+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 01/10/2025

Sign up

Suricata training

3 days (21 hours)

Presentation

Suricata is an open-source intrusion detection (IDS), prevention (IPS) and Network Security Monitoring (NSM) engine developed by OISF. Designed for high-speed inspection and EVE JSON observability, it integrates natively with SIEM and SOC workflows.

Our Suricata training course will enable you to master traffic analysis, rule management (ET/ETPro, custom), IPS mode (NFQUEUE), app-layer and ELK/Splunk integration, while applying performance and hardening best practices.

You will learn how to install, configure, optimize and industrialize Suricata; automate suricata-update via CI/CD, hunt for threats in EVE logs and operate inline IPS securely.

At the end of the course, you'll be able to deploy high-performance sensors, build robust detections, feed your dashboards and tool your incident response.

As with all our training courses, this one is based on the latest stable version and favors a resolutely practical and operational approach.

Objectives

- Install and configure Suricata (IDS/IPS/NSM)
- Design and maintain effective rules
- Integrate EVE JSON logs into a SIEM system
- Enable inline IPS security mode
- Implement automation (suricata-update, CI/CD)
- Supervise performance and operate in production

Target audience

- SOC teams (N1-N3 analysts, threat hunters)
- System/network administrators, security engineers

Prerequisites

- Network knowledge (TCP/IP, VLAN, basic routing)
- Linux basics (shell, services, logs)
- First steps in SIEM / logs desirable

Suricata training program

[Day 1 - Morning]

Principles, installation and first packages

- IDS/IPS/NSM positioning, architecture and SOC use cases
- Network capture: AF-Packet, XDP/eBPF, NFQUEUE
- EVE formats JSON, pcap, extracted files
- OISF ecosystem, suricata-update, ET/ETPro rules
- Hands-on workshop: installation, pcap capture, first logs

[Day 1 - Afternoon]

High-performance installation & capture

- Installation methods (packages, PPA/COPR, source)
- Inline vs passive, bypass, mirror/span
- OS tuning: RSS/RPS/RFS, IRQ, CPU pinning
- AF-Packet vs NFQUEUE comparison
- Practical workshop: micro-bench and runmode selection

Rules & signatures

- Rule syntax (flowbits, thresholds, metadata)
- Management with suricata-update (sources, enable/disable)
- pcap-replay tests and validation
- Reducing false positives
- Practical workshop: writing 3 custom rules

[Day 2 - Morning]

Inspection engine, decoding & observability

- Pipeline decode ? detect, threads and runmodes
- App-Layer (HTTP/2, TLS, DNS, SMTP, SMB...)
- Hyperscan/PCRE regex and performance
- Profiling via stats and tuning
- Practical workshop: profiling & optimization

[Day 2 - Afternoon]

EVE logs & SIEM integration

- EVE JSON schemas (alerts, dns, http, tls, files, stats)
- Enrichment (GeoIP, JA3/JA4)
- Elastic/Logstash, Splunk, Graylog integrations
- Dashboards and alerting
- Practical workshop: ELK for Threat Hunting

IPS mode & security

- Inline IPS with NFQUEUE (verdicts)
- TLS, HTTP/2, DoH management
- Blocklists and detection-prevention switchover
- Health & high availability supervision
- Practical workshop: IPS scenarios

[Day 3 - Morning]

Hunting, automation & operations

- MITRE ATT&CK techniques, C2/DNS-tunnel detection
- Advanced TLS/HTTP/DNS detection
- Correlation with Zeek, NetFlow, EDR
- Hunting playbooks
- Practical workshop: threat hunting course

[Day 3 - Afternoon] Automation &

CI/CD

- suricata-update, rule versioning
- Automated pcap tests and perf gates
- Ansible/Terraform provisioning
- Governance and KPIs MTTD/MTTR
- Practical workshop: CI rules pipeline

Operation, SRE & incident response

- Metrics, Prometheus/Grafana, stats.log
- Runbooks: drops, overflow, degradations
- Sizing NIC/CPU/RAM, rotation/log retention
- IR and post-mortem processes
- Practical workshop: incident simulation & improvement

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format

to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.