MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

CYBER THREAT INTELLIGENCE AUDIT: ASSESSES THE ORGANIZATION\'S ABILITY TO GATHER, ANALYZE, AND ACT UPON CYBER THREAT INTELLIGENCE

"Master Cyber Threat Intelligence to Safeguard Your Organization"

Schedule

Date	Venue	Fees (Face-to-Face)
06 – 10 Aug 2026	London, UK	USD 3495 per delegate

► **Available delivery methods:** Face-to-Face & Online Training

Introduction

This comprehensive five-day training is designed for professionals tasked with assessing and improving their organization\'s ability to handle and respond to cyber threats. Through a series of expert-led sessions, practical exercises, and case studies, participants will learn how to evaluate and enhance their organization\'s cyber threat intelligence capabilities.

Participants will gain in-depth knowledge of how to gather, analyze, and respond to cyber threats, utilizing industry-leading practices and frameworks. The course prepares delegates to effectively audit their organization\'s readiness to handle cyber threats, ensuring that they can proactively defend against increasingly sophisticated attacks.

Objectives

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

- Understand the principles and processes involved in cyber threat intelligence (CTI)
- Evaluate their organization\'s current cyber threat intelligence capabilities
- Identify key indicators of cyber threats and risks
- Implement effective cyber threat intelligence gathering and analysis strategies
- Conduct comprehensive audits to measure cyber threat preparedness
- Develop actionable recommendations for improving organizational security resilience

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Why Attend

- Strengthen your organization\'s ability to respond to and mitigate cyber threats
- Gain practical skills through real-world case studies and audit exercises
- Learn from industry experts and enhance your professional credentials
- Access templates and tools for immediate implementation
- Build a proactive, security-focused organizational culture

Target Audience

This program is designed for:

- IT auditors and cybersecurity professionals
- Risk management officers and compliance managers
- CISO’s and security analysts
- Internal auditors responsible for cybersecurity assessments
- Consultants working on cybersecurity audits and strategies

Individual Benefits

Key competencies that will be developed include:

- Enhanced expertise in cyber threat intelligence and audit practices
- Advanced skills in identifying and mitigating cyber risks
- Ability to lead cybersecurity initiatives within the organization
- Stronger audit and assessment capabilities for organizational security
- Direct experience with industry-leading tools and techniques

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved organizational readiness against cyber threats
- A stronger, more robust cyber threat intelligence framework
- Better coordination and response capabilities during a cyber crisis
- Enhanced compliance with global cybersecurity standards and regulations
- A proactive approach to identifying and managing cyber risks

Instructional Methodology

The course follows a blended learning approach combining theory with practice:

- Strategy Briefings – Deep dive into cyber threat intelligence, audit principles, and organizational frameworks
- Case Studies – Real-world examples of successful threat intelligence strategies and audits
- Workshops – Hands-on exercises to conduct audits, gather intelligence, and analyze cyber threats
- Peer Exchange – Group discussions on challenges and lessons learned in cyber threat management
- Tools – Templates for threat intelligence audits, risk assessments, and security improvement plans

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Course Outline

Detailed 5-Day Course Outline

Training Hours: 7:30 AM – 3:30 PM **Daily Format:** 3–4 Learning Modules | Coffee breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

Day 1: Introduction to Cyber Threat Intelligence and Its Importance

- Module 1: Overview of Cyber Threat Intelligence (07:30 – 09:30)
- Defining cyber threat intelligence and its role in cybersecurity
- Key principles of CTI and its integration into an organization\'s security strategy
- Overview of the threat intelligence lifecycle and audit process
- Module 2: Types of Cyber Threats (09:45 – 11:15)
- Exploring common types of cyber threats: phishing, malware, ransomware
- The evolving landscape of cyber-attacks and their impact on businesses
- Understanding advanced persistent threats (APTs) and their characteristics
- Module 3: Gathering and Analyzing Threat Intelligence (11:30 – 01:00)
- Methods for collecting and sourcing cyber threat intelligence
- Evaluating the quality and relevance of threat intelligence data
- Tools and platforms used for intelligence gathering and analysis

Day 2: Auditing Cyber Threat Intelligence Capabilities

- Module 4: Conducting a Cyber Threat Intelligence Audit (07:30 – 09:30)
- Steps for conducting a CTI audit within an organization
- Identifying gaps in existing threat intelligence practices
- Evaluating existing tools, resources, and personnel for CTI capabilities
- Module 5: Risk Assessment and Threat Analysis (09:45 – 11:15)
- Conducting risk assessments to identify potential cyber vulnerabilities
- Tools for analyzing and mapping cyber threats to organizational assets
- Risk prioritization and response strategies
- Module 6: Evaluating Cybersecurity Infrastructure (11:30 – 01:00)
- Reviewing the effectiveness of cybersecurity controls and infrastructure
- Assessing incident detection and response capabilities
- Understanding the role of firewalls, intrusion detection systems, and SIEM tools

Day 3: Developing Cyber Threat Intelligence Action Plans

- Module 7: Actionable Intelligence and Response Strategies (07:30 – 09:30)
- Turning intelligence into actionable insights for the organization
- Developing response plans for identified cyber threats
- Integrating threat intelligence into incident response protocols
- Module 8: Best Practices for Threat Intelligence Sharing (09:45 – 11:15)
- The importance of threat intelligence sharing within and outside the organization
- Legal, ethical, and privacy considerations in sharing cyber threat data
- Building trust and collaboration with third-party threat intelligence sources
- Module 9: Incident Response and Crisis Management (11:30 – 01:00)
- Handling cyber incidents and coordinating internal responses
- Managing communication during a cyber crisis
-

Post-incident analysis and improving response protocols

Day 4: Monitoring and Improving Cyber Threat Intelligence Programs

- Module 10: Monitoring Threat Intelligence Systems (07:30 – 09:30)
- Continuous monitoring and evaluation of cyber threat intelligence programs
- Real-time threat detection and proactive mitigation strategies
- Implementing continuous feedback loops for system improvement
- Module 11: Audit Reporting and Recommendations (09:45 – 11:15)
- Creating detailed audit reports on cyber threat intelligence practices
- Providing actionable recommendations to improve organizational security posture
- Communicating findings to senior management and stakeholders
- Module 12: Legal and Compliance Aspects of Cyber Threat Intelligence (11:30 – 01:00)
- Understanding legal and regulatory requirements in cyber threat intelligence
- Ensuring compliance with GDPR, HIPAA, and other cybersecurity standards
- Building a compliance framework for CTI programs

Day 5: Final Review and Advanced Cyber Threat Intelligence Practices

- Module 13: Advanced Cyber Threat Intelligence Tools (07:30 – 09:30)
- Overview of advanced threat intelligence platforms and technologies
- Machine learning and AI applications in cyber threat detection
- Emerging technologies and trends in cybersecurity
- Module 14: Leadership in Cybersecurity and Threat Intelligence (09:45 – 11:15)
- Leading a cybersecurity team in the face of evolving threats
- Building a culture of security within the organization
- Engaging executives and stakeholders in cybersecurity decision-making
- Module 15: Final Case Study and Wrap-Up (11:30 – 01:00)
- Applying learning to a comprehensive case study
- Group presentations of solutions and strategies
- Final Q&A and course summary

Certification

Participants will receive a Certificate of Completion in Cyber Threat Intelligence Audit, demonstrating their advanced understanding of cyber threat intelligence practices, auditing techniques, and organizational preparedness against cyber threats.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: **+601116373203**	EMAIL: **info@mawaevents.net**