Masterclass:

Windows Server 2019 - Public Key Infrastructure Management

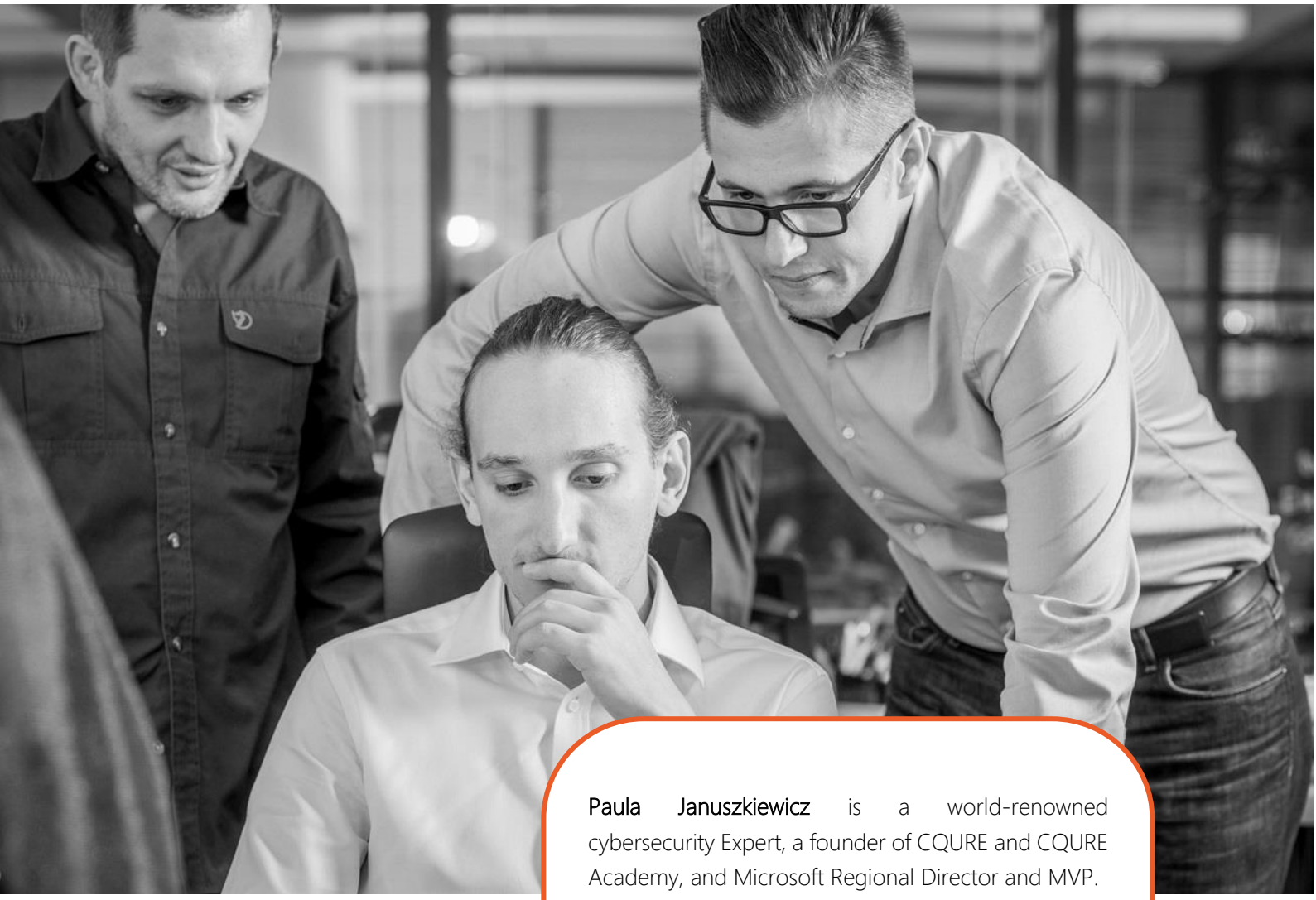
Duration: 5 days

CQURE

Warsaw New York Dubai Zug

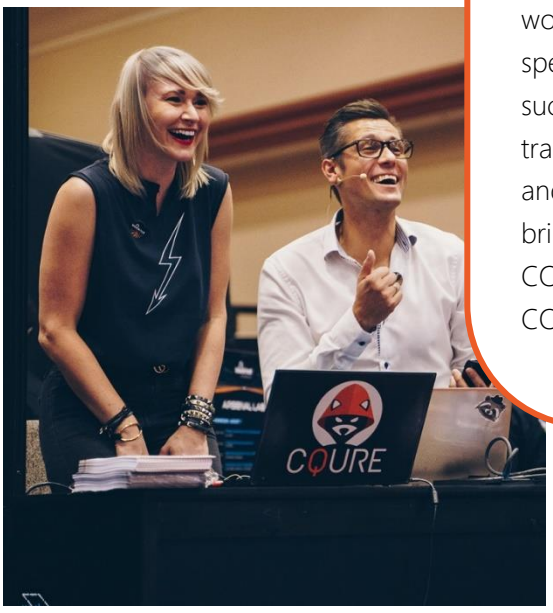
info@cqure.pl

www.cqure.pl
www.cqureacademy.com



Paula Januszkiewicz is a world-renowned cybersecurity Expert, a founder of CQURE and CQURE Academy, and Microsoft Regional Director and MVP.

CQURE Academy focuses on cybersecurity training program consisting of over 20 high-quality technical workshops and seminars and providing certification to specialists. Additionally, in October 2016 CQURE has successfully launched online and subscription-based training. **CQURE Experts** speak at international events and engage in multiple cybersecurity projects – they bring their knowledge and experience to trainings. CQURE Academy also involves R&D – that is why CQURE Team is recognizable in the cybersecurity field.



About the course

This 5-day course is considered essential for anyone who would like to expand knowledge about Public Key Infrastructure (PKI) in Microsoft technologies. During the course PKI is covered in depth, starting from the best practices for implementing secure and reliable PKI and ending up with most common scenarios of certificates usage in the enterprise environment.

At the end of the course you will be able to:

- Understand the core essence of PKI and cryptography.
- Evaluate and select appropriate PKI technologies.
- Install and configure PKI environments according to the best practices taken from practical experience.
- Secure existing PKI infrastructure.
- Choose appropriate types and manage the certificate lifecycle.
- Understand the benefits of certificates used in the infrastructure.
- Adjust PKI to your business needs.
- Become familiar with enterprise solutions that uses PKI and certificates for security.
- Configure and use certificates in: IIS, VPN, Wi-Fi, file encryption, e-mail security and many more.

All exercises are based on newest Windows Server 2019, Windows 10 with additional Linux and virtual network appliances that covers common scenarios.

To be a security expert you just need to know how certificates work. This subject is literally everywhere, even when implementing simple services certificates at least they can be used somewhere within the solution.
You will learn how to implement your PKI and use it to increase security of your organization!

Target audience

Network administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security, Chief Security Officers. What do you need to know? PKI basics, being advanced in administering Windows system. So typical experience in administering Windows systems and server platform.

Materials

After the workshop, you receive demo transcript, PowerPoint slides, PowerShell scripts, tools and lab instructions.

Agenda

Module 1: Essence of PKI

This module introduces cryptography basics and fundamentals of public key infrastructure with detailed information about certificates.

a. Cryptography basics
b. Fundamentals of PKI
c. Certificate types (X.509)
d. Certification authorities
e. Certificate Revocation Lists

Module 2: Designing and implementing CA Hierarchy

Module 2 covers one of the most important topics for successful and secure deployment of PKI in enterprise environment.

a. Planning
b. Preparing AD Environment
c. Implementing CA Hierarchy
d. Securing CA Hierarchy
e. Role separation
f. Security Policy

Module 3: PKI in Windows domain

In this module, you will become familiar with important aspects of implementing PKI in Windows Server 2019 environment.

a. Managing PKI
b. Configuring Certificate Templates
c. Configuring Certificate Enrollment
d. Configuring Key Archival and Recovery
e. Configuring Trust Between Organizations

Module 4: Upgrading PKI Infrastructure

This module focuses on supported scenarios and challenges regarding migration and upgrade of existing infrastructure.

a. Supported scenarios
b. Upgrading certificate templates
c. Migration scenarios

Module 5: PKI Security

This module reviews all aspects of security of PKI and certificates. We also cover physical security and usage of smartcards, TPM and HSM.

a. Deploying certificates to Domain Controllers
b. Certificate Revocation
c. Certificate Validation
d. CDP, AIA and OCSP
e. Planning and implementing disaster recovery
f. Deploying Smart Cards
g. TPM Virtual Smartcard
h. Private key security with HSM

Module 6: Securing applications with PKI

This module focuses on day-to-day operation and challenges in securing applications with certificates.

a. Secure IIS Traffic with SSL
b. IIS certificate store security
c. IIS users authentication
d. Windows logon with Smart Cards
e. E-mail security
f. Encrypting file system
g. Document and code signing

Module 7: PKI for network security

Last module covers how to use to PKI to increase network security.

a. VPN
b. Wireless Networking
c. 802.1X and NPS
d. Radius server
e. Ipsec
f. Mobile devices certificates with MDM, SCEP and NDE