CQURE LIVE WEBINAR

Deadly Cloud Misconfigurations: Mistakes You Should NEVER Make

Click to add text

Tuesday, September 30, 2025
7 pm CEST | 1 pm ET | 10 am PT

Deadly Cloud Misconfigurations: Mistakes You Should NEVER Make

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert, Penetration Tester

CQURE Academy: Trainer

Microsoft MVP on Enterprise and Platform Security

Microsoft Regional Director

paula@cqure.us

@PaulaCqure @CQUREAcademy

www.cqureacademy.com

Deadly Cloud Misconfigurations: Mistakes You Should NEVER Make

Marcin Krawczyk

CQURE: Cloud & Cybersecurity Expert

CQURE Academy: Trainer

mkrawczyk@cqure.pl

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!

Dare to quiz?

CQURE LIVE WEBINAR

Deadly Cloud Misconfigurations: Mistakes You Should NEVER Make

Deadly Cloud Misconfigurations: Mistakes You Should NEVER Make

Marcin Krawczyk

CQURE: Cloud & Cybersecurity Expert

CQURE Academy: Trainer

mkrawczyk@cqure.pl

Agenda

1. Entra ID Conditional Access: Requiring phishing-resistant MFA strength.
2. Entra ID Application Secrets: The risk of long-lived credentials.
3. Multi-Tenant App Consent: Securely managing external user access.
4. Key Vault Access Policies: Enforcing separation of duties.
5. Defender vs. Diagnostics Settings: Why you need both for security.
6. Managed Identity Risks: The danger of command-line access.

and more...

Entra ID Conditional Access with MFA Strength

Entra ID Conditional Access with MFA Strength

Goal: Go beyond basic MFA to ensure users are authenticating with phishing-resistant methods for critical applications.

How it Works: Conditional Access policies are "if-then" statements.

1. **IF** a user wants to access a sensitive app...
2. **THEN** they must satisfy a specific grant control.

Configuration: Instead of just selecting "Require multi-factor authentication," choose "**Require authentication strength**."

This allows you to specify which types of MFA are allowed:

1. **Good:** Multifactor authentication (includes SMS, Authenticator push notifications).
2. **Better:** Passwordless MFA (includes Authenticator app, Windows Hello for Business).
3. **Best:** Phishing-resistant MFA (includes FIDO2 Security Keys, Windows Hello for Business).

Entra ID Application Secrets

Entra ID Application Secrets

Scenario: A developer asks if it's possible to create a client secret for an App Registration that never expires. While technically possible via Public API calls, this is a critical security anti-pattern.

The Problem with Long-Lived Secrets:

1. Increased Attack Window: A compromised secret remains valid indefinitely, giving an attacker persistent access.
2. No Forced Rotation: It violates the fundamental security principle of credential rotation.
3. Secret Sprawl: Permanent secrets are often hard-coded, forgotten, and exposed in source code or configuration files.

Entra ID: Consenting to Multi-Tenant Apps

Entra ID: Consenting to Multi-Tenant Apps

Scenario: Your organization has built an application that needs to be used by users from other companies (other Entra ID tenants).

The Consent Framework: When an external user signs in for the first time, they are asked to grant consent. This allows your application to access their data based on the API permissions you requested.

1. User Consent: The individual user can approve permissions that only affect their own account (e.g., User.Read).
2. Admin Consent: Required for high-privilege permissions that affect the entire tenant (e.g., Directory.Read.All). An administrator from the external tenant must approve this.

Entra ID: Consenting to Multi-Tenant Apps

Security Best Practices:

1. Least Privilege: In your app registration, only request the absolute minimum API permissions required for your app to function.
2. Publisher Verification: Verify your application. This adds a blue checkmark to the consent prompt, building trust with users and admins.
3. Admin Consent Workflow: Enable this in the external tenant so admins can review and approve consent requests in a structured way.

Key Vault Access: Separation of Duties

Key Vault Access: Separation of Duties

Goal: Ensure that an application can only access the specific secrets it needs, and that human access is strictly controlled and audited.

The Principle of Separation: Use unique identities with minimal permissions.

1. Application Access: Each application should have its own dedicated Entra ID App Registration (Service Principal).
2. Human Access: Administrators or auditors should be granted access via Entra ID Groups, not their individual user accounts.

Key Vault Access: Separation of Duties

Example Implementation (using Access Policies):

App Identity: Create an App Registration named WebApp-Prod-SecretsReader.

Key Vault Policy for App:

1. Principal: WebApp-Prod-SecretsReader
2. Secret Permissions: Grant only Get. Do not grant List, Set, or Delete.

Human Identity: Create an Entra ID security group named App-KV-Admins. Add authorized users to this group.

Key Vault Policy for Humans:

1. Principal: App-KV-Admins
2. Secret Permissions: Grant Get, List, Set.

Defender for Cloud vs. Diagnostics Settings

Defender for Cloud vs. Diagnostics Settings

Question: "If I'm using Microsoft Defender for Cloud, why do I still need to configure Diagnostics Settings on my resources?"

They serve two different, complementary purposes:

Microsoft Defender for Cloud (CSPM/CWPP):

1. Purpose: Provides high-level security intelligence.
2. Answers: "Is my environment configured securely?" and "Am I under attack right now?"
3. Data: Curated security alerts, vulnerability findings, compliance recommendations. It tells you the "Why" (e.g., "This is an attack").

Azure Monitor Diagnostics Settings:

1. Purpose: Provides raw operational and audit logs.
2. Answers: "What, exactly, happened on this resource?" and "Who made this API call and when?"
3. Data: Verbose activity logs, performance metrics. It provides the "What" (e.g., "This is the raw log of the user sign-in").

Command-Line Access & Managed Identity Token Theft

Command-Line Access & Managed Identity Token Theft

The Hidden Risk: Gaining shell access to a resource (VM, Web App Console) is often equivalent to stealing its identity.

How Managed Identity Works: An Azure resource (like a VM) authenticates by requesting an access token from a non-routable, local endpoint called the Instance Metadata Service (IMDS).

The Attack Path:

1. Compromise: An attacker gains command-line access to your VM or Web App (e.g., through an RCE vulnerability, weak credentials).
2. Token Request: The attacker executes a simple command to call the local IMDS endpoint.
    1. curl 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://vault.azure.net'
3. Token Theft: The IMDS returns a valid OAuth token. It cannot distinguish between a legitimate application process and the attacker's shell command.
4. Impersonation: The attacker now uses this stolen token to access any resource the Managed Identity had permissions to (e.g., read all secrets from your Key Vault).

Q&A Time!

QUIZ TIME!

Time for the challenge!

Answer the questions:

1. What is the maximum lifetime of secrets for Entra ID Application?
2. What is the maximum lifetime value of the secret for Entra ID Application that you can find in the portal?
3. Do we need to export Diagnostics Logs to SIEM when using Azure Defender?
4. To enforce use of MFA within Azure which option is correct (Multi)?
5. What is the recommended Key Vault Access Policy secret permission for Entra ID Application or Managed Identity?

To answer, scan the QR or go to:

https://cqureacademy.com/cloud-challenge/

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

ADVANCED WINDOWS SECURITY COURSE 2026

COURE

Is *this* course for you?

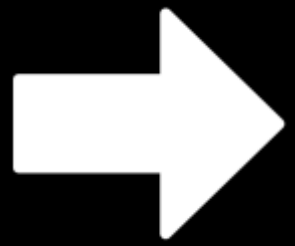
Intermediate/Advanced

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

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

Application

Processing
Limited to 200 seats only

Confirmation
Review within 5 working days

ADVANCED WINDOWS SECURITY COURSE 2026

DISCOVER THE BRAND NEW AGENDA

CQURE ACADEMY CQURE CONSULTING

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

WEBINAR PARTICIPANTS DISCOUNT FOR AWSC26

SPECIAL PRICE

$2599* save $600 net

**Valid only till October 12th, 2025*

https://cqu.re/awsc26

APPLY NOW
with code MISTAKES
PAY LATER.

Available
BY APPLICATION ONLY.

CQURE

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!

COURE

WEBINAR PARTICIPANTS DISCOUNT FOR AWSC26

SPECIAL PRICE

$2599* save $600 net

**Valid only till October 12th, 2025*

https://cqu.re/awsc26

APPLY NOW
with code MISTAKES
PAY LATER.

Available
BY APPLICATION ONLY.

CQURE

CHALLENGE WINNER

Challenge answers!

Answer the questions:

1. What is the maximum lifetime of secrets for Entra ID Application?
2. What is the maximum lifetime value of the secret for Entra ID Application that you can find in the portal?
3. Do we need to export Diagnostics Logs to SIEM when using Azure Defender?
4. To enforce use of MFA within Azure which option is correct (Multi)?
5. What is the recommended Key Vault Access Policy secret permission for Entra ID Application or Managed Identity?

To answer, scan the QR or go to:

https://cqureacademy.com/cloud-challenge/

Challenge answers!

1. What is the maximum lifetime of secrets for Entra ID Application? **7974 years**
2. What is the maximum lifetime value of the secret for Entra ID Application that you can find in the portal? **9999 year**
3. Do we need to export Diagnostics Logs to SIEM when using Azure Defender? **Yes**
4. To enforce use of MFA within Azure which option is correct (Multi)?
   - **Enable Security Defaults in Entra ID**
   - **Enforce Multi Factor Authentication in Conditional Rule with Onetime Password for new user**
   - **Enforce Require authentication strength with Multifactor Authentication with Password setup for new user**
5. What is the recommended Key Vault Access Policy secret permission for Entra ID Application or Managed Identity? **Get**

WINNER!

Q&A Time!

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

https://cqureacademy.com/blog

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