Quantuz Global

Cyberattack Detection & **Response Strategies**

Date 25th-27th March 2024

TIMINGS:
10:00 AM-03:00 PM

info@quantuzglobal.com
https://quantuzglobal.com

LIVE **ONLINE** TRAINING

Course Overview

This program provides the entire process of incident handling and response and hands-on labs that teach the tactical procedures and techniques required to effectively plan, record, triage, notify and contain. Participants will learn the handling of various types of incidents, risk assessment methodologies, as well as laws and policies related to incident handling. After attending the course, participants will be able to create IH&R policies and deal with different types of security incidents such as malware, email security, network security, web application security, cloud security, and insider threat-related incidents

The course also covers post-incident activities such as containment, eradication, evidence gathering and forensic analysis, leading to prosecution or countermeasures to ensure the incident is not repeated.

With over 95 advanced labs, 800 tools covered, and exposure to incident handling activities on many different operating systems, this course provides a well-rounded, but tactical approach to planning for and dealing with cyberattacks.

MODULE 01 INTRODUCTION TO INCIDENT HANDLING AND RESPONSE

- Understand Information Security Threats and Attack Vectors
- Explain Various Attack and Defense Frameworks
- Understand Information Security Concepts
- Understand Information Security Incidents
- Understand the Incident Management Process
- Understand Incident Response Automation and Orchestration
- Describe Various Incident Handling and Response Best Practices
- Explain Various Standards Related to Incident Handling and Response
- Explain Various Cybersecurity Frameworks
- Understand Incident Handling Laws and Legal Compliance

MODULE 02 INCIDENT HANDLING AND RESPONSE PROCESS

- Understand Incident Handling and Response (IH&R) Process
- Explain Preparation Steps for Incident Handling and Response
- Understand Incident Recording and Assignment
- Understand Incident Triage
- Explain the Process of Notification
- Understand the Process of Containment
- Describe Evidence Gathering and Forensics Analysis
- Explain the Process of Eradication
- Understand the Process of Recovery
- Describe Various Post-Incident Activities
- Explain the Importance of Information Sharing Activities

MODULE 03 FIRST RESPONSE

- Explain the Concept of First Response
- Understand the Process of Securing and Documenting the Crime Scene
- Understand the Process of Collecting Evidence at the Crime Scene
- Explain the Process for Preserving, Packaging, and Transporting Evidence

MODULE 04 HANDLING AND RESPONDING TO MALWARE INCIDENTS

- Understand the Handling of Malware Incidents
- Explain Preparation for Handling Malware Incidents
- Understand Detection of Malware Incidents
- Explain Containment of Malware Incidents
- Describe How to Perform Malware Analysis
- Understand Eradication of Malware Incidents
- Explain Recovery after Malware Incidents
- Understand the Handling of Malware Incidents - Case Study
- Describe Best Practices against Malware Incidents

MODULE 05 HANDLING AND RESPONDING TO EMAIL SECURITY INCIDENTS

- Understand Email Security Incidents
- Explain Preparation Steps for Handling Email Security Incidents
- Understand Detection and Containment of Email Security Incidents
- Understand Analysis of Email Security Incidents
- Explain Eradication of Email Security Incidents
- Understand the Process of Recovery after Email Security Incidents
- Understand the Handling of Email Security Incidents - Case Study
- Explain Best Practices against Email Security Incidents

MODULE 06 HANDLING AND RESPONDING TO NETWORK SECURITY INCIDENTS

- Understand the Handling of Network Security Incidents
- Prepare to Handle Network Security Incidents
- Understand Detection and Validation of Network Security Incidents
- Understand the Handling of Unauthorized Access Incidents
- Understand the Handling of Inappropriate Usage Incidents
- Understand the Handling of Denial-of-Service Incidents
- Understand the Handling of Wireless Network Security Incidents
- Understand the Handling of Network Security Incidents - Case Study
- Describe Best Practices against Network Security Incidents

MODULE 07 HANDLING AND RESPONDING TO WEB APPLICATION SECURITY INCIDENTS

- Understand the Handling of Web Application Incidents
- Explain Preparation for Handling Web Application Security Incidents
- Understand Detection and Containment of Web Application Security Incidents
- Explain Analysis of Web Application Security Incidents
- Understand Eradication of Web Application Security Incidents
- Explain Recovery after Web Application Security Incidents
- Understand the Handling of Web Application Security Incidents - Case Study
- Describe Best Practices for Securing Web Applications

MODULE 08 HANDLING AND RESPONDING TO CLOUD SECURITY INCIDENTS

- Understand the Handling of Cloud Security Incidents
- Explain Various Steps Involved in Handling Cloud Security Incidents
- Understand How to Handle Azure Security Incidents
- Understand How to Handle AWS Security Incidents
- Understand How to Handle Google Cloud Security Incidents
- Understand the Handling of Cloud Security Incidents - Case Study
- Explain Best Practices against Cloud Security Incidents

MODULE 09 HANDLING AND RESPONDING TO INSIDER THREATS

- Understand the Handling of Insider Threats
- Explain Preparation Steps for Handling Insider Threats
- Understand Detection and Containment of Insider Threats
- Explain Analysis of Insider Threats
- Understand Eradication of Insider Threats
- Understand the Process of Recovery after Insider Attacks
- Understand the Handling of Insider Threats - Case Study
- Describe Best Practices against Insider Threats

MODULE 10 FIRST RESPONSE

- Understand the Handling of Endpoint Security Incidents
- Explain the Handling of Mobile-based Security Incidents
- Explain the Handling of IoT-based Security Incidents
- Explain the Handling of OT-based Security Incidents
- Understand the Handling of Endpoint Security Incidents - Case Study

Learning Outcomes

- Key issues plaguing the information security world.
- Various types of cyber security threats, attack vectors, threat actors, and their motives, goals, and objectives of cyber security attacks
- Various attack and defense frameworks (Cyber Kill Chain Methodology, MITRE ATT&CK Framework, etc.)
- Performing Shutdown estimating; including the cost of doing the work and the time that it will take to complete it.
- Fundamentals of information security concepts (Vulnerability assessment, risk management, cyber threat intelligence, threat modeling, and threat hunting)
- Fundamentals of incident management (information security incidents, signs and costs of an incident, incident handling and response, and incident response automation and orchestration)
- Different incident handling and response best practices, standards, cybersecurity frameworks, laws, acts, and regulations
- Various steps involved in planning incident handling and response program (Planning, recording and assignment, triage, notification, containment, evidence gathering and forensic analysis, eradication, recovery, and post-incident activities)
- Importance of first response and first response procedure (Evidence collection, documentation, preservation, packaging, and transportation)
- How to handle and respond to different types of cybersecurity incidents in a systematic way (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, insider threat-related incidents, and endpoint security incidents)

Learning Outcomes

01

Lab setup

simulates Real-time Environment with real-life networks and platforms

02

Every learning

objective is demonstrated using Complex and advanced labs

03

Lab-intensive

Program (Demonstration of Various Cybersecurity Incidents via Scenario-based Labs)

04

Hands-on Program

(Dedication of 50% of Training Time to Labs)

05

Latest Patched

Windows operating systems

06

Ubuntu,

Parrot Security, Pfsense Firewall, OSSIM Server, And Android for Performing Labs.

07

Advanced

Forensic Software

08

Latest

Threat Intelligence Platforms

09

Latest

Network Monitoring Solutions Scenario-based labs

10

Learn

to handle and respond to various types of security incidents on a real-time organizational network.

11

Understand

Detect & analyze modern attack TTPs using various incident handling tools

Who Should Attend

1. Incident Handler
2. Incident Responder
3. Incident Response Consultant / Associate / Analyst / Engineer / Specialist / Expert / Manager
4. CSIRT Analyst/Engineer/Manager
5. Cyber Defense Security Consultant/Associate/Analyst
6. IT Security Operations Center Analyst (SOC Analyst/Engineer)
7. Cyber Forensic Investigator/Consultant/Analyst/Manager
8. Digital Forensic Analyst
9. Cyber Risk Vulnerability Analyst / Manager
10. Cyber Intelligence Analyst and Cyber Security Threat Analyst/Specialist
11. Cyber Security Incident Response Team Lead
12. Penetration Tester

Trainer profile

DEAN J.POMPILIO

Mr.Pompilio began his IT career in 1989 and he has worked for several Fortune 500 companies and financial institutions. These include Motorola, Bank of America, Capital One, and the World Bank. He has also held Sr. Security Engineer roles at the U.S. Department of Justice and the U.S. Department of State.

Mr.Pompilio began teaching IT and cybersecurity certification courses. He has trained thousands of IT professionals and military personnel in dozens of countries around the world. Mr.Pompilio is also an adjunct professor at the University of Charleston, WV. He is highly rated by his students for his comprehensive experience in the IT field, in addition to his vast knowledge of cybersecurity and risk management. His students are expertly prepared for certifications from CompTIA, EC-Council, ISACA, Microsoft, VMware, and ISC2.

Mr.Pompilio has extensive hands-on experience in systems administration, network engineering, firewall engineering, security engineering, and penetration testing. In addition to technical skills, he has also focused on the development of policies and procedures, risk management, and business process re-engineering.

Training fee :
$1599 per delegate

Cyberattack Detection & Response Strategies

25th-27th March 2024

Sales Contract

Event Code: **CDRS016**

Please complete this form and mail to : info@quantuzglobal.com office:- +91**9739479900**

Registration Details

☐ Ms: ☐ Mrs: ☐ Mr Surname: ..... ☐ Ms: ☐ Mrs: ☐ Mr Surname: .....

Name: ..... Name: .....

Job Title: ..... Job Title: .....

Email: ..... Email : .....

Organization Details

Country:

Organization: ..... Phone: .....

Contact Person: ..... Fax: .....

Email: ..... Address: .....

City: ..... Nature of Business: .....

Country: ..... Website: .....

Authorization

Booking is invalid without a signature:

Signatory must be authorized on behalf of contracting organization.:

Name: .....

Date: .....

Signature: .....

FEE

☐ **USD 1599** per delegate

20 USD Administration Charges will be applied.
Fees to be paid immediately after registration

Terms and Conditions

- Course fee must be paid in full at time of enrolment. Your enrolments are not guaranteed unless full payment is received by us.
- If we are notified of your enrolment cancellation more than 30 days from the training date, your payment can be 100% refunded to you or applied to another QUANTUZ GLOBAL
- training and/or instructor of your choice. This credit will expire after 1 year and the funds will be considered forfeited.
- If we are notified of your cancellation 15 days or less from the start of training course, your payment will be non-refundable.
- If you voluntarily withdraw from training after the commencement of the class for any reason, your class fee will not be refunded or credited.
- If, for any reason, you are removed from a class you are participating in by the instructor, you are entitled to a 25% refund. The remaining fee is not refundable.
- In the event QUANTUZ GLOBAL or the instructor cancels a class for any reason prior to the class, you have the option to apply your registration payment to another QUANTUZ GLOBAL course or a full refund.
- If the instructor has to suspend a class due to circumstances (i.e. weather, acts of God, etc) outside of the instructor's control, QUANTUZ GLOBAL will make every attempt to reschedule
- the class expeditiously. Refunds will not be issued under such circumstances.
- QUANTUZ GLOBAL, reserves the right to change, update, or alter our policies at any time.
- ASSISTANCE : If you need assistance, please feel free to email info@quantuzglobal.com