Duration: 2 **days**

Masterclass:

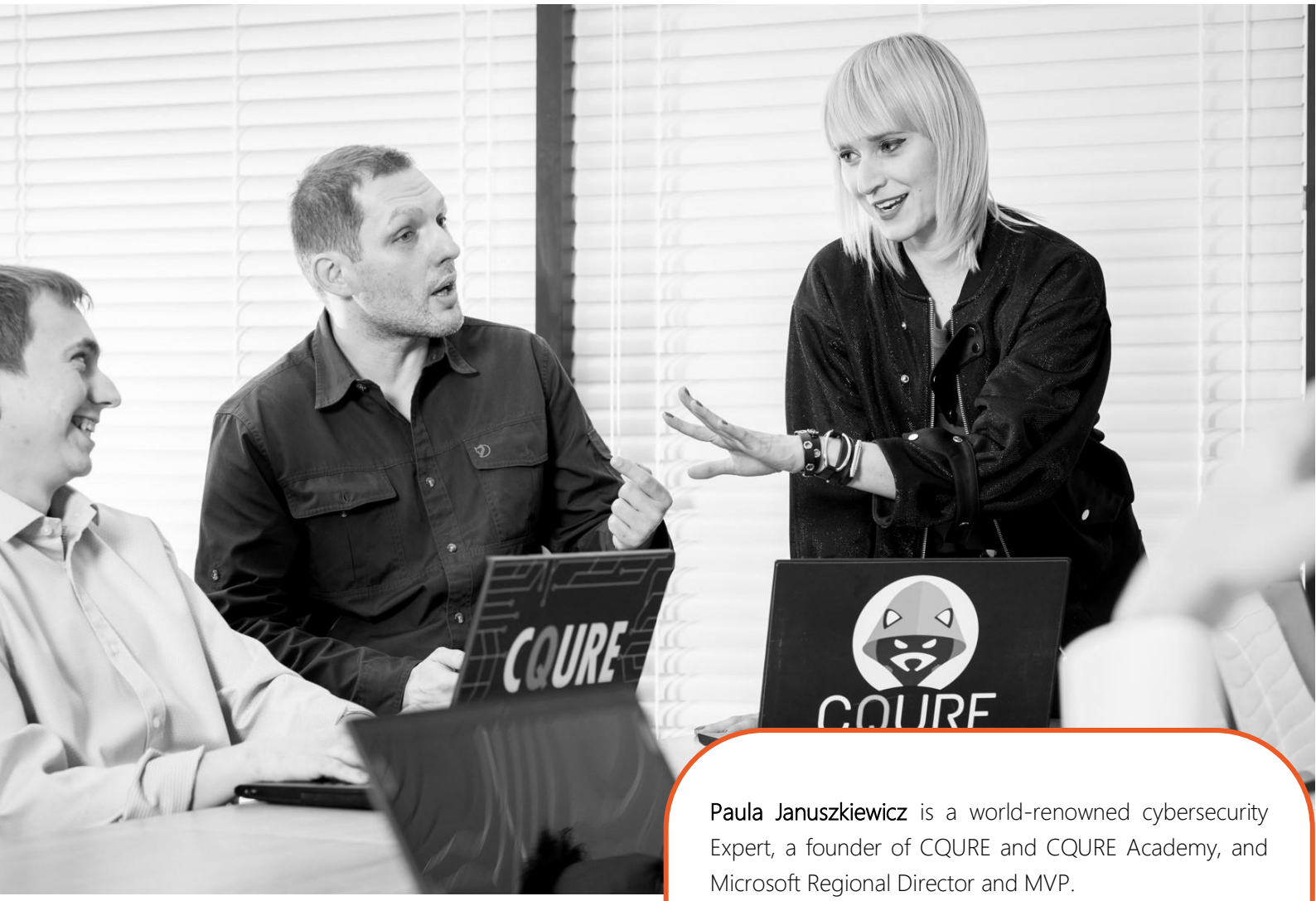
Advanced Malware Hunting

CQURE

Warsaw New York Dubai Zug

info@cqure.pl

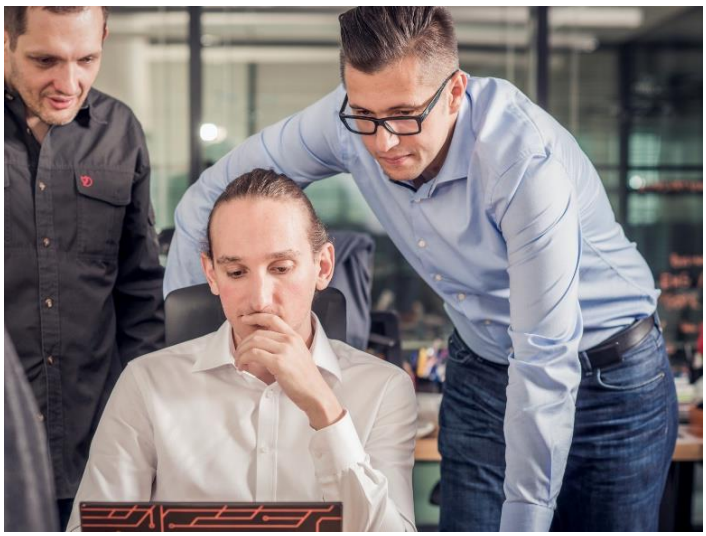
www.cqure.pl
www.cqureacademy.com



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 course teaches the ways of identifying how malware looks like, what malicious activities you should look out for and the ways of removing it. You will also learn how to implement and manage preventive solutions both for small and medium sized for enterprises and organizations. During this course you learn what makes piece of code malicious, go through historic examples and get familiar with different kinds of malware and how to identify various cases. Once we have sufficient understanding of techniques and capabilities of malware, we will start system and network hardening - you will implement security in depth solutions, such as whitelisting or virtualization, in order to protect assets.

Prerequisites

To attend this training, you should have a good hands-on experience in administering Windows infrastructure. At least 5-8 years in the field is recommended.

The course is an intense workshop! During these 2 days we provide caffeine candies – this course is really intense and in order not to miss a thing you MUST stay awake!

Target audience

Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

Materials

Author's unique tools, over 100 pages of exercises, presentations slides with notes.

Module 1: What is Malware

a) Malware History
b) Malware Goals
c) Types of Malware
d) Advanced Persistent Threats
e) Indicators of Compromise

Module 2: Introduction to Malware Analysis

a) Types of malware analysis
b) Goals of malware analysis
c) Impact analysis
d) Containment and mitigation
e) Incident prevention and response playbooks
f) Setting up sandbox environment
g) Cloud-based malware analysis

Module 3: Static Malware Analysis

a) Executable analysis
b) Extracting secrets
c) Determining if file is packed or obfuscated
d) Fingerprinting the malware
e) Pattern matching using YARA

Module 4: Behavioral Malware Analysis

a) Malware detonation
b) Sysinternals suite
c) Network communication analysis
d) Monitoring system events
e) Memory dump analysis
f) Simulating real environment

Module 5: Malicious non-exe files

a) Alternative binaries
b) PowerShell scripts
c) Office documents
d) JScript
e) HTML documents
f) Living off the land binaries

Module 6: Advanced Techniques used by Malware

a) Malware persistence methods
b) Malware stealth techniques
c) Covert channel communication
d) Domain Generator Algorithms
e) Anti-VM and Anti-debugging tricks

Module 7: Defending against Malware

a) Windows security solutions
b) Anti-Virus software
c) EDR software
d) Principle of least privilege
e) Application Whitelisting
f) Virtualization
g) Network and domain segmentation