Masterclass:

Forensics and Incident Handling

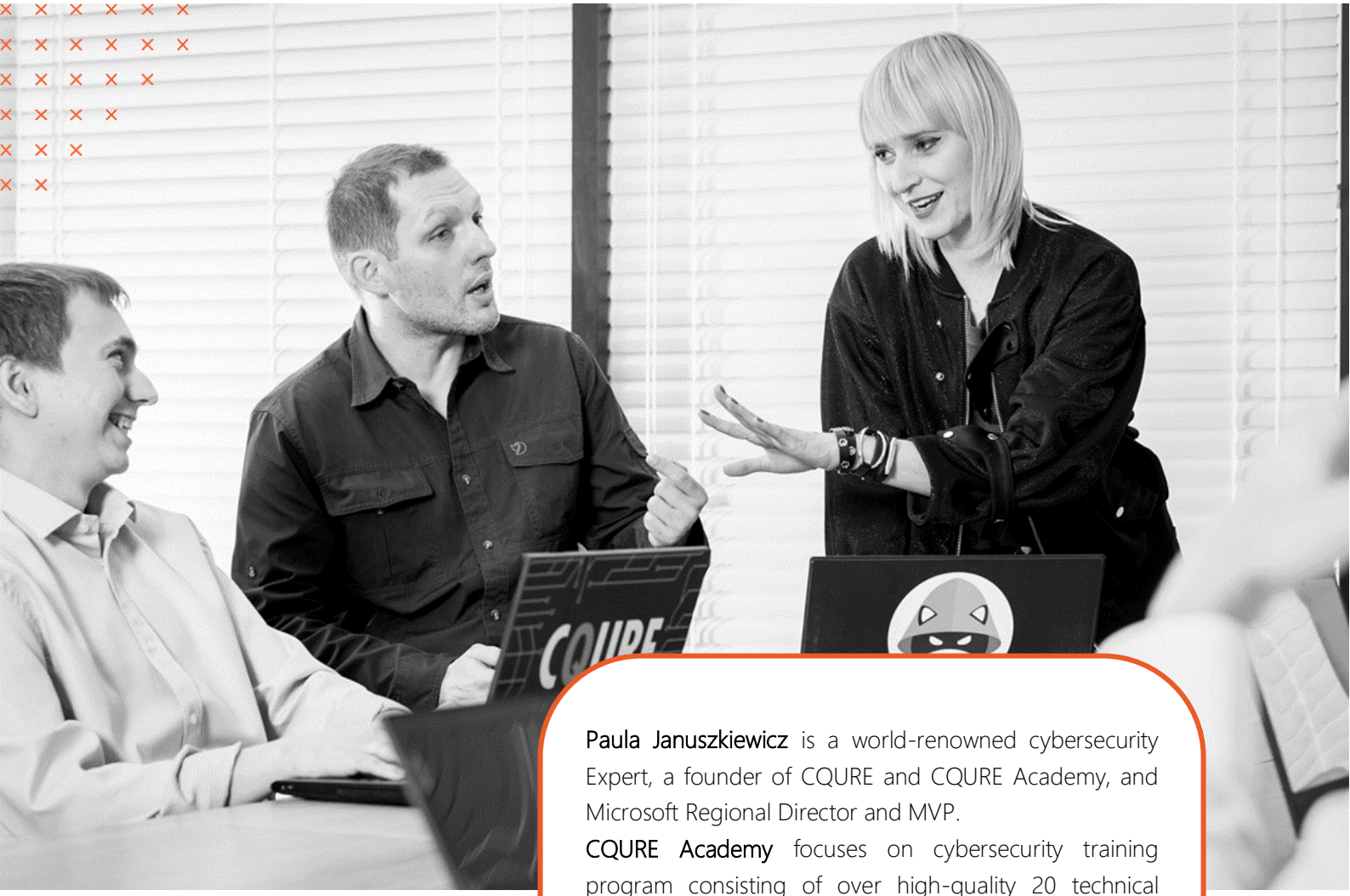
Duration: 2 days

CQURE

Warsaw New York Dubai Zug

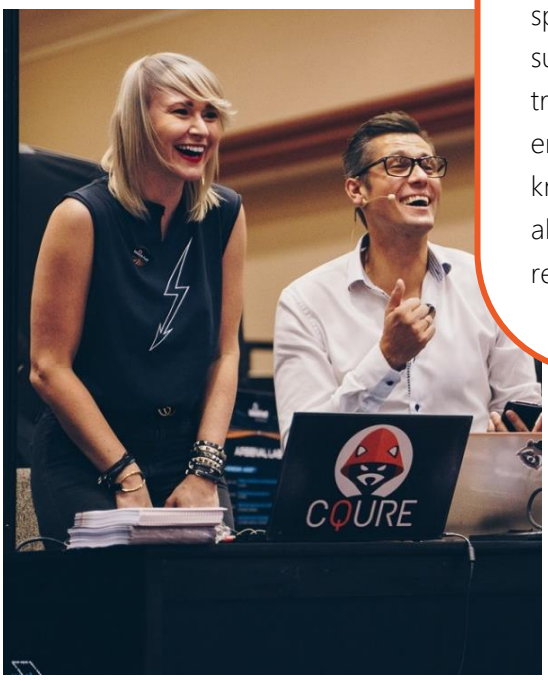
info@cqure.pl

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 high-quality 20 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

Forensics and Incident Handling are constantly evolving and crucial topics in the area of cybersecurity. In order to stay on top of the attackers, the knowledge of Individuals and Teams responsible for collecting digital evidences and handling the incidents has to be constantly enhanced and updated. This advanced training provides skills necessary to find, collect and preserve data in a correct manner, analyze it and get to know as much about the incident as possible. This is an intense hands-on course covering the general approach to forensics and incident handling, network forensics, important aspects of Windows internals, memory and storage analysis, detecting indicators of compromise and a proper way of reporting.

Target audience

IT professionals, Forensics and Incident Handling Specialists, Security Consultants, Enterprise Administrators, Infrastructure Architects, Security Professionals, Systems Engineers, Network Administrators and other people responsible for implementing network and perimeter security.

Materials

Author's unique tools, virtual lab environment, hands-on exercises, presentation slides with notes.

Examples of tools, software and examples used during the course

- Belkasoft RAM Capturer
- Wireshark
- Volatility
- The Sleuth Kit® (TSK)
- Autopsy
- DumpIt
- DC3DD
- Arsenal Image Mounter
- Reclaim Me
- ReFS Images
- SysInternals Toolkit
- ShadowCopyView
- RegRipper
- Rifiuti2
- Registry Explorer/RECmd
- FullEventLogView
- EVTXtract
- Loki IOC Scanner
- Yara
- LECmd
- LinkParser
- PECmd
- SkypeLogViewer
- SQLiteBrowser
- NetWork Miner
- StuxNet Memory Dump

Agenda

Module 1: Introduction to Incident Handling

1. Types and Examples of Cybersecurity Incidents
2. Signs of an Incident
3. Incident Prioritization
4. Incident Response and Handling Steps
5. Procedures and Preparation

Module 2: Securing Monitoring Operations

1. Industry Best Practices
2. Detecting Malware via DNS logs
3. Configuration Change Management
4. Leveraging Proxy and Firewall Data
5. Monitoring Critical Windows Events
6. Detecting Malware via Windows Event Logs

Module 3: Network Forensics and Monitoring

1. Types and approaches to network monitoring
2. Network evidence acquisition
3. Network protocols and Logs
4. LAB: Detecting Data Thievery
5. LAB: Detecting WebShells
6. Gathering data from network security appliances
7. Detecting intrusion patterns and attack indicators
8. Data correlation
9. Hunting malware in network traffic
10. Encoding and Encryption

Module 4: Windows Internals

1. Introduction to Windows Internals
2. Fooling Windows Task Manager
3. Processes and threads
4. PID and TID
5. Information gathering from the running operating system
6. Obtaining Volatile Data
7. A deep dive to Autoruns
8. Effective permissions auditing
9. PowerShell get NTFS permissions
10. Obtaining permissions information with AccessChck
11. Unnecessary and malicious services
12. Detecting unnecessary services with PowerShell

Module 5: Memory Dumping and Analysis

1. Introduction to memory dumping and analysis
2. Creating memory dump - Belkasoft RAM Capturer and DumpIt
3. Utilizing Volatility to analyze Windows memory image
4. Analyzing Stuxnet memory dump with Volatility
5. Automatic memory analysis with Volatile

Module 6: Indicators of compromise

1. Yara rules language
2. Malware detonation
3. Introduction to reverse engineering

Module 7: Storage Acquisition and Analysis

1. Introduction to storage acquisition and analysis
2. Drive Acquisition
3. Mounting Forensic Disk Images
4. Introduction to NTFS File System
5. Windows File System Analysis
6. Autopsy with other filesystems
7. Building timelines

Module 8: Reporting – Digital Evidence

This module covers the restrictions and important details about digital evidence gathering. Moreover, a proper structure of digital evidence report will be introduced.