# Training Course on Advanced Network Flow Data Analysis

Professional Development Training Course Outline

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

## Course Introduction

In the ever-evolving cybersecurity and network monitoring landscape, advanced flow data analytics is vital for proactive threat detection, forensic investigation, performance optimization, and compliance. Training Course on Advanced Network Flow Data Analysis offers an in-depth understanding of NetFlow, IPFIX, and related flow protocols that enable visibility into network behavior at a granular level. Participants will gain hands-on skills in analyzing, visualizing, and responding to flow data patterns using cutting-edge tools and techniques. By leveraging big data analytics, machine learning, and real-time monitoring, this course equips learners with the capabilities to enhance network security posture, improve incident response, and implement intelligent automation.

This course is essential for professionals tasked with cyber threat intelligence, anomaly detection, network traffic engineering, and infrastructure security. Through a blend of theory, practical labs, and real-world case studies, learners will decode the power of NetFlow/IPFIX for scalable monitoring, cloud forensics, IoT traffic analysis, and advanced threat hunting. Whether managing enterprise infrastructure or cloud environments, the course emphasizes how flow data analytics supports compliance mandates like GDPR, HIPAA, and NIST.

## Programme Curriculum

**Training Course on Advanced Network Flow Data Analysis**

**Introduction**

In the ever-evolving cybersecurity and network monitoring landscape, advanced flow data analytics is vital for proactive threat detection, forensic investigation, performance optimization, and compliance. Training Course on Advanced Network Flow Data Analysis offers an in-depth understanding of NetFlow, IPFIX, and related flow protocols that enable visibility into network behavior at a granular level. Participants will gain hands-on skills in analyzing, visualizing, and responding to flow data patterns using cutting-edge tools and techniques. By leveraging big data analytics, machine learning, and real-time monitoring, this course equips learners with the capabilities to enhance network security posture, improve incident

response, and implement intelligent automation.

This course is essential for professionals tasked with cyber threat intelligence, anomaly detection, network traffic engineering, and infrastructure security. Through a blend of theory, practical labs, and real-world case studies, learners will decode the power of NetFlow/IPFIX for scalable monitoring, cloud forensics, IoT traffic analysis, and advanced threat hunting. Whether managing enterprise infrastructure or cloud environments, the course emphasizes how flow data analytics supports compliance mandates like GDPR, HIPAA, and NIST.

**Course Objectives**

1. Understand the structure and function of NetFlow and IPFIX protocols.
2. Analyze network flow data to identify anomalies and threat patterns.
3. Implement flow-based monitoring strategies for enterprise and cloud networks.
4. Leverage open-source and commercial NetFlow/IPFIX analyzers.
5. Detect DDoS attacks, lateral movement, and data exfiltration using flow data.
6. Integrate SIEM systems with NetFlow/IPFIX data pipelines.
7. Perform baselining and anomaly detection using machine learning models.
8. Conduct forensic analysis of past incidents using historical flow data.
9. Visualize flow data with dashboard tools like Grafana, Kibana, and ntopng.
10. Correlate flow data with threat intelligence feeds.
11. Analyze encrypted traffic behaviors without payload access.
12. Optimize network performance and bandwidth usage via flow metrics.
13. Understand legal and compliance considerations in flow data retention.

**Target Audience**

1. Network Security Engineers
2. Cybersecurity Analysts
3. SOC (Security Operations Center) Teams
4. Cloud Security Architects
5. Digital Forensics Investigators
6. Threat Intelligence Professionals
7. IT Compliance Officers
8. Penetration Testers and Ethical Hackers

**Course Duration:** 10 days

**Course Modules**

**Module 1: Introduction to Network Flow Data**

- Concepts: NetFlow vs IPFIX vs sFlow
- Flow record formats and fields
- Flow exporters and collectors
- Metadata enrichment basics
- Tools for flow collection and parsing
- **Case Study**: Mapping flow sources in hybrid networks

**Module 2: NetFlow/IPFIX Architecture**

- Flow collection process lifecycle
- Sampling, aggregation, and deduplication
- Flow templates and field definitions
- Cisco, Juniper, and open-source exporters
- Transport protocols: UDP vs SCTP vs TCP

- **Case Study**: Tuning exporters for low-latency reporting

**Module 3: Threat Detection with Flow Data**

- Behavioral patterns of malware and APTs
- Detecting C2 channels and exfiltration
- Unusual port usage and protocol anomalies
- Flow-based IOC correlation
- Detection using ML/AI models
- **Case Study**: Identifying beaconing behavior

**Module 4: Flow Analysis for DDoS Mitigation**

- Recognizing volumetric attacks via flows
- SYN floods and UDP amplification analysis
- Geo-IP and ASN analysis of attackers
- Rate-limiting and blackholing strategies
- Alerting and dashboard configuration
- **Case Study**: Mitigating a real-world DDoS attack

**Module 5: Flow Data Visualization Tools**

- Grafana and Kibana for NetFlow
- ntopng dashboards and drilldowns
- Time-series data visualization
- Filtering, queries, and alerting
- Building interactive dashboards
- **Case Study**: Designing an alert dashboard for SOC

**Module 6: Integrating Flow Data with SIEM**

- SIEM platforms that support flow ingestion
- Syslog, Kafka, and Logstash pipelines
- Parsing and enrichment techniques
- Correlation with log and endpoint data
- Detection rules and correlation logic
- **Case Study**: Flow-SIEM integration in a hybrid SOC

**Module 7: Network Performance Analysis**

- Flow-based QoS analysis
- Bandwidth usage and capacity planning
- Troubleshooting application slowness
- Network path visibility and jitter analysis
- Traffic segmentation by user/application
- **Case Study**: Resolving performance bottlenecks using flow data

**Module 8: Advanced Flow Data Storage & Retention**

- High-volume data management strategies
- Flow record compression and indexing
- Scalable storage architectures (Elasticsearch, Hadoop)
- Legal and compliance implications
- Retention policy design
- **Case Study**: GDPR-compliant NetFlow archival strategy

**Module 9: Machine Learning for Flow Anomaly Detection**

- ML algorithms for unsupervised detection
- Time-series forecasting of flow metrics
- Clustering abnormal behaviors
- Alert prioritization and noise reduction
- Open-source ML tools for flow analysis
- **Case Study**: Using ML to detect insider threats

**Module 10: Cloud & Multi-cloud Flow Analysis**

- Cloud-native flow log sources (AWS, Azure, GCP)
- VPC Flow Logs and NSG Flow Logs
- Cross-region and multi-cloud flow stitching
- Traffic mirroring and agentless capture
- Flow visibility gaps in cloud
- **Case Study**: Investigating lateral movement in AWS

**Module 11: IoT and OT Traffic Flow Monitoring**

- Flow behavior of industrial protocols
- Segmenting IoT traffic from enterprise traffic
- Device fingerprinting with flow data
- Anomaly detection in smart devices
- Security policy enforcement using flows
- **Case Study**: Securing IoT medical devices via NetFlow

**Module 12: Flow Data Enrichment Techniques**

- DNS and DHCP enrichment
- Threat feed integration
- GeoIP and organization tagging
- Contextualizing with asset inventories
- Visual correlation maps
- **Case Study**: Using enriched flow data for alert triage

**Module 13: Real-Time Alerting with Flow Metrics**

- Setting flow-based thresholds
- Threshold tuning and incident reduction
- Alert routing via Slack, email, SIEM
- Automation scripts and playbooks
- Incident triage best practices
- **Case Study**: Reducing false positives in flow alerts

**Module 14: Legal, Ethical, and Compliance Issues**

- Data privacy and surveillance ethics
- Flow data vs payload inspection legality
- Jurisdictional compliance (HIPAA, NIST, ISO)
- Anonymization and pseudonymization
- Internal policy development
- **Case Study**: Navigating compliance in healthcare networks

**Module 15: Final Capstone Project & Assessment**

- End-to-end flow data pipeline deployment
- Real-time monitoring lab setup

- Threat detection and dashboard design
- Report writing and executive summary
- Oral presentation to stakeholders
- **Case Study**: Student-designed attack simulation and flow analysis

**Training Methodology**

- Hands-on lab simulations using real-world data
- Instructor-led sessions with interactive Q&A
- Use of open-source and enterprise tools
- Case-based learning with practical scenarios
- Group discussions, assignments, and knowledge checks
- Final capstone project presentation for assessment

**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 |
|---|---|---|---|
| **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 |

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **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**

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