AYI NEDJIMI Consultants

Suricata : IDS/IPS/NSM Open Source Multi-thre 2026

10 mai 2026 • Mis à jour le 17 mai 2026 • 23 min de lecture • 4862 mots • 68 vue

Suricata est le moteur IDS/IPS/NSM open source multi-thread de referenc developpe par l'Open Information Security Foundation (OISF) depuis 2009 Distribue sous licence GPLv2, il combine detection passive, prevention inline AF_PACKET/NFQUEUE et Network Security Monitoring dans un binai unique. Avec Hyperscan, RSS multi-queue et eBPF/XDP bypass, il atteint 10-40 Gbps sur du materiel standard et 100+ Gbps avec SmartNIC Napatech. Compatible avec les signatures Snort 3 et Emerging Threats Open (70 000 regles), parser HTTP/2, TLS sans MITM, JA3/JA3S/JA4 fingerprinting, EVE JSON output natif. Version 7.0 LTS jusqu'en 2028, branche 8.0 en developpement.

Suricata est le moteur de **detection d'intrusions res** multi-thread reference, developpe depuis 2009 par l'**Open Inform** **ndation**

(OISF). Distribue sous licence **GPLv2**, il combine trois roles dans un binaire unique **IDS** passif (Intrusion Detection System) en mode promiscuous, **IPS** inline (Intrusion Prevention System) via AF_PACKET, NFQUEUE, IPFW ou Netmap, et **NSM** (Network Security Monitoring) avec extraction de fichiers, parsing protocolaire profond et export EVE JSON. Concu des l'origine pour exploiter les CPU multi-coeurs et les N multi-queue, Suricata depasse les **10 a 40 Gbps** en production sur du materiel x86 grace a l'integration d'**Intel Hyperscan** pour le pattern matching et au support nati RSS, CPU pinning et zero-copy. La version stable en mai 2026 est **Suricata 7.0.10** (Long Term Support jusqu'en 2028) et la branche 8.0 est en developpement actif le moteur **Hyperscan 5.5** et le parser **HTTP/3 sur QUIC**. Suricata se distingue de s ancetre **Snort** (mono-thread historique) par son architecture parallele native et de **Zeek** (ex-Bro) par sa compatibilite directe avec le format de regles signatures Sno Emerging Threats. Au 1er trimestre 2026, le projet compte plus de **9 200 etoiles GitHub**, 280 contributeurs et est deploye chez les operateurs telecom Tier-1, les C nationaux (ANSSI, CERT-FR, CISA), les SOC de defense et la majorite des SIEM hybrides open source bases sur Wazuh.

À RETENIR

A retenir

Suricata est le moteur IDS/IPS/NSM open source multi-thread de reference, developpe par l'OISF sous licence GPLv2 depuis 2009.

Trois modes d'exploitation : IDS passif (sniffing), IPS inline (AF_PACKET, NFQUEUE, IPFW, Netmap, eBPF/XDP) et NSM (logging EVE JSON).

Performance : 10-40 Gbps avec Hyperscan, CPU pinning ; 100+ Gbps possible avec napatech/

Réponse sous 24h

Devis gratuit →