SORINTEQ

SECURITY FUNDAMENTALS IN CYBER OPERATIONS

A 2 Day Intensive specialist course for the 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 digital trail left behind by individuals and organisations is growing in both size and complexity. Every online interaction, connected device, account, and communication creates opportunities for adversaries to identify, track, profile, and exploit targets.

The Security Fundamentals in Cyber Operations Course is a practical 2-day classroom programme designed to equip learners with the essential skills required to both protect their own digital footprint and understand how to identify the traces left behind by others.

This hands-on course focuses on the operational security principles required to work safely in digital environments. Participants will learn how to reduce exposure, secure communications, build protected working environments, and understand how adversaries identify and exploit poor cyber hygiene.

Training includes practical use of public key encryption, virtual machines, secure smartphone builds, and operational tradecraft to ensure learners can operate with confidence and reduce the risk of compromise.

Who is the course for?

This course is designed for professionals who operate in sensitive digital environments, including:

- Investigators and intelligence practitioners
- OSINT and cyber researchers
- Corporate security and protective intelligence teams
- Government and law enforcement personnel
- Security consultants and operational staff
- Individuals responsible for secure digital operations and investigations

No advanced technical background is required, making the course suitable for both operational practitioners and those entering secure cyber environments.

SORINTEQ

Course Content

The course provides practical, hands-on instruction across key operational areas, including:

- Introduction to Digital Operational Security
- Understanding digital footprints, attack surfaces, and adversary targeting
- Digital Identity and Exposure
- How individuals and organisations leave traceable digital signatures
- Public Key Encryption Fundamentals
- Understanding encryption principles and practical secure communication methods
- Virtual Machines and Secure Working Environments
- Building isolated and controlled operational platforms for investigations and research
- Secure Smartphone Builds
- Hardening mobile devices to reduce tracking, surveillance, and exploitation risk
- Browser and Online Security
- Managing privacy, browser security, and investigative separation
- Detecting the Digital Footprint of Others
- Identifying weaknesses, behavioural indicators, and exposure opportunities
- Adversary Awareness and Counter-Surveillance Concepts
- Understanding how hostile actors identify and target digital operators
- Case Studies and Practical Exercises
- Real-world examples of compromise, attribution, and operational security failures

Final Exercise Phase

- Practical Operational Security Scenario
- Learners build and test a secure operational setup for a simulated investigative task
- Digital Footprint Assessment Exercise
- Identifying exposure points and improving defensive posture
- Debrief and Operational Review
- Structured feedback on configuration, methodology, and risk reduction strategies

SORINTEQ

Aims and Objectives of the Course

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

- Understand how digital footprints are created and exploited
- Apply techniques to reduce personal and organisational digital exposure
- Use public key encryption to protect communications and sensitive data
- Build and operate secure virtual machines and isolated environments
- Configure secure smartphones to minimise tracking and adversary targeting
- Recognise indicators of poor operational security and digital compromise
- Identify digital traces left by others to support investigations and threat assessments
- Apply practical cyber operational security (OpSec) principles to daily work

Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations. Our cyber operations training focuses on practical, operational capability—ensuring learners can work securely, protect sensitive activity, and understand how digital footprints can both expose and support investigations.

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.