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

Mis à jour le 01/10/2025

S'inscrire

Formation Suricata

3 jours (21 heures)

Présentation

Suricata est un moteur open-source de détection d'intrusions (IDS), prévention (IPS) et Network Security Monitoring (NSM) développé par l'OISF. Pensé pour l'inspection à haut débit et l'observabilité EVE JSON, il s'intègre nativement aux SIEM et aux workflows SOC.

Notre formation Suricata vous permettra de maîtriser l'analyse de trafic, la gestion des règles (ET/ETPro, personnalisées), le mode IPS (NFQUEUE), l'app-layer ainsi que l'intégration ELK/Splunk, en appliquant les bonnes pratiques de performance et de durcissement.

Vous apprendrez à installer, configurer, optimiser et industrialiser Suricata ; à automatiser suricata-update via CI/CD, à chasser les menaces dans les logs EVE et à opérer en IPS inline de manière sûre.

À l'issue de la formation, vous serez en mesure de déployer des capteurs performants, de construire des détections robustes, d'alimenter vos tableaux de bord et d'outiller votre réponse à incident.

Comme toutes nos formations, celle-ci s'appuie sur la dernière version stable et privilégie une approche résolument pratique et opérationnelle.

Objectifs

- Installer et configurer Suricata (IDS/IPS/NSM)
- Concevoir et maintenir des règles efficaces
- Intégrer les logs EVE JSON dans un SIEM
- Activer le mode IPS inline en sécurité
- Mettre en place l'automation (suricata-update, CI/CD)
- Superviser la performance et opérer en production

Public visé

- Équipes SOC (analystes N1-N3, threat hunters)
- Administrateurs systèmes/réseaux, ingénieurs sécurité

Pré-requis

- Connaissances réseau (TCP/IP, VLAN, routage de base)
- Notions Linux (shell, services, journaux)
- Premiers pas en SIEM / logs souhaités

Programme de notre formation Suricata

[Jour 1 – Matin]

?Principes, installation et premiers paquets

- Positionnement IDS/IPS/NSM, architecture et cas d’usage SOC
- Capture réseau : AF-Packet, XDP/eBPF, NFQUEUE
- Formats EVE JSON, pcap, fichiers extraits
- Écosystème OISF, suricata-update, règles ET/ETPro
- Atelier pratique : installation, capture pcap, premiers logs

[Jour 1 – Après-midi]

Installation & capture haute performance

- Méthodes d’installation (packages, PPA/COPR, source)
- Inline vs passive, bypass, mirror/span
- Tuning OS : RSS/RPS/RFS, IRQ, CPU pinning
- Comparatif AF-Packet vs NFQUEUE
- Atelier pratique : micro-bench et choix runmode

Règles & signatures

- Syntaxe des règles (flowbits, thresholds, métadonnées)
- Gestion avec suricata-update (sources, enable/disable)
- Tests pcap-replay et validation
- Réduction des faux positifs
- Atelier pratique : écrire 3 règles custom

[Jour 2 – Matin]

Moteur d’inspection, décodage & observabilité

- Pipeline decode ? detect, threads et runmodes
- App-Layer (HTTP/2, TLS, DNS, SMTP, SMB…)
- Regex Hyperscan/PCRE et performance
- Profiling via stats et tuning
- Atelier pratique : profiling & optimisation

[Jour 2 – Après-midi]

Logs EVE & intégrations SIEM

- Schémas EVE JSON (alerts, dns, http, tls, files, stats)
- Enrichissement (GeoIP, JA3/JA4)
- Intégrations Elastic/Logstash, Splunk, Graylog
- Tableaux de bord et alerting
- Atelier pratique : ELK pour Threat Hunting

Mode IPS & sécurisation

- Inline IPS avec NFQUEUE (verdicts)
- Gestion TLS, HTTP/2, DoH
- Blocklists et bascule détection ? prévention
- Supervision santé & haute dispo
- Atelier pratique : scénarios IPS

[Jour 3 – Matin]

Chasse, automation & opérations

- Techniques MITRE ATT&CK, détection C2/DNS-tunnel
- Détection avancée TLS/HTTP/DNS
- Corrélation avec Zeek, NetFlow, EDR
- Playbooks de chasse
- Atelier pratique : parcours threat hunting

[Jour 3 – Après-midi]

Automatisation & CI/CD

- suricata-update, versionning des règles
- Tests pcap automatisés et perf gates
- Provision Ansible/Terraform
- Gouvernance et KPIs MTTD/MTTR
- Atelier pratique : pipeline CI de règles

Exploitation, SRE & réponse à incident

- Métriques, Prometheus/Grafana, stats.log
- Runbooks : drops, overflow, dégradations
- Sizing NIC/CPU/RAM, rotation/log retention
- Processus IR et post-mortem
- Atelier pratique : simulation d’incident & amélioration

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format

numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.