SORINTEQ

CYBER INCIDENT INVESTIGATOR

A 5 day specialist training course for Government and commercial sectors

- 5 Day Programme
- Specialist Training for Law Enforcement
- All Training Equipment Provided
- In Association With the University of Buckingham

Contact Us

0333 0063248

Sorinteq Academy

SORINTEQ

Course Overview

The Cyber Incident Investigator course equips participants with the skills to effectively investigate cyber security incidents while ensuring business continuity and service restoration.

The course focuses on evidential recovery and investigative opportunities, enabling delegates to extract actionable intelligence and forensic data during incident response. Training covers both externally and internally initiated cyber attacks, giving participants the knowledge to handle a broad spectrum of threats.

Through scenario-based exercises, hands-on practical labs, and guided investigations, delegates gain the confidence and competence to manage cyber incidents and support forensic investigations.

Who is the course for?

This course is designed for:

- Law Enforcement cyber response officers
- Cyber security teams providing incident response services to clients
- IT and security staff responsible for investigating internal and external cyber threats
- SOC analysts and digital forensics personnel
- Anyone involved in cyber incident investigation and evidence recovery

Prior experience in cyber security or IT systems is beneficial but not mandatory.

SORINTEQ

Course Content

The Cyber Incident Investigator course covers practical, investigative, and operational modules, including:

- Introduction to Cyber Incident Investigation
- Cyber incident types, attack vectors, and response frameworks
- Evidential Recovery and Forensic Principles
- Capturing, preserving, and documenting digital evidence
- Internal vs External Threat Handling
- Identifying insider threats and external cyber attack indicators
- Investigation Methodologies
- Structured approaches to analysing logs, network traffic, and compromised systems
- System Restoration and Continuity
- Balancing forensic investigation with business or client service recovery
- Hands-On Practical Exercises
- Simulated cyber incidents for live investigation and evidence gathering
- Reporting and Legal Considerations
- Documenting investigations, chain of custody, and supporting prosecutions

SORINTEQ

Aims and Objectives of the Course

By the end of the course, participants will be able to:

- Investigate cyber incidents while maintaining service continuity
- Recover forensic evidence to legal and operational standards
- Identify, analyse, and mitigate both internal and external cyber threats
- Understand investigative frameworks and evidential best practices
- Support operational decisions with accurate technical intelligence
- Apply investigative skills in live simulations and scenario-based exercises
- Integrate cyber investigation procedures into organisational policies

Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations. Our Cyber Incident Investigator Course equips participants with specialist knowledge, practical experience, and operational confidence, ensuring they can effectively protect clients and organisations from ransomware threats.

Students undertaking courses provided by Sorinteq may earn credits towards formal academic qualifications such as Post Graduate Certificate, Diploma or MSc at the university of Buckingham.

For further enquiries please email info@sorinteq.com or call Sorinteq on +44 (0)333 0063248.

Sorinteq provide all necessary training equipment including laptop computers, internet connectivity, mobile devices and training material.