SORINTEQ

DHEAT – DIGITAL HOSTILE ENVIRONMENT AWARENESS TRAINING

A 2 day specialist training course for Government and commercial sectors

- 2 Day Programme
- Specialist Training for Law Enforcement
- All Training Equipment Provided

Contact Us

0333 0063248

Sorinteq Academy

SORINTEQ

Course Overview

In today's interconnected world, staff operating in hostile environments face not only physical threats, but also digital vulnerabilities. Traditional Hostile Environment Awareness Training (HEAT) focuses largely on personal safety in high-risk locations, yet fails to address the risks posed by continuous digital communication, remote working, and social media exposure.

The Digital Hostile Environment Awareness Training (DHEAT) course fills this critical gap. Learners acquire the skills to operate safely in both physical and digital domains, protect sensitive information, and manage personnel and assets remotely while mitigating cyber and digital risks. This course prepares participants to navigate hostile environments with both situational awareness and digital security in mind.

Who is the course for?

This course is suitable for professionals whose roles require travel to, or operations within, high-risk or hostile environments, including:

- Government and diplomatic personnel
- Security and protective service staff
- Journalists, field researchers, and humanitarian workers
- Corporate staff operating in high-risk international locations
- Intelligence and cyber operations personnel working remotely in hostile regions

No prior specialist digital security training is required; the course builds both foundational and operational knowledge for safe deployment.

SORINTEQ

Course Content

The course covers practical and operationally relevant content, including:

- Hostile Environment Awareness Fundamentals
- Physical threat identification, situational awareness, and personal safety measures
- Digital Risk Assessment
- Identifying vulnerabilities in communications, devices, and online presence
- Digital Footprint Management
- Securing personal and organisational data, encryption, and secure communication tools
- Remote Operations and Asset Management
- Supervising personnel and resources while operating at a distance
- Threats from Hostile Actors
- Understanding hostile state and non-state actor tactics in both physical and digital spheres
- Operational Procedures and Mitigation Strategies
- Integrating digital security measures with traditional HEAT principles
- Practical Exercises and Scenario-Based Training
- Simulated exercises reflecting real-world hostile environments and digital threat landscapes

SORINTEQ

Aims and Objectives of the Course

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

- Understand the combined risks of physical and digital exposure in hostile environments
- Protect personal and organisational digital footprints from hostile actors
- Operate safely while maintaining communication with remote teams
- Manage staff and assets securely in high-risk areas
- Recognise and mitigate threats posed by hostile state and non-state actors
- Implement operational procedures that integrate digital hygiene and physical security
- Apply learned strategies in realistic scenarios to ensure resilience and safety

Why Choose Sorinteq

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