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

Updated on 10/20/2026

Sign Up

Snort Training

3 days (21 hours)

Overview

Snort is an open-source intrusion detection and prevention engine that monitors networks and identifies suspicious traffic. With Snort 3, detection rules, protocol inspectors, and IDS and IPS modes, you have additional tools to strengthen your network security.

Our Snort training will help you master the essential steps for deploying a sensor, from Lua configuration to handling alerts in a monitoring environment.

You'll learn how to position your sensor, analyze network captures, write custom rules, and tailor signatures to the services actually exposed by your organization.

By the end of the training, you'll be able to classify events, reduce false positives, and implement controlled IPS operations while maintaining the availability of legitimate communications.

This training also covers JSON logging, integration with SOC processes, performance metrics, and rule maintenance. Progressive hands-on workshops will allow you to validate your configurations and prepare for reliable operation.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Deploy a Snort 3 sensor tailored to a network architecture

- Configure traffic capture and the necessary protocol inspectors
- Write and test detection rules on network captures
- Qualify alerts and reduce false positives in an operational context
- Implement IPS operations in a controlled environment
- Organize rule maintenance and performance monitoring

Target Audience

- Network administrator
- Security administrator
- SOC Analyst
- Cybersecurity engineer

Prerequisites

- Knowledge of TCP/IP networks and network addressing
- Practical experience with command-line Linux administration
- Understanding of HTTP and DNS traffic on a network
- Basic experience analyzing network captures using Wireshark or a similar tool
- Knowledge of network filtering and intrusion detection principles

Technical Prerequisites

- Recommended lab workstation with 16 GB of RAM, a 4-core processor, and 60 GB of available disk space
- Hardware virtualization enabled and VirtualBox or an equivalent hypervisor installed
- Virtual machines running Ubuntu Server 24.04 LTS with administrator privileges and isolated virtual networks
- Learning environment including Snort 3, LibDAQ 3, Wireshark, and network captures from test
- Stable internet connection allowing for educational downloads and two dedicated virtual interfaces on the probe for IPS exercises

Snort Training Course Outline

[Day 1 - Morning]

Architecture and installation of the sensor

- Positioning of IDS and IPS in a network security architecture
- Selection of capture points, traffic visibility, and limitations related to encryption
- Snort 3 Architecture: Acquisition, Decoding, Inspection, Detection, and Logging
- Installing the engine and LibDAQ 3, verifying dependencies and available modules
- Setting up the isolated lab, capture permissions, and initial diagnostic commands

- Hands-on Workshop: Install a Snort 3 sensor in the lab and verify that it can read a provided network capture.

[Day 1 - Afternoon]

Configuring and Acquiring Traffic

- Structure of the Lua configuration and role of the main configuration files
- Defining the HOME_NET and EXTERNAL_NET variables based on the monitored scope
- Reading PCAP files, listening on an interface, and selecting the capture module
- Roles of the stream_tcp, wizard, and binder inspectors in processing traffic
- Loading rules, validating the configuration, and generating initial alert_fast outputs
- Hands-on workshop: Configure a passive sensor, load a provided rule, and compare alerts generated from a capture and from test traffic.

[Day 2 - Morning]

Writing and validating rules

- Anatomy of a Snort rule: header, action, protocol, addresses, ports, and direction
- Identifying signatures using msg, sid, rev, and classtype
- Pattern matching with `content` and `nocase`, scoping with `offset` and `depth`
- Accounting for the state and direction of communications with `flow`
- Validation methods using positive and negative traffic sets, managing local identifiers
- Hands-on workshop: writing detection rules for ICMP and HTTP traffic, then verifying the expected results on multiple captures.

[Day 2 - Afternoon]

Application inspection and signature accuracy

- HTTP service rules and application detection on non-standard ports
- Selecting sticky buffers using http_uri, http_header, and file_data
- Combining patterns with "distance" and "within"; introduction to PCRE expressions
- Tracking detection status across rules using flowbits
- Choosing an appropriate `fast_pattern` and reducing false positives through contextualization
- Hands-on workshop: Build a contextualized HTTP signature, verify its detection on an alternative port, and correct false positives on legitimate traffic.

[Day 3 - Morning]

Alert Processing and SOC Integration

- Configure the `alert_json` and `alert_syslog` outputs according to monitoring requirements
- Event classification based on signature, addresses, service, and network context
- Cross-referencing alerts with network captures to confirm or dismiss a detection
- Detection of recurring behavior using `detection_filter` and control of alert volume using `event_filter`
- Preparing alerts for forwarding to a SIEM, including timestamping and traceability of qualification
- Hands-on workshop: Generating JSON alerts, analyzing a provided scenario, and adjusting filters while documenting the effects on visibility.

[Day 3 - Afternoon]

Prevention and maintaining operational readiness

- Switching from passive mode to inline mode with DAQ AFPacket and two dedicated interfaces
- Differences between the "alert," "drop," and "reject" actions; verification of effective blocking
- Gradual deployment of IPS policies, non-regression testing, and rollback procedure
- Monitoring of throughput, packet loss, memory usage, and CPU load
- Lifecycle of community and local rules: selection, updating, versioning, and validation
- Hands-on workshop: Blocking test traffic in the isolated network, verifying that legitimate traffic is maintained
  and establishing a procedure for production deployment.

Target Audience

This training is intended for both individuals and companies—large and small—that wish to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methods.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg