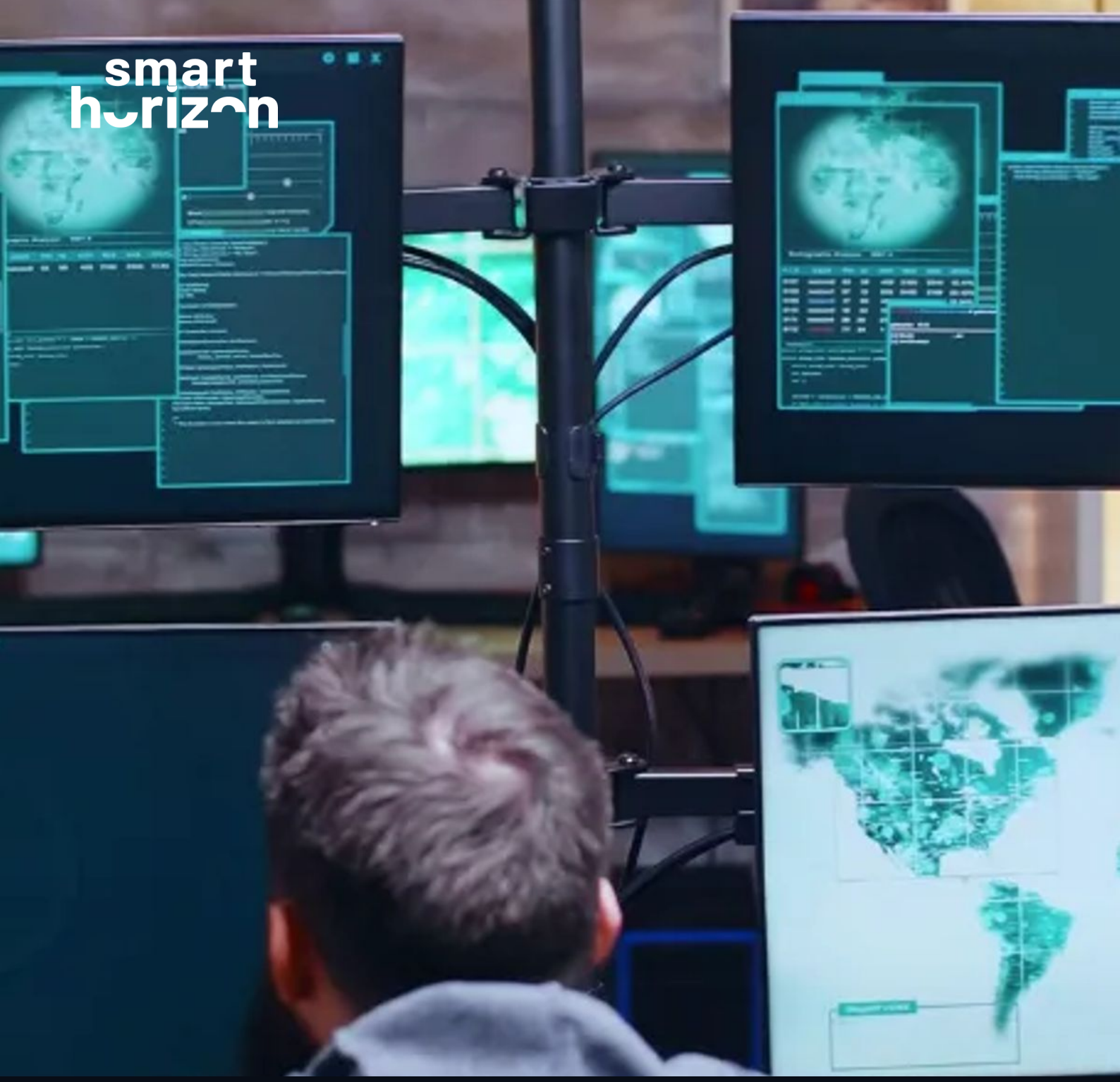


DIGITAL INNOVATION AND TRANSFORMATION | COURSE BROCHURE

Artificial Intelligence (AI) in Cyber Forensics: Investigating Advanced Cyber Crimes

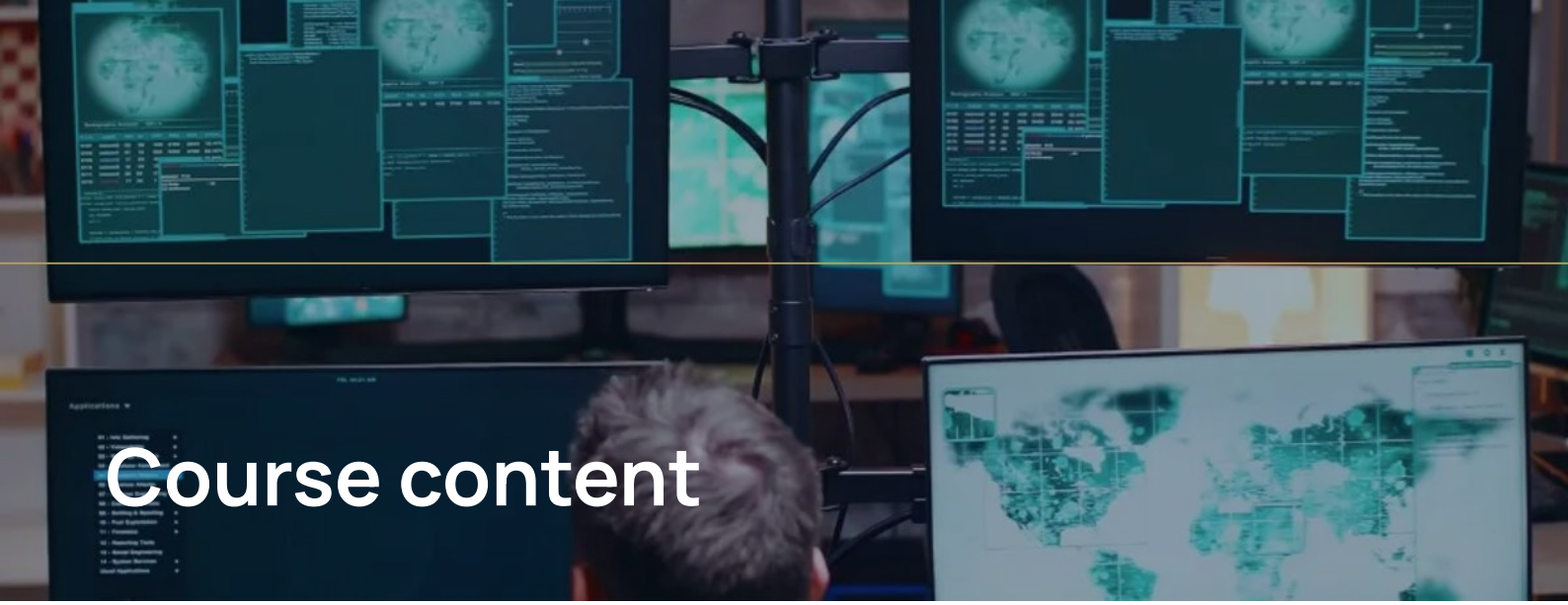
5 days | Classroom training | English

SMART HORIZON

info@smarthorizon.uk
2 Kingdom Street, Paddington
London W2 6BD, United Kingdom

Explore current programmes

https://smarthorizon.uk



Course content

Why attend

This course equips professionals with the skills to leverage artificial intelligence in cyber forensics, focusing on investigating advanced cyber crimes. Participants will explore AI tools and techniques to enhance digital investigations, improve evidence analysis, and respond effectively to cyber threats.

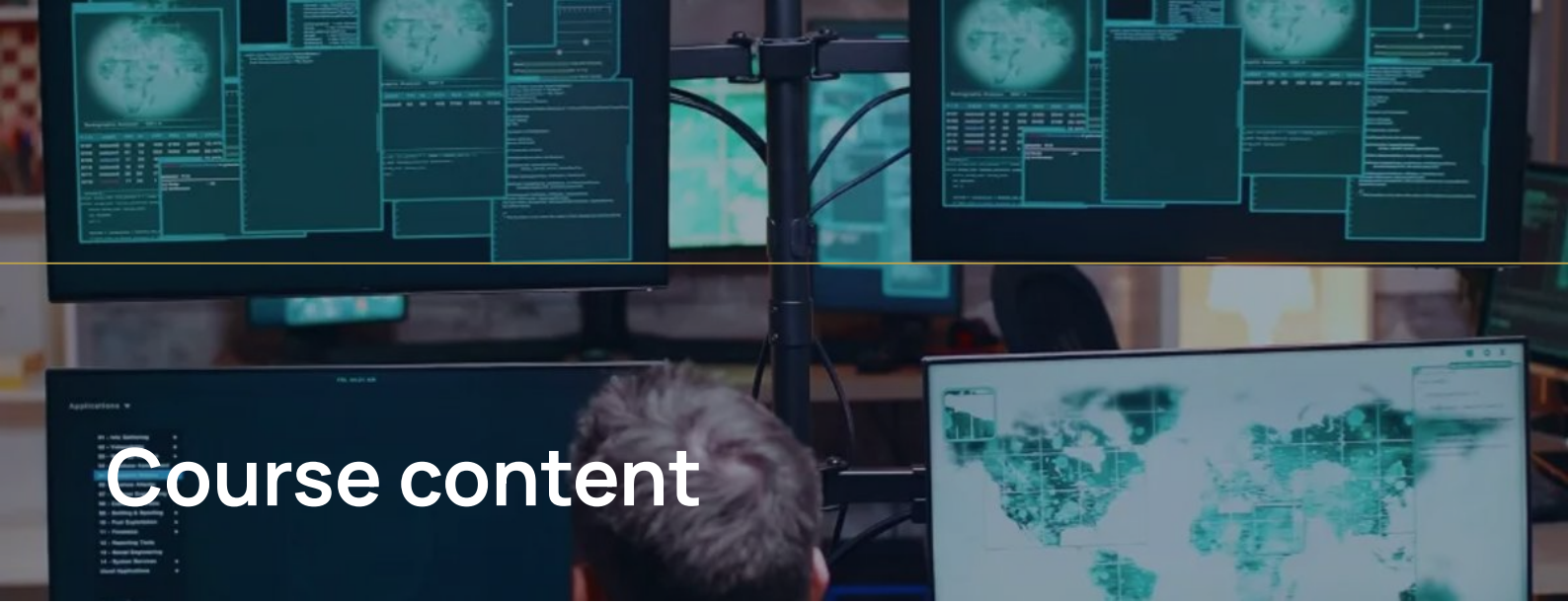
Cyber crimes are becoming increasingly sophisticated, necessitating advanced investigative techniques. Professionals in cyber forensics face challenges in identifying, analysing, and mitigating these threats. This course addresses the critical need for integrating AI into forensic practices to enhance investigative efficiency and accuracy. Participants will learn how to apply AI algorithms for data analysis, enabling them to uncover hidden patterns in large datasets, which is essential for identifying perpetrators and understanding their methods. Moreover, they will explore how AI can automate routine tasks, allowing forensic analysts to focus on more complex investigative challenges, thereby improving overall productivity. Participants will develop practical capabilities in applying AI methodologies to real-world cyber crime scenarios. They will engage in hands-on exercises, learning to utilise AI tools for data analysis, anomaly detection, and evidence gathering. This practical approach ensures that participants can make informed decisions and implement AI solutions effectively in their roles. By the end of the course, they will be equipped to design AI-driven strategies for evidence collection and analysis, assess the ethical implications of AI use, and collaborate with cross-functional teams to enhance their organisation's cyber resilience. This comprehensive skill set is vital for addressing the evolving landscape of cyber threats.

Professional Problems This Course Is Designed to Solve

- Difficulty translating subject knowledge into practical workplace decisions.
- Inconsistent approaches to the activities covered in the course outline.
- Lack of a structured plan for applying and reviewing new skills.

Course methodology

The course employs a blend of interactive workshops, case studies, and simulations to build participants' capabilities in AI-driven cyber forensics. Each session includes hands-on exercises where participants apply AI tools to hypothetical cyber crime scenarios, culminating in the creation of investigative reports and evidence analysis outputs. For instance, participants will engage in simulations that mimic real-world cyber attacks, allowing them to practice using AI for threat detection and evidence gathering. This experiential learning approach ensures that participants can translate theory into practice effectively, reinforcing their understanding and application of AI technologies in cyber forensics. Participants will also collaborate in teams to enhance their problem-solving skills and share insights.



Course content

Course objectives

By the end of this course, participants will be able to:
• Analyse the role of AI in enhancing cyber forensic investigations.
• Evaluate AI tools for detecting and responding to cyber threats.
• Design an AI-driven strategy for evidence collection in cyber crime cases.
• Assess the ethical implications of using AI in cyber forensics.
• Construct a comprehensive report on a simulated cyber crime investigation using AI tools.
• Prioritise AI techniques based on specific cyber crime scenarios.
• Diagnose potential weaknesses in current cyber forensic practices and propose AI solutions.

Target audience

This course is suitable for:
• Cyber forensic analysts seeking to enhance their investigative techniques.
• IT security professionals responsible for incident response and threat mitigation.
• Law enforcement officers involved in cyber crime investigations.
• Compliance officers focused on data protection and security measures.

Target competencies

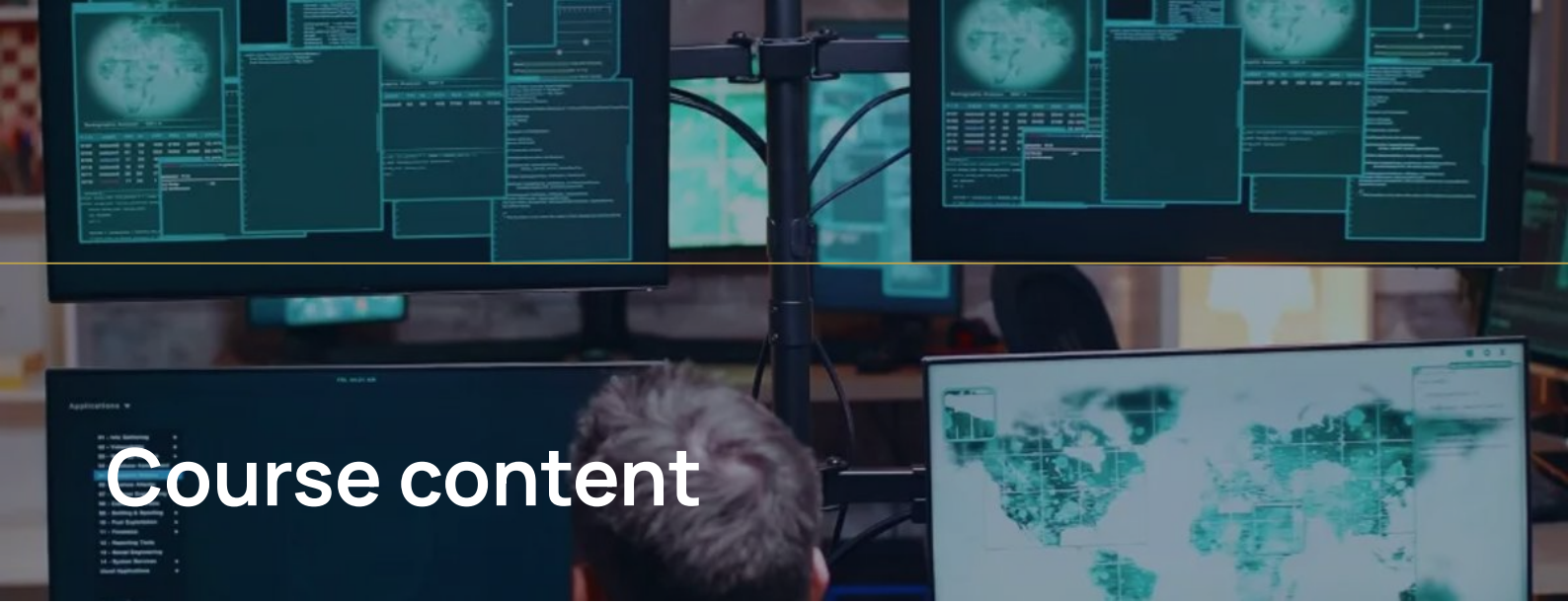
Participants will develop competencies in:
• Utilising AI tools for data analysis in cyber forensics.
• Implementing AI strategies for real-time threat detection.
• Conducting ethical assessments of AI applications in investigations.
• Creating detailed forensic reports based on AI findings.
• Collaborating with cross-functional teams to address cyber threats.
• Adapting AI methodologies to various cyber crime scenarios.

Course outline

Day 1: Introduction to AI in Cyber Forensics

Applied activity: Participants will analyse a case study of a recent cyber crime incident, identifying the challenges faced by investigators and potential AI applications to improve outcomes. They will discuss how AI could have altered the investigation process and outcomes.
Output: A summary report detailing findings and AI recommendations for the case study.

09:00–09:54	Overview of cyber forensics and its challenges in modern investigations.



Course content

09:54–10:48	Introduction to artificial intelligence and machine learning principles.
10:48–11:00	Key AI technologies relevant to cyber forensics, including natural language processing.
11:00–11:30	**Coffee break**
11:30–12:12	Key AI technologies relevant to cyber forensics, including natural language processing. (continued)
12:12–13:06	Understanding the cyber crime landscape, including types of threats and perpetrators.
13:06–14:00	Ethical considerations and legal frameworks surrounding AI applications in forensics.

Day 2: AI Tools for Cyber Threat Detection

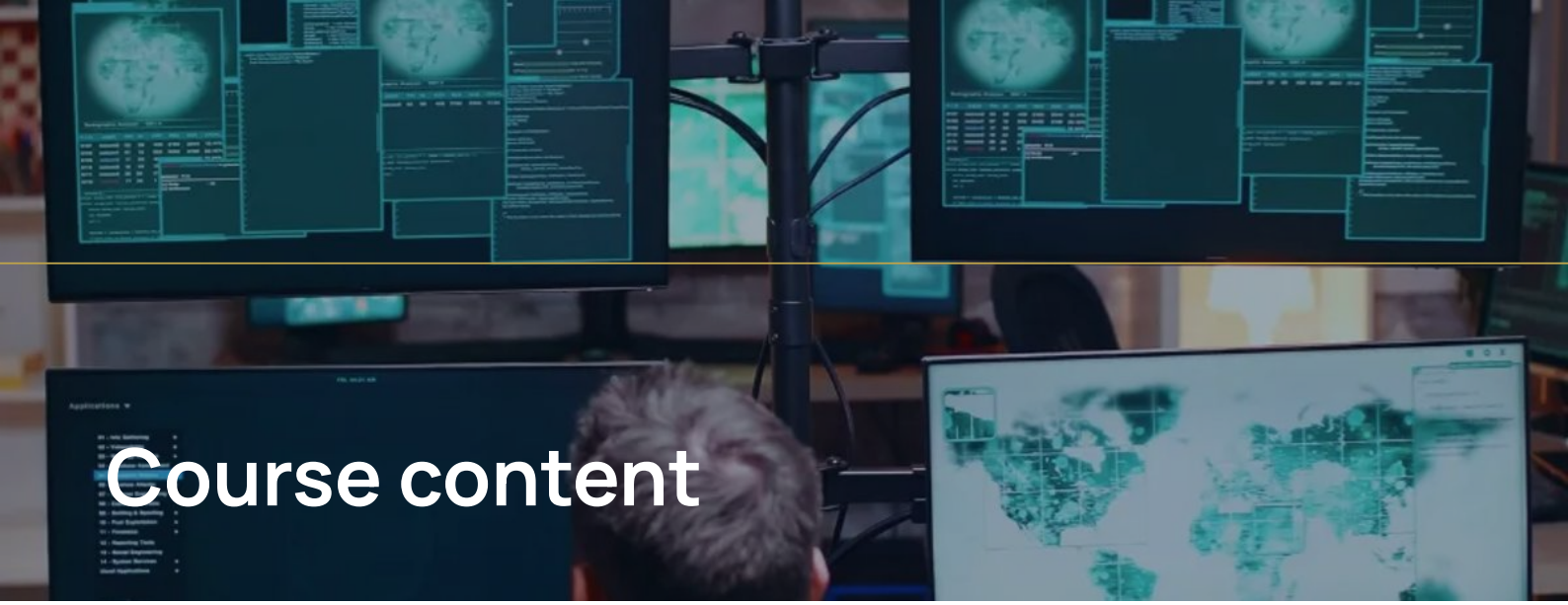
Applied activity: Participants will simulate a cyber attack scenario, using AI tools to detect anomalies in network traffic and generate alerts. They will analyse the results and discuss the implications for incident response and mitigation strategies.
Output: A presentation of detected anomalies and suggested responses based on AI analysis.

09:00–09:54	Exploring AI algorithms for anomaly detection in network traffic.
09:54–10:48	Utilising machine learning for pattern recognition in cyber data analysis.
10:48–11:00	Hands-on with AI tools for threat intelligence gathering and analysis.
11:00–11:30	**Coffee break**
11:30–12:12	Hands-on with AI tools for threat intelligence gathering and analysis. (continued)
12:12–13:06	Evaluating the effectiveness of AI in real-time monitoring and alerting.
13:06–14:00	Integrating AI with existing forensic tools and frameworks for enhanced investigations.

Day 3: Evidence Collection and Analysis with AI

Applied activity: In small groups, participants will create an AI model to analyse a dataset from a fictional cyber crime, focusing on evidence identification and analysis. They will present their findings and discuss the effectiveness of their model.
Output: A detailed analysis report outlining findings, AI model performance, and recommendations.

09:00–09:54	AI methodologies for digital evidence collection and preservation.
09:54–10:48	Best practices for maintaining the integrity of digital evidence during analysis.
10:48–11:00	Using AI for data mining and analysis in investigations, focusing on large datasets.
11:00–11:30	**Coffee break**



Course content

11:30–12:12	Using AI for data mining and analysis in investigations, focusing on large datasets. (continued)
12:12–13:06	Developing AI models for predictive analysis in cyber forensics.
13:06–14:00	Case studies on successful AI evidence analysis and their outcomes.

Day 4: Developing AI Strategies for Cyber Forensic Investigations

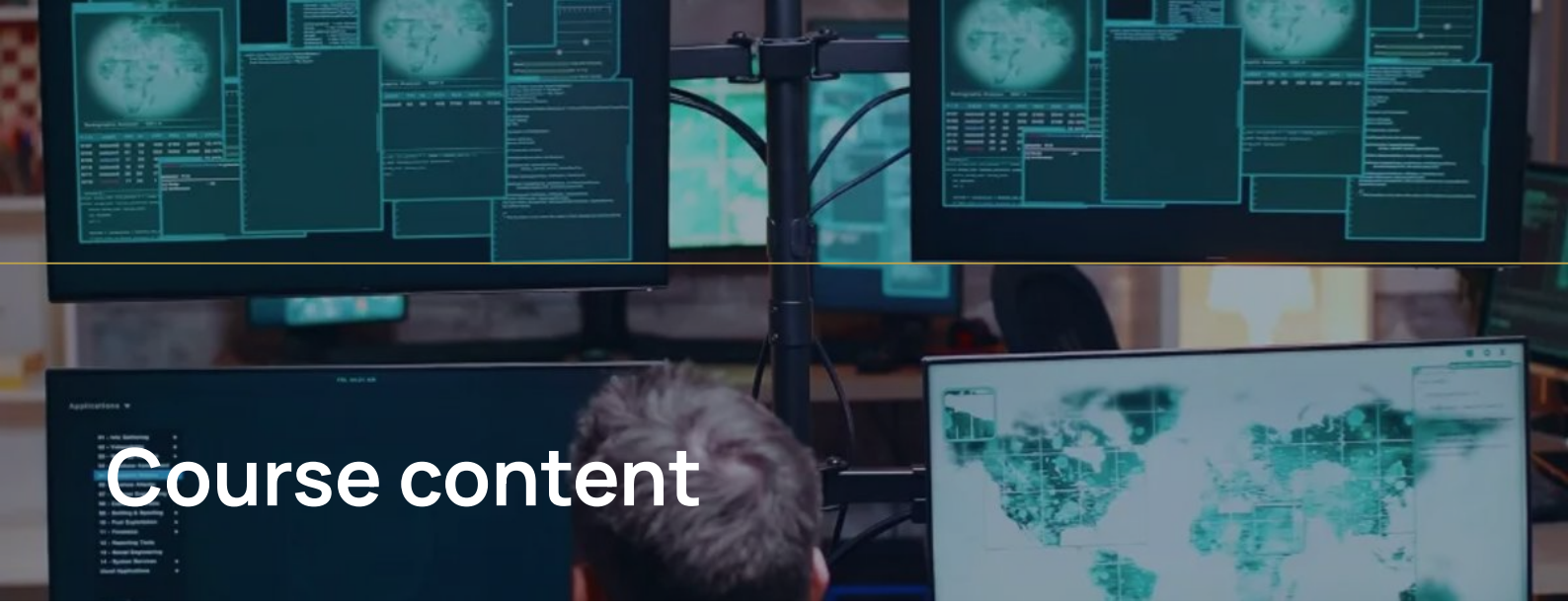
Applied activity: Participants will develop a strategic plan for implementing AI in a fictional cyber forensic unit, considering resources, tools, training needs, and potential challenges. They will present their plans to the group for feedback.
Output: A comprehensive strategic plan document outlining AI integration strategies.

09:00–09:54	Strategic planning for AI integration in cyber forensics operations.
09:54–10:48	Identifying key performance indicators for measuring AI effectiveness in investigations.
10:48–11:00	Risk assessment and management in AI-driven investigations and their implications.
11:00–11:30	**Coffee break**
11:30–12:12	Risk assessment and management in AI-driven investigations and their implications. (continued)
12:12–13:06	Collaborative approaches to developing AI strategies across forensic teams.
13:06–14:00	Future trends in AI and their potential impact on cyber forensics.

Day 5: Integrated Application of AI in Cyber Forensics

Applied activity: Participants will work in teams to respond to a complex, simulated cyber crime scenario, applying all learned AI techniques to investigate, gather evidence, and report findings. They will collaborate to devise a comprehensive response strategy.
Output: A complete investigative report detailing the AI methods used, findings, and case resolution.

09:00–09:54	Combining AI techniques for comprehensive investigations of complex cyber crimes.
09:54–10:48	Real-world applications of AI in cyber crime cases and lessons learned.
10:48–11:00	Evaluating case outcomes and identifying best practices for AI use.
11:00–11:30	**Coffee break**
11:30–12:12	Evaluating case outcomes and identifying best practices for AI use. (continued)
12:12–13:06	Building a cross-functional response team for effective cyber incident management.
13:06–14:00	Preparing for future challenges in cyber forensics and the role of AI.



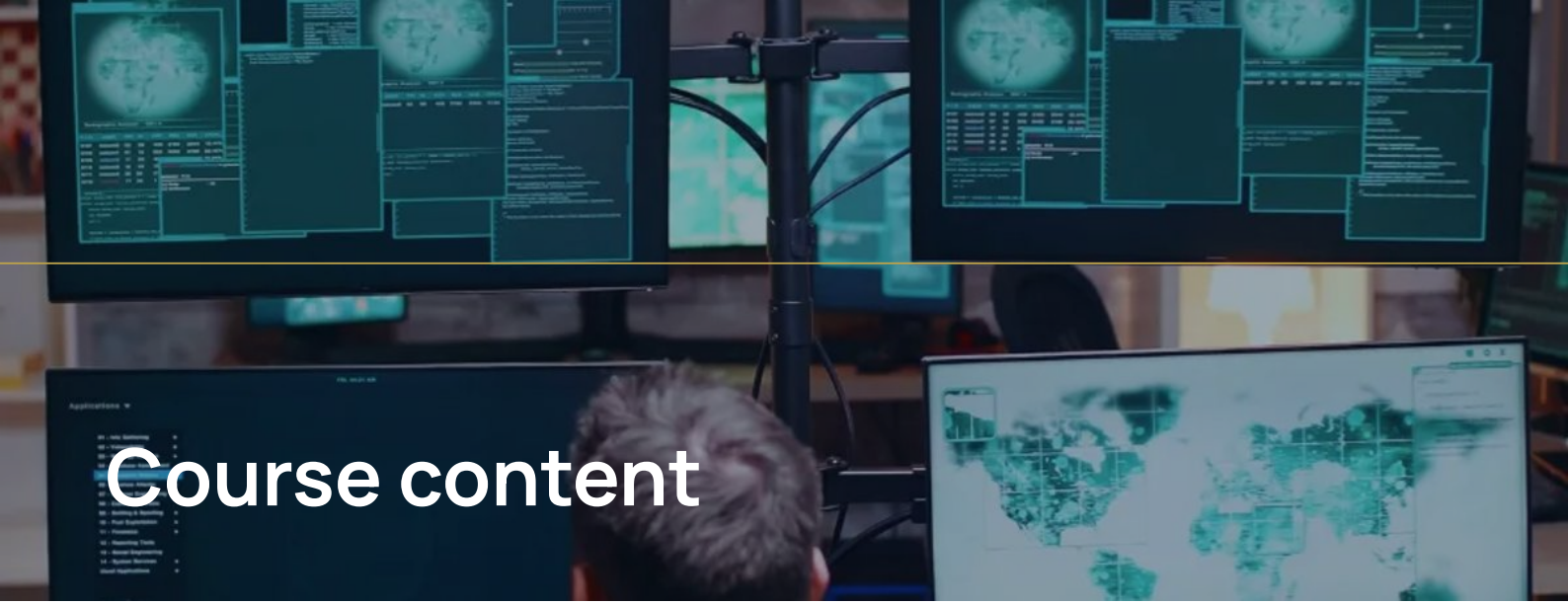
Course content

The timings provided are estimates and may vary depending on the number of participants and the discussions taking place during the sessions. They are indicative only and do not constitute a binding commitment.

Dates, venues and fees

Current published course plans. Fees are per participant in GBP, excluding unconfirmed taxes.

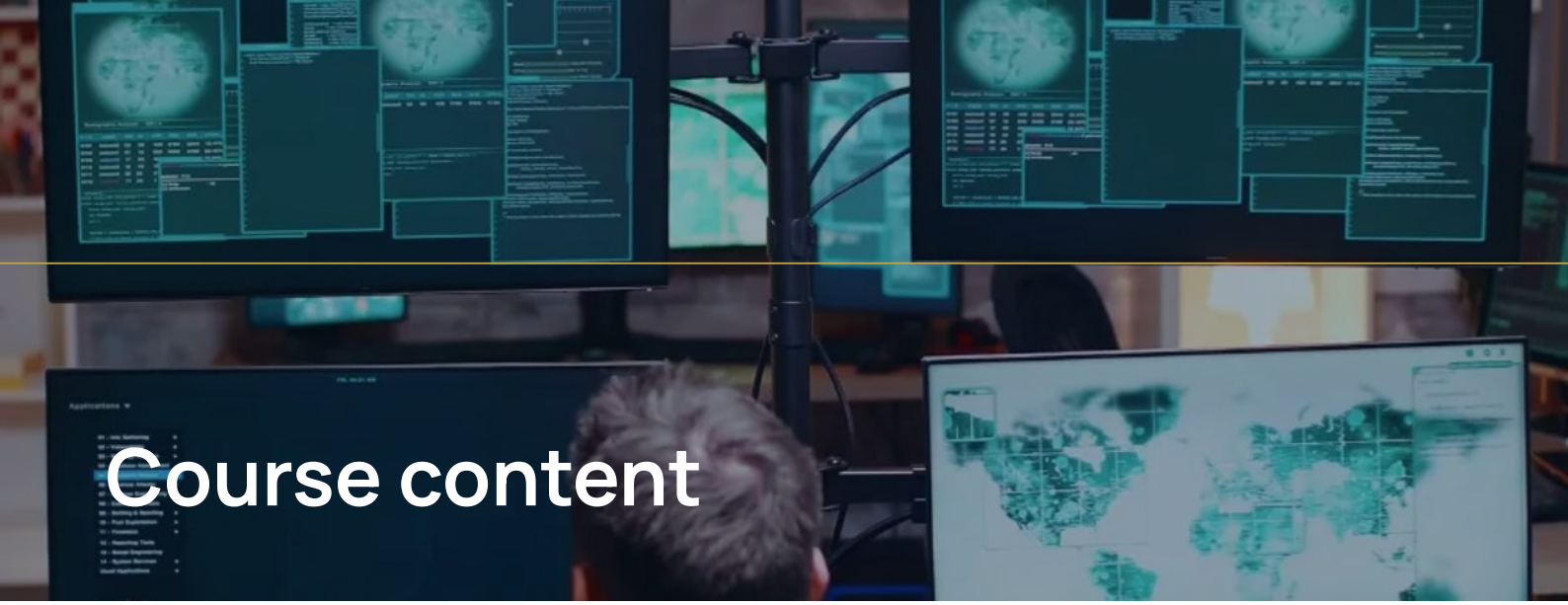
Venue	Start date	End date	Fee (GBP)
Singapore Confirmed dates	9 Nov 2026	13 Nov 2026	**£2,820.–**
Online Confirmed dates	9 Nov 2026	13 Nov 2026	**£1,250.–**
London Confirmed dates	23 Nov 2026	27 Nov 2026	**£2,450.–**
Online Confirmed dates	23 Nov 2026	27 Nov 2026	**£1,250.–**
Dubai Confirmed dates	7 Dec 2026	11 Dec 2026	**£3,150.–**
Online Confirmed dates	7 Dec 2026	11 Dec 2026	**£1,250.–**
Frankfurt Confirmed dates	14 Dec 2026	18 Dec 2026	**£2,650.–**
Online Confirmed dates	14 Dec 2026	18 Dec 2026	**£1,250.–**



Course content

Dates, venues and fees (continued)

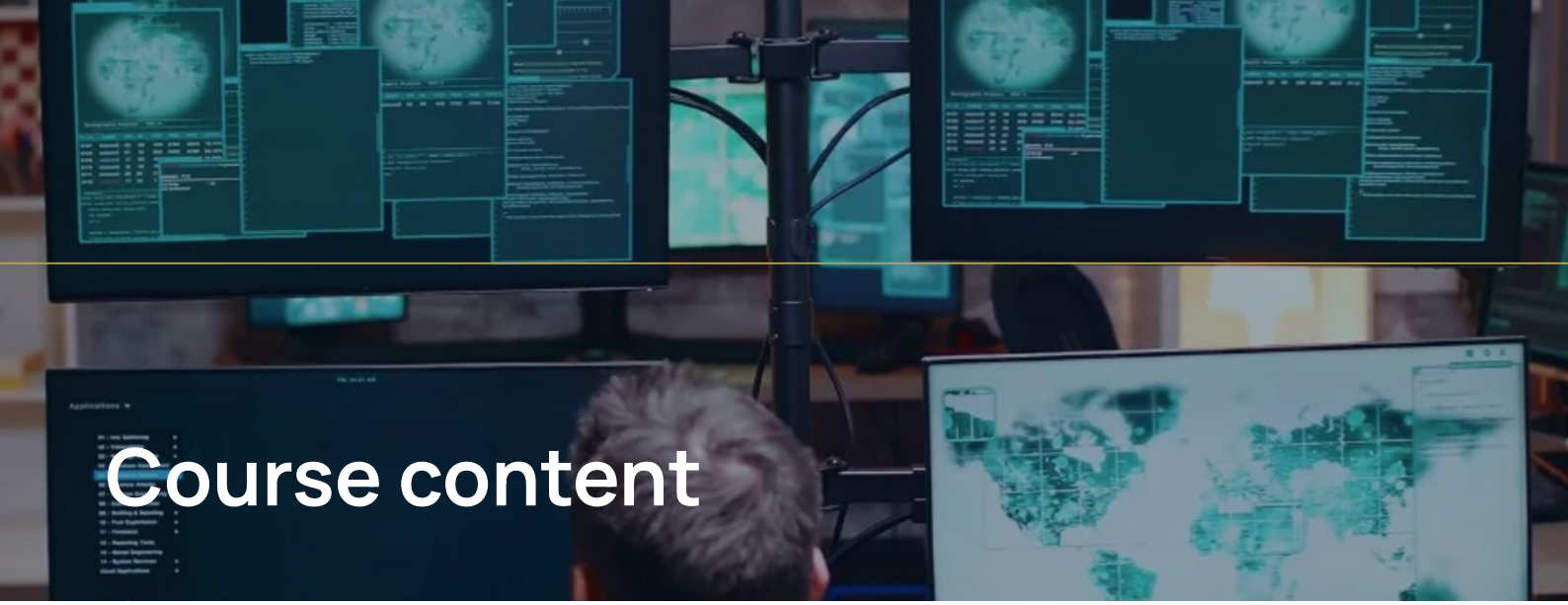
Venue	Start date	End date	Fee (GBP)
Kuala Lumpur Confirmed dates	11 Jan 2027	15 Jan 2027	**£1,450.-**
Online Confirmed dates	11 Jan 2027	15 Jan 2027	**£1,250.-**
Cape Town Confirmed dates	18 Jan 2027	22 Jan 2027	**£1,890.-**
Online Confirmed dates	18 Jan 2027	22 Jan 2027	**£1,250.-**
Paris Confirmed dates	25 Jan 2027	29 Jan 2027	**£2,860.-**
Online Confirmed dates	25 Jan 2027	29 Jan 2027	**£1,250.-**
Istanbul Confirmed dates	8 Feb 2027	12 Feb 2027	**£2,650.-**
Online Confirmed dates	8 Feb 2027	12 Feb 2027	**£1,250.-**
Amsterdam Confirmed dates	22 Feb 2027	26 Feb 2027	**£2,540.-**



Course content

Dates, venues and fees (continued)

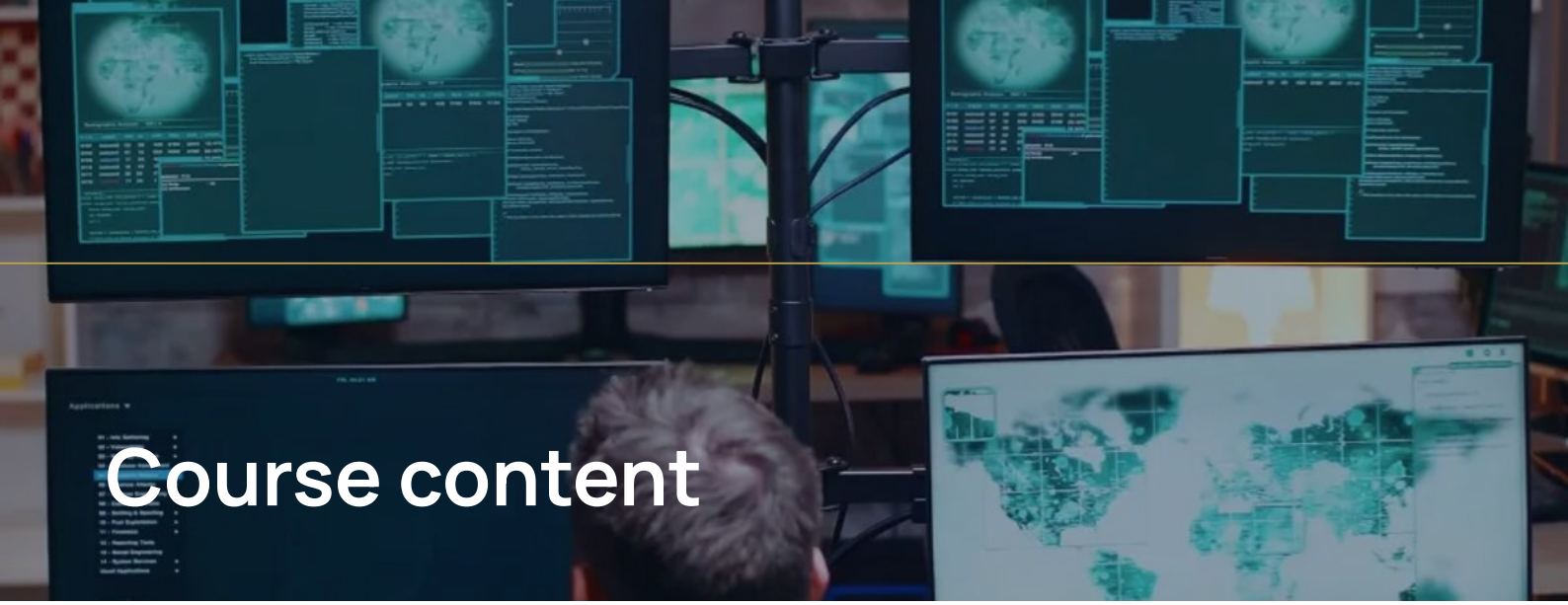
Venue	Start date	End date	Fee (GBP)
Online Confirmed dates	22 Feb 2027	26 Feb 2027	**£1,250.-**
Singapore Confirmed dates	8 Mar 2027	12 Mar 2027	**£2,820.-**
Online Confirmed dates	8 Mar 2027	12 Mar 2027	**£1,250.-**
London Confirmed dates	22 Mar 2027	26 Mar 2027	**£2,450.-**
Online Confirmed dates	22 Mar 2027	26 Mar 2027	**£1,250.-**
Barcelona Confirmed dates	29 Mar 2027	2 Apr 2027	**£2,840.-**
Online Confirmed dates	29 Mar 2027	2 Apr 2027	**£1,250.-**
Dubai Confirmed dates	12 Apr 2027	16 Apr 2027	**£3,150.-**
Online Confirmed dates	12 Apr 2027	16 Apr 2027	**£1,250.-**



Course content

Dates, venues and fees (continued)

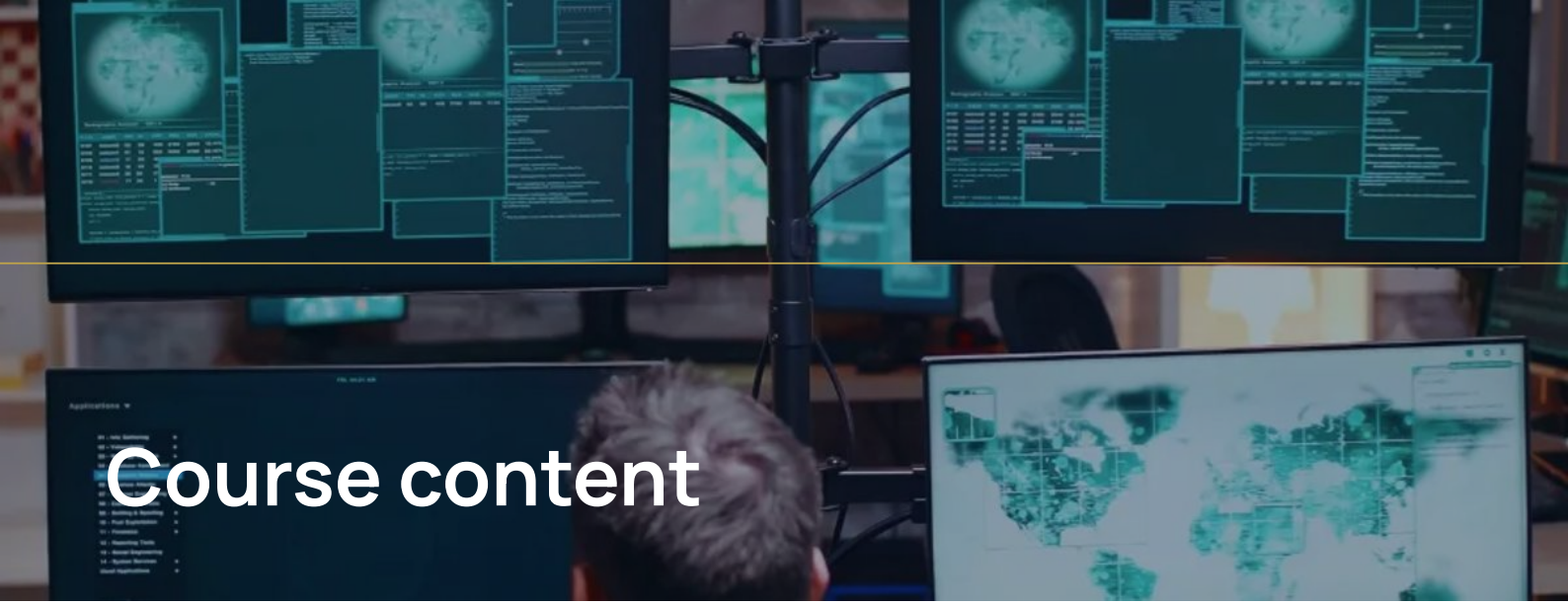
Venue	Start date	End date	Fee (GBP)
Frankfurt Confirmed dates	26 Apr 2027	30 Apr 2027	**£2,650.-**
Online Confirmed dates	26 Apr 2027	30 Apr 2027	**£1,250.-**
Kuala Lumpur Confirmed dates	10 May 2027	14 May 2027	**£1,450.-**
Online Confirmed dates	10 May 2027	14 May 2027	**£1,250.-**
Vienna Confirmed dates	17 May 2027	21 May 2027	**£2,940.-**
Online Confirmed dates	17 May 2027	21 May 2027	**£1,250.-**
Paris Confirmed dates	24 May 2027	28 May 2027	**£2,860.-**
Online Confirmed dates	24 May 2027	28 May 2027	**£1,250.-**
Istanbul Confirmed dates	14 Jun 2027	18 Jun 2027	**£2,650.-**



Course content

Dates, venues and fees (continued)

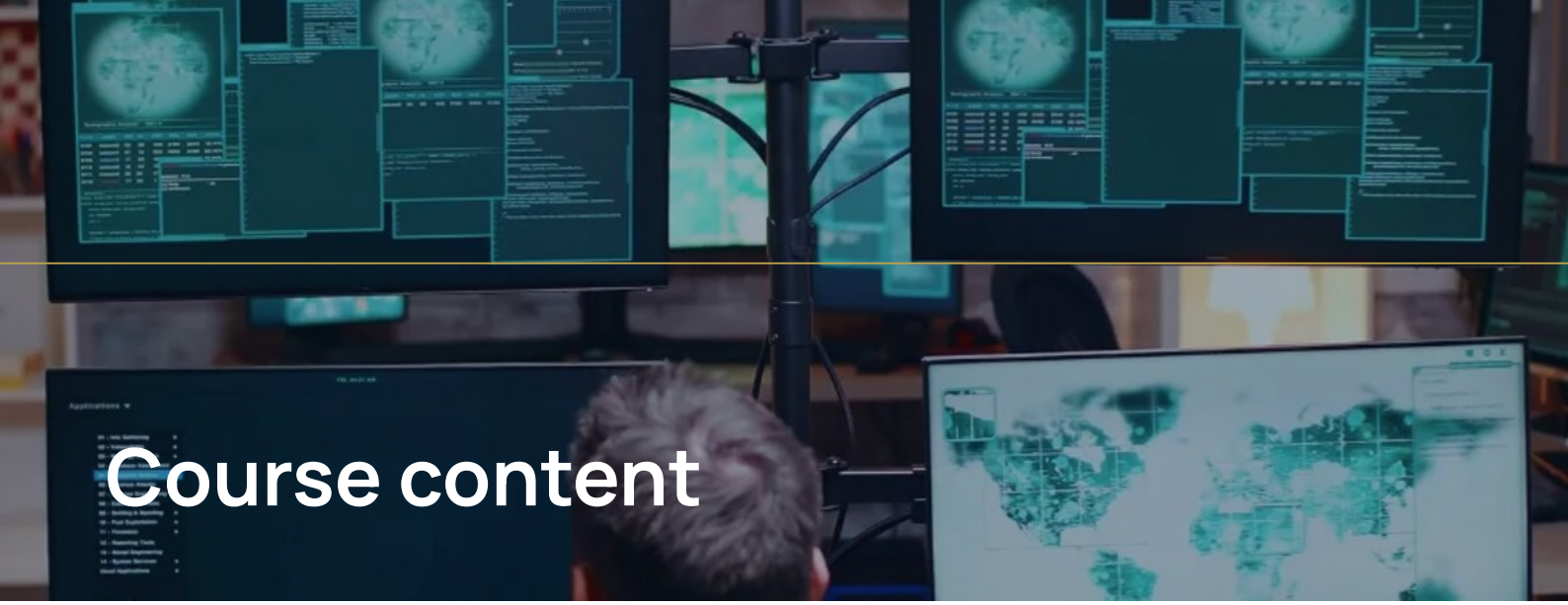
Venue	Start date	End date	Fee (GBP)
Online Confirmed dates	14 Jun 2027	18 Jun 2027	**£1,250.–**
Amsterdam Confirmed dates	21 Jun 2027	25 Jun 2027	**£2,540.–**
Online Confirmed dates	21 Jun 2027	25 Jun 2027	**£1,250.–**
Singapore Confirmed dates	12 Jul 2027	16 Jul 2027	**£2,820.–**
Online Confirmed dates	12 Jul 2027	16 Jul 2027	**£1,250.–**
Cape Town Confirmed dates	19 Jul 2027	23 Jul 2027	**£1,890.–**
Online Confirmed dates	19 Jul 2027	23 Jul 2027	**£1,250.–**
London Confirmed dates	26 Jul 2027	30 Jul 2027	**£2,450.–**
Online Confirmed dates	26 Jul 2027	30 Jul 2027	**£1,250.–**



Course content

Dates, venues and fees (continued)

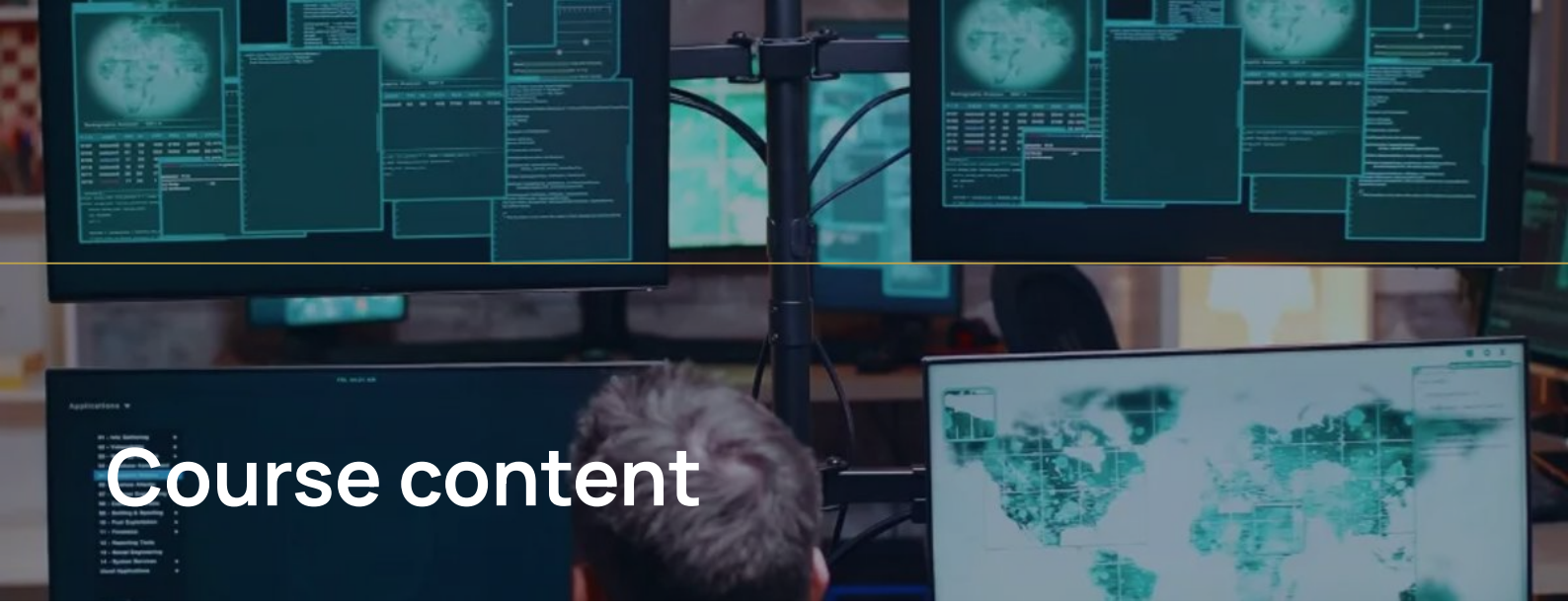
Venue	Start date	End date	Fee (GBP)
Dubai Confirmed dates	9 Aug 2027	13 Aug 2027	**£3,150.-**
Online Confirmed dates	9 Aug 2027	13 Aug 2027	**£1,250.-**
Frankfurt Confirmed dates	23 Aug 2027	27 Aug 2027	**£2,650.-**
Online Confirmed dates	23 Aug 2027	27 Aug 2027	**£1,250.-**
Kuala Lumpur Confirmed dates	13 Sept 2027	17 Sept 2027	**£1,450.-**
Online Confirmed dates	13 Sept 2027	17 Sept 2027	**£1,250.-**
Paris Confirmed dates	20 Sept 2027	24 Sept 2027	**£2,860.-**
Online Confirmed dates	20 Sept 2027	24 Sept 2027	**£1,250.-**
Rome Confirmed dates	27 Sept 2027	1 Oct 2027	**£2,450.-**



Course content

Dates, venues and fees (continued)

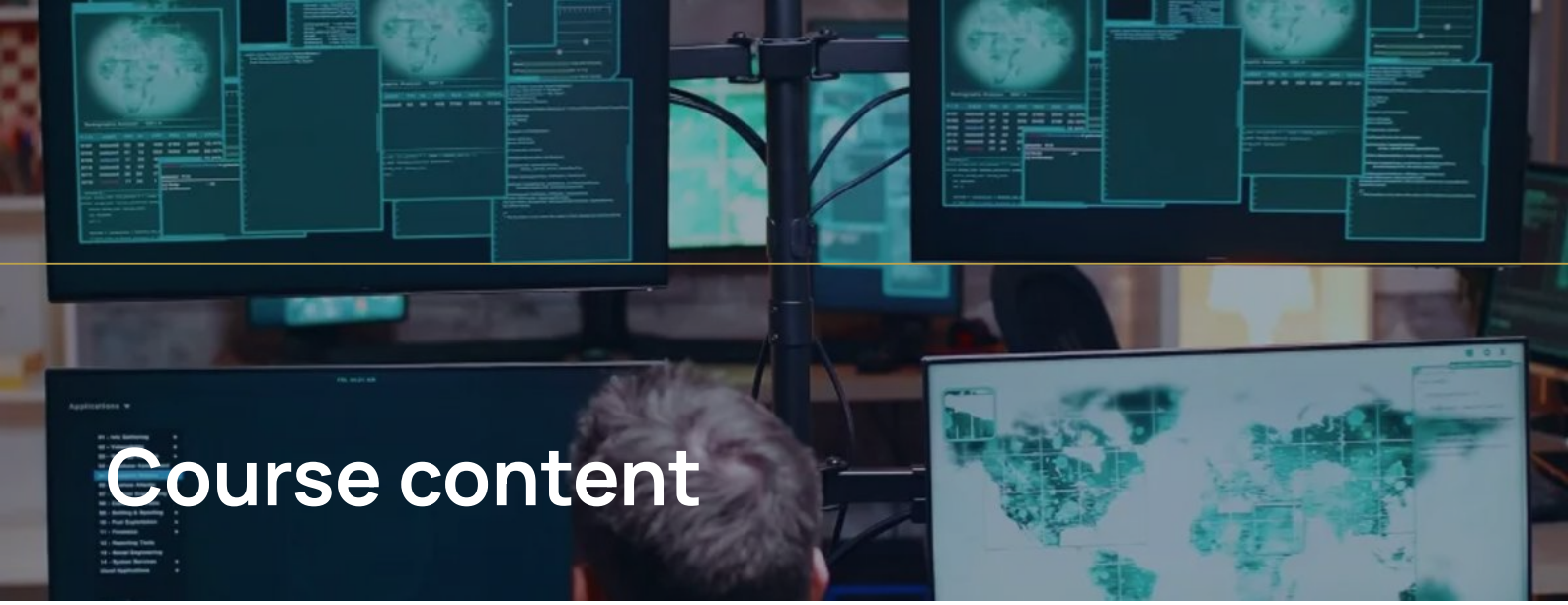
Venue	Start date	End date	Fee (GBP)
Online Confirmed dates	27 Sept 2027	1 Oct 2027	**£1,250.-**
Istanbul Confirmed dates	11 Oct 2027	15 Oct 2027	**£2,650.-**
Online Confirmed dates	11 Oct 2027	15 Oct 2027	**£1,250.-**
Amsterdam Confirmed dates	25 Oct 2027	29 Oct 2027	**£2,540.-**
Online Confirmed dates	25 Oct 2027	29 Oct 2027	**£1,250.-**
Singapore Confirmed dates	8 Nov 2027	12 Nov 2027	**£2,820.-**
Online Confirmed dates	8 Nov 2027	12 Nov 2027	**£1,250.-**
Rome Confirmed dates	15 Nov 2027	19 Nov 2027	**£2,450.-**
Online Confirmed dates	15 Nov 2027	19 Nov 2027	**£1,250.-**



Course content

Dates, venues and fees (continued)

Venue	Start date	End date	Fee (GBP)
London Confirmed dates	22 Nov 2027	26 Nov 2027	**£2,450.-**
Online Confirmed dates	22 Nov 2027	26 Nov 2027	**£1,250.-**
Dubai Confirmed dates	6 Dec 2027	10 Dec 2027	**£3,150.-**
Online Confirmed dates	6 Dec 2027	10 Dec 2027	**£1,250.-**
Frankfurt Confirmed dates	13 Dec 2027	17 Dec 2027	**£2,650.-**
Online Confirmed dates	13 Dec 2027	17 Dec 2027	**£1,250.-**



Course content

Plan your next step

Dates, availability, exact venue, taxes, inclusions and payment terms require written confirmation. This brochure is not a quotation, registration, booking confirmation or visa invitation. Participants receive a Smart Horizon UK certificate of attendance; programmes are not externally accredited and do not award a professional qualification or designation. Confirm arrangements before booking travel.

For group or in-house training, contact our learning team to discuss your objectives and delivery arrangements.

Contact Smart Horizon

info@smarthorizon.uk
2 Kingdom Street, Paddington
London W2 6BD, United Kingdom

View the latest course details online