# Cybersecurity Analyst Assessment Training Course

Professional Development Training Course Outline

| | | | |
|---|---|---|---|
| **Category** | Data Security | **Duration** | 5 Days |
| **Base Fee** | $1,500 USD | **Delivery Mode** | Online / On-site Hybrid |

## Course Introduction

Cybersecurity Analyst Assessment Training Course is engineered to transform aspiring and junior security professionals into proficient analysts capable of defending modern enterprise infrastructures. The escalating global threat landscape, driven by sophisticated ransomware attacks and advanced persistent threats (APTs), mandates a new generation of security experts. This program dives deep beyond theoretical concepts, focusing on the highly demanded, hands-on skills of threat detection, vulnerability management, and incident response.

Our curriculum is meticulously aligned with top industry frameworks like NIST and the MITRE ATT&CK matrix, ensuring career-ready knowledge in SIEM (Security Information and Event Management) tools and digital forensics. Graduates will master the art of analyzing complex security data, performing comprehensive vulnerability assessments, and orchestrating effective cyber incident management. This training provides the practical experience and SOC analyst skills necessary to secure critical assets, mitigate significant cyber risk, and contribute to a robust Zero Trust security posture in any organization. Enroll now to bridge the skills gap and launch your career in the most future-proof domain of technology.

## Programme Curriculum

**Cybersecurity Analyst Assessment Training Course**

**Introduction**

Cybersecurity Analyst Assessment Training Course is engineered to transform aspiring and junior security professionals into proficient analysts capable of defending modern enterprise infrastructures. The escalating global threat landscape, driven by sophisticated ransomware attacks and advanced persistent threats (APTs), mandates a new generation of security experts. This program dives deep beyond theoretical concepts, focusing on the highly demanded, hands-on skills of threat detection, vulnerability management, and incident response.

Our curriculum is meticulously aligned with top industry frameworks like NIST and the MITRE ATT&CK matrix, ensuring career-ready knowledge in SIEM (Security Information and Event Management) tools and digital forensics. Graduates will master the art of analyzing complex security data, performing comprehensive vulnerability assessments, and orchestrating effective cyber incident management. This training provides the practical experience and SOC analyst skills necessary to secure critical assets, mitigate significant cyber risk, and contribute to a robust Zero Trust security posture in any organization. Enroll now to bridge the skills gap and launch your career in the most future-proof domain of technology.

Course Duration

5 days

**Course Objectives**

1. Master advanced threat modeling techniques using the MITRE ATT&CK Framework to proactively identify and categorize potential cyber adversaries and their tactics.
2. Gain expert-level proficiency in configuring, optimizing, and utilizing SIEM platforms for real-time log analysis and threat detection.
3. Develop and implement a complete vulnerability management program, from discovery and scanning to prioritization and effective remediation assessment.
4. Execute structured digital forensics investigations and evidence handling procedures to support incident response and legal requirements.
5. Apply the NIST Incident Response Framework to manage complex security breaches.
6. Analyze and secure environments in leading platforms, focusing on cloud security architecture and identity access management (IAM) vulnerabilities.
7. Implement and analyze data from EDR and XDR tools for effective endpoint security monitoring and containment of malicious activity.
8. Understand attacker methodologies through a defensive perspective, covering phases of ethical hacking and basic penetration testing to preemptively identify weaknesses.
9. Integrate CTI into daily operations, leveraging OSINT and commercial feeds to enhance proactive defense strategies.
10. Articulate and assess security policies based on Zero Trust principles to ensure secure access control across hybrid environments.
11. Utilize scripting languages like Python for security automation, log parsing, and developing custom analysis tools.
12. Configure and analyze network traffic data using tools like Wireshark/tcpdump for network defense and identifying anomalies.
13. Evaluate organizational security posture against key GRC standards and conduct security auditing.

**Target Audience**

1. Aspiring Security Professionals.
2. IT/Network Administrators.
3. Security Specialists.
4. Junior Incident Handlers.
5. Risk and Compliance Officers.
6. Developers/DevOps Engineers
7. Help Desk Technicians.
8. Career Changers

**Course Modules**

**Module 1: Foundations of Cyber Threat Management**

- Introduction to the Cyber Kill Chain and MITRE ATT&CK.
- Understanding the role of the SOC Analyst and Security Operations Centre
- Principles of Confidentiality, Integrity, and Availability.
- Analyzing common threat vectors
- Case Study: The rise and analysis of a recent, major ransomware variant's TTPs

**Module 2: Network Security and Traffic Analysis**

- Deep dive into TCP/IP, network topology, and security controls
- Hands-on Network Security Monitoring (NSM) using packet sniffers.
- Identifying suspicious network traffic patterns and anomalies.
- Understanding common network-level attacks.
- Case Study: Analyzing a compromised network segment to identify lateral movement using NetFlow and PCAP data.

**Module 3: Security Information and Event Management (SIEM)**

- SIEM architecture, log aggregation, and normalization.
- Developing effective search queries and custom detection rules
- Tuning SIEM to minimize false positives and prioritize high-fidelity alerts.
- Correlation of events from multiple data sources.
- Case Study: Configuring a SIEM to track a multi-stage Advanced Persistent Threat campaign across different organizational systems.

**Module 4: Vulnerability Assessment and Scanning**

- The Vulnerability Management Lifecycle and asset inventory importance.
- Conducting authenticated and unauthenticated vulnerability scans.
- Analyzing scan reports, prioritizing risks using CVSS scoring, and reporting findings.
- Remediation strategies and patch management best practices.
- Case Study: Performing a full vulnerability assessment on a mock web application and prioritizing remediation based on business criticality.

**Module 5: Windows and Linux Log Analysis**

- Navigating and interpreting critical Windows Event Logs and Linux system logs.
- Identifying indicators of compromise on host systems.
- Using command-line tools for local system forensics and analysis.
- Understanding user, process, and file system monitoring.
- Case Study: Investigating a successful phishing attack by tracing user activity and unauthorized file creation in Windows Event Logs.

**Module 6: Incident Response and Digital Forensics**

- Applying the NIST Incident Response Framework to real-world scenarios.
- Containment, eradication, and recovery strategies.
- Chain of custody and best practices for digital evidence preservation.
- Malware analysis techniques.

- Case Study: Simulating the response to a live-fire data breach, including isolating the affected systems and commencing forensic imaging.

**Module 7: Cloud and Application Security Assessment**

- Fundamentals of Cloud Security and shared responsibility model.
- Assessing IAM policies, secure configuration, and misconfigurations in AWS/Azure.
- Introduction to basic web application vulnerabilities.
- Using cloud-native tools for log monitoring and security posture management.
- Case Study: Reviewing the security configuration of an S3 bucket or Azure Storage Account after a public data exposure incident.

**Module 8: Threat Hunting, Automation, and Career Path**

- Developing proactive threat hunting methodologies and hypotheses.
- Introduction to scripting for security automation and log parsing.
- Soft skills: Communication of cyber risk to executive management.
- Exam preparation, certifications, and career roadmapping for senior analyst roles.
- Case Study: Designing and running a threat hunt for dormant malicious activity that bypassed initial EDR and SIEM alerts.

## Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

**Register as a group from 3 participants for a Discount**

**Send us an email: info@fineskilltrainingcenter.org or call** +254769199797

**Certification**

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

**Tailor-Made Course**

We also offer tailor-made courses based on your needs.

**Key Notes**

**a.** The participant must be conversant with English.

**b.** Upon completion of training the participant will be issued with an Authorized Training Certificate

**c.** Course duration is flexible and the contents can be modified to fit any number of days.

**d.** The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

**e.** One-year post-training support Consultation and Coaching provided after the course.

**f.** Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

## Upcoming Scheduled Sessions

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **23 Nov 2026** | 27 Nov 2026 | Online | $1,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $1,500 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $3,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $3,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $6,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $4,500 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $6,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $6,000 |

Ready to enroll or request a customized program? Book online or contact us:

**Register Online Now**

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com