SORINTEQ

KRATOS PROGRAMME

CERTIFIED SECURITY PROFESSIONAL

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 security professionals must be capable of operating across both the physical and digital environments. Traditional security training often focuses only on physical protection, while cyber security training focuses solely on networks and technology. In reality, professional security provision requires the integration of both disciplines.

The Kratos Programme – Certified Security Professional (CSP) is Sorinteq's flagship pathway for learners entering the security industry who require the full range of professional skills necessary to work competently and confidently as a modern security practitioner.

This comprehensive 12-month professional development pathway equips delegates with the knowledge, operational confidence, and practical capability required to provide end-to-end security solutions for employers, clients, and organisations. Learners develop competence across protective security, personnel security, digital security, risk analysis, surveillance awareness, technical security support, and intelligence-led security operations.

The programme is designed to fit around professional and personal commitments, with delivery available as a part-time weekend programme across 12 months or as a block learning format depending on organisational needs.

Successful learners achieve a Postgraduate Certificate (PgCert) in Cyber Security & Intelligence, becoming certified security professionals and joining a recognised pathway for progression within the private security industry and under Skills Governance.

SORINTEQ

Programme Structure

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

9 Specialist Modules
Each module delivered over 2 days, combining theory, operational practice, and practical assessment.

Academic Written Assignment
A 5,000-word essay focused on Conducting a Client Security Assessment, testing both operational understanding and academic application.

Final Operational Exercise
A month-long practical exercise designed to test all learned capabilities within a realistic protective security environment.

Final Dissertation Submission
A substantial written submission demonstrating professional competence, strategic thinking, and applied operational methodology.

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

Who is this Programme For?

This programme is designed for individuals who are new to the security industry or those seeking to formalise and professionalise their existing operational experience, including:

- Aspiring security professionals
- Close protection and executive protection staff
- Corporate security personnel
- Protective surveillance teams
- Security supervisors and team leaders
- Private security operatives
- Risk and protective intelligence practitioners
- Professionals transitioning from military or law enforcement backgrounds

The programme is ideal for learners seeking a professional qualification and a structured pathway into the private security sector.

SORINTEQ

Programme Modules

1. Physical Security Module
Understanding the foundations of protective and physical security provision.
Including:

- Site security and access control
- Threat identification
- Protective planning
- Security operations management
- Physical vulnerability reduction

2. Personnel Security Module
Protecting people through effective risk management and due diligence.
Including:

- Background checks and vetting awareness
- Threat profiling
- Behavioural indicators
- Insider risk awareness
- Personnel security assessments

3. Digital Security Module
Protecting clients and organisations in the digital environment.
Including:

- Digital footprint management
- Cyber awareness for security professionals
- Device security
- Secure communications
- Online reputation and vulnerability assessment

4. Application and Design of Security Module
Building professional security solutions for clients and organisations.
Including:

- Security planning and implementation
- Layered security design
- Threat-led protection models
- Operational security planning
- Client requirement assessment

SORINTEQ

Programme Modules

5. Security Risk Analysis & Investigative 101 Module
Developing professional investigative and risk assessment capability.
Including:

- Threat and vulnerability analysis
- Incident response awareness
- Security reporting
- Basic investigative methodology
- Decision-making under operational pressure

6. Physical and Technical Counter-Surveillance Module
Recognising and mitigating hostile observation and surveillance threats.
Including:

- Surveillance awareness
- Counter-surveillance planning
- Technical surveillance threats
- Protective route planning
- Hostile reconnaissance identification

7. Technical Security Support to Physical Security Module
Using technical capabilities to strengthen protective operations.
Including:

- CCTV and monitoring considerations
- Alarm and intrusion systems
- Tracking and location awareness
- Secure communications platforms
- Technical support to protective deployments

8. OSINT Supporting the Protective Security Role Module
Using intelligence gathering to support proactive security decision-making.
Including:

- Subject profiling
- Digital due diligence
- Threat actor identification
- Travel and event intelligence
- Open source threat monitoring

SORINTEQ

Programme Modules

9. Integrated Professional Practice Module
Bringing together all disciplines to deliver full-spectrum client security.
Including:

- End-to-end security provision
- Team and solo operational planning
- Client engagement and professional standards
- Incident escalation and management
- Preparation for final operational exercise

Final Exercise Phase
Month-Long Live Operational Exercise
Delegates will participate in a realistic protective security deployment where all programme disciplines must be applied in a professional operational environment.
This exercise includes:

- Client threat assessments
- Protective planning and deployment
- Physical and digital risk management
- Surveillance awareness and countermeasures
- Due diligence and intelligence gathering
- Security reporting and operational review
- Supervisory debrief and performance assessment

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

Academic Assessment
5,000-Word Essay
A formal academic submission focused on Conducting a Client Security Assessment, testing analytical thinking, operational understanding, and academic application.
Final Dissertation Submission
A substantial professional dissertation demonstrating mastery of the programme and the practical application of protective security methodologies.

The Outcome
Qualified students will be a valuable asset to any professional security team and fully capable of operating independently in support of client needs, bringing:

- Strong physical and digital security capability
- Professional investigative and risk assessment skills
- Intelligence-led protective security awareness
- Technical support competence for operational security
- Academic credibility through a recognised PgCert award

Kratos
Modern security demands more than presence—
it demands intelligence, professionalism, and capability.
Train to become the complete security professional.

SORINTEQ

Aims and Objectives of the Course

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

- Operate independently as a professional Certified Security Professional
- Assess and manage physical, digital, and personnel security risks
- Design and implement protective security strategies for individuals and organisations
- Conduct professional due diligence and threat assessments
- Support clients with both physical and cyber security requirements
- Understand surveillance threats and apply counter-surveillance methodologies
- Integrate OSINT and intelligence gathering into protective security operations
- Support investigations and incident response within the security environment
- Deliver security solutions that are proportionate, professional, and defensible
- Build a long-term professional pathway within the private security industry

Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations worldwide. The Kratos Programme is designed by experienced security professionals who understand the reality of modern protective security and the demands placed upon today's practitioners.

This is not simply security training—it is a complete professional transformation pathway.

Graduates leave as highly capable, operationally credible Certified Security Professionals, equipped with both academic accreditation and practical 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.