COURSE OUTLINE

INCIDENT RESPONSE
Certified Security Operations Centre Analyst (CSOCA)

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

This fundamentals-level course provides the basic skills and knowledge for individuals who are looking to be or are currently employed within a private or public sector Security Operations Centre (SOC).

COURSE OVERVIEW

This five-day course will enable you to understand how a SOC functions and provide you with the fundamental knowledge and understanding required for employment within a SOC.

You will spend a good portion of the course practising and honing key skills and methodologies which replicate real-life security threat scenarios faced by SOC's today.

THE SKILLS YOU WILL LEARN

You will learn and practice core level and advanced skills to be an effective SOC analyst or team member.

Upon completion of the course you will have learnt:

- The threats and risks to a business network
- Gain a better understanding of threat intelligence using OSINT
- How malicious software can compromise a system
- Using SIEM tools to collate and analyse data of interest
- Fundamental and in-depth logging
- Analytical techniques

KEY BENEFITS

This course will enable you to gain confidence within a SOC environment by reinforcing or learning new information and methodologies.

WHO SHOULD ATTEND?

This course was specifically designed for individuals who intend to be or have recently joined as a SOC analyst or team member or to recognise those more seasoned individuals employed within the SOC.

SYLLABUS

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

PREREQUISITES

You will need a basic understanding of IT infrastructure.

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA's Certified Security Operations Centre Analyst (CSOCA) qualification.

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
Certified Security Operations Centre Analyst (CSOCA)

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

SYLLABUS

1. The Security Operations Centre
a. What is a SOC
b. SOC types
c. Staff Roles
d. Decision Making

2. Threats & Risks
a. The Threat
b. Attacker Motivation
c. Attack Types
d. Threat Attribution
e. Threat Assessments
f. Business Threats
g. Employee Threats
h. Cyber Kill Chain
i. ATT&CK Framework

3. Computer Networks
a. Network Types
b. Network Topologies
c. Network Models
d. IP Address & MAC Address
e. Ports
f. Protocols

4. Malicious Software
a. The Basics
b. Identification
c. Infection Methods
d. Persistence Mechanisms
e. Beacons
f. Understanding Antivirus technologies

5. Open Source Intelligence
a. Search Engines
b. WHOIS
c. Online Tools
d. Social Networking & Communities
e. Internet Archive
f. Dark Web
g. Threat Reporting
h. Threat Intelligence
i. IOC Concepts

6. Cyber Security Incident Response
a. CSIR Plan
b. CSIR Models

7. Logging Fundamentals
a. Sources
b. Formats
c. Implementation & Use
d. Analysis

8. Security Event & Incident Management
a. What are SIEMs?
b. Logging
c. Evaluation
d. Analytics
e. Detection
f. Threat Intelligence

9. Preservation & Collection
a. Reasons
b. Initial Considerations
c. Guidelines & Standards
d. Further Considerations

10. Logging In-Depth
a. Normalising Logs
b. False Positive Reduction
c. Prioritising Alerts
d. Identifying Genuine Incidents
e. Analytics

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

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