SORINTEQ

RANSOMWARE RESPONDER

A 2 day specialist training course for Government and commercial sectors

- 2 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 Ransomware Responder Course is an intensive, practical programme designed to equip participants with the skills and knowledge to detect, respond to, and recover from ransomware incidents.

Delegates gain hands-on experience in incident handling, threat analysis, and mitigation techniques. Training emphasises practical solutions to ransomware attacks, covering the full lifecycle from detection and containment to recovery and post-incident review.

The course blends scenario-based exercises, interactive workshops, and guided simulations, ensuring participants can respond effectively in real-world ransomware situations.

Who is the course for?

This course is designed for professionals providing dedicated ransomware response services, including:

- Cyber security incident responders
- IT and network security staff
- Security operations centre (SOC) analysts
- Managed service providers (MSPs) supporting ransomware response
- Personnel responsible for organisational ransomware preparedness and resilience

Participants come from varied roles but share the goal of protecting clients or organisations against ransomware threats.

SORINTEQ

Course Content

The Ransomware Responder course covers practical and operational modules, including:

- Introduction to Ransomware Threats
- Understanding attack types, delivery mechanisms, and threat actors
- Detection and Identification
- Recognising ransomware activity and impacted systems
- Containment and Mitigation Strategies
- Limiting impact, isolating affected systems, and preventing propagation
- Investigation and Forensic Analysis
- Tracing infection sources, understanding encryption methods, and evidence gathering
- System Recovery and Restoration
- Safe restoration of systems and data without spreading the infection
- Ransomware Prevention and Resilience
- Implementing defensive measures, backups, and contingency planning
- Scenario-Based Exercises
- Hands-on simulations of ransomware incidents to develop operational skills
- Reporting and Stakeholder Communication
- Structured reporting, lessons learned, and compliance considerations

SORINTEQ

Aims and Objectives of the Course

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

- Detect ransomware attacks early and assess their scope and severity
- Contain infected systems and prevent further spread
- Conduct structured ransomware investigations, including forensic analysis
- Implement system recovery and restoration procedures safely
- Apply ransomware-specific mitigation and prevention strategies
- Prepare incident reports and communicate findings to stakeholders
- Integrate ransomware response into organisational policies and continuity plans

Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations. Our Ransomware Responder 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.