

DIGITAL INNOVATION AND TRANSFORMATION | COURSE BROCHURE

Artificial Intelligence (AI)-Based Cybersecurity Defense Strategies

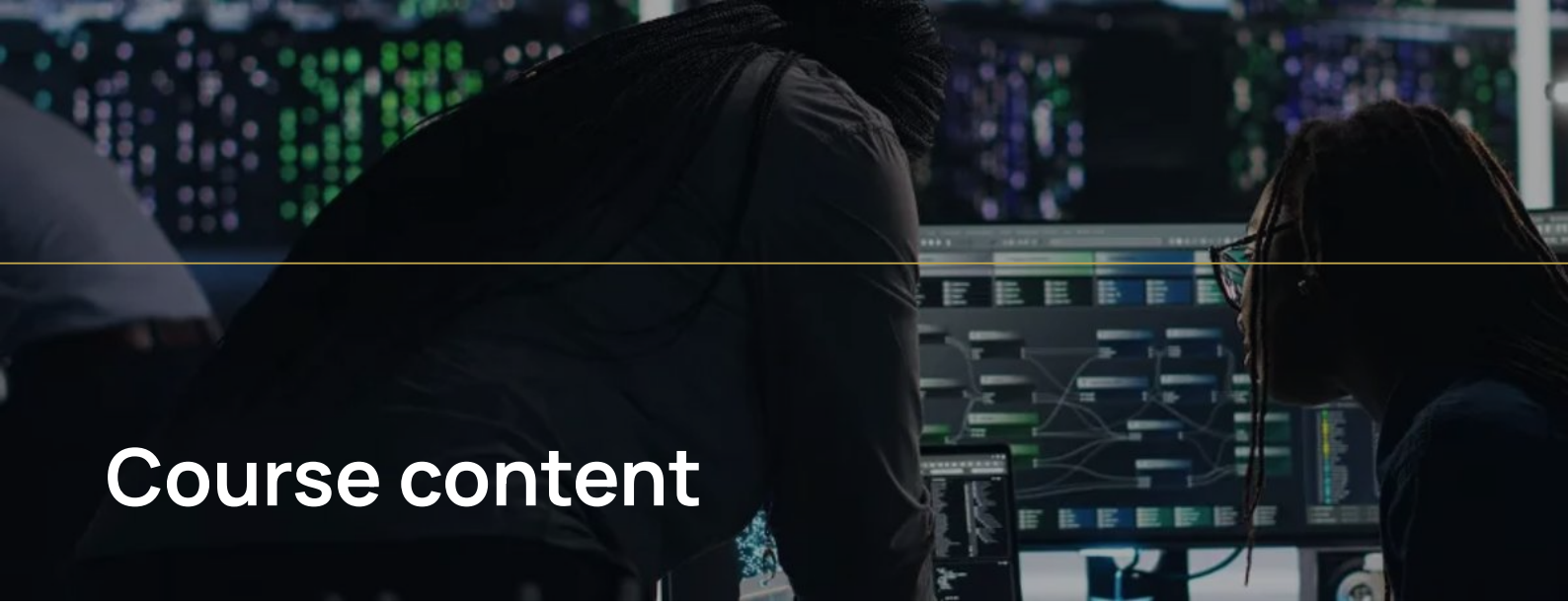
5 days | Classroom training | English

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 provides a comprehensive exploration of AI-based strategies for enhancing cybersecurity defenses. Participants will learn to identify threats, implement AI tools, and develop proactive measures to safeguard digital assets against evolving cyber threats, ensuring robust protection for their organisations.

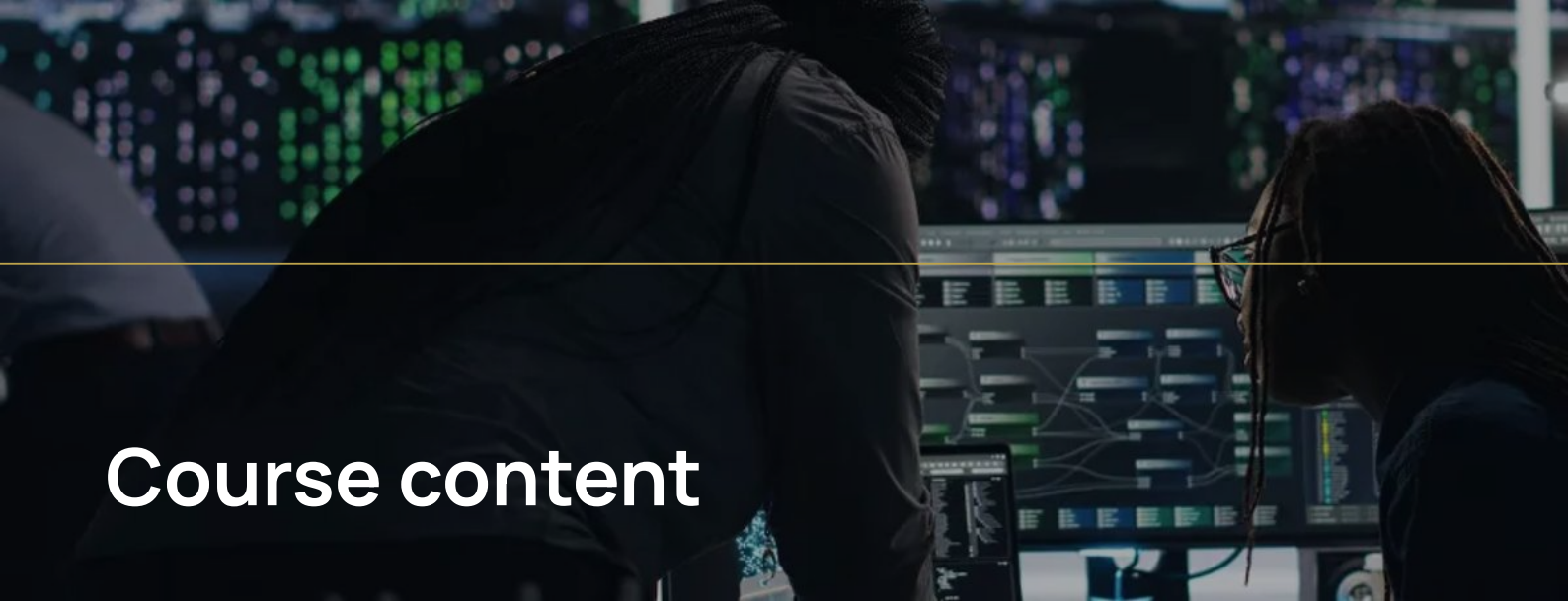
Cybersecurity professionals face increasing challenges from sophisticated cyber threats that traditional methods struggle to counter effectively. The integration of AI technologies into cybersecurity practices is essential for developing adaptive defence strategies that can respond to new attack vectors. This course addresses the urgent need for professionals to understand how AI can enhance threat detection, automate responses, and improve overall security posture. Participants will explore real-world scenarios where AI could mitigate risks, making their roles more impactful in safeguarding sensitive data and organisational integrity. By mastering AI applications, they will be better prepared to protect their organisations against potential breaches.
Engaging in practical exercises, participants will simulate real-world cyber-attack scenarios, applying AI tools to detect and respond to threats. This hands-on approach enables attendees to develop critical decision-making skills and implement AI-driven strategies tailored to their organisations' unique needs. By mastering these capabilities, participants will be better equipped to enhance their cybersecurity frameworks, ensuring they can proactively defend against potential breaches and data loss. The course fosters collaboration and knowledge sharing, empowering professionals to leverage AI effectively in their cybersecurity initiatives. Participants will also learn to assess the effectiveness of AI tools in their environments, enhancing their strategic capabilities.

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 hands-on simulations to build participants' capabilities in AI-based cybersecurity. Each day includes practical exercises where participants will analyse threat scenarios, implement AI tools, and develop defence strategies. For example, participants will engage in simulations that mimic real cyber threats, allowing them to apply theoretical knowledge in practical settings. They will also collaborate in teams to design and evaluate comprehensive security plans based on AI insights. Participants will produce actionable security plans, threat assessment reports, and strategic documents as evidence of their learning, ensuring they can apply these skills directly to their roles and enhance their organisations' cybersecurity measures.



Course content

Course objectives

By the end of this course, participants will be able to:
• Analyse current cybersecurity threats and vulnerabilities in organisational systems.
• Implement AI tools to enhance threat detection and response capabilities.
• Design an AI-driven cybersecurity strategy tailored to specific organisational needs.
• Evaluate the effectiveness of various AI algorithms in identifying cyber threats.
• Construct a risk assessment report based on simulated cyber-attack scenarios.
• Prioritise security measures based on AI-generated insights and threat intelligence.

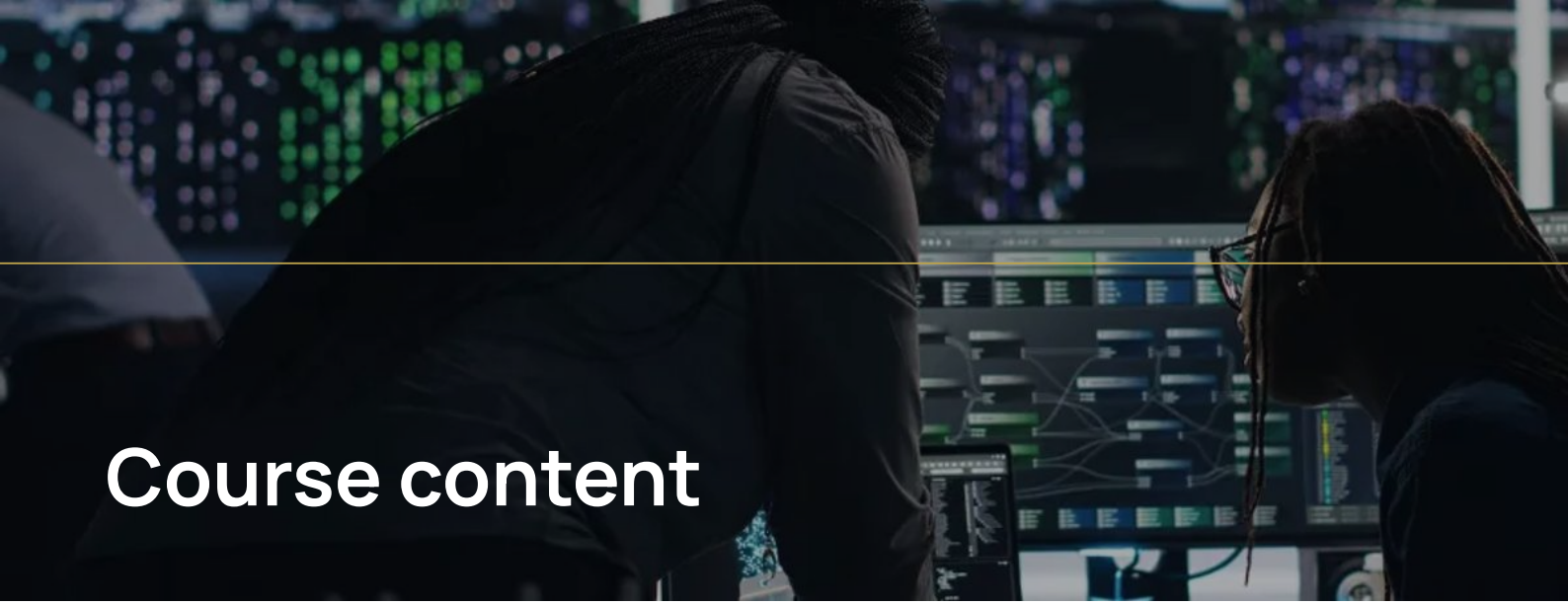
Target audience

This course is suitable for:
• Cybersecurity Analysts: Responsible for monitoring and responding to security incidents, they will benefit from enhanced threat detection techniques.
• IT Security Managers: Overseeing security teams, they need to understand AI applications to improve overall security posture.
• Network Security Engineers: Tasked with protecting network infrastructure, they will learn to integrate AI tools into existing systems.
• Risk Management Professionals: Focused on assessing and mitigating risks, they will gain insights into AI's role in proactive defence strategies.

Target competencies

Participants will develop competencies in:
• Evaluate AI technologies for cybersecurity applications.
• Implement proactive measures using AI-driven insights.
• Develop comprehensive cybersecurity strategies incorporating AI.
• Conduct risk assessments using AI tools and methodologies.
• Integrate AI solutions into existing cybersecurity frameworks.
• Enhance incident response capabilities through AI applications.

Course outline



Course content

Day 1: Introduction to AI in Cybersecurity

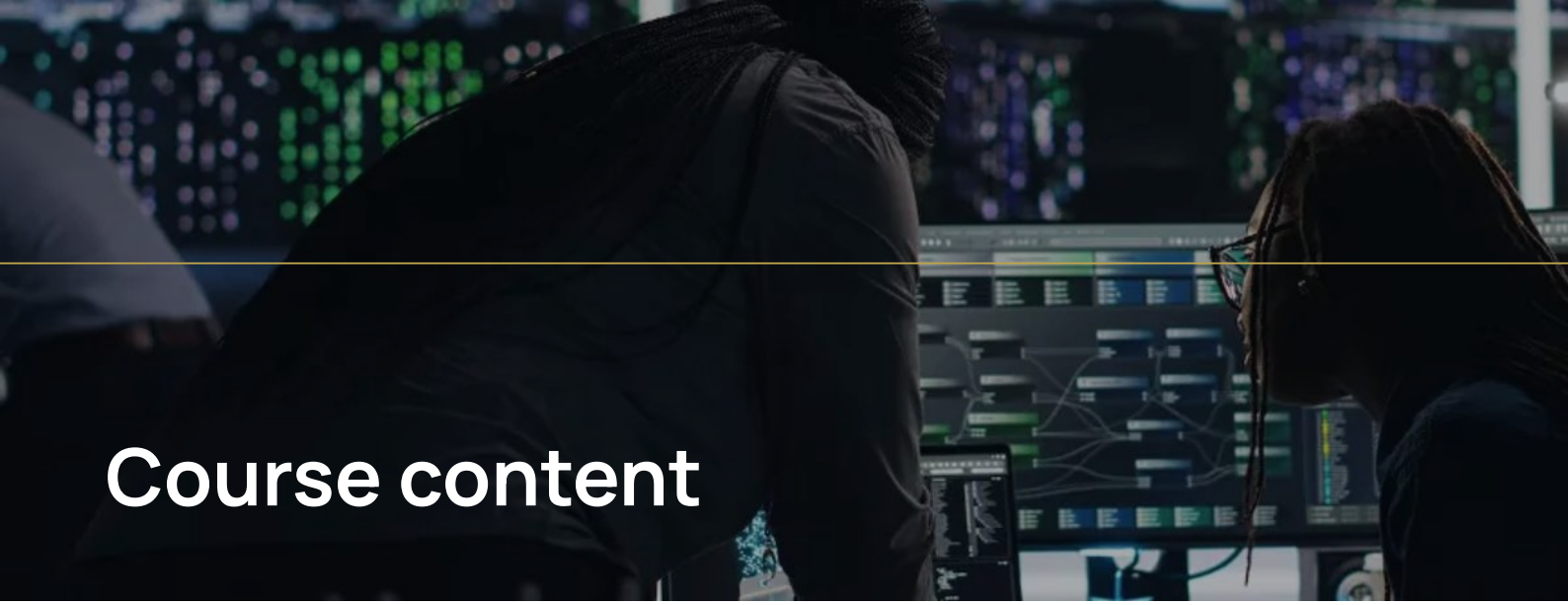
Applied activity: Participants will analyse a case study of a recent cyber-attack and identify how AI could have mitigated the impact. They will discuss their findings in groups, focusing on specific AI applications that could have been employed to prevent the attack.
Output: A group presentation summarising AI applications that could have prevented the attack.

09:00–09:54	Overview of AI technologies relevant to cybersecurity and their applications in threat detection and response
09:54–10:48	Understanding machine learning and its role in identifying vulnerabilities
10:48–11:00	Current landscape of cyber threats and the need for AI solutions
11:00–11:30	**Coffee break**
11:30–12:12	Current landscape of cyber threats and the need for AI solutions (continued)
12:12–13:06	AI's role in enhancing threat detection and incident response
13:06–14:00	Ethical considerations and challenges in deploying AI technologies

Day 2: Implementing AI Tools for Threat Detection

Applied activity: Participants will set up a simulated AI tool to detect anomalies in network traffic and assess its effectiveness in identifying potential threats. They will analyse the results and suggest improvements based on their findings and industry best practices.
Output: A report detailing the AI tool's performance and recommended enhancements.

09:00–09:54	Introduction to AI-based threat detection tools and their functionalities in real-world scenarios
09:54–10:48	Setting up AI algorithms for anomaly detection in network traffic and system logs
10:48–11:00	Integrating AI tools with existing security systems for enhanced monitoring and response
11:00–11:30	**Coffee break**
11:30–12:12	Integrating AI tools with existing security systems for enhanced monitoring and response (continued)
12:12–13:06	Real-time monitoring and alerting mechanisms using AI technologies
13:06–14:00	Evaluating the performance of AI tools in identifying and mitigating threats



Course content

Day 3: Developing AI-Driven Cybersecurity Strategies

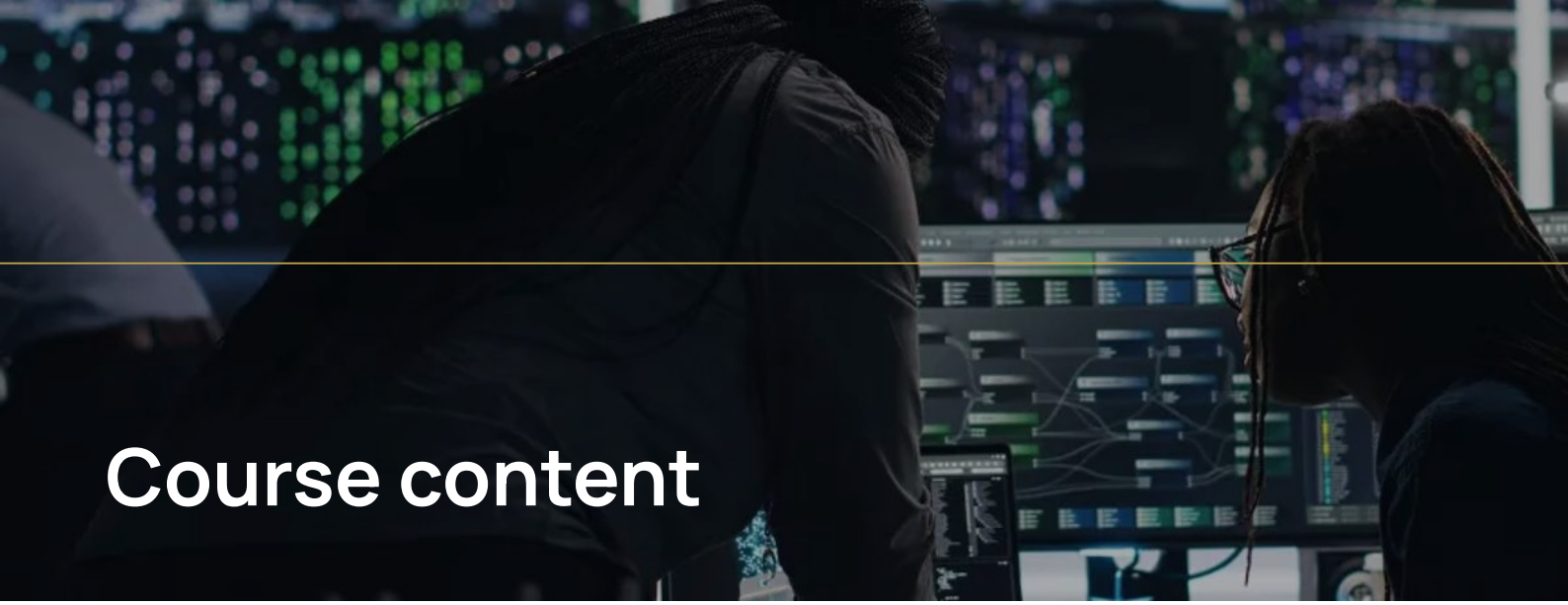
Applied activity: In teams, participants will design a comprehensive AI-driven cybersecurity strategy for a fictional organisation, considering its specific risks, operational needs, and regulatory compliance. They will present their strategies to the class for feedback.
Output: A strategic plan document outlining the proposed AI-driven cybersecurity measures and their expected outcomes.

09:00–09:54	Frameworks for developing AI-driven cybersecurity strategies tailored to organisational needs
09:54–10:48	Aligning AI capabilities with organisational security goals and compliance requirements
10:48–11:00	Creating incident response plans informed by AI insights and threat intelligence
11:00–11:30	**Coffee break**
11:30–12:12	Creating incident response plans informed by AI insights and threat intelligence (continued)
12:12–13:06	Proactive versus reactive security measures in AI contexts and their implications
13:06–14:00	Case studies of successful AI implementations in cybersecurity across various industries

Day 4: Evaluating AI Algorithms for Cyber Threat Identification

Applied activity: Participants will evaluate different AI algorithms based on a set of criteria, presenting their findings on which algorithms are most effective for specific cyber threats and why. They will also discuss potential limitations and challenges.
Output: A comparative analysis report on selected AI algorithms, highlighting their strengths, weaknesses, and recommended applications.

09:00–09:54	Comparative analysis of AI algorithms used in cybersecurity, including supervised and unsupervised learning
09:54–10:48	Understanding performance metrics for evaluating AI effectiveness in identifying threats
10:48–11:00	Case studies of algorithm application in real-world cybersecurity scenarios and their outcomes
11:00–11:30	**Coffee break**
11:30–12:12	Case studies of algorithm application in real-world cybersecurity scenarios and their outcomes (continued)
12:12–13:06	Future trends in AI and their implications for evolving cybersecurity challenges
13:06–14:00	Best practices for selecting and implementing AI algorithms in organisational contexts



Course content

Day 5: Integrated Application of AI in Cybersecurity Defense

Applied activity: Participants will work in teams to simulate a cyber-attack on their developed AI-driven strategy, testing its resilience and effectiveness in real-time. They will analyse the outcomes and recommend improvements based on their findings and lessons learned.
Output: A detailed report on the simulation outcomes and recommendations for enhancing the strategy.

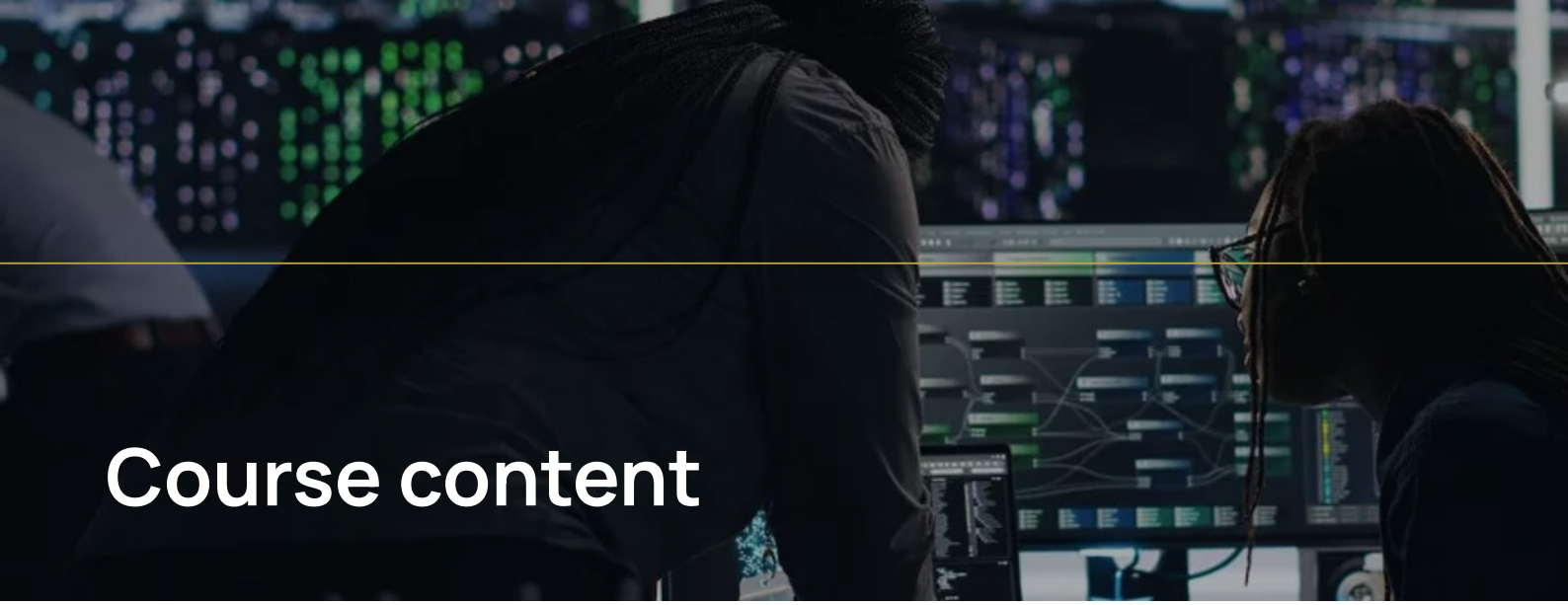
09:00–09:54	Combining AI tools for a layered security approach to enhance overall defence
09:54–10:48	Developing a comprehensive risk assessment using AI methodologies and data analytics
10:48–11:00	Simulating a cyber-attack and response using AI-driven strategies to test resilience
11:00–11:30	**Coffee break**
11:30–12:12	Simulating a cyber-attack and response using AI-driven strategies to test resilience (continued)
12:12–13:06	Collaborative defence strategies across teams and departments leveraging AI insights
13:06–14:00	Future-proofing cybersecurity with advancements in AI technologies and continuous learning

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.

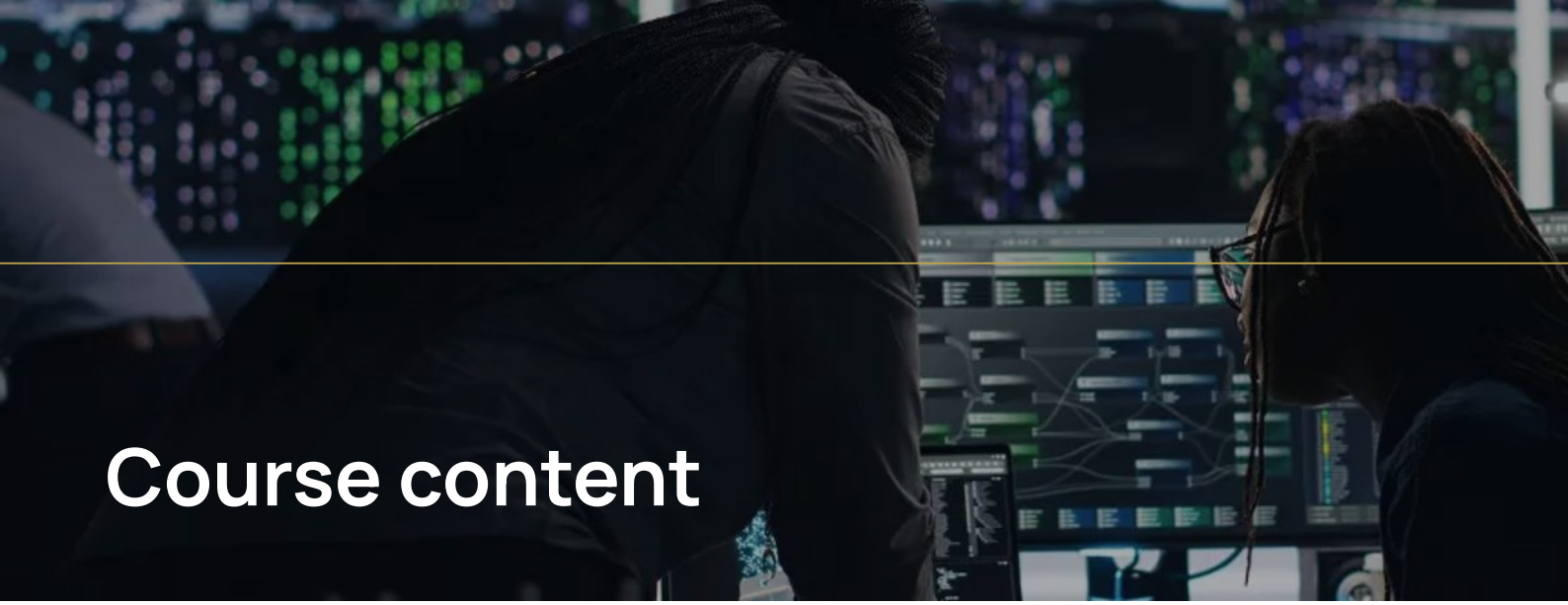
Venue	Start date	End date	Fee (GBP)
Singapore Confirmed dates	16 Nov 2026	20 Nov 2026	**£2,820.-**
Online Confirmed dates	16 Nov 2026	20 Nov 2026	**£1,250.-**
Rome Confirmed dates	30 Nov 2026	4 Dec 2026	**£2,450.-**



Course content

Dates, venues and fees (continued)

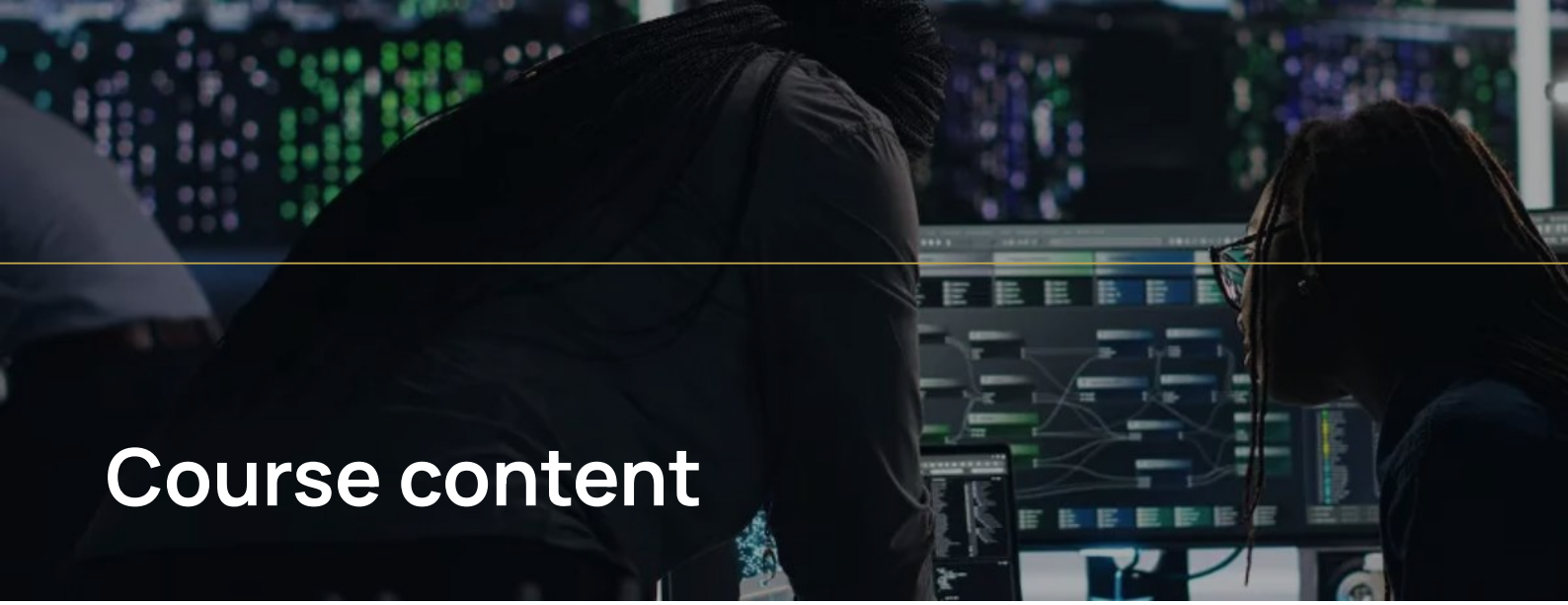
Venue	Start date	End date	Fee (GBP)
Online Confirmed dates	30 Nov 2026	4 Dec 2026	**£1,250.–**
London Confirmed dates	7 Dec 2026	11 Dec 2026	**£2,450.–**
Online Confirmed dates	7 Dec 2026	11 Dec 2026	**£1,250.–**
Dubai Confirmed dates	14 Dec 2026	18 Dec 2026	**£3,150.–**
Online Confirmed dates	14 Dec 2026	18 Dec 2026	**£1,250.–**
Frankfurt Confirmed dates	4 Jan 2027	8 Jan 2027	**£2,650.–**
Online Confirmed dates	4 Jan 2027	8 Jan 2027	**£1,250.–**
Kuala Lumpur Confirmed dates	18 Jan 2027	22 Jan 2027	**£1,450.–**
Online Confirmed dates	18 Jan 2027	22 Jan 2027	**£1,250.–**



Course content

Dates, venues and fees (continued)

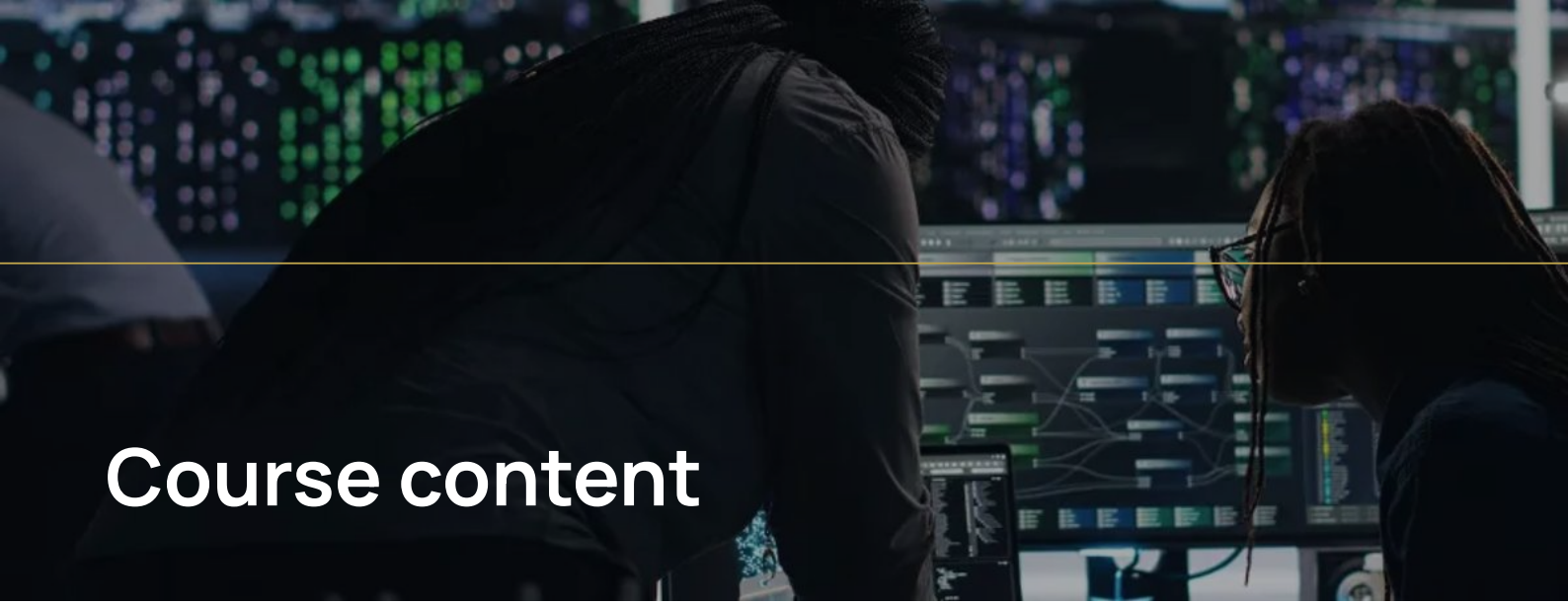
Venue	Start date	End date	Fee (GBP)
Paris Confirmed dates	1 Feb 2027	5 Feb 2027	**£2,860.-**
Online Confirmed dates	1 Feb 2027	5 Feb 2027	**£1,250.-**
Istanbul Confirmed dates	15 Feb 2027	19 Feb 2027	**£2,650.-**
Online Confirmed dates	15 Feb 2027	19 Feb 2027	**£1,250.-**
Amsterdam Confirmed dates	1 Mar 2027	5 Mar 2027	**£2,540.-**
Online Confirmed dates	1 Mar 2027	5 Mar 2027	**£1,250.-**
Cape Town Confirmed dates	8 Mar 2027	12 Mar 2027	**£1,890.-**
Online Confirmed dates	8 Mar 2027	12 Mar 2027	**£1,250.-**
Singapore Confirmed dates	15 Mar 2027	19 Mar 2027	**£2,820.-**



Course content

Dates, venues and fees (continued)

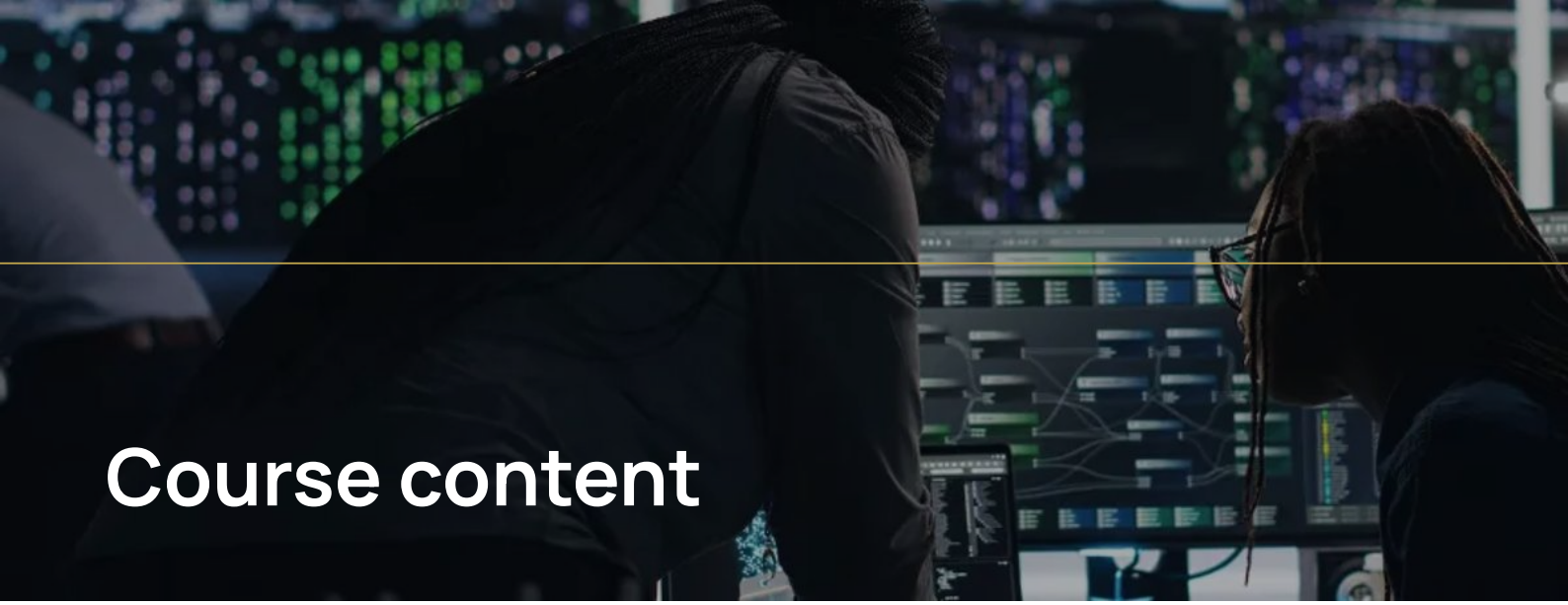
Venue	Start date	End date	Fee (GBP)
Online Confirmed dates	15 Mar 2027	19 Mar 2027	**£1,250.-**
London Confirmed dates	5 Apr 2027	9 Apr 2027	**£2,450.-**
Online Confirmed dates	5 Apr 2027	9 Apr 2027	**£1,250.-**
Dubai Confirmed dates	19 Apr 2027	23 Apr 2027	**£3,150.-**
Online Confirmed dates	19 Apr 2027	23 Apr 2027	**£1,250.-**
Frankfurt Confirmed dates	3 May 2027	7 May 2027	**£2,650.-**
Online Confirmed dates	3 May 2027	7 May 2027	**£1,250.-**
Rome Confirmed dates	10 May 2027	14 May 2027	**£2,450.-**
Online Confirmed dates	10 May 2027	14 May 2027	**£1,250.-**



Course content

Dates, venues and fees (continued)

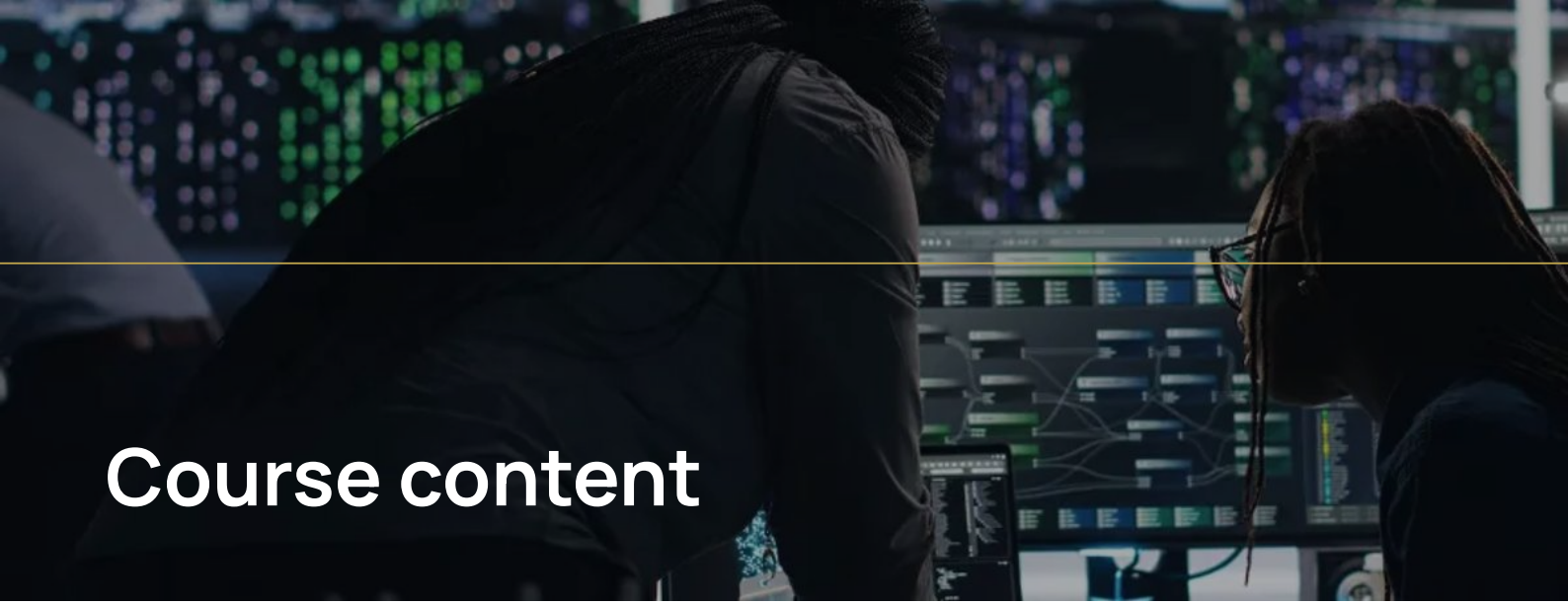
Venue	Start date	End date	Fee (GBP)
Kuala Lumpur Confirmed dates	17 May 2027	21 May 2027	**£1,450.-**
Online Confirmed dates	17 May 2027	21 May 2027	**£1,250.-**
Paris Confirmed dates	7 Jun 2027	11 Jun 2027	**£2,860.-**
Online Confirmed dates	7 Jun 2027	11 Jun 2027	**£1,250.-**
Istanbul Confirmed dates	21 Jun 2027	25 Jun 2027	**£2,650.-**
Online Confirmed dates	21 Jun 2027	25 Jun 2027	**£1,250.-**
Amsterdam Confirmed dates	5 Jul 2027	9 Jul 2027	**£2,540.-**
Online Confirmed dates	5 Jul 2027	9 Jul 2027	**£1,250.-**
Barcelona Confirmed dates	12 Jul 2027	16 Jul 2027	**£2,840.-**



Course content

Dates, venues and fees (continued)

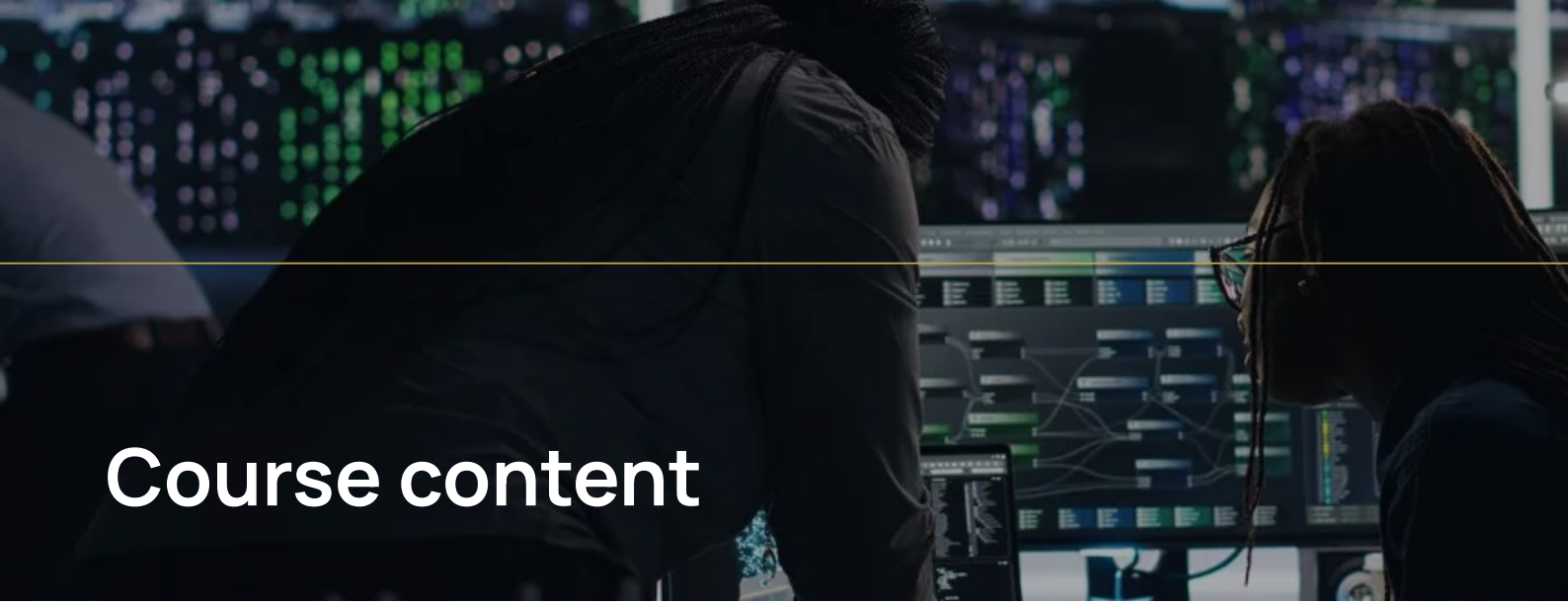
Venue	Start date	End date	Fee (GBP)
Online Confirmed dates	12 Jul 2027	16 Jul 2027	**£1,250.-**
Singapore Confirmed dates	19 Jul 2027	23 Jul 2027	**£2,820.-**
Online Confirmed dates	19 Jul 2027	23 Jul 2027	**£1,250.-**
London Confirmed dates	2 Aug 2027	6 Aug 2027	**£2,450.-**
Online Confirmed dates	2 Aug 2027	6 Aug 2027	**£1,250.-**
Dubai Confirmed dates	16 Aug 2027	20 Aug 2027	**£3,150.-**
Online Confirmed dates	16 Aug 2027	20 Aug 2027	**£1,250.-**
Frankfurt Confirmed dates	6 Sept 2027	10 Sept 2027	**£2,650.-**
Online Confirmed dates	6 Sept 2027	10 Sept 2027	**£1,250.-**



Course content

Dates, venues and fees (continued)

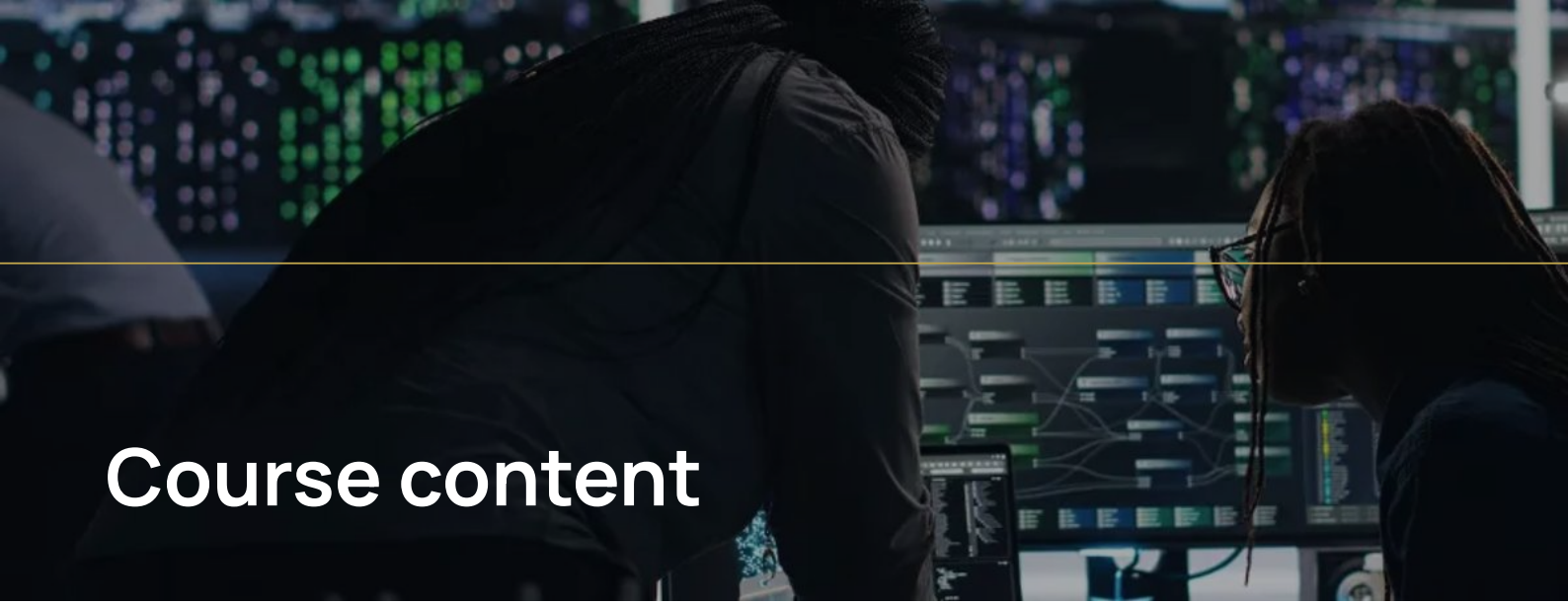
Venue	Start date	End date	Fee (GBP)
Cape Town Confirmed dates	13 Sept 2027	17 Sept 2027	**£1,890.–**
Online Confirmed dates	13 Sept 2027	17 Sept 2027	**£1,250.–**
Kuala Lumpur Confirmed dates	20 Sept 2027	24 Sept 2027	**£1,450.–**
Online Confirmed dates	20 Sept 2027	24 Sept 2027	**£1,250.–**
Paris Confirmed dates	4 Oct 2027	8 Oct 2027	**£2,860.–**
Online Confirmed dates	4 Oct 2027	8 Oct 2027	**£1,250.–**
Istanbul Confirmed dates	18 Oct 2027	22 Oct 2027	**£2,650.–**
Online Confirmed dates	18 Oct 2027	22 Oct 2027	**£1,250.–**
Amsterdam Confirmed dates	1 Nov 2027	5 Nov 2027	**£2,540.–**



Course content

Dates, venues and fees (continued)

Venue	Start date	End date	Fee (GBP)
Online Confirmed dates	1 Nov 2027	5 Nov 2027	**£1,250.-**
Vienna Confirmed dates	8 Nov 2027	12 Nov 2027	**£2,940.-**
Online Confirmed dates	8 Nov 2027	12 Nov 2027	**£1,250.-**
Singapore Confirmed dates	15 Nov 2027	19 Nov 2027	**£2,820.-**
Online Confirmed dates	15 Nov 2027	19 Nov 2027	**£1,250.-**
London Confirmed dates	6 Dec 2027	10 Dec 2027	**£2,450.-**
Online Confirmed dates	6 Dec 2027	10 Dec 2027	**£1,250.-**
Dubai Confirmed dates	13 Dec 2027	17 Dec 2027	**£3,150.-**
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