CQURE LIVE WEBINAR

# Ready for 2026: Biggest Vulnerabilities & Cybersecurity Skills That Matter

Click to add text

Tuesday, September 9, 2025
7 pm CEST | 1 pm ET | 10 am PT

# YOUR HOSTS

# Ready for 2026: Biggest Vulnerabilities & Cybersecurity Skills That Matter

**Paula Januszkiewicz**
CEO and Founder
Cybersecurity Expert
Microsoft RD and MVP

paula@cqure.us
𝕏 @PaulaCqure

**Sami Laiho**
Cybersecurity Expert
Microsoft MVP

sami@adminize.com
𝕏 @SamiLaiho

**Amr Thabet**
Cybersecurity Expert

amr@cqure.pl
𝕏@Amr_Thabet

**Marcin Krawczyk**
Cybersecurity Expert

mkrawczyk@cqure.pl

# Ready for 2026: Biggest Vulnerabilities & Cybersecurity Skills That Matter

Paula Januszkiewicz

**CQURE:** CEO, Cybersecurity Expert, Penetration Tester

**CQURE Academy:** Trainer

Microsoft MVP on Enterprise and Platform Security

Microsoft Regional Director

paula@cqure.us

𝕏 @PaulaCqure @CQUREAcademy

**www.cqureacademy.com**

CQURE

# Ready for 2026: Biggest Vulnerabilities & Cybersecurity Skills That Matter

Sami Laiho

**CQURE:** Cybersecurity Expert

**CQURE Academy:** Trainer

**ADMINIZE:** Founder, Senior Technical Fellow, CEO

Microsoft MVP on Windows and Devices, Security

sami@adminize.com

𝕏 @samilaiho

# Ready for 2026: Biggest Vulnerabilities & Cybersecurity Skills That Matter

Amr Thabet

**CQURE:** Cybersecurity Expert

**CQURE Academy:** Trainer

amr@cqure.pl

𝕏 @Amr_Thabet

CQURE

# Ready for 2026: Biggest Vulnerabilities & Cybersecurity Skills That Matter

Marcin Krawczyk

**CQURE:** Cloud & Cybersecurity Expert

**CQURE Academy:** Trainer

mkrawczyk@cqure.pl

CQURE

# What does CQURE do?

**1. Consulting Services:**

a) Extensive IT Security Audits and Penetration Tests of all kinds
b) Configuration Audit and Architecture
c) Design Social Engineering Tests
d) Advanced Troubleshooting and Debugging
e) Emergency Response Services

**2. R&D & CQLabs Tools & Hacks Publications.**

**3. Trainings & Seminars:**

a) Offline (mainly via our partners worldwide)
b) Online (you will hear more about it at the end of this webinar, so stay with us!)

# To ensure good quality of your experience:

1. If you have problems with watching the webinar, try re-logging into Zoom session.
2. If the streaming on Zoom breaks for any reason, please observe the chat for news from our Team – we should be back shortly.
3. If there is a connection or software problem, please check your email inbox for instructions.
4. Should the problems persist, please let us know in the comment section or via email – info@cqureacademy.com.
5. We will be answering your questions at the end of the webinar during the Q&A session, so write them down in the chat!

# What to expect today:

1. A presentation and technical demos from our Experts
2. Tips on how you can learn with us
3. Live Q&A!
4. You will get access to the tools we will be using here!

# Time for the challenge!

One of the key emerging threats is prompt injection in LLMs. Developers often give AI access to various non-public information so that it has knowledge on a given topic and can answer user questions. Since LLMs work by predicting the most likely next word in the text and see the developer's instructions and the user's input the same way, we can craft prompts that make the LLM reveal different information it has access to. This challenge is about talking with an LLM simulator and using the right keywords to get the flag.

**To answer, scan the QR or go to:**

**https://cqureacademy.com/challenge2026/**

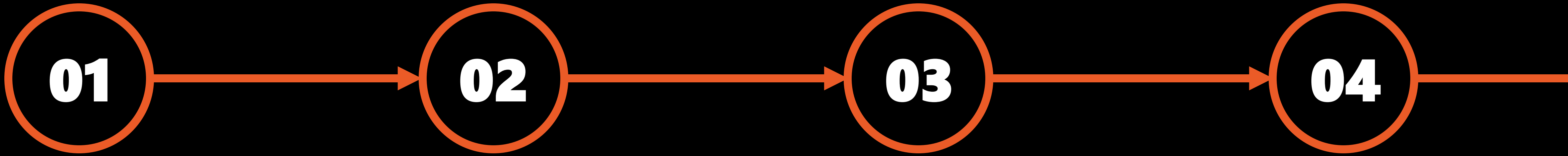
# Challenge Instructions

1. Navigate to https://llm-pi.cqure.ninja and log in using `ctf_user`:`ctf_password`
2. Once logged in, a chat with the LLM simulator will appear.
3. Our message must contain the right keyword. We need to check which words and phrases make the LLM respond differently.
   There are several such words.
4. Upon finding the right word, the LLM will give us access to special commands. It's worth checking if the developers may have left some commands that are usually used in test environments.
5. Our goal is to determine which command will give us the flag.
   We can use other discovered commands to get hints.
6. After guessing the correct command, we will receive the flag.

**To answer, scan the QR or go to:**

**https://cqureacademy.com/challenge2026/**

# Agenda



01

The best practices for safely disabling NTLM in Active Directory environments

Transitioning your organization to secure Kerberos authentication

Paula Januszkiewicz

02

Protecting Admin Access - Correct use of high privilege users & high privileged devices

Sami Laiho

03

Detecting Malicious Activities Using Powershell

Amr Thabet

04

Secure Data Sources in Azure Cloud

Marcin Krawczyk

05

**Challenge Feedback**

**Q&A**

Time to ask your questions

CQURE LIVE WEBINAR

# Ready for 2026:
# Biggest Vulnerabilities & Cybersecurity Skills That Matter

Click to add text

# Ready for 2026: Biggest Vulnerabilities & Cybersecurity Skills That Matter

Paula Januszkiewicz

**CQURE:** CEO, Cybersecurity Expert, Penetration Tester

**CQURE Academy:** Trainer

Microsoft MVP on Enterprise and Platform Security

Microsoft Regional Director

paula@cqure.us

𝕏 @PaulaCqure @CQUREAcademy

**www.cqureacademy.com**

CQURE

# Best practices for safely disabling NTLM in AD environments & secure Kerberos authentication

In June 2024, Microsoft said:

"All versions of NTLM, including LANMAN, NTLMv1, and NTLMv2, are no longer under active feature development and are deprecated."

"Calls to NTLM should be replaced by calls to Negotiate, which tries to authenticate with Kerberos and only falls back to NTLM when necessary."

"[Update - November 2024]: NTLMv1 is removed starting in Windows 11, version 24H2 and Windows Server 2025."

# NTLM Authentication

NTLM2

Client<-Server:  SC

Client->Server:  H(P,H'(SC,CC)), CC

Server->DomCntl: H(P,H'(SC,CC)), H'(SC,CC)

Server<-DomCntl: yes or no

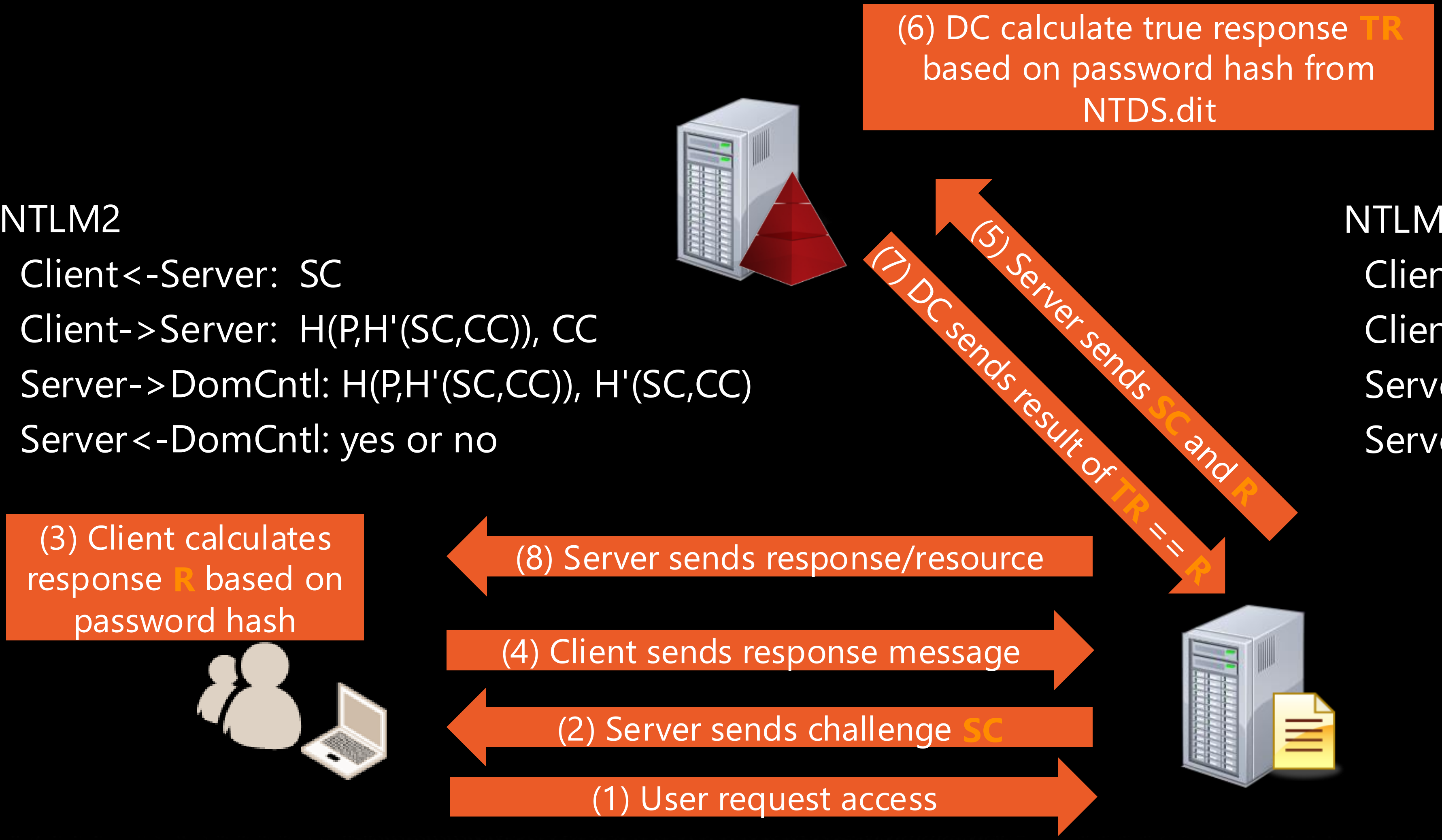
NTLMv1

Client<-Server:  SC

Client->Server:  H(P,SC)

Server->DomCntl: H(P,SC), SC

Server<-DomCntl: yes or no



(1) User request access

(2) Server sends challenge SC

(3) Client calculates response R based on password hash

(4) Client sends response message

(5) Server sends SC and R

(6) DC calculate true response TR based on password hash from NTDS.dit

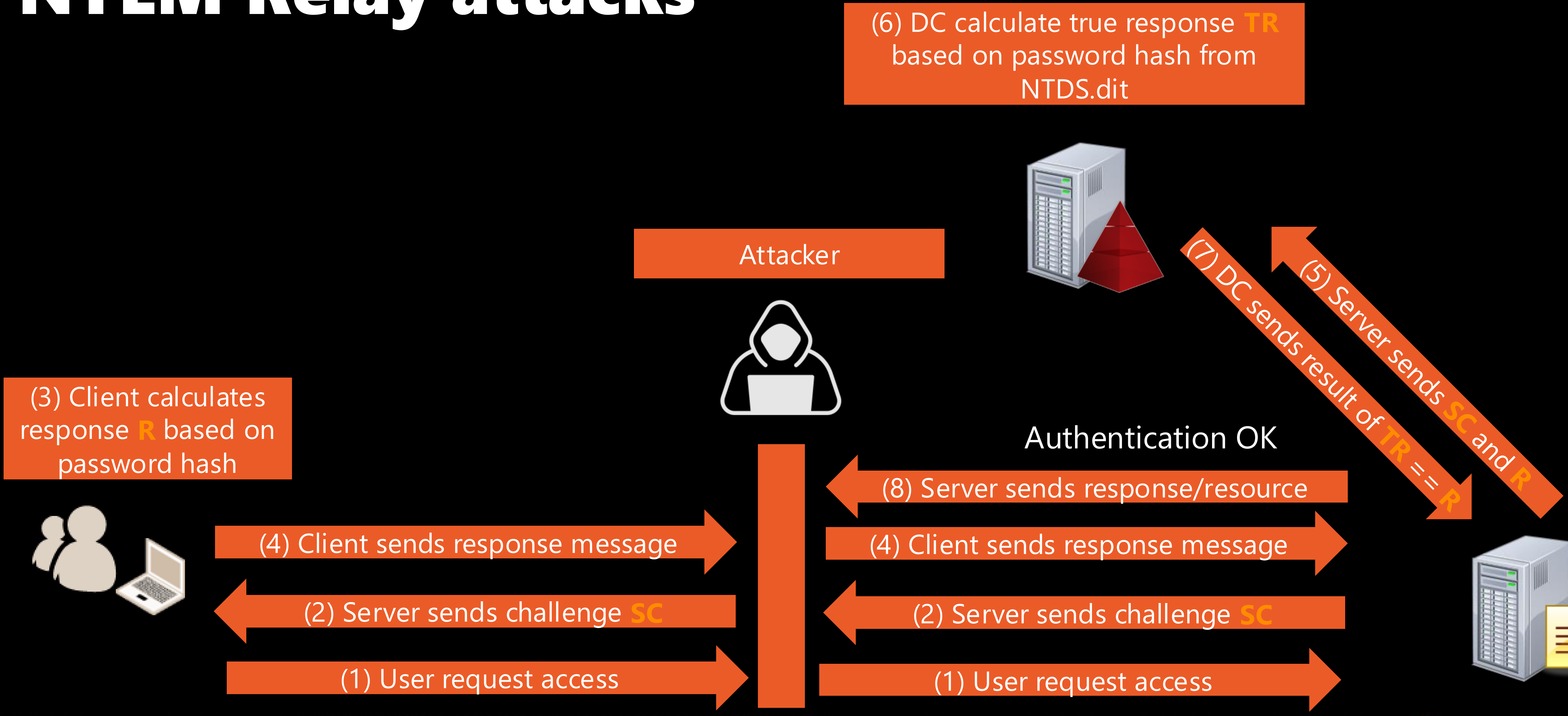
(7) DC sends result of TR == R

(8) Server sends response/resource

# NTLM Versions

| | LM | NTLMv1 | NTLMv2 |
|---|---|---|---|
| Password case sensitive | No | Yes | Yes |
| Hash key length | 56bit + 56bit | - | - |
| Password hash algorithm | DES (ECB mode) | MD4 | MD4 |
| Hash value length | 64bit + 64bit | 128bit | 128bit |
| C/R key length | 56bit + 56bit + 16bit | 56bit + 56bit + 16bit | 128bit |
| C/R algorithm | DES (ECB mode) | DES (ECB mode) | HMAC_MD5 |
| C/R value length | 64bit + 64bit + 64bit | 64bit + 64bit + 64bit | 128bit |

# NTLM Relay attacks



(6) DC calculate true response TR based on password hash from NTDS.dit

Attacker

(3) Client calculates response R based on password hash

Authentication OK

(8) Server sends response/resource

(7) DC sends result of TR == R

(5) Server sends SC and R

(4) Client sends response message

(2) Server sends challenge SC

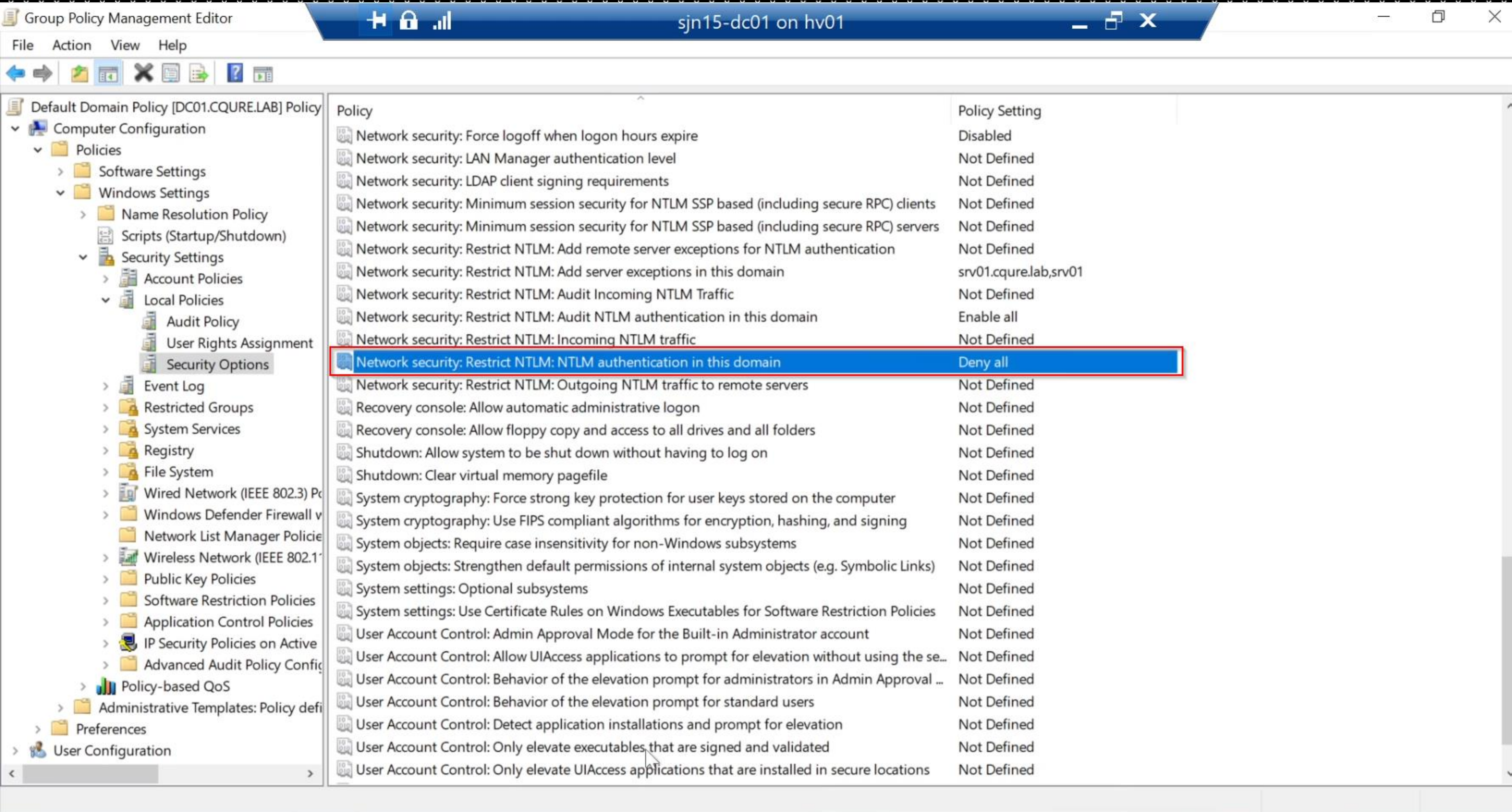
(1) User request access

(4) Client sends response message

(2) Server sends challenge SC

(1) User request access

# Demo:
# NTLM Relay with Responder


Group Policy Management Editor
sjn15-dc01 on hv01
File
Action
View
Help
Default Domain Policy [DC01.CQURE.LAB] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Defender Firewall v
Network List Manager Policie
Wireless Network (IEEE 802.1
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active
Advanced Audit Policy Config
Policy-based QoS
Administrative Templates: Policy defi
Preferences
User Configuration

| Policy | Policy Setting |
|---|---|
| Network security: Force logoff when logon hours expire | Disabled |
| Network security: LAN Manager authentication level | Not Defined |
| Network security: LDAP client signing requirements | Not Defined |
| Network security: Minimum session security for NTLM SSP based (including secure RPC) clients | Not Defined |
| Network security: Minimum session security for NTLM SSP based (including secure RPC) servers | Not Defined |
| Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication | Not Defined |
| Network security: Restrict NTLM: Add server exceptions in this domain | srv01.cqure.lab,srv01 |
| Network security: Restrict NTLM: Audit Incoming NTLM Traffic | Not Defined |
| Network security: Restrict NTLM: Audit NTLM authentication in this domain | Enable all |
| Network security: Restrict NTLM: Incoming NTLM traffic | Not Defined |
| Network security: Restrict NTLM: NTLM authentication in this domain | Deny all |
| Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers | Not Defined |
| Recovery console: Allow automatic administrative logon | Not Defined |
| Recovery console: Allow floppy copy and access to all drives and all folders | Not Defined |
| Shutdown: Allow system to be shut down without having to log on | Not Defined |
| Shutdown: Clear virtual memory pagefile | Not Defined |
| System cryptography: Force strong key protection for user keys stored on the computer | Not Defined |
| System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing | Not Defined |
| System objects: Require case insensitivity for non-Windows subsystems | Not Defined |
| System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) | Not Defined |
| System settings: Optional subsystems | Not Defined |
| System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies | Not Defined |
| User Account Control: Admin Approval Mode for the Built-in Administrator account | Not Defined |
| User Account Control: Allow UIAccess applications to prompt for elevation without using the se... | Not Defined |
| User Account Control: Behavior of the elevation prompt for administrators in Admin Approval ... | Not Defined |
| User Account Control: Behavior of the elevation prompt for standard users | Not Defined |
| User Account Control: Detect application installations and prompt for elevation | Not Defined |
| User Account Control: Only elevate executables that are signed and validated | Not Defined |
| User Account Control: Only elevate UIAccess applications that are installed in secure locations | Not Defined |

# Demo:
# NTLM Enabled / Disabled

# Ready for 2026: Biggest Vulnerabilities & Cybersecurity Skills That Matter

Sami Laiho

**CQURE:** Cybersecurity Expert

**CQURE Academy:** Trainer

**ADMINIZE:** Founder, Senior Technical Fellow, CEO

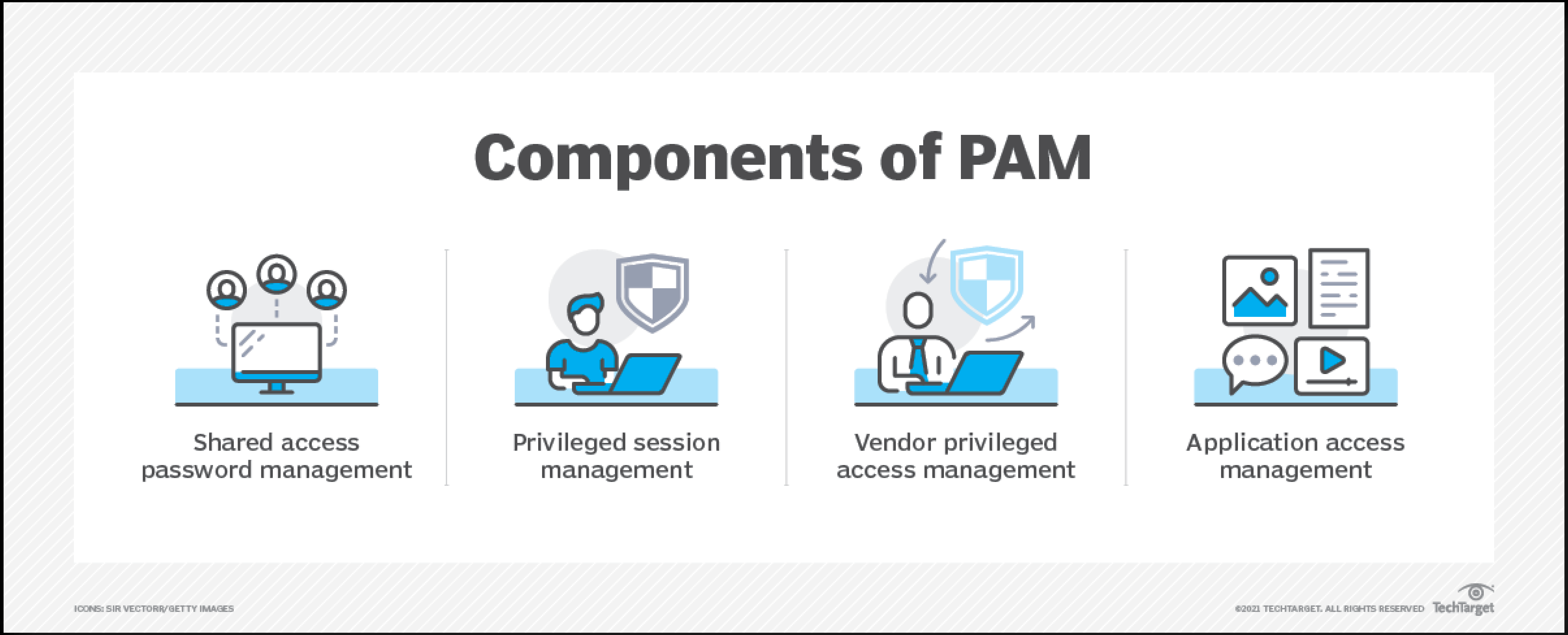
Microsoft MVP on Windows and Devices, Security

sami@adminize.com

𝕏 @samilaiho

CQURE

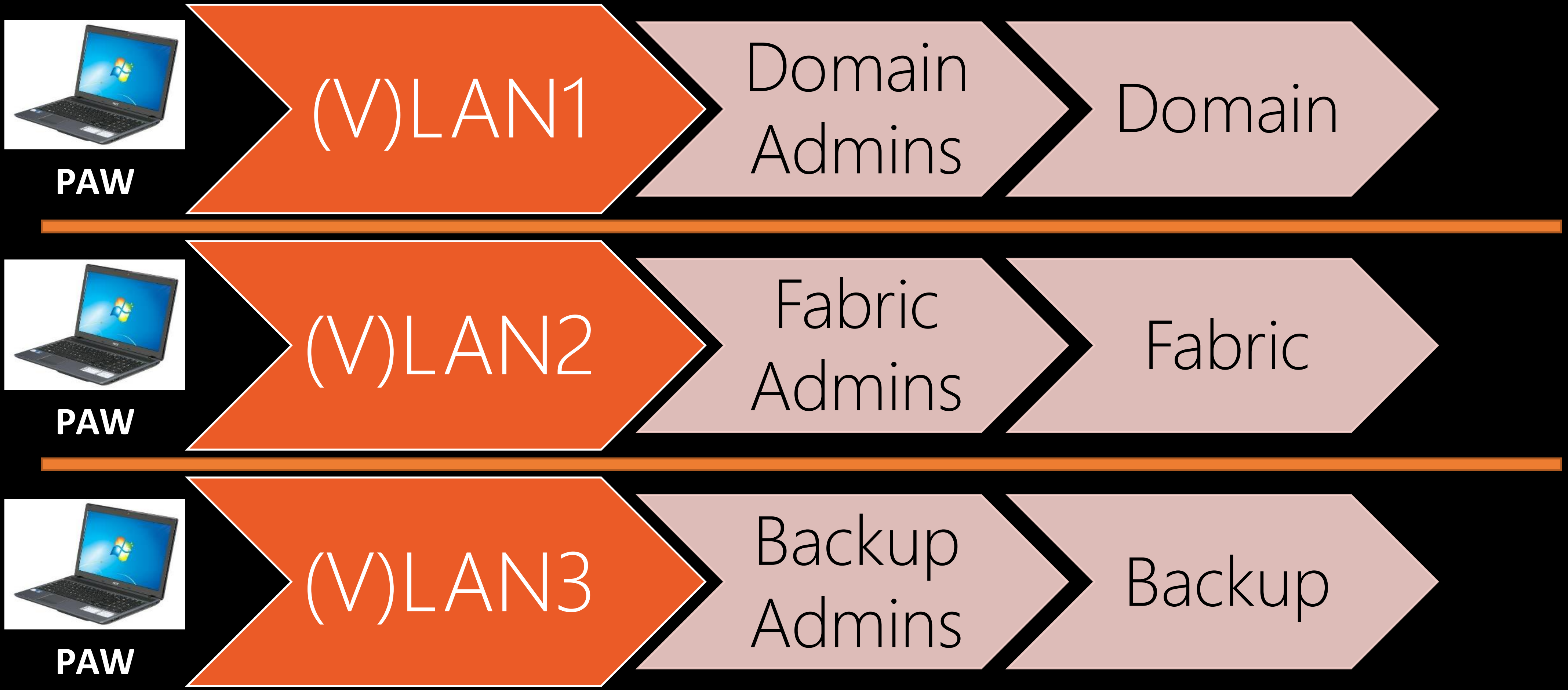
# Protecting Admin Access - Correct use of high privilege users & high privileged devices



# Components of PAM

- Shared access password management
- Privileged session management
- Vendor privileged access management
- Application access management

ICONS: SIR VECTORR/GETTY IMAGES



PAW

(V)LAN1

Domain Admins

Domain

PAW

(V)LAN2

Fabric Admins

Fabric

PAW

(V)LAN3

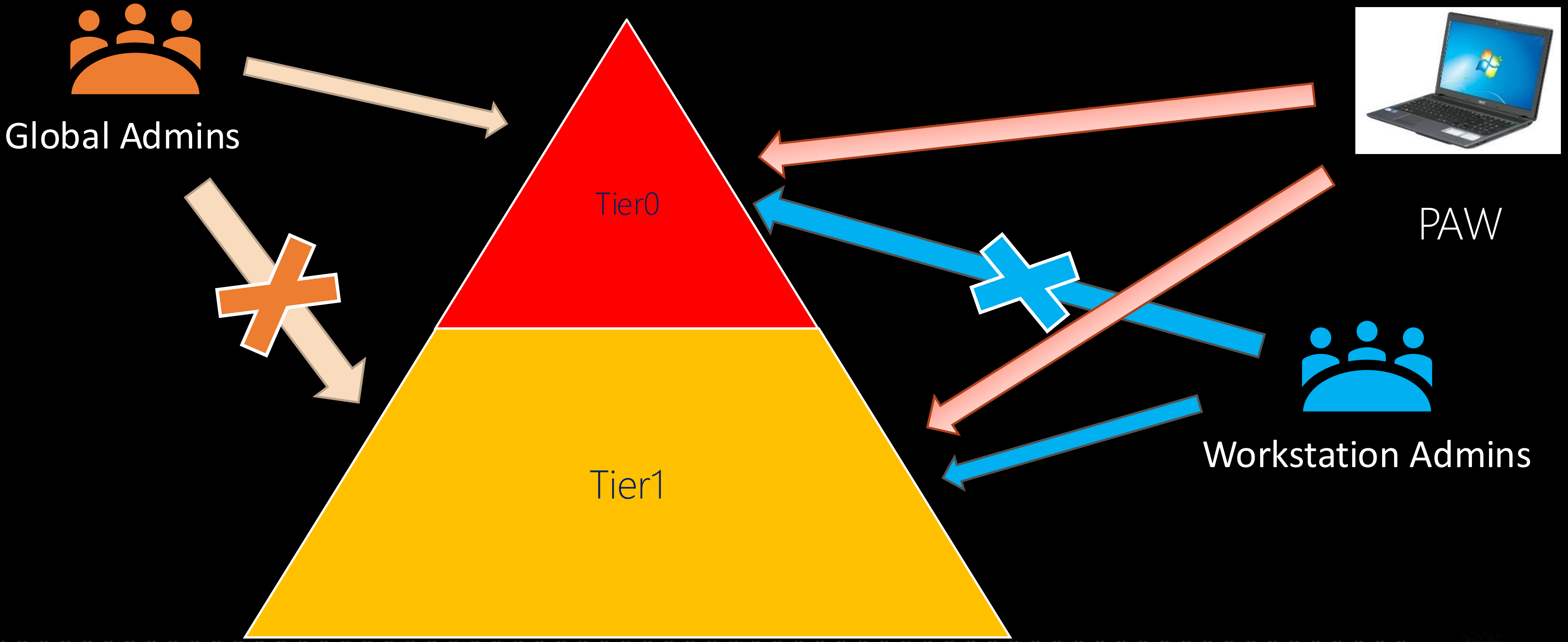
Backup Admins

Backup

# … or in the Cloud

Split your environment into two layers

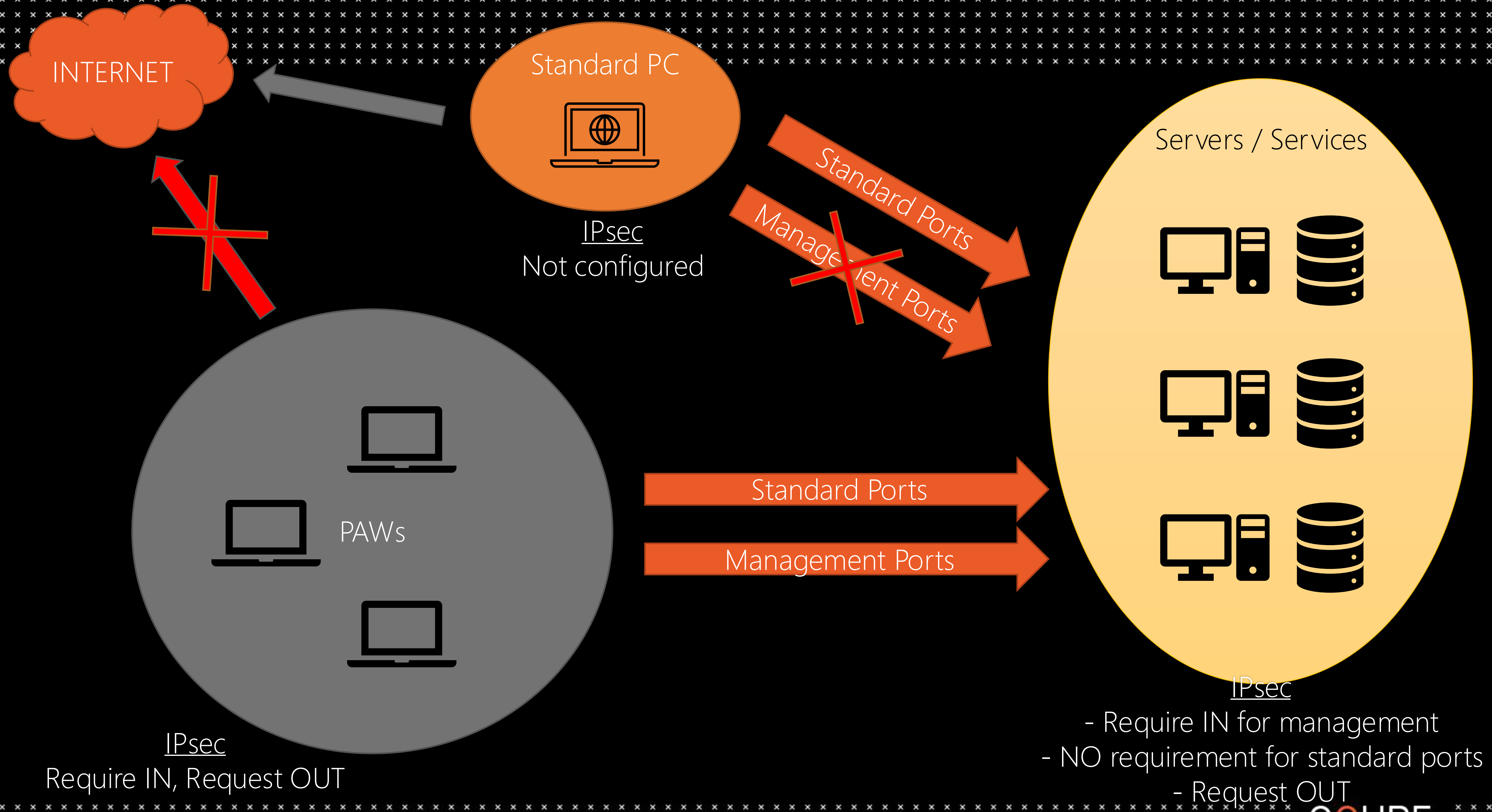
Never allow higher layer admins to logon to lower layers



# What are Tier 0 assets?

Good resource: https://specterops.github.io/TierZeroTable/

# Privileged Access Workstation (PAW)



INTERNET

Standard PC

IPsec

Not configured

Standard Ports

~~Management Ports~~

Servers / Services

PAWs

Standard Ports

Management Ports

IPsec

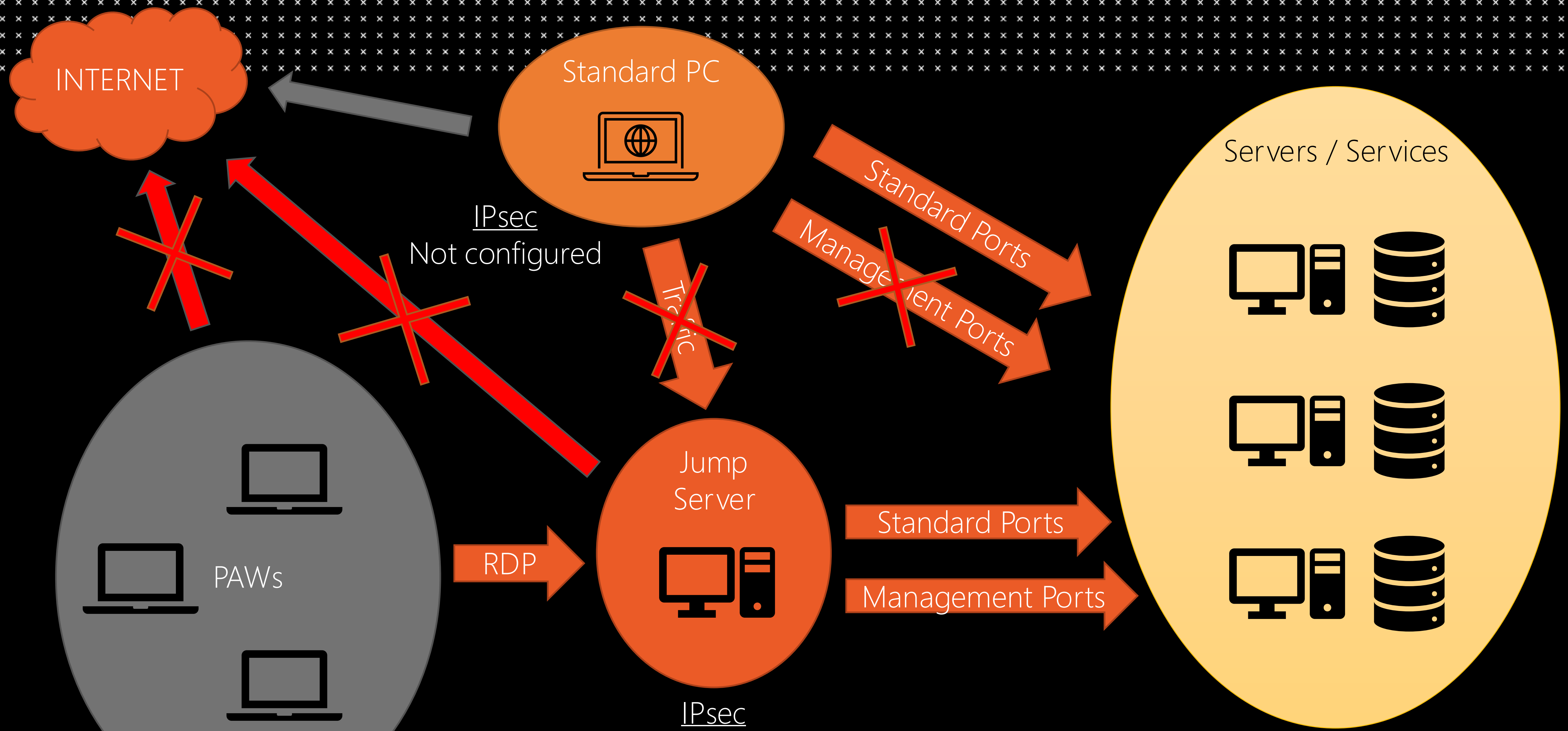
Require IN, Request OUT

IPsec

- Require IN for management

- NO requirement for standard ports

- Request OUT



Standard PC — IPsec
Not configured

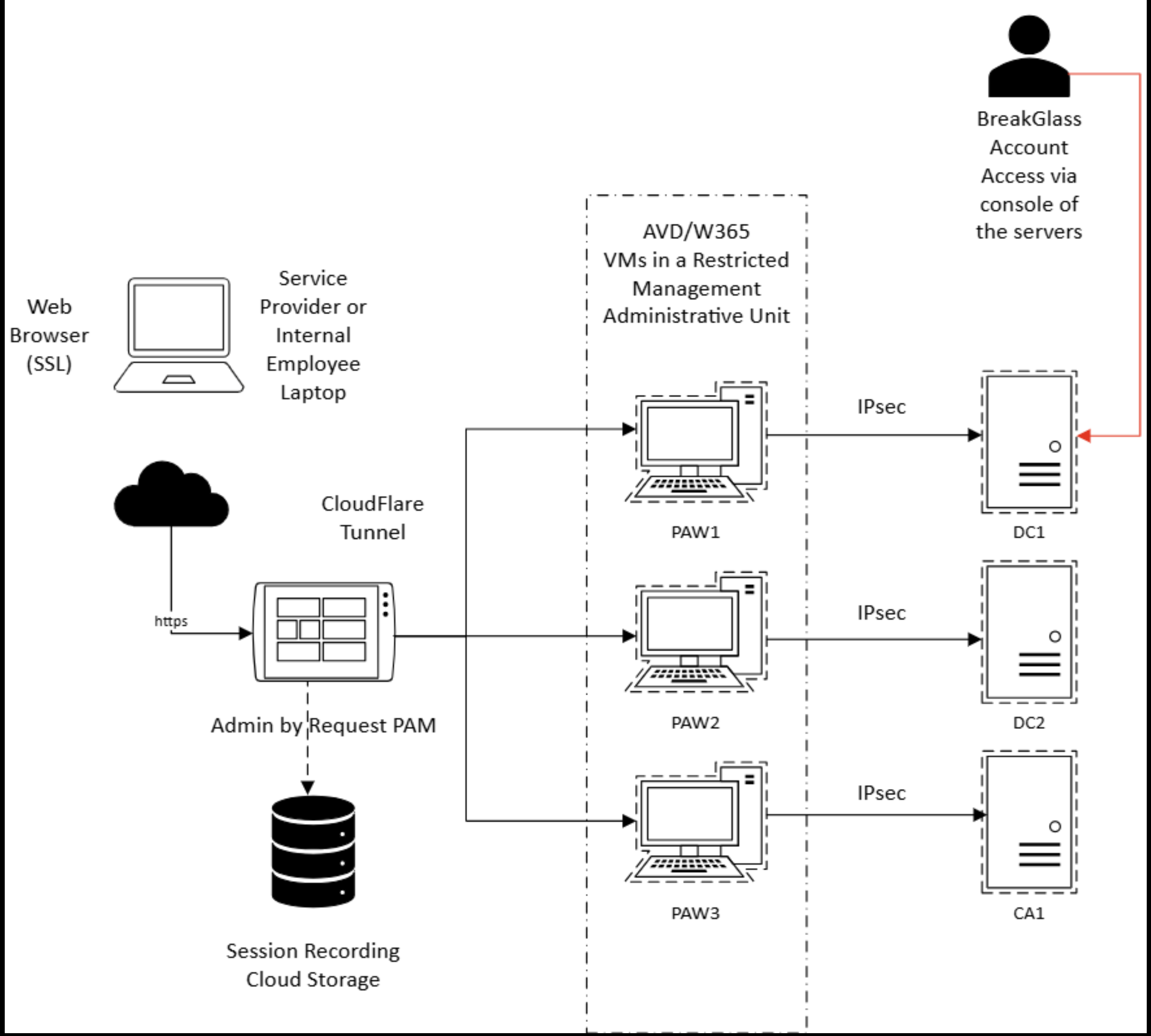
PAWs — IPsec
Require IN, Request OUT

Jump Server — IPsec
Require IN, Request OUT

Servers / Services — IPsec
- Require IN for management
- NO requirement for standard ports
- Request OUT

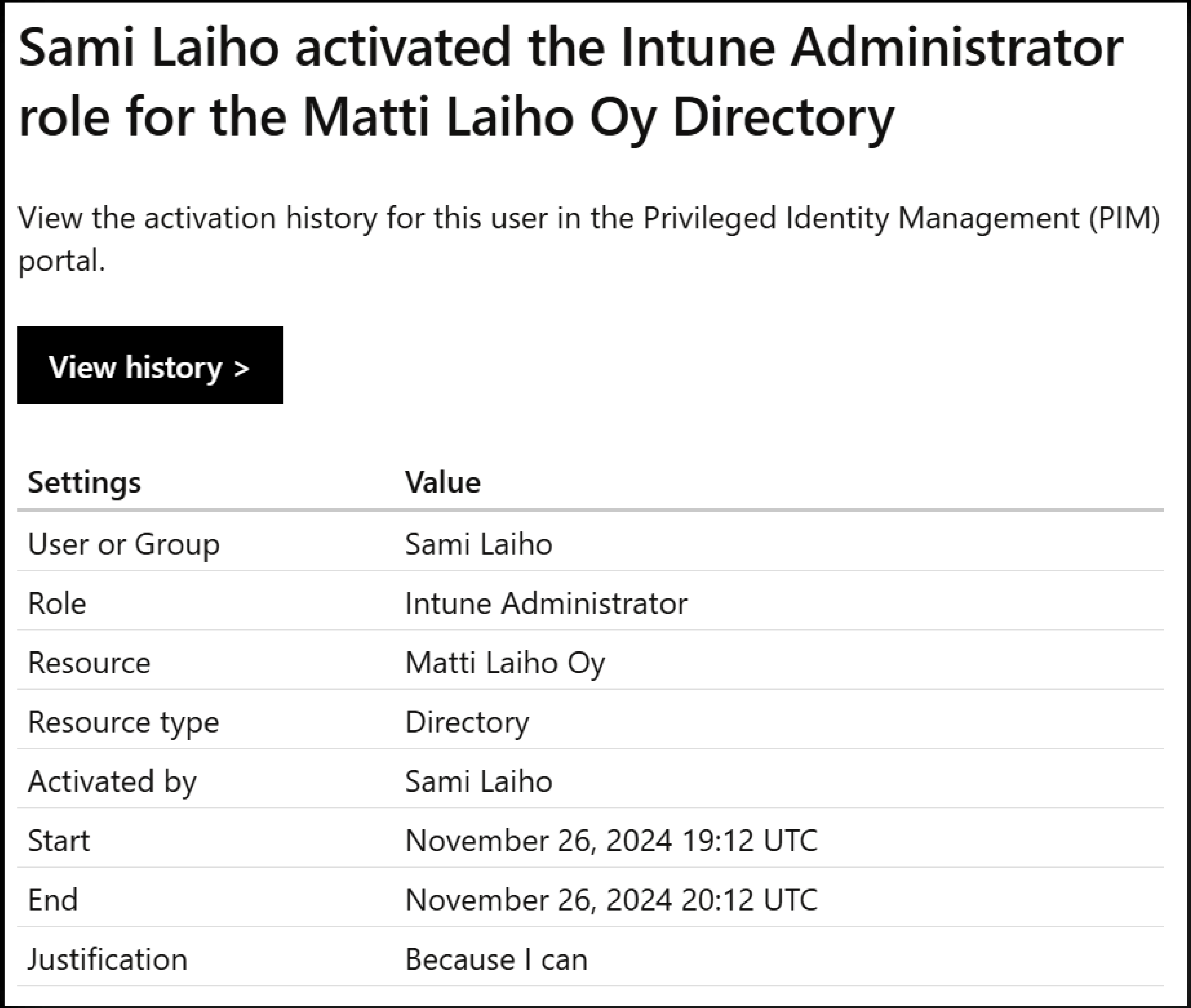
# Example

- Outsourcing makes things… different…
- Remember: no PAM/PAW are the same as every environment is different


BreakGlass Account Access via console of the servers
AVD/W365 VMs in a Restricted Management Administrative Unit
Web Browser (SSL)
Service Provider or Internal Employee Laptop
CloudFlare Tunnel
https
Admin by Request PAM
Session Recording Cloud Storage
PAW1
PAW2
PAW3
IPsec
IPsec
IPsec
DC1
DC2
CA1

CQURE

# Privileged Identity Management (PIM)



# Sami Laiho activated the Intune Administrator role for the Matti Laiho Oy Directory

View the activation history for this user in the Privileged Identity Management (PIM) portal.

View history >

| Settings | Value |
|---|---|
| User or Group | Sami Laiho |
| Role | Intune Administrator |
| Resource | Matti Laiho Oy |
| Resource type | Directory |
| Activated by | Sami Laiho |
| Start | November 26, 2024 19:12 UTC |
| End | November 26, 2024 20:12 UTC |
| Justification | Because I can |

# Ready for 2026: Biggest Vulnerabilities & Cybersecurity Skills That Matter

Amr Thabet

**CQURE:** Cybersecurity Expert

**CQURE Academy:** Trainer

amr@cqure.pl

𝕏 @Amr_Thabet

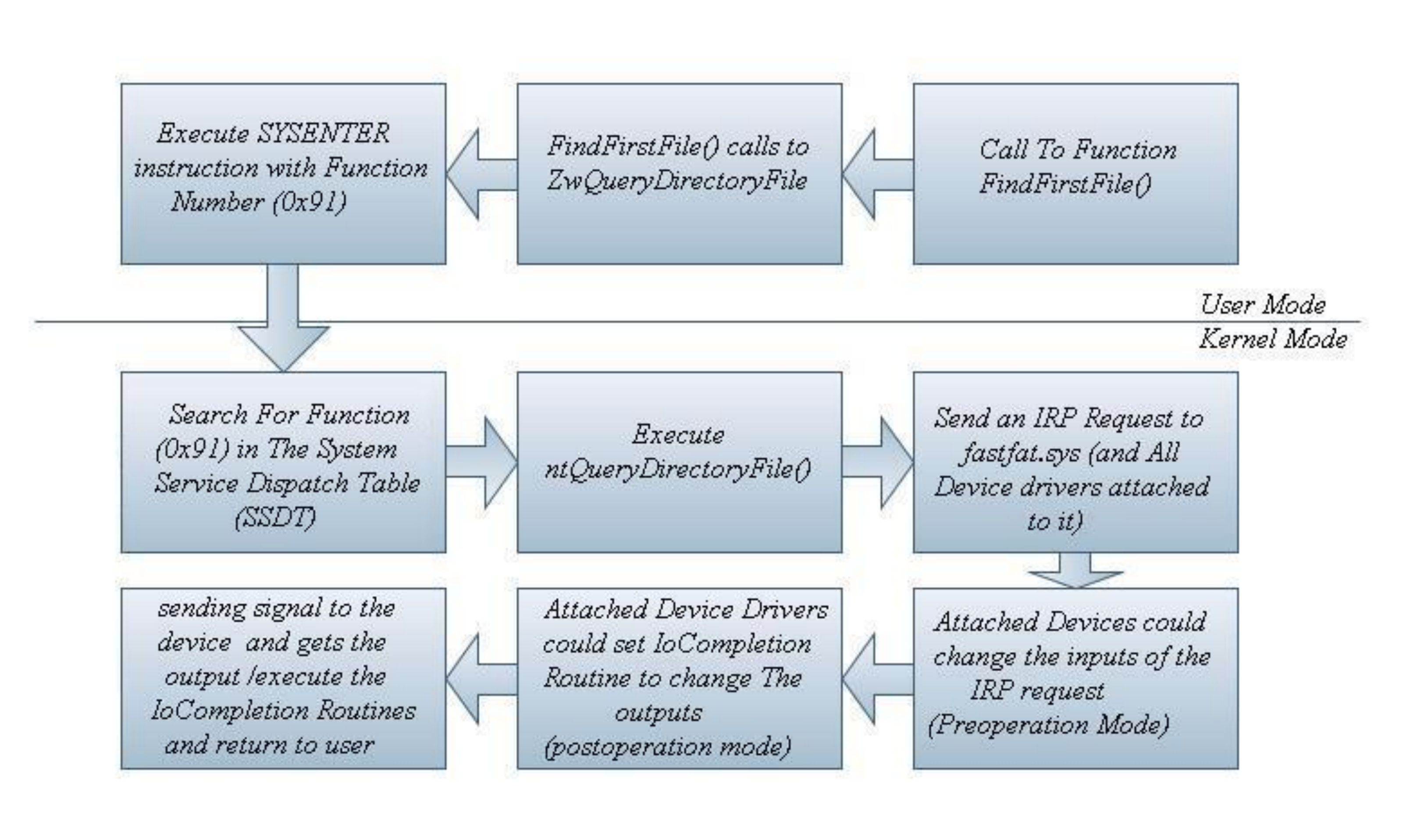
# Detecting Malicious Activities Using Powershell

# Powershell For Investigations & Threat Hunting

# EDR is not as strong as you think

EDR hooks are visible to the malware and can be bypassed

# Where EDR Hooks?



Call To Function FindFirstFile()

FindFirstFile() calls to ZwQueryDirectoryFile

Execute SYSENTER instruction with Function Number (0x91)

User Mode

Kernel Mode

Search For Function (0x91) in The System Service Dispatch Table (SSDT)

Execute ntQueryDirectoryFile()

Send an IRP Request to fastfat.sys (and All Device drivers attached to it)

Attached Devices could change the inputs of the IRP request (Preoperation Mode)

Attached Device Drivers could set IoCompletion Routine to change The outputs (postoperation mode)

sending signal to the device and gets the output /execute the IoCompletion Routines and return to user

# EDR is not as strong as you think

1. EDR hooks are visible to the malware and can be bypassed
2. EDR is light and real-time, missing a lot of memory scanning functionalities

# EDR is not as strong as you think

1. EDR hooks are visible to the malware and can be bypassed
2. EDR is light and real-time, missing a lot of memory scanning functionalities
3. EDR always balances between false positives and negatives

# Memory Forensics is not the only solution

1. Memory dumps takes a lot of time to capture and space to store
2. They are missing files’ hashes and digital signatures
3. They are missing key non-volatile data like registry hives, MFT and Zone.Indentifier

# Why Powershell

1. Powershell remoting is safe
2. Doesn’t leak credentials
3. Fast way to collect volatile and non-volatile data
4. Can perform packet capture, log collection, in-memory investigation and much more

# What to do in Powershell investigation

Investigating attacks with PowerShell gives you the ability to go deeper into the system

It gives you the ability to automate across thousands of machines

All through a secure remoting protocol

We will look into:

1. Processes List and Loaded DLLs
2. Running Services
3. Scheduled Tasks
4. Network Connections
5. Non-Volatile Data (Registry, MFT … etc)
6. Windows Event Logs
7. Installed Apps

# Powershell Threat hunting

Hunting through Powershell gives us the ability to hunt for known malware techniques:

1. Malware disguised as svchost.exe (svchost should only run under services.exe)
2. Unknown or unsigned DLL (Probably injected, a suspicious extension, DLL side-loading)
3. URLs in commandlines (common for LOLBins type of fileless attacks)
4. Memory Injection or DLL injection (RWE private memory and probably starts with MZ)
5. Suspicious services (powershell or LOLBins related services)
6. Scheduled tasks with powershell or rundll32.exe, tasks with writable paths
7. Non-whitelisted/unknown Domains by non-browser application. Multiple domains by one application
8. Ngrok, team viewer or a remote-control app installed (not used by the company)
9. Maintaining persistence through registry.

# Powershell Hunting – Zone.Identifier

You can read alternative stream like this:

```
Get-Content C:\Users\amrth\Downloads\xmrig.tar.gz:Zone.Identifier
```

Zone.Identifier stream is added by default by browsers to the downloaded files

They include the downloaded URL (which helps in finding the origin of this file)

# Conclusions

Don’t rely 100% on EDR and log analysis

Perform in-depth Powershell investigations and threat hunting

Look for malware patterns (process injection, autorun, token impersonation … etc)

Watch out for legitimate tools used by malware (AnyDesk, Team Viewer, ngrok, rclone … etc)

# Ready for 2026: Biggest Vulnerabilities & Cybersecurity Skills That Matter

Marcin Krawczyk

**CQURE:** Cloud & Cybersecurity Expert

**CQURE Academy:** Trainer

mkrawczyk@cqure.pl

CQURE

# Secure Data Sources in Azure Cloud

# Network Hardening for Key Vault

Best Practice: Private Endpoints

1. Projects your Key Vault directly into your Virtual Network (VNet) with a private IP.
2. Traffic **never** traverses the public internet.
3. The Key Vault is effectively invisible to the outside world.
4. Alternative: VNet Service Endpoints
5. Restricts access to traffic originating from a specific subnet.
6. Good, but the endpoint itself remains public.

# Key & Secret Rotation

The Risk: A secret that never expires is a permanent backdoor.

1. Secret Sprawl: Old, forgotten credentials in config files, code, and CI/CD variables.
2. Increased Blast Radius: If a long-lived secret is compromised, the attacker has a long window of access.
3. Manual Rotation Fails: Relying on calendar reminders and manual processes is unreliable and prone to human error.

# Implementing Automated Rotation

The Risk: A secret that never expires is a permanent backdoor.

1. Secret Sprawl: Old, forgotten credentials in config files, code, and CI/CD variables.
2. Increased Blast Radius: If a long-lived secret is compromised, the attacker has a long window of access.
3. Manual Rotation Fails: Relying on calendar reminders and manual processes is unreliable and prone to human error.

# Managed Identity: The Token Risk

Managed Identities are the best practice for service-to-service authentication. **No passwords in code!**

**The Misconception:** "Passwordless" means there is no credential to steal.

**The Reality:** The credential is a short-lived **OAuth 2.0 Bearer Token**.

1. This token is like a temporary master key.
2. Anyone who holds ("bears") this token can use it to impersonate your service.
3. The new target for an attacker is not a password, but this token.

# Diagnostic Settings: Incomplete Audit Trails

The Truth: You can't protect what you can't see.

Diagnostic Settings are your eyes and ears. They stream logs from Azure resources (Storage, SQL, Key Vault) to a Log Analytics Workspace.

This is ESSENTIAL for threat detection and incident response.

The Risk: What if there are no logs for your most critical API?

# Do You Want to *Enhance* Your Windows Security Knowledge?

# ADVANCED WINDOWS SECURITY COURSE 2026

CQURE

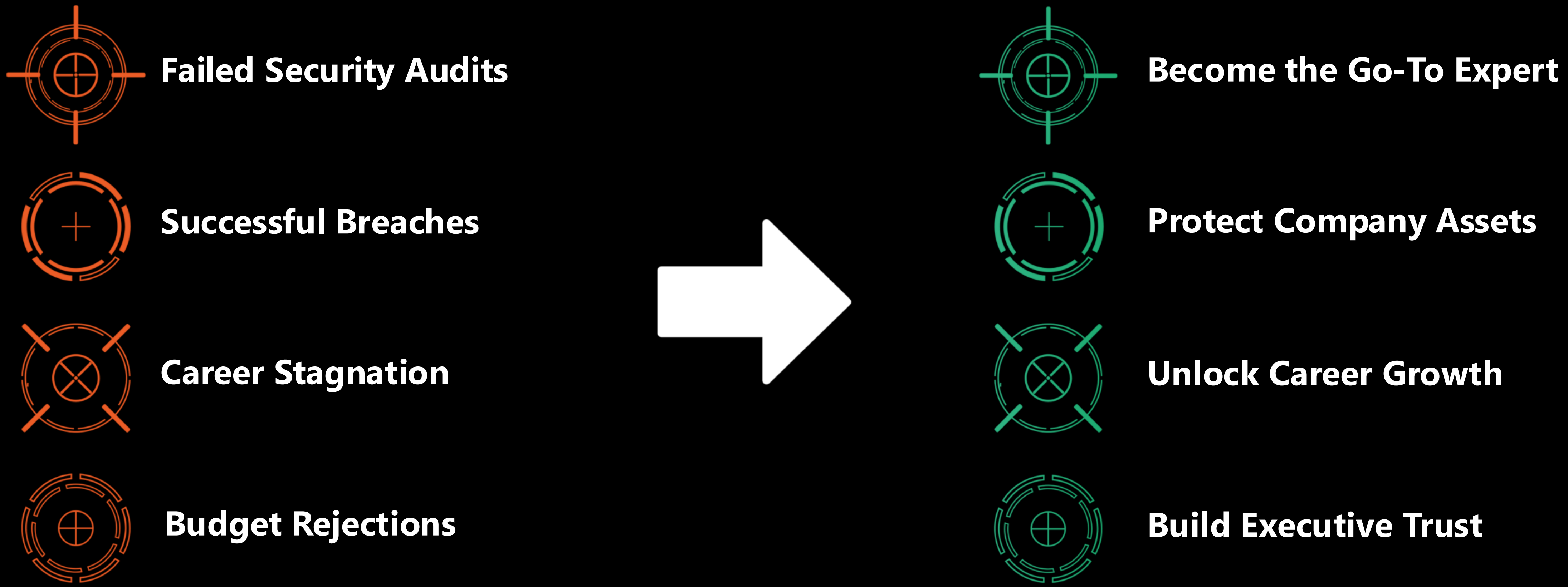
# Is *this* course for you?

**Intermediate/Advanced**

**Ethical hacker**

**Brave Newbies**

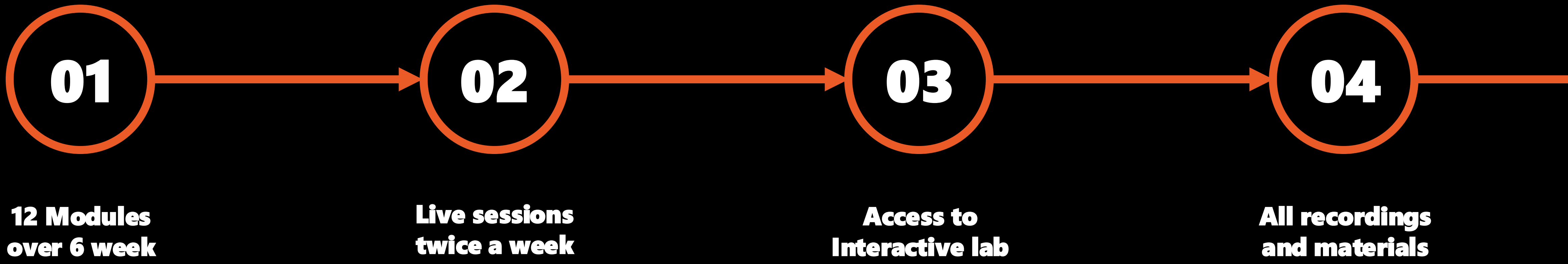
# What's *Really at Stake* If You Don't Level Up?



- Failed Security Audits
- Successful Breaches
- Career Stagnation
- Budget Rejections

- Become the Go-To Expert
- Protect Company Assets
- Unlock Career Growth
- Build Executive Trust

# What’s inside ADVANCED WINDOWS SECURITY COURSE *2026* ?



01

12 Modules
over 6 week

02

Live sessions
twice a week

03

Access to
Interactive lab

04

All recordings
and materials

# What’s inside ADVANCED WINDOWS SECURITY COURSE *2026* ?

05

CQURE Tools/Examples Scripts

06

Discord community

07

Final certification

# You Could Do It Alone.

# *Or You Could Do It Right.*

## *Advanced Windows Security Course is:*

*Structured*

*Time efficient*

*Expert Led*

CQURE

# Advanced Windows Security Course 2026

**LIVE Trainings**
You'll join our 2-hour long live classes on a special interactive plaform – happening twice a week at 7PM CET (10 AM PST / 1 PM EST).

**Action packed**
You'll go through 12 modules in 6 weeks. We're not fluffing around, you've been warned.

**Once a Year Only**
We organize this course only once a year, in its last quarter. The 2026 edition is updated with latest trends, new tools, and challenges.

**Extra Materials**
We've prepared for you tools, slides, extra materials, and homework for each session.

**12-month Access**
You'll get a full year of online access to all the recordings counted from the first class.

**The Training Lab**
During the course, you'll have access to a special training platform where you can safely test your hacks.

**Social & Network**
You'll become a member of a closed Discord group, where you can not only share your challenges and geeky jokes, but also network.

**CQURE Certificate – "Windows Security Master 2026"**
You'll receive an official CQURE certificate "Windows Security Master 2026" after passing the final exam. Yes, there will be a final exam.

**Interactive Classroom**
After every class, you'll be able to ask questions.

# Here’s How to Apply

01

**Application**

02

**Processing**

Limited to200 seats only

03

**Confirmation**

Review within 5 working days

# WEBINAR PARTICIPANTS DISCOUNT FOR AWSC26

*SPECIAL PRICE*

**$2199* save $1000 net**

**Valid only till September 19th, 2025*

https://cqu.re/awsc26

APPLY NOW
with code READY
PAY LATER.

Available
*BY APPLICATION ONLY.*

CQURE

# ADVANCED WINDOWS SECURITY COURSE 2026

October 28th - December 4th

## COURSE AGENDA

Attack Case Studies and Building Incident Response Readiness Strategy
*by Paula Januszkiewicz & Artur Kalinowski*

Zero Trust in Practice: Building Secure Architectures Beyond the Perimeter
*by Sami Laiho*

Discover Your External Perimeter and Open Source Intelligence in Azure
*by Przemysław Tomasik*

AI Agents for Attack Investigation
*by Amr Thabet*

Azure Cloud Incident Response – Part 1: Detection
*by Marcin Krawczyk*

Azure Cloud Incident Response – Part 2: Response and Recovery
*by Marcin Krawczyk*

CQURE ACADEMY CQURE CONSULTING

# ADVANCED WINDOWS SECURITY COURSE 2026

October 28th - December 4th

## COURSE AGENDA

Privileged Access Abuse in Databases: Detection and Defense
*by Damian Widera*

Real-World Pentesting: Windows Tips, Tricks, and Countermeasures
*by Artur Kalinowski*

PowerShell for Digital Investigation & Threat Hunting
*by Amr Thabet*

Tiering, Just-In-Time, and Admin Forest in "Real Life"
*by Peter Kloep*

How to Think About Azure Kubernetes Security
*by Michał Furmankiewicz*

Securing Windows Server and Applications in .NET with TLS:
Implementation, Pitfalls, and Best Practices
*by Przemysław Tomasik*

CQURE ACADEMY CQURE CONSULTING

# Your Instructors

**Paula Januszkiewicz**

Founder & CEO, Microsoft Regional Director, MVP, MCT

**Sami Laiho**

Windows OS Expert, MVP

**Peter Kloep**

Cybersecurity Expert, Principal IT Architect

# Your Instructors

**Marcin Krawczyk**

Cloud & Cybersecurity Expert

**Amr Thabet**

Cybersecurity Expert

**Artur Kalinowski**

Cybersecurity Expert

# Your Instructors

**Przemysław Tomasik**

Cybersecurity Expert

**Damian Widera**

Data Platform MVP, MCT,
Software Engineer,
Cybersecurity Expert

# Ready to join?

# APPLY NOW!

CQURE

# WEBINAR PARTICIPANTS DISCOUNT FOR AWSC26

*SPECIAL PRICE*

**$2199* save $1000 net**

**Valid only till September 19th, 2025*

https://cqu.re/awsc26

APPLY NOW
with code READY
PAY LATER.

Available
*BY APPLICATION ONLY.*

CQURE

# CHALLENGE WINNER

# Q&A Time!

CQURE

# Visit our BLOG and discover more about cybersecurity solutions & tools:

https://cqureacademy.com/blog

CQURE

# DOWNLOAD THE TOOLS

https://resources.cqureacademy.com/tools/

Username: student
Password: CQUREAcademy#123!

# If you want level up your Windows Cybersecurity Skills

## JOIN OUR ONLINE TRAININGS

CQURE