Training Course on Security Data Science for Threat Hunting

Professional Development Training Course Outline

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

Course Introduction

In today's rapidly evolving cyber landscape, traditional perimeter defenses are no longer sufficient to combat sophisticated and **persistent threats**. Organizations face an urgent need to shift from reactive incident response to proactive **threat hunting**. This course addresses that critical need by empowering cybersecurity professionals with **cutting-edge data science methodologies** and **machine learning techniques** to uncover hidden threats, reduce **dwell time**, and strengthen overall **cyber resilience**. We delve into the practical application of data-driven insights to identify anomalies, predict malicious activities, and effectively neutralize **advanced persistent threats (APTs)** and **insider threats** before they escalate into full-blown breaches.

Training Course on Security Data Science for Threat Hunting is designed to bridge the gap between cybersecurity operations and advanced analytics. Participants will gain hands-on experience with **big data platforms**, learn to leverage **AI for security analytics**, and master the art of transforming raw security logs into actionable **threat intelligence**. By focusing on **behavioral analytics**, **anomaly detection**, and **predictive modeling**, this course equips professionals with the skills to proactively defend against the most elusive cyber adversaries, ensuring a robust and adaptive security posture in the face of ever-increasing cyber risks.

Programme Curriculum

Training Course on Security Data Science for Threat Hunting

Introduction

In today's rapidly evolving cyber landscape, traditional perimeter defenses are no longer sufficient to combat sophisticated and **persistent threats**. Organizations face an urgent need to shift from reactive incident response to proactive **threat hunting**. This course addresses that critical need by empowering cybersecurity professionals with **cutting-edge data science methodologies** and

machine learning techniques to uncover hidden threats, reduce **dwell time**, and strengthen overall **cyber resilience**. We delve into the practical application of data-driven insights to identify anomalies, predict malicious activities, and effectively neutralize **advanced persistent threats (APTs)** and **insider threats** before they escalate into full-blown breaches.

Training Course on Security Data Science for Threat Hunting is designed to bridge the gap between cybersecurity operations and advanced analytics. Participants will gain hands-on experience with **big data platforms**, learn to leverage **AI for security analytics**, and master the art of transforming raw security logs into actionable **threat intelligence**. By focusing on **behavioral analytics**, **anomaly detection**, and **predictive modeling**, this course equips professionals with the skills to proactively defend against the most elusive cyber adversaries, ensuring a robust and adaptive security posture in the face of ever-increasing cyber risks.

Course Duration

5 days

Course Objectives

1. Develop a deep understanding of hypothesis-driven and unstructured threat hunting techniques.
2. Apply core data science principles, including statistical analysis and data visualization, to cybersecurity datasets.
3. Utilize supervised and unsupervised learning algorithms to identify anomalous behaviors and suspicious patterns.
4. Proficiently collect, clean, and process vast volumes of security event data from diverse sources (SIEM, EDR, network logs).
5. Detect sophisticated, long-term attack campaigns using data-driven indicators of compromise (IoCs) and tactics, techniques, and procedures (TTPs).
6. Identify malicious or negligent insider activities by analyzing user behavior patterns and deviations from baselines.
7. Build and deploy machine learning models for proactive threat prediction and risk assessment.
8. Integrate OSINT and threat intelligence feeds to enrich hunting efforts.
9. Learn to script and automate data analysis tasks and integrate findings into security orchestration, automation, and response (SOAR) platforms.
10. Explore the application of deep neural networks for advanced malware analysis, phishing detection, and complex anomaly identification.
11. Improve incident investigation and remediation processes through advanced data correlation and forensic analysis.
12. Analyze security data from cloud environments to detect threats in cloud workloads and configurations.
13. Formulate and implement a comprehensive threat hunting program within an organizational security framework.

Organizational Benefits

- Significantly decrease the time malicious actors remain undetected within the network, minimizing potential damage and data exfiltration.
- Shift from reactive incident response to proactively identifying and neutralizing threats before they impact operations.

- Strengthen overall organizational security by continuously identifying and remediating vulnerabilities and gaps in existing defenses.
- Provide richer, data-driven insights to accelerate incident investigation, containment, and recovery.
- Validate and improve the effectiveness of current security tools (SIEM, EDR) by identifying missed threats and refining alert mechanisms.
- Generate valuable, context-rich threat intelligence specific to the organization's environment and industry.
- Aid in meeting regulatory compliance requirements and reduce the financial and reputational risks associated with cyber breaches.
- Prevent costly data breaches, legal fees, regulatory fines, and reputational damage by early threat detection.

Target Audience

1. Security Operations Center (SOC) Analysts
2. Threat Hunters.
3. Incident Responders.
4. Cybersecurity Engineers and Architects.
5. Data Scientists with Security Interest.
6. IT Security Managers.
7. Forensic Investigators.
8. Network Security Specialists.

Course Outline

Module 1: Foundations of Security Data Science & Threat Hunting

- Introduction to Threat Hunting
- The Role of Data in Cybersecurity).
- Key Data Science Concepts for Security
- Threat Intelligence Integration
- **Case Study: Identifying Initial Access Vectors**: Analyzing firewall logs and web proxy data to detect common initial access techniques (e.g., phishing attempts, vulnerable services).

Module 2: Data Acquisition, Preprocessing & Feature Engineering

- Sources of Security Data.
- Data Collection and Ingestion
- Data Cleaning and Normalization
- Feature Engineering for Security
- **Case Study: Preparing for Ransomware Detection**: Preprocessing endpoint and network data to extract features indicative of ransomware activity

Module 3: Statistical Methods for Anomaly Detection

- Descriptive Statistics for Baselines
- Univariate and Multivariate Anomaly Detection
- Time-Series Analysis for Security
- Clustering Techniques.
- **Case Study: Detecting Command and Control (C2) Traffic**: Applying statistical analysis to DNS queries and network flow data to identify unusual communication patterns indicative of C2.

Module 4: Machine Learning for Threat Detection

- Supervised Learning for Classification.
- Unsupervised Learning for Novel Threats.
- Ensemble Methods and Boosting
- Model Evaluation and Validation
- **Case Study: Malware Classification**: Building a machine learning model to classify executables as benign or malicious based on static and dynamic features.

Module 5: User & Entity Behavior Analytics (UEBA)

- Understanding Insider Threats
- Data Sources for UEBA
- Behavioral Baselines and Deviation Scoring
- Identifying Suspicious Activities.
- **Case Study: Detecting Data Exfiltration by a Compromised Account**: Analyzing user activity logs and network egress data to identify unusual data transfers to external sources.

Module 6: Network-Based Threat Hunting with Data Science

- Network Flow Analysis (NetFlow/IPFIX)
- Deep Packet Inspection (DPI) and PCAP Analysis
- Protocol Anomaly Detection
- Graph Analysis for Network Relationships
- **Case Study: Hunting for Lateral Movement**: Analyzing internal network traffic for suspicious authentication attempts (e.g., Pass-the-Hash), unusual port scanning, or unexpected internal connections.

Module 7: Advanced Analytics & Deep Learning for Security

- Introduction to Deep Learning in Cybersecurity.
- Anomaly Detection with Autoencoders.
- Natural Language Processing (NLP) for Log Analysis
- Adversarial Machine Learning
- **Case Study: Detecting Polymorphic Malware with Deep Learning**: Training a convolutional neural network (CNN) on byte patterns to identify polymorphic malware variants.

Module 8: Operationalizing Threat Hunting & Future Trends

- Integrating Data Science into SOC Operations
- Threat Hunting Playbooks and Automation.
- Visualization and Reporting for Threat Hunters
- Legal and Ethical Considerations.
- **Case Study: Building a Proactive Threat Hunting Dashboard**: Designing and implementing a custom Splunk/Elasticsearch dashboard that visualizes key indicators for ongoing threat hunting operations.

Training Methodology

This course employs a **highly practical and interactive training methodology** designed to foster hands-on skills and real-world applicability.

- **Hands-on Labs and Exercises**: Extensive practical labs using real-world or simulated security datasets, leveraging popular data science tools (Python with Pandas, NumPy, Scikit-learn, TensorFlow/Keras) and security platforms (SIEMs like Splunk/Elastic Stack, EDR data simulators).
- **Instructor-Led Sessions**: Engaging lectures and discussions to introduce core concepts, explain complex algorithms, and provide practical insights from industry experts.
- **Case Study-Driven Learning**: In-depth analysis of actual cyberattack scenarios and real-world data breaches to illustrate the application of data science for threat hunting.
- **Interactive Demos**: Live demonstrations of tools, techniques, and data analysis workflows.
- **Group Activities and Discussions**: Collaborative exercises to encourage peer learning, problem-solving, and sharing of best practices.
- **Q&A and Troubleshooting Sessions**: Dedicated time for participants to ask questions, resolve technical challenges, and gain deeper understanding.
- **Capstone Project**: A culminating project where participants apply learned skills to a comprehensive threat hunting scenario, from data ingestion to final reporting.

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
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