Cybersecurity Data Analytics and Threat Intelligence Training Course

Professional Development Training Course Outline

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

Course Introduction

In an era marked by relentless cyber threats, organizations are seeking skilled professionals who can combine the power of cybersecurity analytics, threat intelligence, and data science to proactively defend against attacks. Cybersecurity Data Analytics and Threat Intelligence Training Course equips participants with cutting-edge skills to detect anomalies, monitor cyber threats, analyze logs, and apply predictive modeling in cyber defense. This course is designed for professionals aiming to gain hands-on experience with industry tools like Splunk, Wireshark, Python, SIEM, MITRE ATT&CK, and machine learning algorithms for security analytics.

Through an immersive, case-based learning experience, learners will build capabilities in cyber threat detection, incident response, risk modeling, and real-time threat intelligence gathering. This course prepares participants to become critical assets in any cybersecurity operations center (SOC) or cyber threat intelligence team.

Programme Curriculum

Cybersecurity Data Analytics and Threat Intelligence Training Course

Introduction

In an era marked by relentless cyber threats, organizations are seeking skilled professionals who can combine the power of cybersecurity analytics, threat intelligence, and data science to proactively defend against attacks. Cybersecurity Data Analytics and Threat Intelligence Training Course equips participants with cutting-edge skills to detect anomalies, monitor cyber threats, analyze logs, and apply predictive modeling in cyber defense. This course is designed for professionals aiming to gain hands-on experience with industry tools like Splunk, Wireshark, Python, SIEM, MITRE ATT&CK, and machine learning algorithms for security analytics.

Through an immersive, case-based learning experience, learners will build capabilities in cyber threat detection, incident response, risk modeling, and real-time threat intelligence gathering. This course prepares participants to become critical assets in any cybersecurity operations center (SOC) or cyber threat intelligence team.

Course Objectives

1. Understand the fundamentals of cybersecurity threat intelligence.
2. Apply data analytics techniques in cyber defense operations.
3. Utilize machine learning for threat detection and prediction.
4. Perform network traffic analysis using Wireshark and Zeek.
5. Investigate SIEM alerts and apply incident response tactics.
6. Analyze malware behavior using sandboxing and threat feeds.
7. Implement MITRE ATT&CK framework for adversary emulation.
8. Use Python scripting to automate security tasks.
9. Correlate logs from multiple sources to identify insider threats.
10. Generate threat intelligence reports using structured data.
11. Use threat hunting strategies to detect hidden anomalies.
12. Evaluate risk through vulnerability assessment and scoring.
13. Design and implement cyber threat models using real-time data.

Target Audiences

1. Cybersecurity Analysts
2. Data Scientists in Security Domains
3. IT Security Engineers
4. Threat Intelligence Researchers
5. Security Operations Center (SOC) Teams
6. Government Cybersecurity Officials
7. Network Security Administrators
8. Cybersecurity Enthusiasts and Graduates

Course Duration: 5 days

Course Modules

Module 1: Foundations of Cybersecurity Analytics

- Introduction to cybersecurity and data analytics
- Overview of threat intelligence lifecycle
- Data sources: logs, NetFlow, endpoints, and dark web
- Cybersecurity metrics and KPIs
- Tools overview: ELK stack, Splunk, and SIEM
- **Case Study**: Identifying threats using log correlation in Splunk

Module 2: Network Traffic and Packet Analysis

- Understanding network protocols and packet flow
- Deep packet inspection using Wireshark
- Detecting anomalies in traffic with Zeek
- Network flow analytics and visualization
- Signature-based vs anomaly-based detection
- **Case Study**: DDoS detection through packet analysis

Module 3: SIEM Implementation and Log Analytics

- Introduction to SIEM and its architecture

- Log parsing, normalization, and correlation
- Event investigation using Splunk or IBM QRadar
- Alert tuning and noise reduction
- Creating dashboards and custom alerts
- **Case Study**: Insider threat detection using SIEM

Module 4: Threat Intelligence Platforms and Feeds

- Overview of TIPs and open-source threat feeds
- Integrating CTI into existing security operations
- Analyzing IOC, TTPs, and STIX/TAXII
- Threat data enrichment and validation
- Attribution and actor profiling
- **Case Study**: Using MISP to track APT group activity

Module 5: Machine Learning for Threat Detection

- ML concepts applied to cybersecurity
- Supervised vs unsupervised models
- Anomaly detection using clustering and SVM
- Feature engineering for security datasets
- Model evaluation and improvement
- **Case Study**: Malware classification using machine learning

Module 6: Adversary Emulation and MITRE ATT&CK

- Introduction to adversary tactics, techniques, and procedures
- Navigating the MITRE ATT&CK matrix
- Mapping incidents to ATT&CK framework
- Red vs Blue teaming strategies
- Automating detection rules with ATT&CK
- **Case Study**: Emulating APT29 attack lifecycle

Module 7: Python for Cybersecurity Automation

- Python scripting basics for cybersecurity tasks
- Automating log parsing and IOC extraction
- Creating security bots and scripts
- Integrating APIs for threat feeds
- Visualizing security data with matplotlib and seaborn
- **Case Study**: Building a threat hunting script in Python

Module 8: Real-Time Threat Hunting and Incident Response

- Threat hunting methodologies and frameworks
- IOC-based and hypothesis-driven hunting
- Incident lifecycle and response phases
- Root cause analysis and forensic investigation
- Building a threat hunting playbook
- **Case Study**: Threat hunting in a simulated SOC breach

Training Methodology

- Instructor-led live virtual sessions
- Hands-on labs and sandbox environments
- Weekly quizzes and self-paced learning content

- Real-world case study simulations
- Capstone project on cybersecurity threat modeling
- Peer-reviewed discussions and feedback

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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