Duration: 2 days

Masterclass:

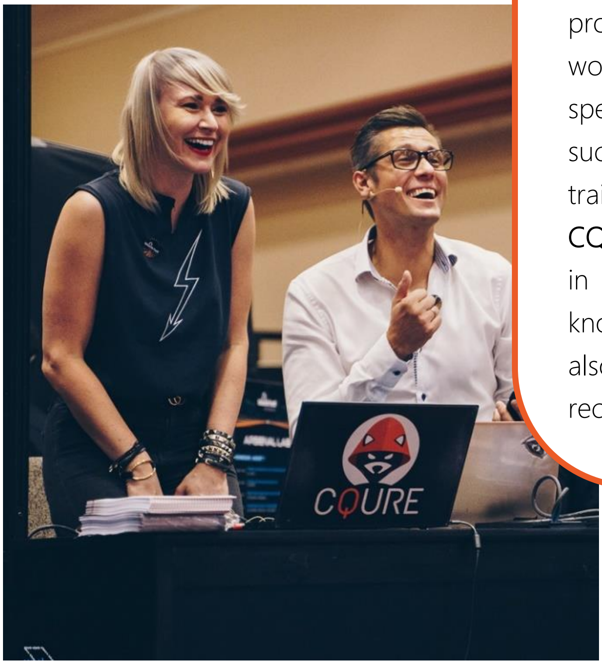
Managing and Defending Against Current Threats

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

On completion of this course you will be able to:

1. Analyze emerging trends in attacks.
2. Identify areas of vulnerability within your organization.
3. Prepare a risk assessment for your organization.
4. Report and recommend countermeasures.
5. Develop a threat management plan for your organization.

Prerequisites:

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

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 200 pages of exercises, presentation slides with notes.

Agenda:

Module 1: Identifying Areas of Vulnerability (Day 1)

This part introduces the new cybersecurity challenges and trends, emphasizing on data security and integration through and into the cloud and the challenges of the coordination of the cloud and on-premise security solutions. Security is a business enabler, and it is only when it is viewed from a business perspective that we can truly make the right decisions. You will learn how to define values of your company which needs to be protected or restricted. You will know how to find obvious and not so obvious sensitive information which can be monetized by adversaries. Having that scope defined and knowing your resources you will know where the biggest gaps in your security posture are.

1. Defining the assets which your company needs to protect
2. Defining the other sensitive information that needs to be protected

Module 2: Modern Attack Techniques (Day 1)

In this world where most of the things happen online, hacking provides wider opportunities for the hackers to gain unauthorized access to the unclassified information like credit card details, email account details, and other personal information. So, it is also important to know some of the hacking techniques that are commonly used to get your personal information in an unauthorized way. In this module you will become familiar with the modern hacking techniques.

1. OS platform threats and attacks
2. Web based threats and attacks
3. E-mail threats and attacks
4. Physical access threats and attacks
5. Social threats and attacks
6. Wireless threats and attacks

Module 3: Malicious Software Techniques (Day 2)

The hacker can run a malicious program which the user believes to be authentic. This way, after installing the malicious program, the hacker gets unprivileged access. Techniques are becoming more sophisticated than ever. In this module you will learn how modern malware works and what are the ways to discover its operations.

1. Types of the attacks
2. Points of entry
3. Persistence methods
4. Hiding traces
5. Case study: ransomware examples

Module 4: Discovery and Analysis of the Modern Attacks (Day 2)

Most computer vulnerabilities can be exploited in a variety of ways. Hacker attacks may use a single specific exploit, several exploits at the same time, a misconfiguration in one of the system components or even a backdoor from an earlier attack. Due to this, detecting hacker attacks is not an easy task. This module gives a few basic guidelines to help you figure out either if your machine is under attack or if the security of your system has been compromised.

1. Host, Port and Service Discovery
2. Monitoring Patching, Applications, Service Logs
3. Detecting the most common attacks:
    a. DNS Reconnaissance
    b. Directory Service Enumeration
    c. Enumerating high privileges accounts
    d. SMB Session Enumeration
    e. Enumerate Credentials stored in memory
    f. Overpass – the – hash
    g. Harvesting Credentials
    h. Pass – The – Ticket
    i. Remote Code Execution
    j. Compromise KRBTGT Account
    k. Golden Ticket
4. Using Sysmon in the advanced monitoring configuration
5. Log Collection
6. Scripting and Automation