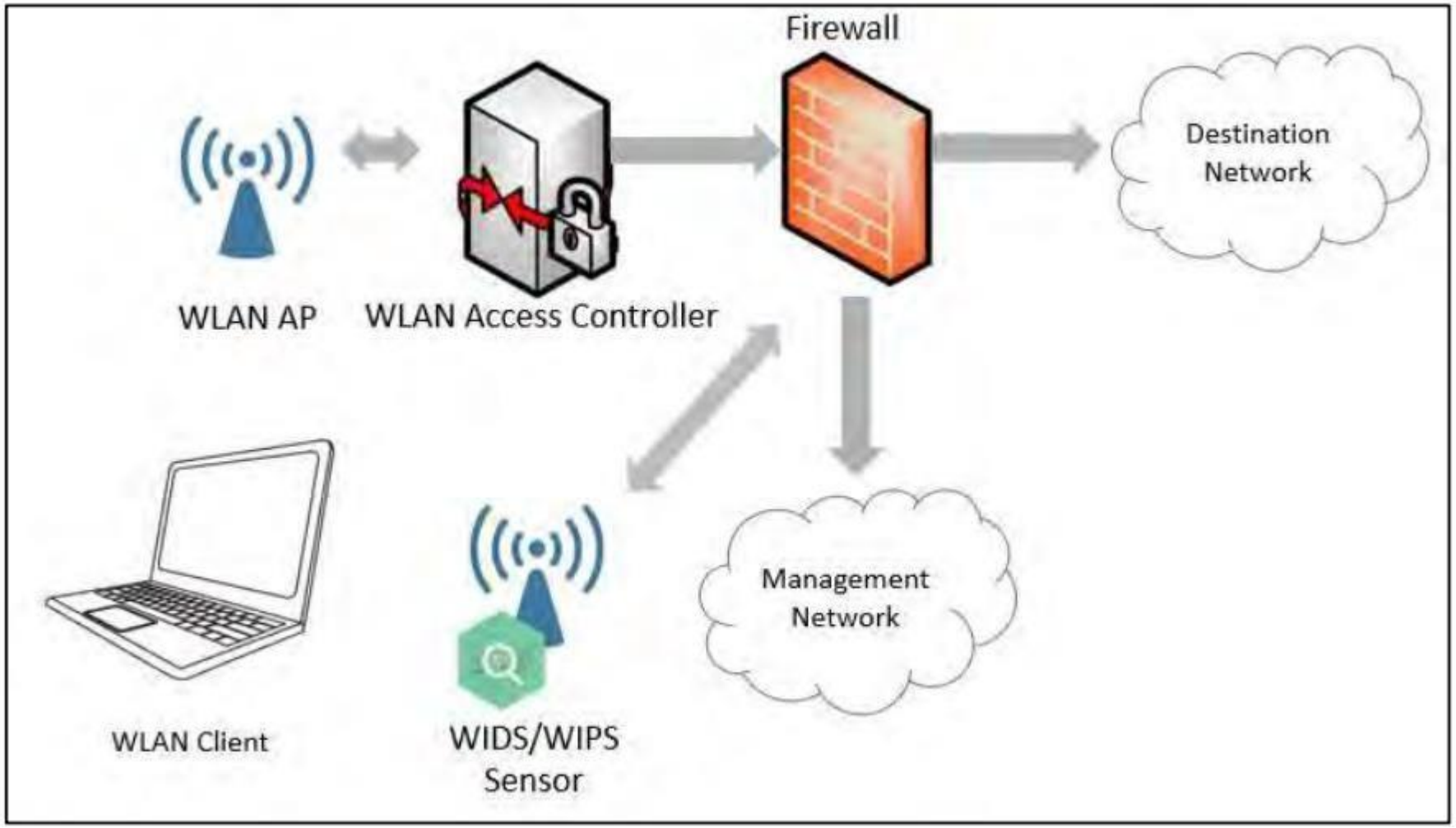




NIDS vs HIDS


NIDS VS HIDS
INTERNET
Packet Sniffer
NIDS
INTERNET
HIDS
HIDS
HIDS
LOG
LOG
LOG
Centralized Control Module

WIDS/WIPS


Firewall
Destination Network
WLAN AP
WLAN Access Controller
Management Network
WLAN Client
WIDS/WIPS Sensor

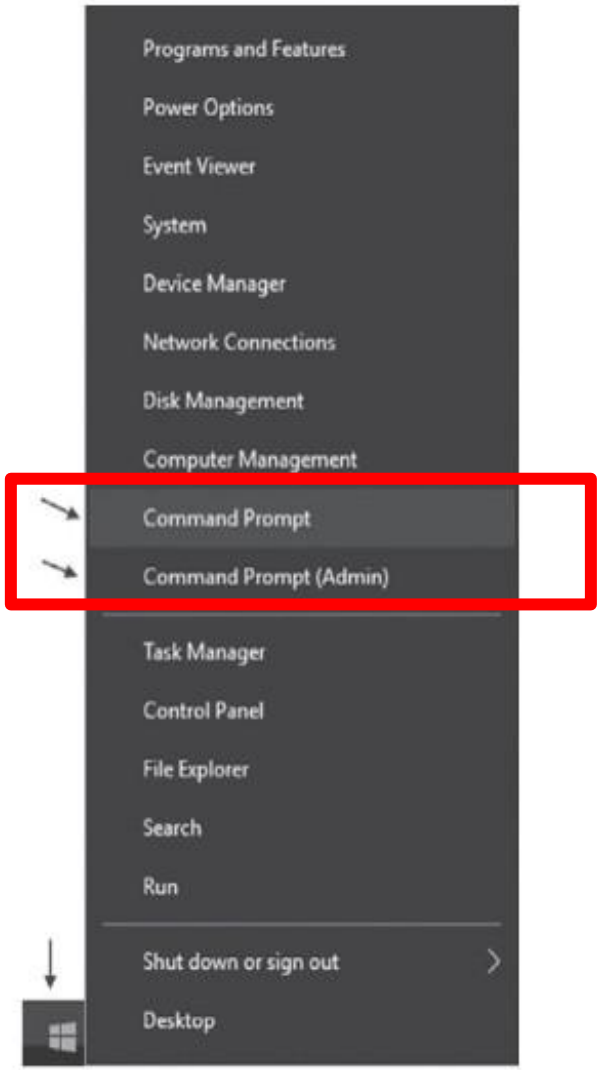
Introduction

- Understanding Core Security Goals DONE
- Introducing Basic Risk Concepts DONE
- Understanding Security Controls DONE
- Using Command-Line Tools
- Understanding Logs

Using Command-Line Tools

Using Command–Line Tools

- Windows
  - Launch Command Prompt
  - Launch Command Prompt (Admin)



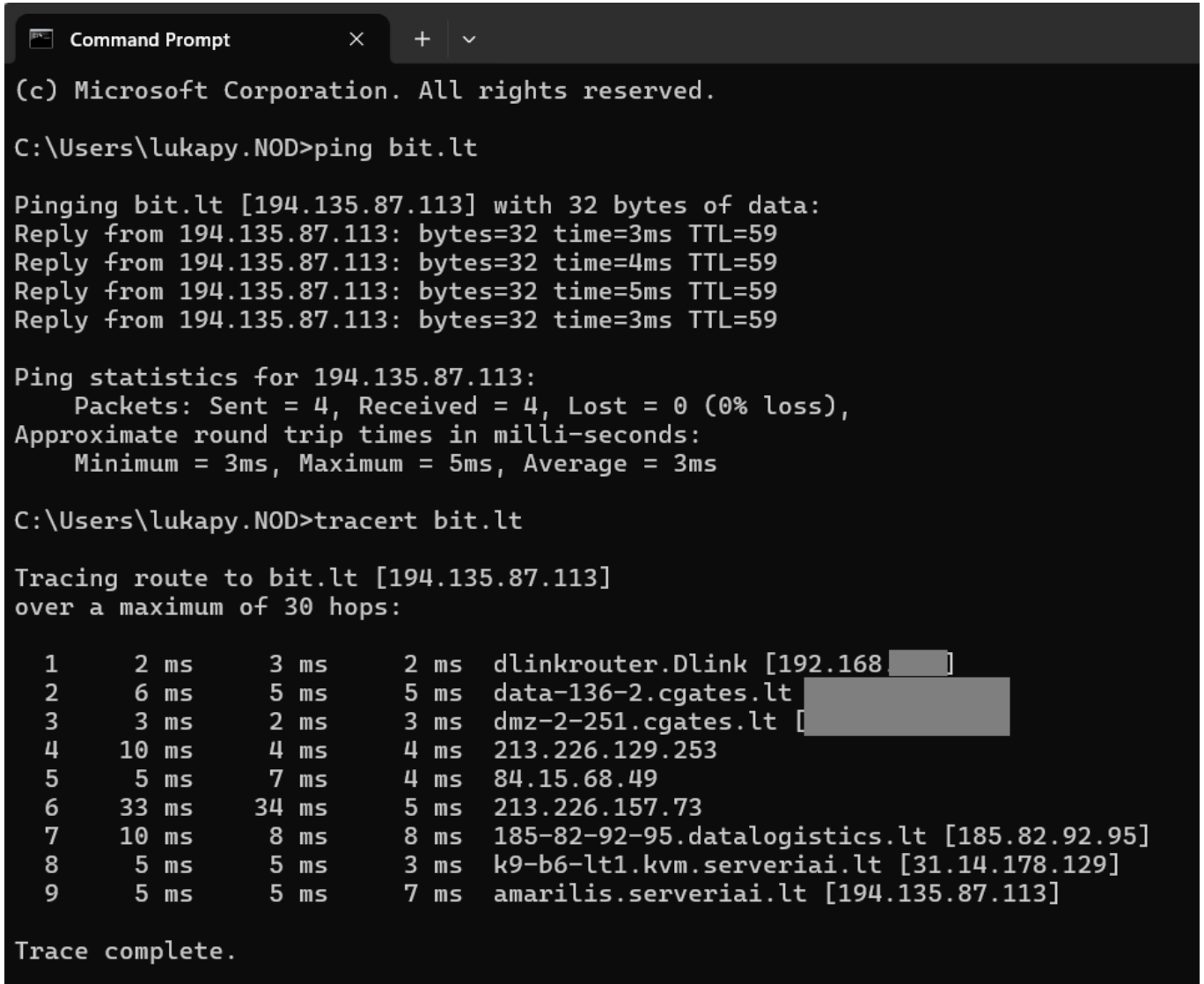
Using Command–Line Tools

- Linux
  - Launch terminal in Kali

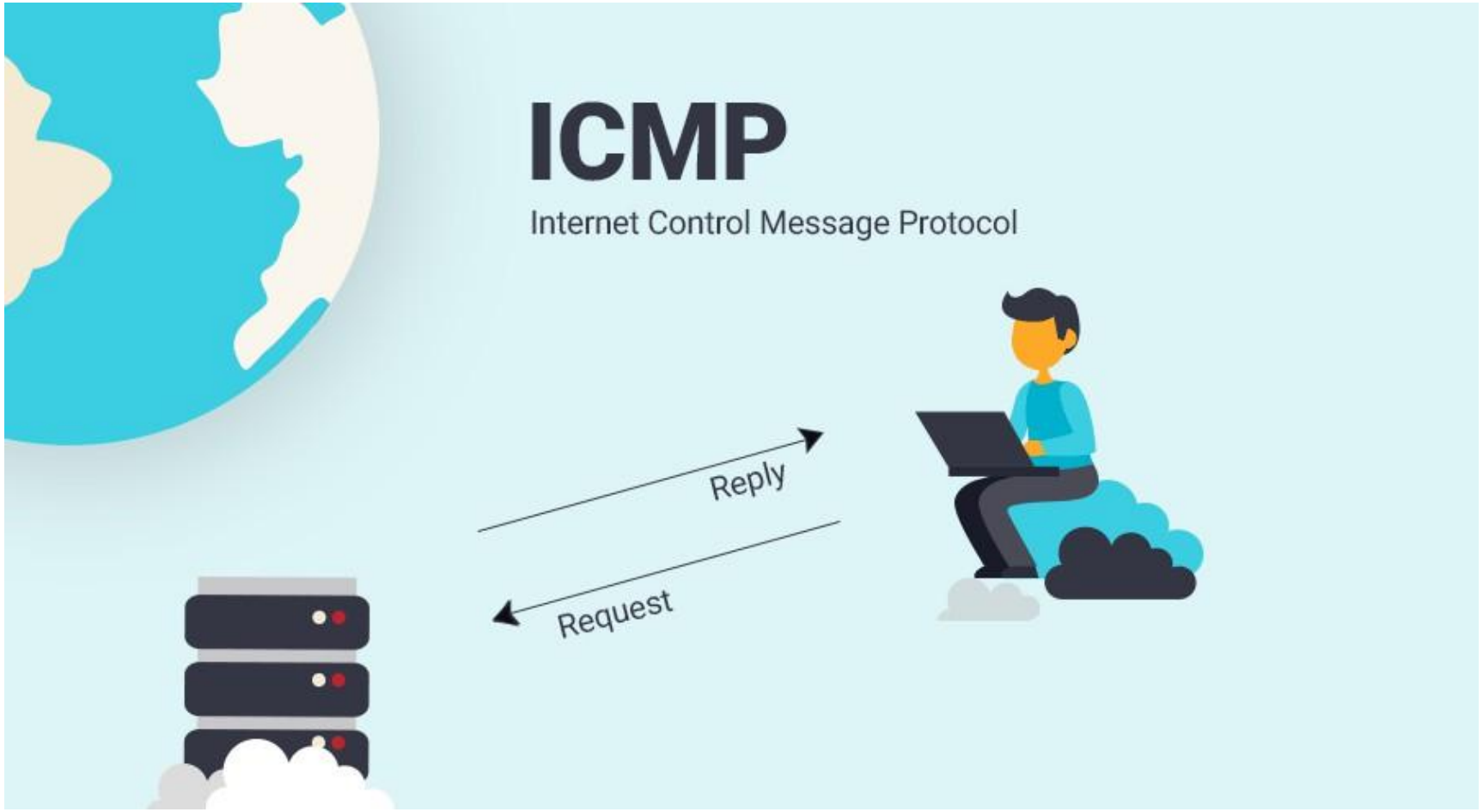
Commands

- Ping
  - Basic command to test connectivity
    - ping 192.168.1.1
    - hping3 192.168.1.1 (hping)
  - Firewalls and ICMP
  - Checking DNS name resolution

Commands


Command Prompt
(c) Microsoft Corporation. All rights reserved.
C:\Users\lukapy.NOD>ping bit.lt
Pinging bit.lt [194.135.87.113] with 32 bytes of data:
Reply from 194.135.87.113: bytes=32 time=3ms TTL=59
Reply from 194.135.87.113: bytes=32 time=4ms TTL=59
Reply from 194.135.87.113: bytes=32 time=5ms TTL=59
Reply from 194.135.87.113: bytes=32 time=3ms TTL=59
Ping statistics for 194.135.87.113:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 5ms, Average = 3ms
C:\Users\lukapy.NOD>tracert bit.lt
Tracing route to bit.lt [194.135.87.113]
over a maximum of 30 hops:
1 2 ms 3 ms 2 ms dlinkrouter.Dlink [192.168.
2 6 ms 5 ms 5 ms data-136-2.cgates.lt
3 3 ms 2 ms 3 ms dmz-2-251.cgates.lt [
4 10 ms 4 ms 4 ms 213.226.129.253
5 5 ms 7 ms 4 ms 84.15.68.49
6 33 ms 34 ms 5 ms 213.226.157.73
7 10 ms 8 ms 8 ms 185-82-92-95.datalogistics.lt [185.82.92.95]
8 5 ms 5 ms 3 ms k9-b6-lt1.kvm.serveriai.lt [31.14.178.129]
9 5 ms 5 ms 7 ms amarilis.serveriai.lt [194.135.87.113]
Trace complete.

ICMP



ICMP

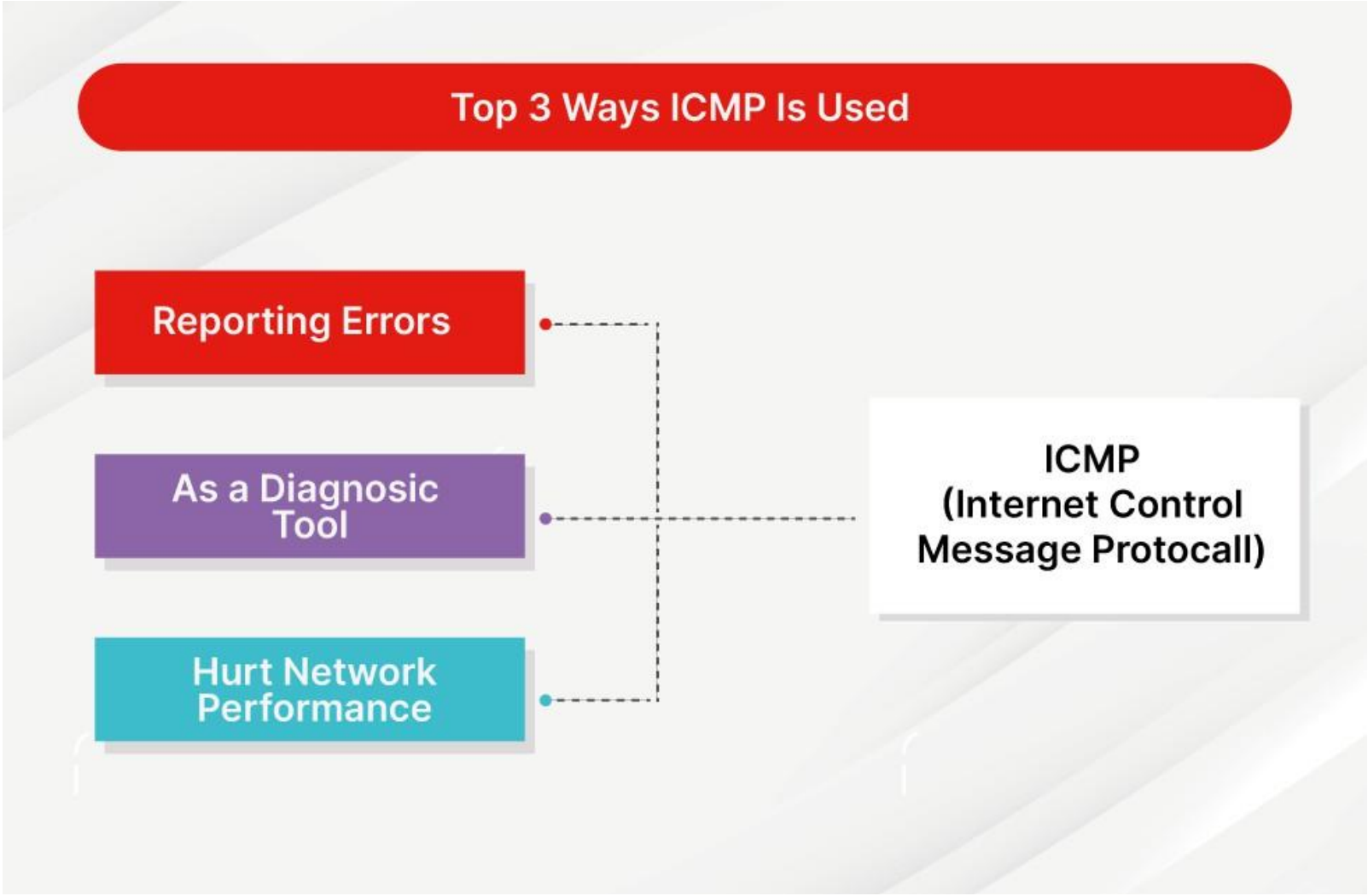
- Internet Control Message Protocol (ICMP) is **used for reporting errors and performing network diagnostics**.
- In the error reporting process, ICMP sends messages from the receiver to the sender when data does not come though as it should.
- **ICMP has no concept of ports**, as TCP and UDP do, but instead uses types and codes. Commonly used ICMP types are echo request and echo reply (used for ping) and time to live exceeded in transit (used for traceroute).

ICMP protocol messages types :

1.Error-reporting messages: In this router will have encounter a problem when it gets processed the IP packet the user will get a message.

2.Query messages: This is one type of message which helps the host to get information of another host. If you have a client and a server, clients want to know whether the server is going for live or not. That time it sends the ICMP message so that it can get the confirmation.

ICMP


Top 3 Ways ICMP Is Used
Reporting Errors
As a Diagnosic Tool
Hurt Network Performance
ICMP (Internet Control Message Protocall)

ICMP

- Internet Control Message Protocol (ICMP) is **used for reporting errors and performing network diagnostics**.
- In the error reporting process, ICMP sends messages from the receiver to the sender when data does not come though as it should.
- **ICMP has no concept of ports**, as TCP and UDP do, but instead uses types and codes. Commonly used ICMP types are echo request and echo reply (used for ping) and time to live exceeded in transit (used for traceroute).

The error-reporting messages are classified into categories :

1.Destination unreachable: When the packet data does not reach the destination at that time, it's called destination unreachable. If the sender sends a message, it will not reach the destination that time the intermediate router will report.

2.Source Quench: In this, there is no flow of control mechanism that works; while sending the packet to send, do not think whether the receiver is ready to receive those packets or not. In this case, ICMP provides the feedback. Sometimes sender sends the packet in a higher rate which the router will not handle and make this situation proper source quench convey the sender to send the packet in a lower price.

3.Time exceeded: Sometimes the situation becomes like this in that many routers are between sender and receiver. The sender usually sends the packet then it gets to move to the routing loop. Time will get exceeded depending on the time-to-live value. The value will decrease as soon as the packet traverses through the router that time. When the router gets discarded, that time will get exceeded compared to the original one.

4.Parameter problem: Usually, the destination host needs to send the parameter problem message when the parameters are not set properly.

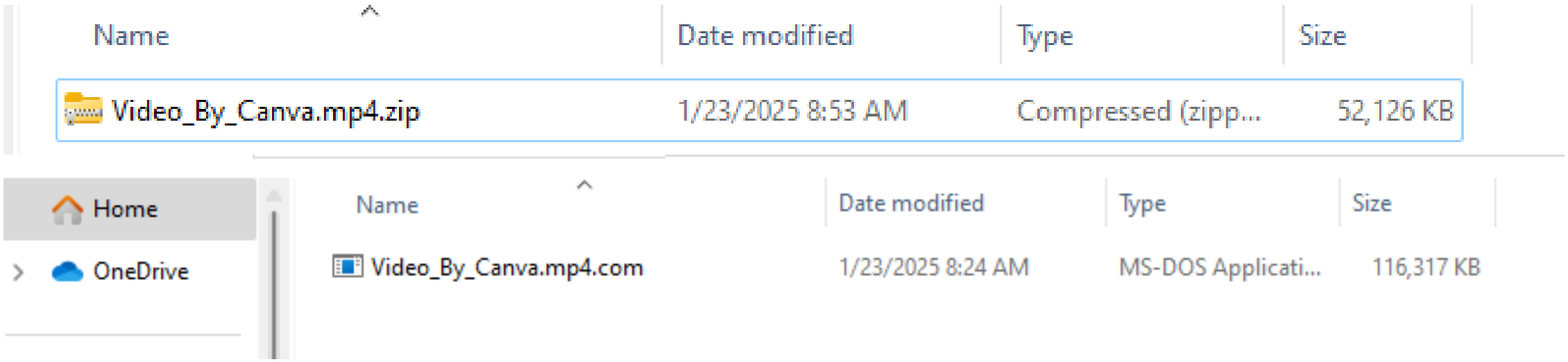
5.Redirection: As soon as packet gets sent the routing table gets updated and the user gets the redirection message.

Commands

- hping3 (hping)
- Ipconfig (Windows)
- Linux :
  - ✓ ifconfig
  - ✓ nmcli dev show | grep 'DNS’
  - ✓ route
- netstat
- tracert (Windows) and traceroute (Linux)
- pathping (Windows) and mtr (Linux)
- arp (-s and -d)

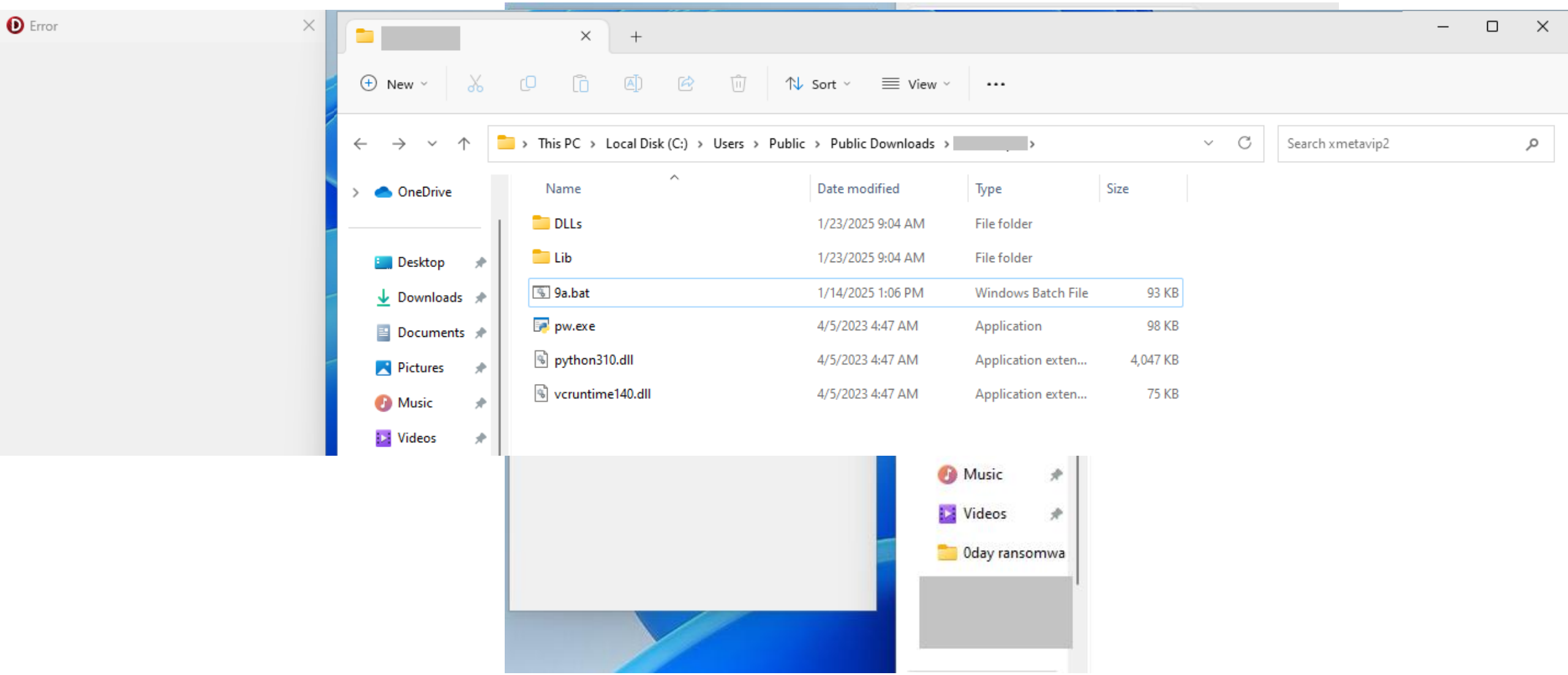
Bonus

ESET Inspect (XDR) matomumas



⚠	Win32/ShellCode.Donut.A	Contained inf...	file:///pw.exe(8900)
⚠	Win32/GenCBL.FNB	Cleaned by d...	file:///C:/Users/MTest/Desktop/25
⚠	MSIL/Agent.DWN	Contained inf...	file:///pw.exe(8900)
⚠	Block execution of known bad files according to LiveGrid	Blocked	C:\Users\MTest\Desktop\250123-1

ESET Inspect (XDR) matomumas



ESET Inspe

High Priority AV Detection [I0100]

Execution of Potentially Malicious Scripts and Credential Theft on w11-zt

Registry Modification and Malware Execution on w11-zt

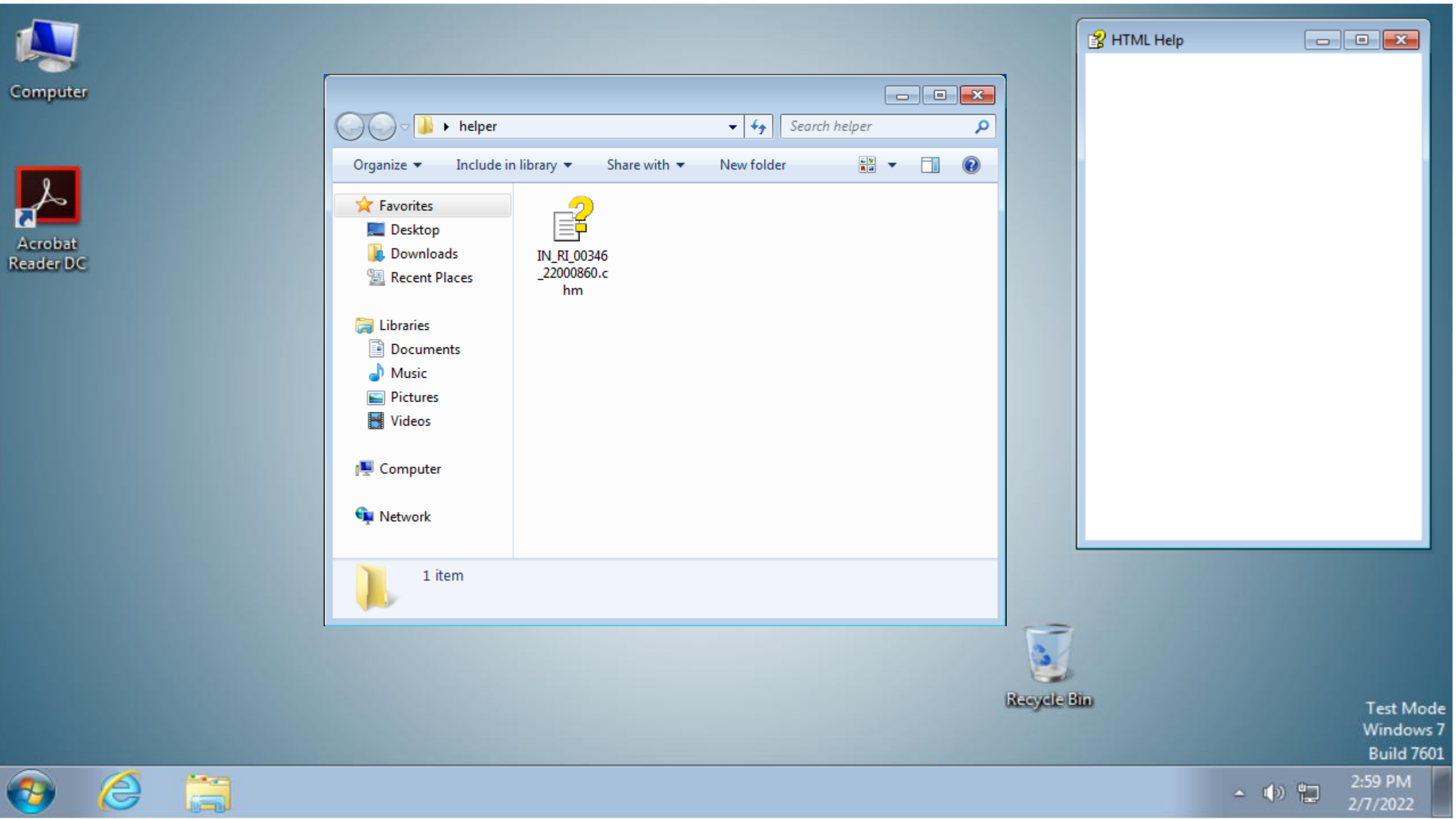
Status	Open
Severity	Medium
Assignee	*None*
Tags	Select tags
Description	On computer w11-zt, user w11-zt\mtest execu PowerShell to modify the Run registry key, adc 'WindowsSecurity' to execute cmd.exe with a s located at C:\Users\Public\Downloads\xmetavi upon login. Additionally, user nt authority\syst executed trusted process svchost.exe to query antivirus products via WMI. Malware Win32/ShellCode.Donut.A was detected and cl after being executed by process pw.exe (PID 8 %HOME%\downloads\xmetavip2\ by user w11 which was initiated from a command in cmd.e: IMPORTANT: Generated by AI. Verify informati accuracy.

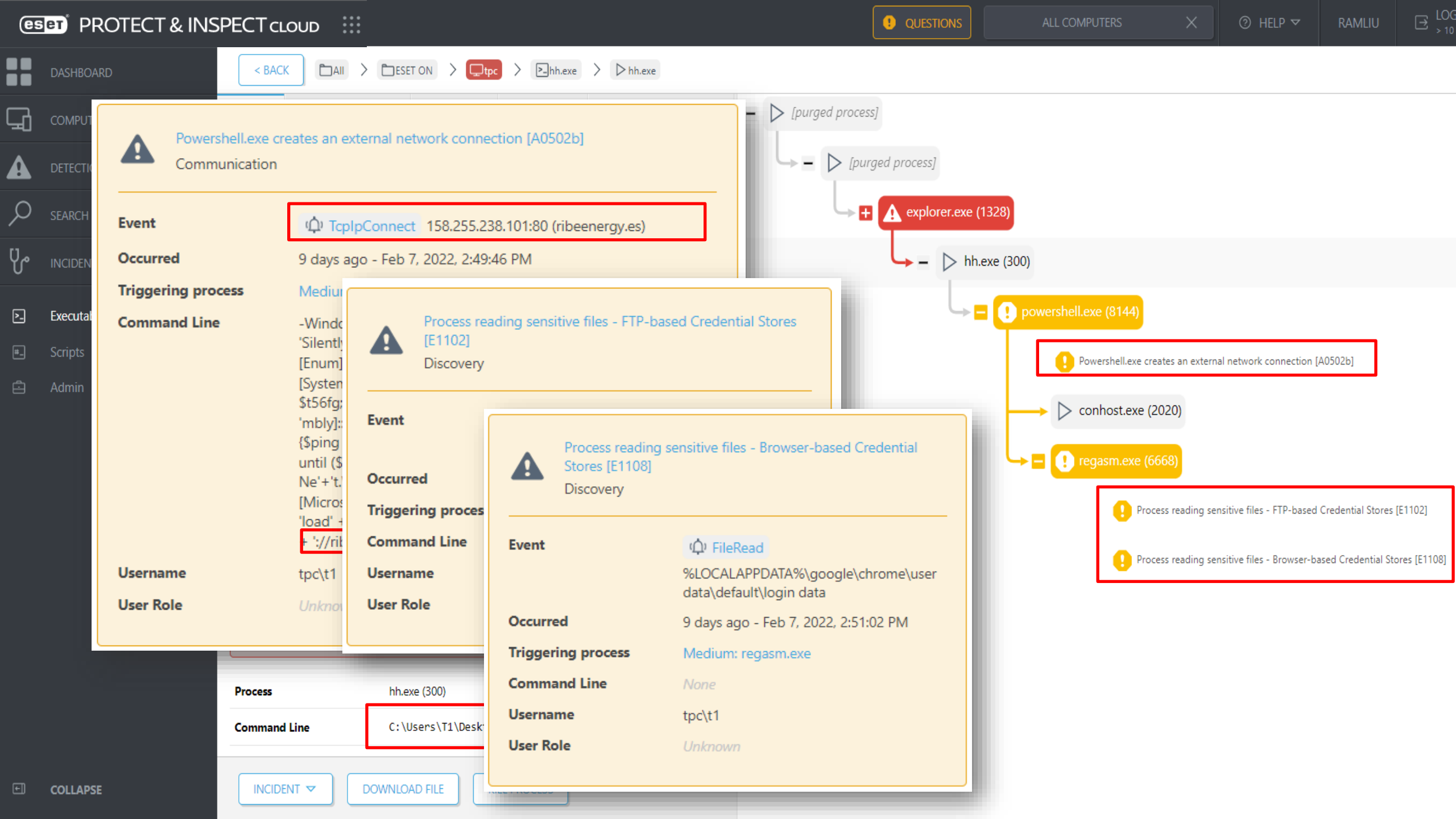
Scheduled Task Creation for Daily Backup on [redacted]

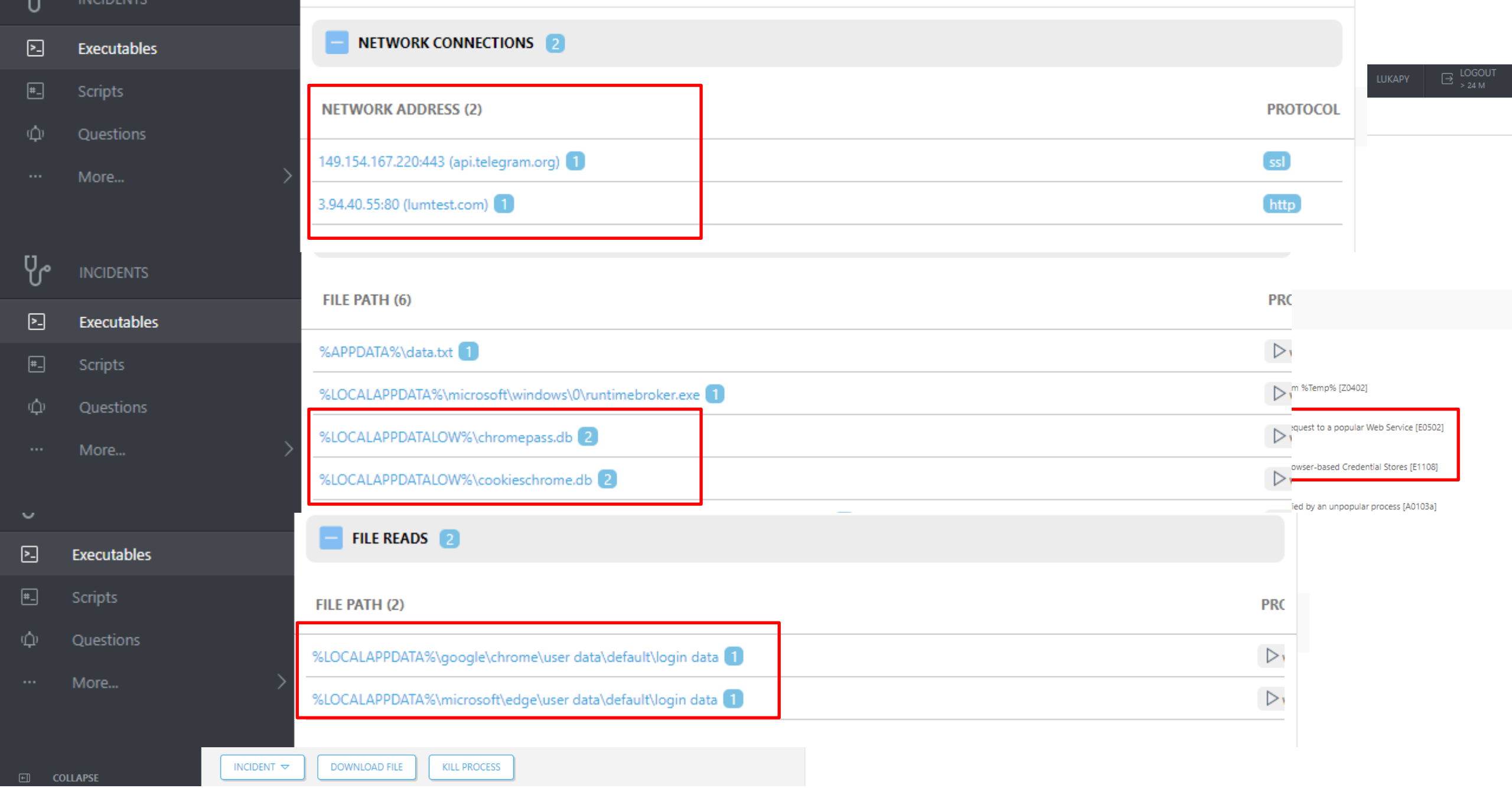
Status	Open
Severity	Medium
Assignee	ESET
Tags	Select tags
Description	User [redacted]\administrator on computer [redacted] created a scheduled task named [redacted] on remote computer [redacted] to run daily at 01:00:00 using schtasks.exe. This task is configured to execute the script located at "C:\Program Files (x86)\[redacted]J.cmd" at the specified time. IMPORTANT: Generated by AI. Verify information for accuracy.
Recommended actions	*None*

from http://ip-api.com/json?fields=8195, indicating further malicious activity.

IMPORTANT: Generated by AI. Verify information for accuracy.

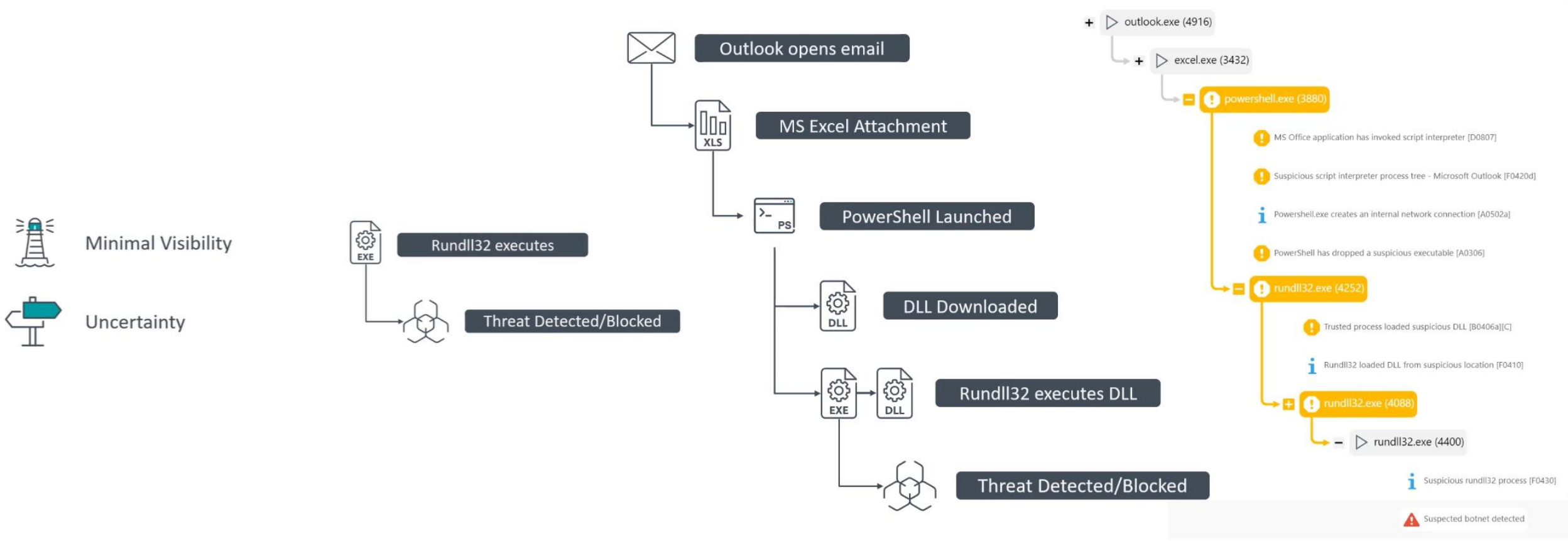

Computer
Acrobat Reader DC
helper
Search helper
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
IN_RI_00346_22000860.chm
1 item
HTML Help
Recycle Bin
Test Mode
Windows 7
Build 7601
2:59 PM
2/7/2022

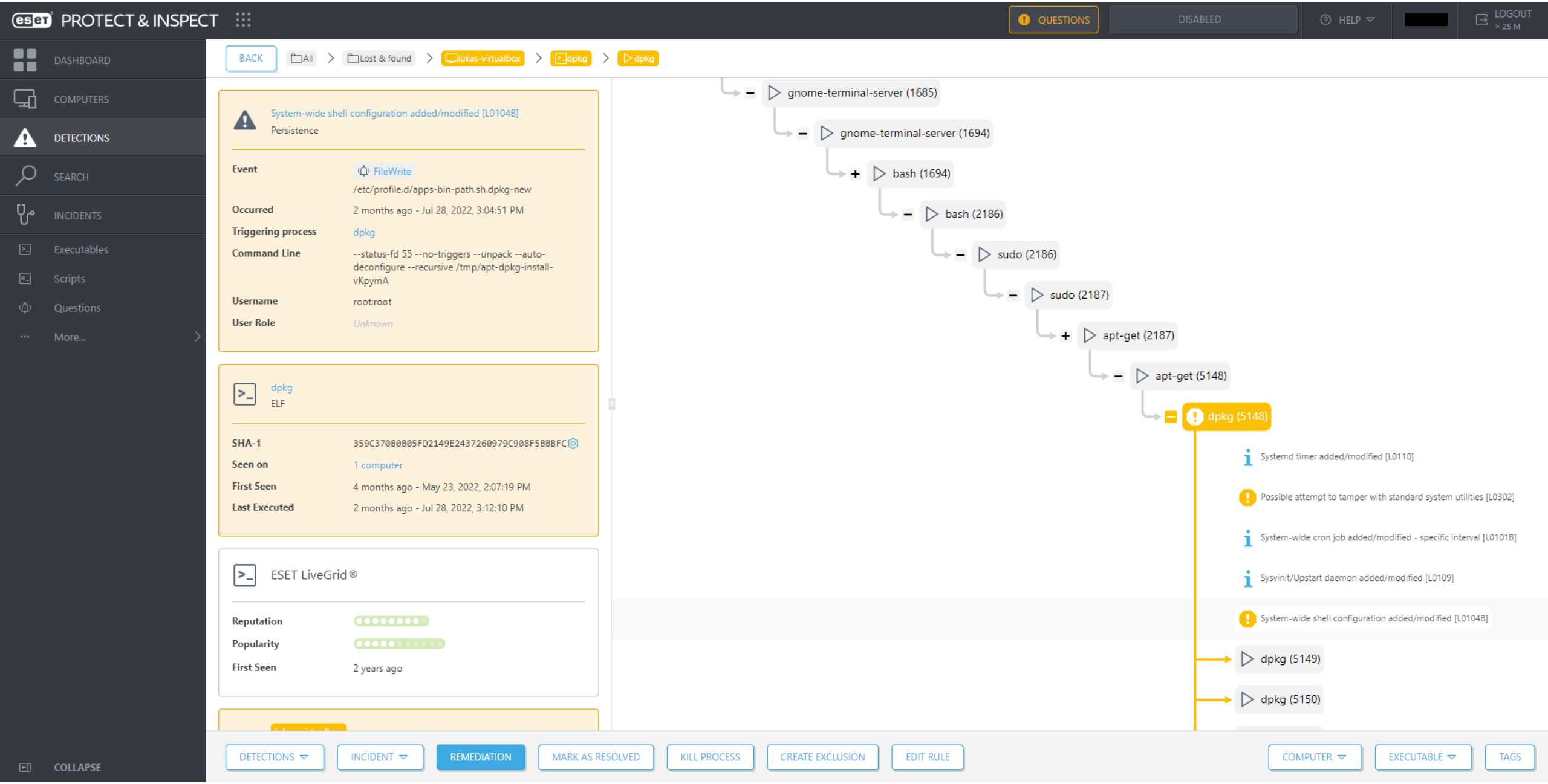

PROTECT & INSPECT CLOUD
QUESTIONS
ALL COMPUTERS
HELP
RAMLIU
DASHBOARD
SEARCH
Executa
Scripts
Admin
COLLAPSE
< BACK
All
ESET ON
tpc
hh.exe
hh.exe
Powershell.exe creates an external network connection [A0502b]
Communication
Event
TcpIpConnect 158.255.238.101:80 (ribeenergy.es)
Occurred
9 days ago - Feb 7, 2022, 2:49:46 PM
Triggering process
Command Line
Username
tpc\t1
User Role
Process reading sensitive files - FTP-based Credential Stores [E1102]
Discovery
Event
Occurred
Triggering proces
Command Line
Username
User Role
Process reading sensitive files - Browser-based Credential Stores [E1108]
Discovery
Event
FileRead
%LOCALAPPDATA%\google\chrome\user data\default\login data
Occurred
9 days ago - Feb 7, 2022, 2:51:02 PM
Triggering process
Medium: regasm.exe
Command Line
None
Username
tpc\t1
User Role
Unknown
Process
hh.exe (300)
Command Line
C:\Users\T1\Desk
INCIDENT
DOWNLOAD FILE
[purged process]
[purged process]
explorer.exe (1328)
hh.exe (300)
powershell.exe (8144)
Powershell.exe creates an external network connection [A0502b]
conhost.exe (2020)
regasm.exe (6668)
Process reading sensitive files - FTP-based Credential Stores [E1102]
Process reading sensitive files - Browser-based Credential Stores [E1108]


Executables
Scripts
Questions
More...
INCIDENTS
Executables
Scripts
Questions
More...
Executables
Scripts
Questions
More...
COLLAPSE
NETWORK CONNECTIONS 2
NETWORK ADDRESS (2)
PROTOCOL
149.154.167.220:443 (api.telegram.org) 1
ssl
3.94.40.55:80 (lumtest.com) 1
http
LUKAPY
LOGOUT
> 24 M
FILE PATH (6)
PRC
%APPDATA%\data.txt 1
%LOCALAPPDATA%\microsoft\windows\0\runtimebroker.exe 1
%LOCALAPPDATALOW%\chromepass.db 2
%LOCALAPPDATALOW%\cookieschrome.db 2
m %Temp% [Z0402]
equest to a popular Web Service [E0502]
owser-based Credential Stores [E1108]
ied by an unpopular process [A0103a]
FILE READS 2
FILE PATH (2)
PRC
%LOCALAPPDATA%\google\chrome\user data\default\login data 1
%LOCALAPPDATA%\microsoft\edge\user data\default\login data 1
INCIDENT
DOWNLOAD FILE
KILL PROCESS

Be XDR sprendimo

Su XDR sprendimu



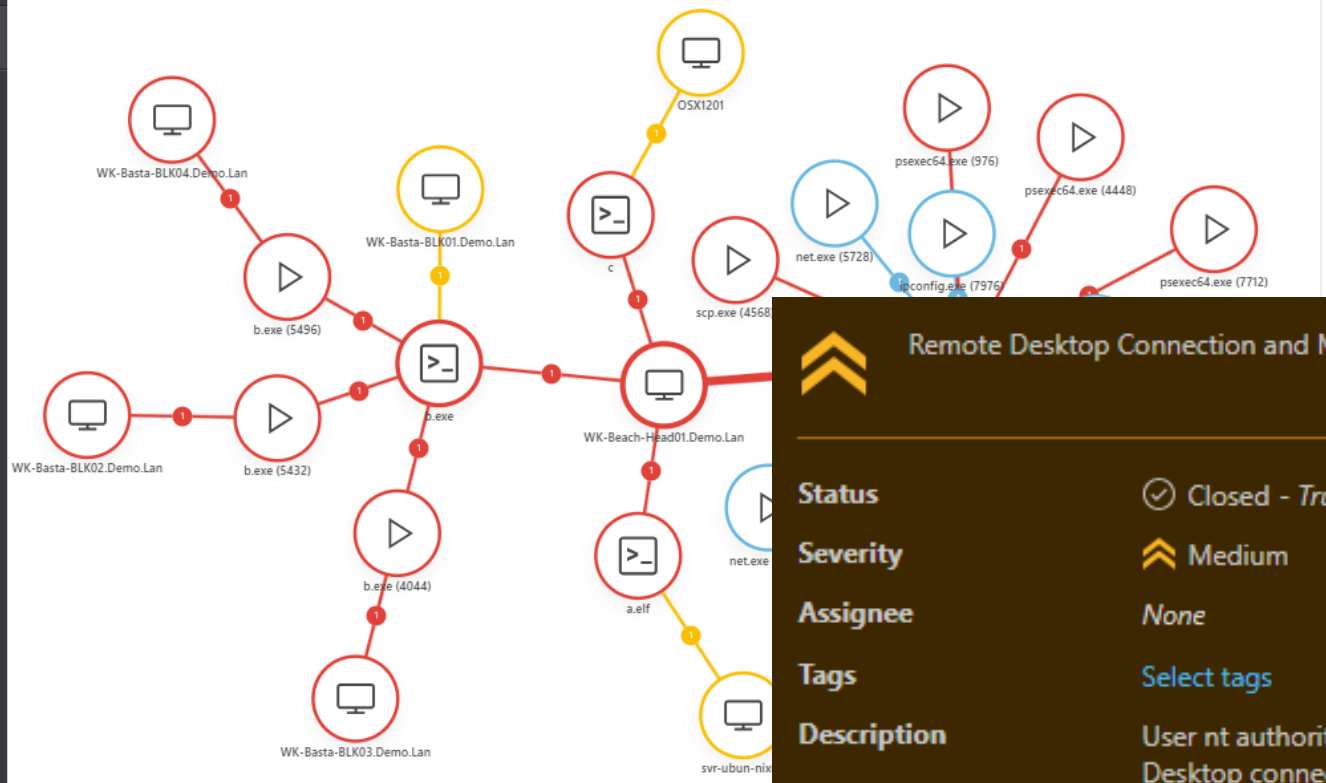

ESET PROTECT & INSPECT
QUESTIONS
DISABLED
HELP
LOGOUT
> 25 M
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE
BACK
All
Lost & found
lukas-virtualbox
dpkg
dpkg
System-wide shell configuration added/modified [L0104B]
Persistence
Event
FileWrite
/etc/profile.d/apps-bin-path.sh.dpkg-new
Occurred
2 months ago - Jul 28, 2022, 3:04:51 PM
Triggering process
dpkg
Command Line
--status-fd 55 --no-triggers --unpack --auto-deconfigure --recursive /tmp/apt-dpkg-install-vKpymA
Username
root:root
User Role
Unknown
dpkg
ELF
SHA-1
359C370B0B05FD2149E2437260979C908F5BBBFC
Seen on
1 computer
First Seen
4 months ago - May 23, 2022, 2:07:19 PM
Last Executed
2 months ago - Jul 28, 2022, 3:12:10 PM
ESET LiveGrid®
Reputation
Popularity
First Seen
2 years ago
gnome-terminal-server (1685)
gnome-terminal-server (1694)
bash (1694)
bash (2186)
sudo (2186)
sudo (2187)
apt-get (2187)
apt-get (5148)
dpkg (5148)
Systemd timer added/modified [L0110]
Possible attempt to tamper with standard system utilities [L0302]
System-wide cron job added/modified - specific interval [L0101B]
Sysvinit/Upstart daemon added/modified [L0109]
System-wide shell configuration added/modified [L0104B]
dpkg (5149)
dpkg (5150)
DETECTIONS
INCIDENT
REMEDIATION
MARK AS RESOLVED
KILL PROCESS
CREATE EXCLUSION
EDIT RULE
COMPUTER
EXECUTABLE
TAGS

DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE

BACK

Filecoder activity across multiple endpoints

Timeline | Relation graph | Detections | Computers | Executables | Processes



Incident | Timeline

Filecoder activity across multiple endpoints

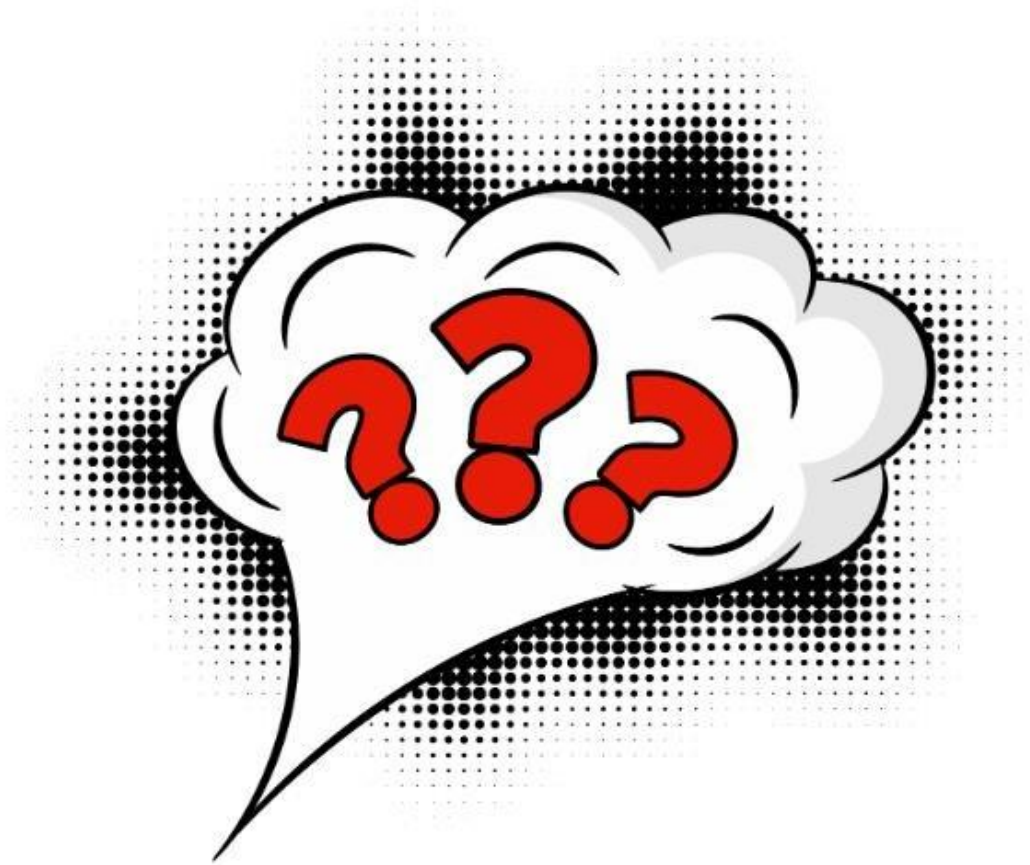
Status	Open
Severity	High
Assignee	
Tags	Ransomware Atta... Select tags
Description	None

Threat indicators (28)

Remote Desktop Connection and Multiple Exploitation Attempts on [redacted]

Status	Closed - *True positive*
Severity	Medium
Assignee	*None*
Tags	Select tags
Description	User nt authority\network service on computer [redacted] accepted a Remote Desktop connection from external IP [redacted]7.143.250 to port 3389 through trusted svchost.exe. Multiple security vulnerability exploitation attempts were blocked on the same computer from various public IPs (202.160.11.182, 178.211.139.188, 87.120.114.171, 182.66.83.50, 147.185.132.9, 147.45.112.17) targeting public IP [redacted] on ports 445 and 80 (HTTP), indicating that the destination device likely has all ports exposed to the world. Additionally, risky RDP communication over non-standard port 6516 from IP 147.45.112.222 was detected, raising further suspicions. IMPORTANT: Generated by AI. Verify information for accuracy.

INCIDENT | REMEDIATION | COMMENT | EDIT | ASSIGN



Labs

Assignments

- CompTIA Security+ Advanced labs
  58, 59, 60, 61

sudo apt-get update
sudo apt-get upgrade