

Mis à jour le 20/10/2026

S'inscrire

Formation Snort

3 jours (21 heures)

Présentation

Snort est un moteur open source de détection et de prévention des intrusions permettant de surveiller les réseaux et de repérer les communications suspectes. Avec Snort 3, les règles de détection, les inspecteurs protocolaires et les modes IDS et IPS, vous disposez de leviers complémentaires pour renforcer votre sécurité réseau.

Notre formation Snort vous permettra de maîtriser les étapes essentielles du déploiement d'une sonde, depuis la configuration Lua jusqu'à l'exploitation des alertes dans un environnement de supervision.

Vous apprendrez à positionner votre sonde, à analyser des captures réseau, à écrire des règles personnalisées et à adapter les signatures aux services réellement exposés par votre organisation.

À l'issue de la formation, vous serez en mesure de qualifier les événements, de réduire les faux positifs et de mettre en place un fonctionnement IPS contrôlé, tout en préservant la disponibilité des communications légitimes.

Cette formation aborde également la journalisation JSON, l'intégration aux processus SOC, les indicateurs de performance et la maintenance des règles. Des ateliers progressifs vous permettront de valider vos configurations et de préparer une exploitation fiable.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Déployer une sonde Snort 3 adaptée à une architecture réseau

- Configurer l'acquisition du trafic et les inspecteurs protocolaires nécessaires
- Écrire et tester des règles de détection sur des captures réseau
- Qualifier les alertes et réduire les faux positifs en contexte opérationnel
- Mettre en œuvre un fonctionnement IPS dans un environnement contrôlé
- Organiser la maintenance des règles et le suivi des performances

Public visé

- Administrateur réseau
- Administrateur sécurité
- Analyste SOC
- Ingénieur cybersécurité

Pré-requis

- Connaissance des réseaux TCP/IP et de l'adressage réseau
- Pratique de l'administration Linux en ligne de commande
- Compréhension des échanges HTTP et DNS sur un réseau
- Première expérience de l'analyse de captures avec Wireshark ou un outil équivalent
- Connaissance des principes de filtrage réseau et de détection des intrusions

Pré-requis techniques

- Poste de laboratoire recommandé avec 16 Go de RAM, processeur 4 cœurs et 60 Go d'espace disque disponible
- Virtualisation matérielle activée et installation de VirtualBox ou d'un hyperviseur équivalent
- Machines virtuelles sous Ubuntu Server 24.04 LTS avec droits administrateur et réseaux virtuels isolés
- Environnement pédagogique comprenant Snort 3, LibDAQ 3, Wireshark et des captures réseau de test
- Connexion Internet stable autorisant les téléchargements pédagogiques et deux interfaces virtuelles dédiées sur la sonde pour les exercices IPS

Programme de notre formation Snort

[Jour 1 - Matin]

Architecture et installation de la sonde

- Positionnement des IDS et IPS dans une architecture de sécurité réseau
- Choix des points de capture, visibilité du trafic et limites liées au chiffrement
- Architecture de Snort 3 : acquisition, décodage, inspection, détection et journalisation
- Installation du moteur et de LibDAQ 3, vérification des dépendances et des modules disponibles
- Organisation du laboratoire isolé, droits de capture et commandes de diagnostic initial

- Atelier pratique : installer une sonde Snort 3 dans le laboratoire et vérifier la lecture d'une capture réseau fournie.

[Jour 1 - Après-midi]

Configuration et acquisition du trafic

- Structure de la configuration Lua et rôle des fichiers de configuration principaux
- Définition des variables HOME_NET et EXTERNAL_NET selon le périmètre surveillé
- Lecture des fichiers PCAP, écoute d'une interface et sélection du module d'acquisition
- Rôles des inspecteurs stream_tcp, wizard et binder dans le traitement des échanges
- Chargement des règles, validation de configuration et premières sorties alert_fast
- Atelier pratique : configurer une sonde passive, charger une règle fournie et comparer les alertes issues d'une capture et d'un trafic de test.

[Jour 2 - Matin]

Écriture et validation des règles

- Anatomie d'une règle Snort : en-tête, action, protocole, adresses, ports et direction
- Identification des signatures avec msg, sid, rev et classtype
- Recherche de motifs avec content et nocase, cadrage par offset et depth
- Prise en compte de l'état et du sens des communications avec flow
- Méthode de validation sur des jeux de trafic positifs et négatifs, gestion des identifiants locaux
- Atelier pratique : écrire des règles de détection sur des échanges ICMP et HTTP, puis vérifier les résultats attendus sur plusieurs captures.

[Jour 2 - Après-midi]

Inspection applicative et précision des signatures

- Règles de service HTTP et détection applicative sur des ports non standards
- Sélection des sticky buffers avec http_uri, http_header et file_data
- Combinaison de motifs avec distance et within, introduction aux expressions pcre
- Suivi d'un état de détection entre règles avec flowbits
- Choix d'un fast_pattern pertinent et réduction des faux positifs par contextualisation
- Atelier pratique : construire une signature HTTP contextualisée, vérifier sa détection sur un port alternatif et corriger les déclenchements sur du trafic légitime.

[Jour 3 - Matin]

Exploitation des alertes et intégration SOC

- Configuration des sorties alert_json et alert_syslog selon les besoins de supervision
- Qualification d'un événement à partir de la signature, des adresses, du service et du contexte réseau
- Rapprochement des alertes avec les captures réseau pour confirmer ou écarter une détection
- Détection de comportements répétés avec detection_filter et maîtrise du volume d'alertes avec event_filter
- Préparation de l'acheminement vers un SIEM, horodatage et traçabilité des décisions de qualification
- Atelier pratique : produire des alertes JSON, analyser un scénario fourni et ajuster les filtres en documentant les effets sur la visibilité.

[Jour 3 - Après-midi]

Prévention et maintien en conditions opérationnelles

- Passage du mode passif au mode inline avec DAQ AFPacket et deux interfaces dédiées
- Différences entre les actions alert, drop et reject, validation du blocage effectif
- Déploiement progressif des politiques IPS, tests de non-régression et procédure de retour arrière
- Suivi du débit, des pertes de paquets, de la consommation mémoire et de la charge processeur
- Cycle de vie des règles communautaires et locales : sélection, mise à jour, versionnement et validation
- Atelier pratique : bloquer un trafic de test dans le réseau isolé, vérifier le maintien des échanges légitimes et établir une procédure de mise en production.

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.