Masterclass:

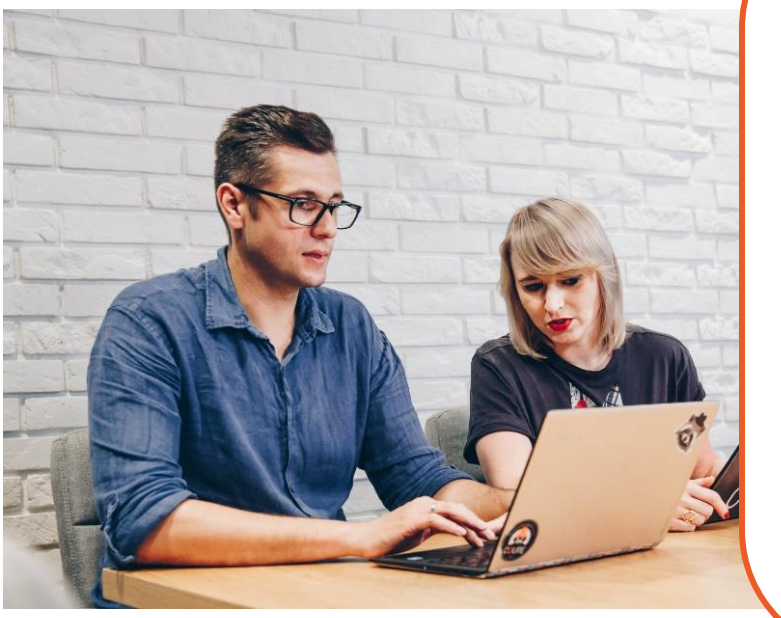
Developing a Cybersecurity Crisis Management Plan

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

Every organization should have a valid and tested Cybersecurity Crisis Management Plan in place. Forensics and Incident Handling are constantly evolving and crucial topics in the area of cybersecurity. What often seems to be an issue is that the crisis can emerge in a multitude of ways and all possible scenarios have to be taken care of. If your organization has not taken care of it then this cannot wait any longer! In this workshop you will learn how to define what a certain type of a cyber incident will mean to your organization and how to develop a internal plan for handling the compromise.

During the training you will also learn the crucial steps that need to be taken care of during an incident and what to do subsequently – including your team's action plan, evidence gathering as well as the any legal actions and crisis communication that needs to be taken care of.

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.

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: Incident Response and Handling Steps

1. How to Identify an Incident
2. Handling Incidents Techniques
3. Incident Response Team Services
4. Defining the Relationship between Incident Response, Incident Handling, and Incident Management
5. Incident Response Best Practices
6. Incident Response Policy
7. Incident Response Plan Checklist
8. Incident Handling Preparation
9. Incident Prevention
10. Following the Containment Strategy to Stop Unauthorized Access
11. Eradication and Recovery
12. Detecting the Inappropriate Usage Incidents
13. Multiple Component Incidents
14. Containment Strategy to Stop Multiple Component Incidents

Module 3: Securing Monitoring Operations and Evidence Gathering

1. Industry Best Practices
2. Objectives of Forensics Analysis
3. Role of Forensics Analysis in Incident Response
4. Forensic Readiness And Business Continuity
5. Types of Computer Forensics
6. Computer Forensic Investigator
7. Computer Forensics Process
8. Collecting Electronic Evidence
9. Challenging Aspects of Digital Evidence
10. Forensics in the Information System Life Cycle
11. Forensic Analysis Guidelines
12. Forensics Analysis Tools
13. Memory acquisition techniques