Training Course on Machine Learning for Anomaly Detection in Threat Hunting

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

This comprehensive training course delves into the critical intersection of **Machine Learning (ML)** and **Cybersecurity**, empowering security professionals to leverage advanced analytical techniques for **proactive threat detection** and **efficient threat hunting**. Participants will gain hands-on experience in building, deploying, and optimizing ML models to identify **anomalous behaviors** and **zero-day threats** within complex network environments. Training Course on Machine Learning for Anomaly Detection in Threat Hunting focuses on practical applications, bridging the gap between theoretical ML concepts and real-world **security operations center (SOC)** challenges, ultimately enhancing an organization's **cyber resilience** against evolving attack vectors.

In today's dynamic **threat landscape**, traditional signature-based detection methods are increasingly insufficient to combat sophisticated, **AI-powered cyberattacks** and **advanced persistent threats (APTs)**. This course provides the essential **data science** and **security analytics** skills needed to move beyond reactive security. Through practical case studies and hands-on labs, attendees will master techniques for **behavioral analytics**, **unsupervised learning**, and **deep learning** to uncover hidden patterns, detect **insider threats**, and perform effective **threat intelligence** driven hunting, leading to faster **incident response** and a stronger **security posture**.

Programme Curriculum

Training Course on Machine Learning for Anomaly Detection in Threat Hunting

Introduction

This comprehensive training course delves into the critical intersection of **Machine Learning (ML)** and **Cybersecurity**, empowering security professionals to leverage advanced analytical techniques for **proactive threat detection** and **efficient threat hunting**. Participants will gain hands-on experience in building, deploying, and optimizing ML models to identify **anomalous behaviors** and **zero-day threats** within complex network environments. Training Course on Machine

Learning for Anomaly Detection in Threat Hunting focuses on practical applications, bridging the gap between theoretical ML concepts and real-world **security operations center (SOC)** challenges, ultimately enhancing an organization's **cyber resilience** against evolving attack vectors.

In today's dynamic **threat landscape**, traditional signature-based detection methods are increasingly insufficient to combat sophisticated, **AI-powered cyberattacks** and **advanced persistent threats (APTs)**. This course provides the essential **data science** and **security analytics** skills needed to move beyond reactive security. Through practical case studies and hands-on labs, attendees will master techniques for **behavioral analytics**, **unsupervised learning**, and **deep learning** to uncover hidden patterns, detect **insider threats**, and perform effective **threat intelligence** driven hunting, leading to faster **incident response** and a stronger **security posture**.

Course Duration

10 days

Course Objectives

1. Master foundational Machine Learning algorithms for Anomaly Detection.
2. Implement real-time threat detection systems using ML.
3. Perform advanced behavioral analytics for user and entity behavior analytics (UEBA).
4. Develop robust models to identify zero-day attacks and unknown malware.
5. Utilize deep learning architectures for enhanced network intrusion detection.
6. Conduct hypothesis-driven threat hunting with ML-powered insights.
7. Engineer relevant features from diverse security data sources.
8. Evaluate and optimize ML model performance using key metrics.
9. Integrate ML solutions into existing Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) platforms.
10. Mitigate false positives and improve alert prioritization in SOC operations.
11. Apply unsupervised learning techniques for discovering novel attack patterns.
12. Leverage cloud-native ML services for scalable threat detection.
13. Build a proactive cybersecurity defense strategy using AI-driven insights.

Organizational Benefits

- Proactive identification of sophisticated and novel cyber threats, including zero-day attacks and insider threats, significantly reducing breach risk.
- Automated anomaly detection and alert prioritization streamline security operations, leading to quicker investigation and containment of incidents.
- Improved accuracy of threat alerts, minimizing alert fatigue for security analysts and allowing them to focus on genuine threats.
- Development of an adaptive and intelligent defense mechanism that continuously learns and evolves with the threat landscape.
- Automation of routine threat analysis tasks frees up security personnel for more strategic threat hunting and complex investigations.
- Gaining actionable insights from vast volumes of security data to inform and refine cybersecurity strategies.
- Support for compliance requirements by providing robust detection and auditing capabilities for unusual activities.

Target Audience

1. Security Analysts and SOC Engineers
2. Threat Hunters and Incident Responders

3. Cybersecurity Professionals seeking to upskill in ML
4. Data Scientists interested in cybersecurity applications
5. Network Administrators and Security Architects
6. IT Managers overseeing cybersecurity operations
7. Cloud Security Engineers
8. Security Researchers

Course Outline

Module 1: Introduction to Machine Learning in Cybersecurity

- Understanding the evolving cyber threat landscape and limitations of traditional security.
- Overview of Machine Learning fundamentals: Supervised, Unsupervised, and Semi-supervised learning.
- Why ML is crucial for anomaly detection in modern threat hunting.
- Key challenges and opportunities in applying ML to cybersecurity data.
- **Case Study:** The rise of polymorphic malware and the need for ML-driven detection.

Module 2: Cybersecurity Data Sources and Preprocessing

- Identifying and collecting relevant data: Network flows (NetFlow, IPFIX), system logs (Syslog, Windows Events), endpoint telemetry, cloud logs.
- Data cleaning, normalization, and handling missing values.
- Feature engineering: Extracting meaningful attributes from raw security data.
- Addressing imbalanced datasets in cybersecurity.
- **Case Study:** Feature engineering for detecting unusual user login patterns from Active Directory logs.

Module 3: Statistical and Rule-Based Anomaly Detection

- Baseline profiling and thresholding techniques.
- Statistical methods: Z-score, IQR, Gaussian distribution for outliers.
- Rule-based systems and their limitations in dynamic environments.
- Combining statistical methods with expert rules.
- **Case Study:** Detecting unusual network bandwidth spikes using statistical process control.

Module 4: Unsupervised Learning for Anomaly Detection

- Clustering algorithms: K-Means, DBSCAN for grouping normal behavior.
- Density-based methods: Isolation Forest and Local Outlier Factor (LOF).
- One-Class SVM for learning the boundaries of normal data.
- Techniques for determining optimal clusters and outlier thresholds.
- **Case Study:** Identifying novel network attack patterns using Isolation Forest on NetFlow data.

Module 5: Supervised Learning for Threat Classification

- Classification algorithms: Decision Trees, Random Forests, Support Vector Machines (SVM).
- Training models on labeled datasets of malicious and benign activities.
- Handling concept drift and evolving threat signatures.
- Feature importance and interpretability of supervised models.
- **Case Study:** Building a supervised model to classify phishing emails based on header and content features.

Module 6: Deep Learning for Advanced Anomaly Detection

- Introduction to Neural Networks and Deep Learning architectures.
- Autoencoders for learning compact representations and anomaly detection through reconstruction error.
- Recurrent Neural Networks (RNNs) for time-series anomaly detection (e.g., sequential user behavior).
- Convolutional Neural Networks (CNNs) for analyzing network packet payloads or malware binaries.
- **Case Study:** Using an Autoencoder to detect anomalous network traffic flows indicative of data exfiltration.

Module 7: User and Entity Behavior Analytics (UEBA)

- Establishing baselines of normal user and entity behavior.
- Detecting deviations: unusual login times, data access patterns, application usage.
- Graph-based analytics for identifying suspicious relationships between entities.
- Risk scoring and prioritizing anomalous user activities.
- **Case Study:** Uncovering insider threats by detecting abnormal access to sensitive documents by an authorized user.

Module 8: Network Anomaly Detection

- Analyzing network traffic for unusual protocols, ports, and communication patterns.
- Detecting command and control (C2) communication and lateral movement.
- Applying ML to detect DDoS attacks and port scanning.
- Leveraging network telemetry for real-time anomaly detection.
- **Case Study:** Identifying a covert C2 channel through ML analysis of encrypted traffic metadata.

Module 9: Endpoint Anomaly Detection

- Monitoring process execution, file system changes, and registry modifications.
- Detecting suspicious API calls and privilege escalation attempts.
- Behavioral analysis of endpoint activities to identify malware and ransomware.
- Integrating endpoint detection and response (EDR) data with ML models.
- **Case Study:** Using ML to detect a fileless malware infection based on abnormal process behavior.

Module 10: Cloud Security Anomaly Detection

- Monitoring cloud infrastructure logs (AWS CloudTrail, Azure Activity Logs).
- Detecting unusual access to cloud resources, misconfigurations, and privilege abuses.
- Anomaly detection in serverless functions and containerized environments.
- Securing cloud-native applications with ML.
- **Case Study:** Identifying unauthorized access to an S3 bucket or Azure Blob storage using ML on cloud logs.

Module 11: Model Evaluation and Optimization

- Key performance metrics: Precision, Recall, F1-Score, ROC-AUC curves.
- Understanding and mitigating false positives and false negatives.
- Hyperparameter tuning and cross-validation techniques.
- Techniques for continuous model improvement and retraining.

- **Case Study:** Optimizing a fraud detection model to reduce false alerts in a financial institution.

Module 12: Operationalizing ML for Threat Hunting

- Integrating ML models into SIEM and XDR platforms.
- Building automated alert triage and incident response workflows.
- Data pipelines for real-time inference and continuous monitoring.
- Orchestration and automation of threat hunting playbooks.
- **Case Study:** Automating the investigation of suspicious network connections flagged by an ML model.

Module 13: Threat Intelligence and Adversary Emulation

- Leveraging external threat intelligence feeds to enrich anomaly detection.
- Mapping detected anomalies to the MITRE ATT&CK framework.
- Using adversary emulation to test and validate ML models.
- Proactive threat hunting methodologies driven by intelligence.
- **Case Study:** Using ML to detect TTPs associated with a known APT group based on recent threat intelligence.

Module 14: Explainable AI (XAI) in Cybersecurity

- Understanding the importance of model interpretability in security.
- Techniques for explaining ML model decisions (SHAP, LIME).
- Building trust and confidence in AI-driven security systems.
- Debugging and troubleshooting ML model misclassifications.
- **Case Study:** Explaining why an ML model flagged a specific user activity as anomalous to a security analyst.

Module 15: Future Trends and Advanced Topics

- Federated Learning for collaborative threat intelligence.
- Reinforcement Learning in adaptive security systems.
- Quantum Machine Learning and its potential impact on cybersecurity.
- Ethical considerations and bias in AI for security.
- **Case Study:** Discussion on the potential of adversarial ML and how to build more robust models against evasion attacks.

Training Methodology

This course adopts a **blended learning approach**, combining theoretical foundations with extensive **hands-on labs** and **real-world case studies**.

- **Interactive Lectures:** Engaging presentations on core concepts and trending topics.
- **Practical Demonstrations:** Live coding and tool demonstrations for implementing ML solutions.
- **Hands-on Labs:** Participants will work on real and simulated cybersecurity datasets to build, train, and evaluate ML models using popular libraries (e.g., Scikit-learn, TensorFlow, PyTorch) and programming languages (Python).
- **Case Study Analysis:** In-depth examination of real-world cybersecurity breaches and how ML-driven anomaly detection could have prevented or mitigated them.
- **Group Exercises & Discussions:** Collaborative problem-solving and sharing of best practices.

- **Q&A Sessions:** Dedicated time for participants to address their specific challenges and questions.
- **Capstone Project:** A culminating project where participants apply their learned skills to a complex threat hunting scenario.

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

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now