COURSE OUTLINE

INCIDENT RESPONSE
Cyber Security Incident Response (CSIR)

●●●● **SPECIALIST-LEVEL COURSE** Cost: **£3,250.00** + VAT Duration: **5 days**

This specialist-level course is for technical professionals who are looking to develop or improve their knowledge or ability in the Cyber Security Incident Response (CSIR) field.

COURSE OVERVIEW

This five-day course follows the CREST incident response model and focuses on the knowledge and key skills required to effectively respond to a cyber incident.

You will spend a good proportion of the course practising and honing your CSIR skills and methodologies utilising virtualised environments which replicate real-life scenarios and the unique challenges faced by CSIR consultants.

THE SKILLS YOU WILL LEARN

You will learn and practice core level and advanced CSIR skills needed to effectively respond to a cyber breach together with methods to identify and examine relevant artefacts of interest.

Upon completion of the course you will have learnt:

- Advanced use of PowerShell and exploitation of WMI
- Writing of bespoke PowerShell scripts and parsers
- Identification of suspect processes
- Advanced detection and analysis of injected processes
- Identification and analysis of infected documents (MS Office e & PDF)
- Infection vector analysis
- Rebuilding network traffic
- Breakdown and examination of log files

KEY BENEFITS

This course will enable you to learn new methodologies for responding to CSIR events and practice both core and advanced techniques. You will also gain confidence and improve your CSIR skills for when responding to a cyber event.

WHO SHOULD ATTEND

This is an intensive training course designed for CSIR practitioners and cyber security practitioners involved in the discipline, or forensic practitioners who wish to extend their knowledge and skills in this unique field. These include:

- Cyber security incident response team members
- System/network administrators/ engineers
- IT security personnel/security officers
- Forensic practitioners
- Law enforcement officers & agents

PREREQUISITES

You will need an understanding or experience of:

- The CSIR process
- Forensic investigations
- Windows operating system
- CLI

We strongly recommend completion of the PA CFIP and CMI courses or similar as a minimum before attending this course.

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA's Cyber Security Incident Responder (CSIR) qualification. The course will also provide underpinning knowledge required to undertake the CREST CRIA certification.

To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email cybereducation@paconsulting.com

COURSE OUTLINE

INCIDENT RESPONSE
Cyber Security Incident Response (CSIR)

●●●● **SPECIALIST-LEVEL COURSE** Cost: £3,250.00 + VAT Duration: **5 days**

SYLLABUS

Throughout the course, your time will be split between being taught the methods and principles of CSIR and applying these in practical, hands-on exercises based on real-life scenarios.

PA Consulting
Global Innovation & Technology Centre
Back Lane, Melbourn
Herts, SG8 6DP, United Kingdom
tel: +44(0) 1763 285285
email: cybereducation@paconsulting.com
www: cybereducation.paconsulting.com

SYLLABUS

1. Law & Compliance
a. Applicable legislation
b. Regulatory compliance
c. ACPO guidelines
d. Reporting matters
e. Chain of custody

2. Cyber Security
a. The threat
b. CSIR planning

3. File Systems
a. Data storage fundamentals
b. Partitioning schemes
c. FAT32 file system
d. NT file system

4. Storage Media
a. Storage media types
b. RAID types
c. Network storage

5. Data Acquisition - Host
a. Collection sites
b. Order of volatility
c. Image types
d. Image methods
e. Protecting source data

6. Windows OS Essentials
a. OS information
b. Windows Registry
c. Startup methods
d. Account types
e. User profiles
f. Temporary files
g. Virtual memory files
h. System processes
i. System restore
j. Executed programs
k. Extracting data from memory for analysis
l. Memory analysis basics
m. Access control

7. Windows OS Advanced
a. Intel x86/x64 instruction set
b. Virtual memory implementation
c. Virtualisation technology
d. Windows NT kernel
e. API calls

8. Networking
a. OSI model
b. Protocols
c. Ports
d. IP addresses
e. Network types
f. Network topologies
g. Network cable types
h. IP address routing
i. Windows domain
j. Protocol security

9. Cryptography
a. Encoding schemes
b. Encryption systems
c. Modes of operation
d. Digital signatures
e. PKI
f. Encryption software
g. Bitwise operators
h. Key storage
i. Hashing
j. EFS

10. Log File Types
a. Log file types
b. Log file analysis

11. Metadata
a. Email
b. Documents
c. File formats

12. Malicious Software
a. The basics
b. Identification
c. Infection methods
d. Obfuscation techniques
e. Analysis environments
f. Analysis methods
g. Hooking techniques
h. Botnets
i. Persistence mechanisms
j. Detecting beacons
k. Removal

13. Investigation Techniques
a. Web browser artefacts
b. OSINT & investigations
c. Fingerprinting
d. Data of interest
e. Timelines
f. Packed files
g. Network security & configuration
h. IT audit
i. Network traffic capture
j. MS Office documents & applications
k. PDF documents
l. Understanding anti-virus
m. Reporting

To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email cybereducation@paconsulting.com