CQURE ACADEMY CQURE CONSULTING

ADVANCED WINDOWS SECURITY COURSE 2026

6-week online cybersecurity certification course for advanced professionals by Paula Januszkiewicz & CQURE Cybersecurity Experts

OCTOBER 28TH - DECEMBER 4TH, 2025

COURSE OVERVIEW

Everything you need to know to prepare against the threats heading our way in 2026 has been meticulously curated into 12 intensive and focused live modules which are taught over six weeks. Join Paula Januszkiewicz (CEO CQURE, Microsoft RD and MVP) and the team of CQURE Cybersecurity Experts including Sami Laiho, Peter Kloep, Amr Thabet, Michał Furmankiewicz, Damian Widera, Marcin Krawczyk, Artur Kalinowski.

TOPICS EXPLORED

Throughout the training, you will get to know multiple techniques for building an incident response readiness strategy and a ransomware attack IR playbook, digital investigation, discovering external perimeter, threat detection and OSINT in Azure, designing and implementing Zero Trust & ZT Network Access, AI and Machine Learning usages for cybersecurity. Also, we will go through penetration testing and information gathering methods including advanced ways of escalating privileges to domain admin, privileged access abuse in Microsoft SQL Server, investigating with PowerShell, tiering, Just-In-Time, and Admin-Forest solutions, Azure Kubernetes Security, implementing and managing the TLS protocol on Windows Server, and many more!

cqu.re/awsc26

PRICE $3199

CQURE ACADEMY CQURE CONSULTING

COURSE FORMULA

LIVE Training

You'll join our 2-hour live classes on a special interactive platform – happening twice a week at 7 PM CET | 10 AM PST.

Action-packed

You'll go through 12 modules in 6 weeks. We're not fluffing around, you've been warned. Look forward to some juicy surprises!

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 tools, slides, extra materials, and homework for you. Directly from Microsoft MVPs!

12-month Access

You'll get a full year of online access to all the recordings. Counted from the exam.

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 & CPE Points – "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 and receive detailed replies.

CQURE ACADEMY CQURE CONSULTING

MODULE 1

October 28, 2025

Attack Case Studies and Building Incident Response Readiness Strategy

Paula Januszkiewicz & Artur Kalinowski

A solid understanding of how ransomware attacks are conducted is key to securing your organization's infrastructure against a wide range of security incidents. From attack vectors and event timelines to their significance and consequences, Paula Januszkiewicz and Artur Kalinowski – CQURE Academy Experts – will guide you with the help of real-world examples. You will gain insight into critical organizational mistakes, postmortems of major incidents, and the characteristics of insider threats and data exfiltration methods.

Following case studies full of lessons learned, you'll discover how to create a swift and effective incident response. We will explain what it means to be "ready" for an incident by introducing the core principles of an effective Incident Response strategy, along with useful playbooks, tabletop exercises, and metrics for measuring readiness within your organization.

You'll also get a hands-on walkthrough of how to build a basic IR playbook, plus practical tips on templates and checklists. Tools included!

1. Case Study: Real-World Ransomware Attack

- Attack vectors (phishing, RDP, exploits)
- Event timeline (detection → response → recovery)
- Key organizational and technical mistakes
- Lessons learned from the incident

2. Case Study: Insider Threat & Data Exfiltration

- Characteristics of insider threats
- How the attacker bypassed security controls
- Security team's response
- What failed, what worked

3. Building an Effective Incident Response Strategy

- What does it mean to be "ready" for an incident?
- Six key IR pillars: detection, escalation, communication, documentation, Accountability, recovery
- The role of playbooks and tabletop exercises
- Example metrics for measuring readiness

4. Hands-On Walkthrough: Building a Basic IR Playbook

- How to build a simple playbook for a ransomware attack
- Tools
- The role of templates and checklists

5. Helpful Frameworks

- Overview of frameworks (e.g., NIST, SANS IR Steps, MITRE ATT&CK)

CQURE ACADEMY CQURE CONSULTING

MODULE 2

October 30, 2025

Zero Trust in Practice: Building Secure Architectures Beyond the Perimeter

Sami Laiho

In today's world, there is no such thing as a trusted network. The era of internal networks and network segments is over, and trust must be based on the identities of devices and users, rather than IP addresses. Join this AWSC Module, where Sami Laiho goes through one of the core pillars of Zero Trust - The Zero Trust Network Access. In this class, you will get a truthful SWOT analysis of this new way of thinking about network barriers. Many people see it as "Before it was only difficult when you were outside the office, but now on the internal network", but ZTNA is an Enabler that enables people to work the same way with the same level of security whether they are at the office or Starbucks.

1. Zero Trust and ZTNA

- What are they
- What are the benefits?
- Who are they for?

2. Zero Trust Networking

- Different approaches
- Various technologies
- SWOT of ZTNA

3. SWOT of ZTNA

- Best practices
- Lessons learned

MODULE 3

November 4, 2025

Discover your External Perimeter and Open Source Intelligence in Azure

Przemysław Tomasik

During this Module, CQURE Academy Expert, Przemysław Tomasik, will introduce core techniques of Open Source Intelligence Tools (OSINT) and explore their role in discovering the company's external perimeter. OSINT helps you (and the attacker) dig through public data to find exactly what is needed.

Join this session to learn practical techniques and leverage automated scripts to discover exposed assets, identify misconfigurations, and understand what attackers see by just 'glancing' at what public information holds. We'll delve into Azure-specific challenges and queries to enhance a proactive security strategy by collecting valuable data.

1. Introduction and Core OSINT Techniques
2. Information Gathering Beyond Infrastructure
3. Azure-specific Queries
4. Automated Discovery & Practical Application

CQURE ACADEMY CQURE CONSULTING

MODULE 4

November 6, 2025

AI Agents for Attack Investigation

Amr Thabet

During this Module, CQURE Academy Expert, Amr Thabet, will show you the MITRE ATT&CK framework together with the current attack landscape, case studies, and methods for the response process & digital investigation. You will go through AI and Machine Learning fundamentals, generative AI, and large language models, to get a Hands-on Lab: a chatbot for threat analysis and reporting. You will learn prompt engineering best practices, along with Retrieval-Augmented Generation (RAG), and get details on AI automations, tools, and their obstacles.

1. MITRE ATT&CK & Attack Investigation

- Understanding the MITRE ATT&CK framework
- Using the current attack landscape with attack examples
- Understand incident eesponse process & digital investigation

2. Introduction to AI for Cybersecurity

- AI and machine learning fundamentals
- Supervised vs unsupervised learning
- Generative AI and large language models
- Hands-on lab: simple chatbot for threat analysis & reporting

3. Prompt Engineering & Retrieval-Augmented Generation (RAG)

- Prompt engineering best practices
- Different prompt templates for cybersecurity use cases
- Intro to retrieval-augmented generation (RAG)
- Incorporating RAG & prompt engineering

4. Intro To AI Automations & Tool Calling:

- AI automation & n8n workflows
- Tool calling principles in AI
- Hands-on DNS domain check

5. AI Pitfalls & Obstacles

- AI hallucinations & how to avoid it
- Prompt injections & AI security

CQURE ACADEMY CQURE CONSULTING

MODULE 5

November 11, 2025

Azure Cloud Incident Response Part 1. Detection

Marcin Krawczyk

Cloud-related security incidents happen all the time. Why are they among the biggest security risks? What should be the principles and priorities during and after detection? Join our Expert, Marcin Krawczyk, in his AWSC Module on Azure Cloud Incident Response, and get fresh knowledge of attack foundations and detection. To understand the Azure security landscape and the possibilities of threat detection, we will go through its architecture and the usage of tools: Microsoft Defender for Cloud and Azure Sentinel, along with their threat detection and analytics aspects. The class will be full of practice; therefore, be prepared for hands-on demos, interactive exercises, and real-world case studies. Writing KQL queries included! This Module has its follow-up – check out Module 9.

1. Opening & Introductions

- Welcome and participant introductions
- Training objectives and expected outcomes
- Overview of azure security landscape

2. Azure Security Architecture Overview

- Microsoft defender for cloud
- Azure sentinel architecture and capabilities
- Integration with azure monitor and log analytics
- Native security tools ecosystem

3. Threat Detection in Azure

- Hands-on demo: navigating the defender for cloud dashboar
- Understanding security alerts and severity levels
- Azure sentinel analytics rules and detection methods
- Custom KQL queries for threat hunting
- Interactive exercise: writing basic KQL queries

4. Incident Classification and Initial Response

- Azure incident categorization framework
- Severity assessment and business impact analysis
- Escalation procedures and notification workflows
- Case study: real-world incident classification examples

CQURE ACADEMY CQURE CONSULTING

MODULE 6

November 13, 2025

Privileged Access Abuse in Databases: Detection and Defense

Damian Widera

Join our Expert and Microsoft MVP, Damian Widera, in his Module, on a comprehensive overview of privileged access abuse in Microsoft SQL Server environments, focusing on real-world risks, attacker techniques, and detection strategies. Participants will explore high-risk roles such as sysadmin, CONTROL SERVER, and db_owner, to understand how misconfigurations, role chaining, and impersonation can lead to privilege escalation and unauthorized actions. The session covers popular attack scenarios along with detection techniques using SQL Server Audit, Extended Events, and the Default Trace. We will go through defense methods like least privilege, role hygiene, privilege reviews, and real-time alerting. Advanced detection patterns and SIEM integration are also addressed.

1. Opening & Introductions

- Definition of privileged access abuse
- Real-world examples of incidents
- Common abuse scenarios: data theft, privilege escalation, creation of hidden accounts, tampering with audit logs

2. Privileged Access in SQL Server – Architecture and Risks

- Overview of high-risk roles: sysadmin, CONTROL SERVER, db_owne
- Differences between logins and users
- Role chaining and impersonation
- Common misconfigurations and privilege creep

3. Abuse Scenarios – What Attackers Do With Privileges

- Creating backdoor logins
- Granting roles silently
- Disabling auditing or deleting logs

4. Detection Techniques – How to Identify Privileged Abuse

- Using SQL server audit (Enterprise edition)
- Extended events for tracking GRANT, REVOKE, ALTER, EXECUTE AS
- Default trace usage
- Monitoring login attempts, privilege changes, and schema modifications

5. Defense and Mitigation

- Principle of least privilege
- Avoiding fixed server roles when possible
- Regular review of privileges
- Implementing alerts and controls

6. Advanced Detection Patterns (Optional)

- Tracking EXECUTE AS usage
- Detecting chained escalation scenarios
- Forwarding audit logs to an external SIEM

CQURE ACADEMY CQURE CONSULTING

MODULE 7

November 18, 2025

Real-World Pentesting: Windows Tips, Tricks, and Countermeasures

Artur Kalinowski

This module provides a hands-on exploration of advanced Windows attack techniques, focusing on tactics commonly observed during penetration tests, including tips, tricks, and countermeasures directly from the field. Our Expert, Artur Kalinowski, will guide you through real-life cases to get you a practical understanding of how attackers leverage built-in Windows features to bypass defenses. Crucial offensive techniques: obfuscation, LOLBins, covert exfiltration, SMB relay, payloads within ADS, and IFEO, are covered. Join this AWSC Module to understand threats and vulnerabilities along with practical tips and detection considerations. The gained knowledge will be ready to implement into a realistic internal pentest chain!

1. Opening & Introductions

- Scope: practical Windows attacks in real-world pentest
- Focus on obfuscation, LOLBins, covert exfiltration, SMB relay, ADS, IFEO

2. Obfuscation

- PowerShell and binary obfuscation basics
- Practical examples of obfuscation
- for stealth
- Why attackers use obfuscation during engagements

3. Using LOLBins

- Using built-in Windows binaries for payload execution and file transfer
- Key LOLBins: rundll32, regsvr32, certutil, bitsadmin
- Using LOLBins for stealth data exfiltration

4. Covert Exfiltration

- Exfiltrating data via ICMP, DNS, HTTP
- HTML smuggling for bypass and delivery
- Using malicious links + LLMNR/NBT-NS
- to capture/relay credential

5. SMB Relay Attacks

- LLMNR/NBT-NS poisoning for credential capture
- Performing SMB relay when SMB signing is disabled

6. Using Alternate Data Streams (ADS)

- Hiding and executing payloads within ADS
- Practical usage and detection considerations

7. Abuse of Image File Execution Options (IFEO)

- Using IFEO for persistence or defensive evasion
- Practical examples from engagements

8. Practical Attack Flow Example

- Combining covered techniques into a realistic internal pentest chain

CQURE ACADEMY CQURE CONSULTING

MODULE 8

November 20, 2025

PowerShell for Digital Investigation & Threat Hunting

Amr Thabet

This Module provides a practical introduction to PowerShell usage in incident response (IR) scenarios. Participants will learn PowerShell benefits for IR, as well as the risks and common abuse patterns seen during attacks. The session covers evidence collection techniques using PowerShell, including processes, network connections, event logs, registry entries, and scheduled tasks. Attendees will gain hands-on experience with threat hunting, learning to detect suspicious processes, scripts, lateral movement, and persistence mechanisms. A real-world case study demonstrates how to use PowerShell to build a forensic timeline and uncover an attacker's activities during an ongoing breach. You will learn detection strategies, with a focus on Power-Shell logging, Script Block Logging, and correlation with tools like Sysmon and EDR platforms. You will get tips from the fieldwork to minimize the risk of data contamina-tion and create a validated evidence collection.

1. Why PowerShell for IR

- Benefits for live investigations
- Risks and common abuse patterns

2. Collecting Evidence

- Processes, network connections, event logs
- Registry and scheduled tasks

3. Threat Hunting Techniques

- Detecting suspicious processes and scripts
- Finding lateral movement and persistence

4. Case Study: Live Investigation with PowerShell

- Using powershell for timeline building
- Identifying attacker activities

5. Detection and Logging

- Powerhell logging and scsript block logging
- Correlating with sysmon and EDR

6. Best Practices

- Safe evidence collection
- Avoiding contamination and ensuring validation

CQURE ACADEMY CQURE CONSULTING

MODULE 9

November 25, 2025

Azure Cloud Incident Response Part 2. Response and Recovery

Marcin Krawczyk

Follow-up to Module 5! This time, our Expert, Marcin Krawczyk, will focus on the response and recovery stages, starting from Evidence Collection and Investigation, through Containment and Remediation Strategies, Automation, Orchestration, to Recovery and Post-Incident Activities. Participants will utilize Microsoft Azure tools to explore logging architecture, key data sources, activity logs, diagnostic logs, VM snapshots, and network flow logs. Through hands-on labs, they will collect and preserve forensic evidence. The Module also covers containment remediation strategies, including network isolation using NSGs and Azure Firewall, identity-based containment through access revocation and MFA, and quarantine procedures for virtual machines. Participants will learn how to build incident response workflows with dedicated tools. The Module also addresses recovery and post-incident activities such as restoring systems from backups or identifying potential improvements to the company's security system. We will show you how to learn from mistakes and take advantage of documentation.

1. Evidence Collection and Investigation

- Azure logging architecture and data sources
- Hands-on lab: collecting evidence using azure tools
  - Activity logs and diagnostic logs
  - VM snapshots and network flow logs
  - Using azure resource graph for investigation
- Preserving evidence for forensic analysis

2. Containment and Remediation Strategies

- Network isolation using NSGs and azure firewall
- Identity-based containment (revoking access, MFA)
- Practical exercise: incident containment scenarios
- VM isolation and quarantine procedures

3. Automation and Orchestration

- Azure sentinel playbooks demonstration
- Logic apps for incident response automation
- Demo: automated response workflow creation
- Integration with external ticketing systems

4. Recovery and Post-Incident Activities

- System restoration from backups
- Security posture improvement
- Documentation and lessons learned process

CQURE ACADEMY CQURE CONSULTING

MODULE 10

November 27, 2025

Tiering, Just-In-Time, and Admin-Forest in „Real-Life" (Experience From the Field)

Peter Kloep

This Module, delivered by Peter Kloep, CQURE Academy Expert and Principal IT Architect, provides a practical introduction to implementing a tiering to secure the system. It starts with planning and defining Tier0, to explore its fundamental role. Common misconfigurations and lessons learned from real-world deployments will be discussed to highlight what works and what doesn't. Tips and tricks included! Next, participants will explore tiering implementation methods. The module also covers Just-In-Time Administration along with required and useful tools, and Admin Forest with its practical application and dedicated tools.

1. Planning and Processes

- From zero to "Tier0"
- Why is tiering essential?
- Which systems are Tier0?
- Common misconfiguration in current networks
- Naming convention and role- and permission-definition

2. Lessons from the Field

- What works in real-world deployments
- What stopped customers from successfully implementing tiering
- How to get from A to B?
- How to achieve user / admin-acceptance?

3. Implement Tiering

- Powershell-scripts
- GPOs
- Moving resources
- Administrative workstation / jump-host

4. Just-In-Time-Administration

- Simple just-in-time solutio
- Required / useful tools

5. Administrative Forest

- Benefits of an admin forest
- Automatic synchronization
- Tools for easy management

CQURE ACADEMY CQURE CONSULTING

MODULE 11

December 2, 2025

How to Think About Azure Kubernetes Security

Michał Furmankiewicz

This Module, delivered by Michał Furmankiewicz, MVP Alumni, architect, and consultant, explores key aspects of securing Azure Kubernetes. You'll learn how to protect the base infrastructure, manage cluster networking, and implement identity and access controls using the RBAC model. The session also covers security monitoring, data and host encryption, and ingress controllers or service meshes. You'll understand policy management best practices and secure application deployment strategies. By the end, you'll have a comprehensive foundation for thinking about Kubernetes security on Azure.

1. *Base Infrastructure of the Cluster*
2. *Cluster Networking (Traffic Going Outside, Coming Inside, and Within the Cluster)*
3. *Identity & Permissions (RBAC Model)*
4. *Monitoring and Security Monitoring*
5. *Data and Host Encryption*
6. *Ingress Controller/Service Mesh*
7. *Policy Management*
8. *Apps Deployment*

MODULE 12

December 4, 2025

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

Przemysław Tomasik

This Module provides a guide to securing Windows Server environments and .NET applications using Transport Layer Security (TLS). To secure the Windows Server and the company's applications, understanding how to properly configure TLS can significantly enhance the cybersecurity posture. During this Module, Przemek Tomasik, CQURE Academy Expert, will teach you how to implement and manage the TLS protocol on Windows Server and understand how it can impact the security of in-house developed applications. We will explore common TLS implementation pitfalls, such as weak cipher suites and improper certificate handling, offering practical strategies to mitigate these risks. Through code review exercises, participants will gain the skills to audit client-side and server-side TLS communication within .NET applications.

1. *TLS Fundamentals and Windows Server Implementation*
2. *Scanning and Hardening the System-Wide TLS Settings*
3. *Securing .NET Applications with TLS*
4. *Discovering, Understanding, and Fixing Issues in Code*

CQURE ACADEMY CQURE CONSULTING

YOUR EXPERTS

PAULA JANUSZKIEWICZ

CQURE Founder & CEO, Microsoft Regional Director, MVP, MCT

A world-class Cybersecurity Expert with over 20 years of experience in the field. She is often a top-rated speaker at the world's biggest conferences, including MS Ignite, and RSA, as her unique stage presence is always well-received among diverse audiences. Honorable Microsoft Regional Director and Enterprise Security MVP. To top it all, she has access to the source code of Windows!

SAMI LAIHO

Windows OS Expert, MVP

One of the world’s leading professionals in Windows OS troubleshooting and security. Sami has been working with and teaching OS troubleshooting, management, and security for more than 25 years. In the past, Sami’s two sessions were evaluated as the Top 2 sessions (out of 1700+ sessions) at Microsoft Ignite in Orlando.

PETER KLOEP

Cybersecurity Expert, Principal IT Architect

Principal IT Architect, specializing in secure Windows infrastructures and Public Key Infrastructure (PKI) solutions. His work bridges deep technical expertise with real-world implementation strategies, making him a trusted advisor in the IT security community.

AMR THABET

Cybersecurity Expert, Vulnerability Researcher

Malware researcher and incident handler with over 12 years of experience. He has worked in some of the Fortune 500 companies. He is the author of “Mastering Malware Analysis”. Amr had spoken at top cybersecurity conferences all around the world, including DEFCON.

MARCIN KRAWCZYK

Cloud & Cybersecurity Expert, MCT

Cybersecurity Expert with 13+ years in cloud architecture, specializing in Azure Security. Marcin designs, implements, and maintains secure and scalable cloud solutions for various business needs. Marcin’s core competencies include cloud security, cloud migration, cloud integration, cloud automation, and cloud optimization.

CQURE ACADEMY CQURE CONSULTING

YOUR EXPERTS

DAMIAN WIDERA

Cybersecurity Expert, Software Engineer, MVP, MCT

Software engineer with over 25 years of experience, now focused on modern data platforms, data analytics, and cloud technologies. His expertise is Microsoft Data Platform, including Microsoft SQL Server, Microsoft Fabric, and Azure services. He works with complex, data-driven systems, covering database architecture, optimization, and performance tuning in both on-premises and cloud environments.

MICHAŁ FURMANKIEWICZ

Azure Solutions Architect Expert, former MVP, MCT

Experienced professional (with 15+ years in business) working in various roles as a consultant, architect, and team leader, keen on problem-solving and business enablement through technology. Michal has spent the last 10 years working with various Cloud technologies on the market, helping customers to understand the broader concept, build solutions, and achieve business outcomes.

ARTUR KALINOWSKI

Cybersecurity Expert, Pentester

During almost 20 years of his IT career Artur developed his skills in cybersecurity from different perspectives. His experience ranges from a forensic analytics and a university lecturer to a security administrator. Artur worked for government financial institutions and for global cybersecurity companies.

PRZEMYSŁAW TOMASIK

Cybersecurity Expert, Pentester

Cybersecurity Expert with over 18 years of IT experience, focusing the last decade on security and compliance. He has worked for the financial, e-commerce, and hospitality industries in Fortune 500 companies. Przemek has delivered many penetration tests, scoped from Web Applications to Infrastructure, Configuration, and Code review.

cqu.re/awsc26