SORINTEQ

# INTERMEDIATE CYBER RECONNAISSANCE

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

As digital investigations become increasingly complex, cyber reconnaissance practitioners must move beyond tool usage and begin to understand how to shape, adapt, and build investigative capability through code.

The Intermediate Cyber Reconnaissance Course is designed for experienced OSINT practitioners who are already proficient in using code-based tools and now wish to deepen their technical capability. The course focuses on the practical use of the Python programming language to enhance cyber reconnaissance activity, enabling learners to construct structured commands, automate workflows, and develop tailored investigative techniques that support real-world operations.

This is an advanced-skill-level course, delivered by practitioners, and is intended for those who already use technical methods within their investigations.

# Who is the course for?

This course is suitable for professionals with existing experience in technical OSINT and cyber reconnaissance, including:

- Experienced OSINT analysts and researchers
- Cyber intelligence and cyber threat analysts
- Law enforcement and government investigators
- Security and risk professionals conducting digital investigations
- Analysts seeking to move from tool usage to capability development

Participants should be comfortable working with Linux environments and have prior exposure to code-based investigative tools.

SORINTEQ

## Course Content

The course provides hands-on, technically focused instruction covering:

- Intermediate Cyber Reconnaissance Methodology
- Moving from tool-led investigation to technique-driven reconnaissance
- Python for Cyber Recon Practitioners
- Python fundamentals for investigators, focusing on practical application rather than software development
- Building Structured Investigative Commands
- Creating repeatable scripts to support data collection, parsing, and analysis
- Automation of OSINT and Recon Tasks
- Enhancing efficiency through scripting and workflow optimisation
- Data Handling and Enrichment
- Processing, filtering, and enriching data gathered through cyber reconnaissance
- Operational Integration and Tradecraft
- Security, legality, scalability, and responsible use of code-based techniques
- Practical Exercises and Scenarios
- Realistic investigative tasks designed to reinforce learning and reflect operational challenges

SORINTEQ

# Aims and Objectives of the Course

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

- Understand how Python can be applied to enhance cyber reconnaissance workflows
- Write and adapt simple Python scripts to support investigative objectives
- Build structured, repeatable commands to automate elements of research
- Improve the scale, consistency, and efficiency of online investigations
- Customise investigative techniques rather than relying solely on pre-built tools
- Integrate Python-based methods into existing OSINT and cyber recon processes
- Apply code-based investigative skills confidently in operational environments

# Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations. Our Intermediate Cyber Reconnaissance equips participants with specialist knowledge, practical experience, and operational confidence.

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.