MAWA EVENTS

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

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

AUDIT LOGGING AND MONITORING: REVIEWS THE IMPLEMENTATION OF LOGGING AND MONITORING PRACTICES TO DETECT AND RESPOND TO SECURITY INCIDENTS

"Strengthening Security Posture Through Effective Log Management and Continuous Monitoring"

Schedule

Date	Venue	Fees (Face-to-Face)
04 – 08 May 2026	London, UK	USD 3495 per delegate

Introduction

Log data is a critical source of truth in cybersecurity, compliance, and operational auditing. Without robust logging and monitoring systems in place, organizations risk missing early warning signs of security incidents, breaches, or control failures. This course delivers comprehensive, hands-on training in implementing and auditing logging and monitoring practices aligned with industry best practices and compliance frameworks such as ISO 27001, NIST, PCI-DSS, and CIS Controls.

Participants will learn how to evaluate the effectiveness of log collection, analyze logs for anomalies, configure alerts, and assess the integration of Security Information and Event Management (SIEM) tools. The course bridges security operations with audit assurance to improve incident detection, response readiness, and regulatory compliance.

Objectives

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

- Assess the completeness and effectiveness of logging policies and procedures
- Evaluate the design and implementation of monitoring systems (SIEM, IDS, SOC)
- Identify gaps in log collection, retention, correlation, and alerting
- Analyze event logs for suspicious patterns, insider threats, and policy violations
- Ensure logging and monitoring meet legal, regulatory, and internal control requirements

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

- Gain critical skills in assessing log management across IT, security, and business systems
- Understand how to audit SIEM tools, event correlation, and response procedures
- Develop actionable findings and recommendations for logging and monitoring weaknesses
- Strengthen cybersecurity governance and incident response capabilities
- Prepare for regulatory audits by aligning practices with global standards

Target Audience

This program is designed for:

- IT and cybersecurity auditors
- Information security professionals and SOC analysts
- Governance, Risk, and Compliance (GRC) personnel
- Internal auditors focusing on IT systems and operations
- Anyone responsible for IT monitoring, incident detection, or control assurance

Individual Benefits

Key competencies that will be developed include:

- Log lifecycle auditing (generation, transmission, storage, analysis)
- Assessment of log integrity, access controls, and alert effectiveness
- Understanding of SIEM architecture and log correlation techniques
- Root cause analysis and timeline reconstruction from logs
- Documentation of audit findings and recommendations

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved visibility into system and user activities across the enterprise
- Early detection of suspicious events and faster incident response
- Compliance with standards such as ISO 27001, NIST 800-92, and PCI-DSS
- Enhanced coordination between audit, IT, and security teams
- Reduced risk of undetected breaches, fraud, and policy violations

Instructional Methodology

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

- Strategy Briefings – Logging policies, monitoring architecture, global standards
- Case Studies – Real-world security incidents identified via logs
- Workshops – Evaluate logs, test alert systems, assess configurations
- Peer Exchange – Cross-sector approaches to audit and security logging
- Tools – SIEM checklists, log audit templates, log correlation worksheets

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

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: Foundations of Audit Logging & Monitoring

- Module 1: The Role of Logging in Security & Compliance (07:30 – 09:30) • Logs as evidence, audit trails, chain of custody
- Module 2: Logging Frameworks and Standards (09:45 – 11:15) • NIST SP 800-92, ISO 27001, PCI-DSS logging controls
- Module 3: Components of an Effective Log Management Policy (11:30 – 01:00) • Log sources, formats, access and retention
- Module 4: Workshop – Evaluate a Logging Policy (02:00 – 03:30) • Identify gaps and improvement opportunities

Day 2: Log Collection and Aggregation

- Module 5: Identifying Critical Log Sources (07:30 – 09:30) • Servers, endpoints, firewalls, applications, databases
- Module 6: Log Aggregation and Centralization Tools (09:45 – 11:15) • Syslog, agents, APIs, cloud integrations
- Module 7: Ensuring Log Integrity and Security (11:30 – 01:00) • Log tampering, secure storage, access controls
- Module 8: Workshop – Map a Log Collection Architecture (02:00 – 03:30) • Design an enterprise-wide log pipeline

Day 3: Real-Time Monitoring and Alerting

- Module 9: Introduction to SIEM and IDS Systems (07:30 – 09:30) • Splunk, QRadar, ELK, Snort—key concepts and uses
- Module 10: Event Correlation and Rule Design (09:45 – 11:15) • Indicators of compromise, false positives, tuning
- Module 11: Alerting and Escalation Workflows (11:30 – 01:00) • Triage models, SLA setting, SOC response
- Module 12: Workshop – Create a Log Correlation Scenario (02:00 – 03:30) • Simulate event pattern detection with SIEM rules

Day 4: Incident Response and Investigations

- Module 13: Using Logs for Incident Detection (07:30 – 09:30) • Unauthorized access, lateral movement, privilege abuse
- Module 14: Timeline Reconstruction and Forensic Techniques (09:45 – 11:15) • Log correlation for incident reconstruction
- Module 15: Reporting and Escalating Audit Findings (11:30 – 01:00) • Risk ratings, root causes, mitigation
- Module 16: Workshop – Analyze a Security Incident Using Logs (02:00 – 03:30) • Hands-on review of sample breach data

Day 5: Compliance and Audit Integration

- Module 17: Aligning Logging with Audit and GRC Requirements (07:30 – 09:30) • SOX, GDPR, HIPAA logging obligations
- Module 18: Auditing Cloud Logging Practices (09:45 – 11:15) • Azure Monitor, AWS CloudTrail, GCP audit logs
- Module 19: Building a Continuous Monitoring Program (11:30 – 01:00) • Automation, dashboards, audit trails
- Module 20: Final Workshop – Design an Audit Logging Program (02:00 – 03:30) • Create a complete strategy from log collection to compliance

Certification

Participants will receive a Certificate of Completion in Audit Logging and Monitoring, validating their expertise in assessing, designing, and auditing enterprise logging and monitoring practices for improved security, compliance, and operational integrity.

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.

MAWA EVENTS

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

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

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