Training Course on SD-WAN and SASE Forensics

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 digital ecosystem, cybersecurity professionals, network engineers, and digital forensic analysts must understand the intricacies of Software-Defined Wide Area Networking (SD-WAN) and Secure Access Service Edge (SASE). As enterprises migrate to cloud-first architectures and adopt hybrid work models, the forensic analysis of SD-WAN and SASE technologies is critical in detecting, investigating, and mitigating cyber threats. Training Course on SD-WAN and SASE Forensics provides a cutting-edge curriculum that equips participants with practical skills in packet inspection, encrypted traffic analysis, zero-trust network architecture (ZTNA), and real-time threat detection within SD-WAN and SASE environments.

Leveraging real-world case studies and incident simulations, this course bridges the knowledge gap between network forensics and cloud security architectures. Trainees will gain proficiency in log correlation, anomaly detection, digital evidence preservation, and cross-platform investigations, empowering them to address complex security incidents effectively. The program aligns with industry demands and trending skills, ensuring that learners are prepared to meet the cybersecurity challenges of tomorrow.

Programme Curriculum

Training Course on SD-WAN and SASE Forensics

Introduction

In today’s rapidly evolving digital ecosystem, cybersecurity professionals, network engineers, and digital forensic analysts must understand the intricacies of Software-Defined Wide Area Networking (SD-WAN) and Secure Access Service Edge (SASE). As enterprises migrate to cloud-first architectures and adopt hybrid work models, the forensic analysis of SD-WAN and SASE technologies is critical in detecting, investigating, and mitigating cyber threats. Training Course on SD-WAN and SASE Forensics provides a cutting-edge curriculum that equips participants with practical skills in packet inspection, encrypted traffic analysis, zero-trust network architecture (ZTNA), and real-time threat detection within SD-WAN and SASE environments.

Leveraging real-world case studies and incident simulations, this course bridges the knowledge gap between network forensics and cloud security architectures. Trainees will gain proficiency in log correlation, anomaly detection, digital evidence preservation, and cross-platform investigations, empowering them to address complex security incidents effectively. The program aligns with industry demands and trending skills, ensuring that learners are prepared to meet the cybersecurity challenges of tomorrow.

Course Objectives

1. Understand SD-WAN architecture and packet flow analysis
2. Investigate SASE components including CASB, SWG, and ZTNA
3. Apply forensic techniques in SD-WAN routing and segmentation
4. Analyze encrypted traffic and SSL inspection logs
5. Detect advanced persistent threats (APT) using SD-WAN telemetry
6. Conduct log correlation in multi-vendor SASE platforms
7. Implement evidence handling and data preservation methods
8. Integrate forensic tools with SIEM for incident detection
9. Apply threat intelligence in SD-WAN anomaly detection
10. Forensically analyze policy misconfigurations in SASE
11. Perform root cause analysis of SD-WAN-based breaches
12. Develop automated response using SOAR integration
13. Prepare comprehensive forensic reports for regulatory compliance

Target Audience

1. Network Forensics Analysts
2. Cybersecurity Engineers
3. Cloud Security Architects
4. SOC Analysts
5. Threat Intelligence Teams
6. IT Risk and Compliance Officers
7. Penetration Testers
8. Incident Response Managers

Course Duration: 5 days

Course Modules

Module 1: Introduction to SD-WAN and SASE Architecture

- Overview of SD-WAN overlays and underlays
- Key SASE components: SWG, CASB, FWaaS, and ZTNA
- SD-WAN routing and segmentation models
- Cloud-native security principles
- Integration of SD-WAN and SASE platforms
- **Case Study:** Migrating a traditional WAN to SD-WAN with SASE integration

Module 2: Traffic Monitoring and Packet Analysis

- Capturing data flows in SD-WAN environments
- Tools for packet inspection and flow reconstruction
- Encrypted traffic challenges and solutions
- SSL/TLS inspection in SASE
- Session replay and protocol analysis
- **Case Study:** Identifying exfiltration via DNS tunneling

Module 3: Log Management and Correlation

- Aggregating logs from SD-WAN edge devices
- Analyzing SASE logs for anomalies
- Correlating multi-source logs with SIEM
- Time-stamping and log integrity validation
- Visualizing data using dashboards
- **Case Study:** Tracing lateral movement in hybrid SD-WAN network

Module 4: Threat Detection and Analysis

- Detecting threats with machine learning in SASE
- Behavioral analytics and network baselines
- Indicators of compromise (IOC) identification
- Using threat feeds in SD-WAN/SASE forensics
- Alert triaging and false-positive reduction
- **Case Study:** Uncovering command-and-control (C2) traffic

Module 5: Incident Response and Evidence Preservation

- Incident lifecycle in SD-WAN environments
- Forensic chain of custody and documentation
- Data carving and preservation techniques
- Capturing volatile memory in SASE devices
- Reporting for law enforcement and internal use
- **Case Study:** Ransomware attack response on SD-WAN nodes

Module 6: Policy Auditing and Misconfiguration Analysis

- Reviewing access control and routing policies
- Detecting privilege escalation vulnerabilities
- Policy drift and rollback methods
- Misconfigured SASE profiles analysis
- Automation in policy validation
- **Case Study:** Insider threat via misconfigured access policy

Module 7: Integration with SIEM, SOAR, and Threat Intelligence

- Connecting forensic data to SIEM tools
- Automating response using SOAR workflows
- Integrating with threat intelligence platforms
- Real-time threat sharing and IOC updates
- Playbook creation for common forensic scenarios
- **Case Study:** Automated threat containment with SOAR & SD-WAN telemetry

Module 8: Reporting, Compliance, and Legal Aspects

- Compliance standards (NIST, ISO, GDPR, HIPAA)
- Drafting forensic-ready reports
- Legal considerations in multi-cloud investigations
- Regulatory audit preparedness
- Secure data sharing and retention policies
- **Case Study:** Compliance audit in a multi-jurisdiction SD-WAN deployment

Training Methodology

- Hands-on labs using real-world SD-WAN and SASE toolsets

- Case-based learning for scenario-driven analysis
- Instructor-led virtual or in-person sessions
- Capture-the-flag forensic exercises
- Post-course assessments and certification

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

Start Date	End Date	Location	Price
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