SORINTEQ

ATHENA PROGRAMME

COVERT NETWORK ADMINISTRATOR

Postgraduate Certificate
(PgCert)
in Cyber Security & Intelligence

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

Contact Us

0333 0063248

Sorinteq Academy

SORINTEQ

Overview of the Programme

Modern digital investigations depend on far more than investigators alone. Behind every successful covert online operation is a secure, resilient, and intelligently managed technical environment. From secure deployment platforms and hardened devices to encrypted communications, server infrastructure, and discreet operational networks, success depends on the ability to build, manage, and protect the environment in which investigations take place.

The Athena Programme – Covert Network Administrator (CNA) is designed for network investigators and technical practitioners who are already operating at an advanced stage of their investigative career and require the skills to move into high-level covert network administration and operational support.

This flagship 12-month professional development pathway takes learners from the fundamentals of computer networking and secure infrastructure through to advanced operational capability in supporting covert investigative activity, discreet online operations, and technical security management.

Delegates will develop the ability to identify vulnerabilities, resolve security issues, manage secure operational environments, and support colleagues conducting sensitive digital investigations. Successful learners achieve a Postgraduate Certificate (PgCert) in Cyber Security & Intelligence, combining academic recognition with advanced technical operational capability.

The Athena Programme produces highly capable professionals able to support and manage covert network investigation activity at the highest level.

SORINTEQ

Programme Structure

The Athena Programme is delivered across 12 months and consists of:

9 Specialist Modules

Each module delivered over 2 days, combining theory, technical practice, and operational assessment.

Academic Written Assignment

A 5,000-word essay focused on Building Your Covert Exploitation Toolkit, testing both technical understanding and academic application.

Final Operational Exercise

A month-long live technical exercise designed to test all learned capabilities in a realistic covert operational environment.

Final Dissertation Submission

A substantial written submission demonstrating professional competence, technical understanding, and strategic operational planning.

Successful completion results in the award of a PgCert in Cyber Security & Intelligence.

Who is this Programme For?

This programme is designed for experienced network investigators, technical specialists, and operational support staff seeking to develop into advanced covert network administrators, including:

- Digital investigators with technical operational roles
- Cyber security and cyber intelligence practitioners
- Government technical support teams
- Network and infrastructure investigators
- Operational security specialists
- Digital forensic and technical recovery teams
- Staff supporting covert internet investigations and discreet online operations

The programme is ideal for delegates who already possess investigative or technical experience and require advanced development into full-spectrum network administration and covert operational support.

SORINTEQ

Programme Modules

1. Building a Secure Deployment Platform
Creating safe, resilient, and discreet environments for operational cyber activity.
Including:

- Secure Linux builds
- Platform hardening
- Virtualisation and isolated environments
- Secure operational workflows
- Risk reduction and resilience planning

2. Security Device Management
Managing devices used in sensitive operational environments.
Including:

- Device hardening
- Authentication controls
- Hardware security keys
- Secure remote access
- Device loss mitigation and recovery planning

3. Android Operating System
Understanding Android as both an operational tool and investigative target.
Including:

- Android internals
- Secure mobile builds
- Privacy configurations
- Device management and monitoring
- Mobile operational security considerations

4. Operating Systems Overview
Understanding how operating systems support or compromise operational security.
Including:

- Windows, Linux, macOS, Android comparisons
- System architecture fundamentals
- User management and permissions
- Logging and security controls
- Operational deployment considerations

SORINTEQ

Programme Modules

5. Network Communications
Developing strong understanding of network structure and communications.
Including:

- TCP/IP fundamentals
- Network traffic awareness
- DNS, VPNs, and routing
- Network mapping and visibility
- Identifying investigative opportunities in communications data

6. Language Module
Understanding how language supports technical operations and investigations.
Including:

- Command-line language awareness
- Basic coding logic
- Technical reading and interpretation
- Scripting fundamentals
- Communication precision in operational environments

7. Infrastructure of the Internet
Understanding the global architecture supporting digital investigations.
Including:

- Hosting environments
- Domains and DNS
- Cloud infrastructure
- Service providers and operational relationships
- Investigative opportunities across internet infrastructure

8. Encryption and Secure Data Transmission
Protecting communications and sensitive operational data.
Including:

- Public key encryption
- Secure communications methods
- Encryption standards and weaknesses
- Secure storage considerations
- Transmission security and operational resilience

SORINTEQ

Programme Modules

9. Server Creation and Interrogation
Building and analysing servers used in discreet operational environments.
Including:

- Server creation and deployment
- Secure hosting principles
- Monitoring and interrogation
- Log analysis and incident identification
- Supporting covert operational infrastructure

Final Exercise Phase
Month-Long Live Operational Exercise
Delegates will participate in a complex live technical environment where they must build, secure, manage, and support covert operational infrastructure.
This exercise includes:

- Building secure deployment platforms
- Managing covert operational devices
- Supporting live investigative teams
- Identifying and resolving security vulnerabilities
- Secure server creation and infrastructure management
- Encryption and secure communications deployment
- Supervisory review and structured debrief

This phase replicates real-world operational demands and confirms readiness for independent technical deployment.

Academic Assessment
5,000-Word Essay
A formal academic submission focused on Building Your Covert Exploitation Toolkit, testing analytical thinking, technical understanding, and academic application.
Final Dissertation Submission
A substantial professional dissertation demonstrating mastery of the programme and the practical application of covert network administration methodologies.

The Outcome
Qualified students will be a critical asset to any digital investigation, cyber intelligence, or covert operational support team, bringing:

- Advanced technical infrastructure capability
- Strong operational security judgement
- Secure deployment and network resilience skills
- Professional support for covert investigative activity
- Academic credibility through a recognised PgCert award

The Athena
The best covert investigators rely on the unseen professional who builds the environment they trust.
Train to become that professional.

SORINTEQ

Aims and Objectives of the Course

By the end of the Athena Programme, learners will be able to:

- Operate independently as a professional Covert Network Administrator
- Build, secure, and manage covert deployment platforms for digital investigations
- Understand advanced operating systems and their role in operational security
- Support discreet investigative activity through secure device and infrastructure management
- Identify and rectify network vulnerabilities and security weaknesses
- Build and manage secure servers and investigative environments
- Understand encryption methodologies and secure communications frameworks
- Support colleagues conducting covert and sensitive online operations
- Deliver technical resilience, security assurance, and operational continuity
- Maintain evidential integrity and operational security in complex digital environments

Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations worldwide. The Athena Programme is designed by operational specialists who understand the reality of discreet online operations and the technical infrastructure required to support them.

This is not simply network administration training—it is a professional transformation pathway.

Graduates leave as highly capable, operationally credible Covert Network Administrators, equipped with both academic accreditation and advanced technical capability.

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.