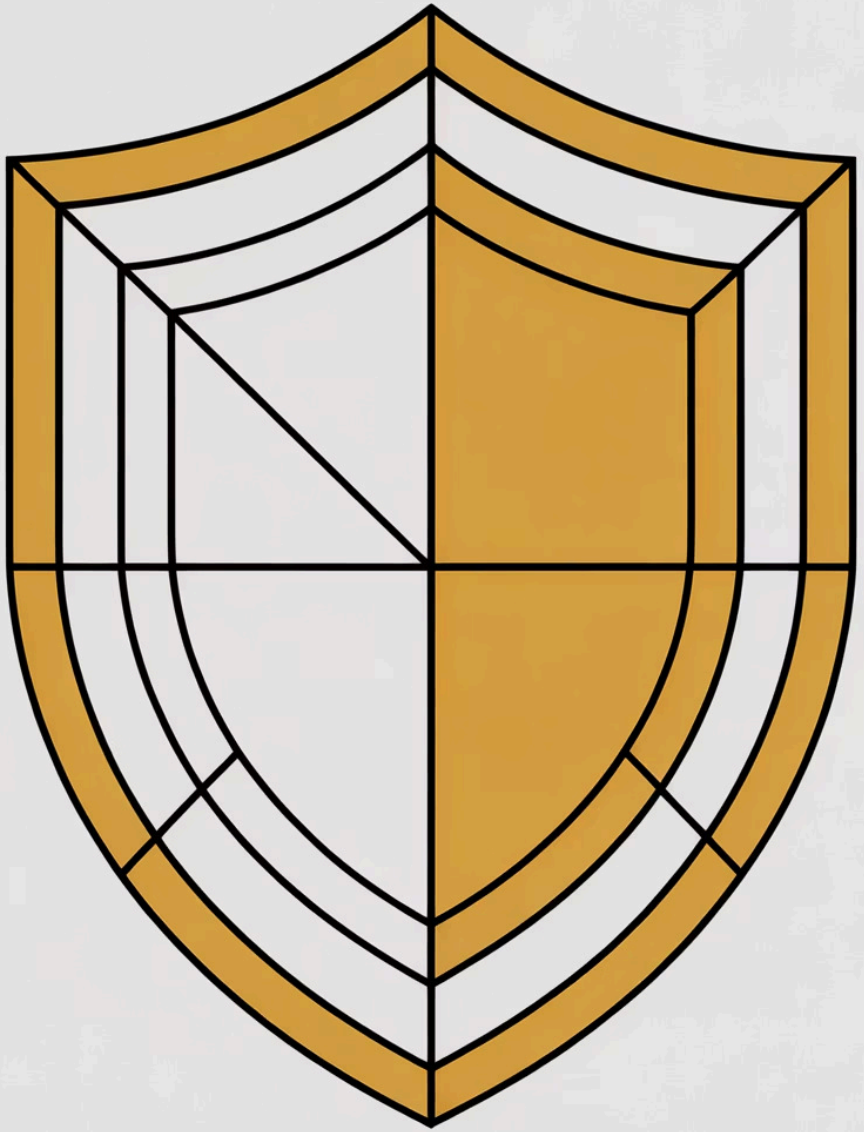


Intrusion Detection Systems and Their Types

Protecting Networks from Cyber Threats

What is an Intrusion Detection System?

Continuous Monitoring

Software or hardware tracking network and system traffic 24/7

Real-Time Alerts

Notifies administrators of suspicious activity and policy violations

Security Scout

Detects unauthorized access attempts before damage occurs

Why IDS Matter: The Stakes Are High

800K+

Cybercrime Complaints

FBI reported incidents in 2021 alone

$7B

Financial Losses

Total damages from cybercrimes annually

90%

Reduced Damage

When threats detected early

Advanced evasion tactics like spoofing and fragmentation make early detection critical for organizational survival

The Five Main Types of IDS

Network IDS

Monitors entire network segments

Host IDS

Protects individual devices

Protocol IDS

Watches communication protocols

Application Protocol IDS

Focuses on app-level security

Hybrid IDS

Combines multiple approaches

Network Intrusion Detection System (NIDS)

01

Strategic Placement

Positioned at critical network points near firewalls and subnet boundaries

02

Traffic Analysis

Examines all inbound and outbound packets in real-time

03

Pattern Recognition

Identifies known attack signatures and anomalous behavior

04

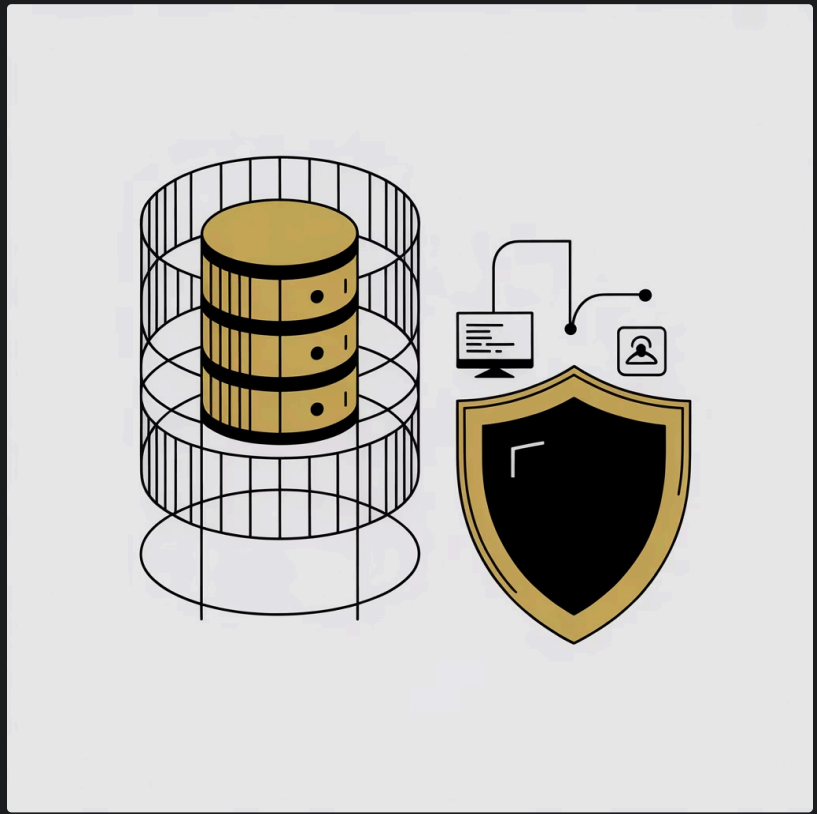
Threat Prevention

Detects port scans and firewall bypass attempts before damage occurs

Host Intrusion Detection System (HIDS)

Device-Level Protection

HIDS provides granular security for individual systems



Installation Target

Deployed on servers, workstations, and critical endpoints

Monitoring Scope

Tracks system files, security logs, and host-specific network packets

Detection Focus

Identifies unauthorized file modifications and suspicious local activity

Use Case Example

Catches Trojan horse infections and insider threats immediately

Protocol-Based and Application Protocol-Based IDS

Protocol-Based IDS (PIDS)

Monitors communication protocols between users and servers

- HTTP traffic analysis
- FTP connection monitoring
- Protocol vulnerability detection

Application Protocol-Based IDS (APIDS)

Focuses on application-level protocol security

- Database query inspection
- API call monitoring
- Application-specific attack detection

On VM

In the vm terminal type the command below

```
sudo apt update && sudo apt upgrade -y
```

Capture some network traffic

```
tcpdump -i ens3 -w net_cap.pcap
```

Download pcap file from link below

Netresec

Public PCAP files for download

A list of publicly available pcap files / network traces that can be downloaded for free

Setting Up Snort on Linux

Snort is a popular open-source Network Intrusion Detection System (NIDS) capable of real-time traffic analysis and packet logging. Deploying it on a Linux system provides a robust layer of defense against various cyber threats.

Installation

```
sudo apt install snort
```

Make sure snort is installed

```
snort -V
```

If Snort doesn't install try

Install all required dependencies

```
sudo apt install -y \
build-essential cmake make gcc g++ autoconf libtool pkg-config \
libpcap-dev libpcre3-dev zlib1g-dev \
libdumbnet-dev \
luajit libluajit-5.1-dev \
libhwloc-dev liblzma-dev \
openssl libssl-dev libnghttp2-dev \
libunwind-dev libmnl-dev \
bison flex git
```

Install PCRE2 (fix for CMake PCRE2 error)

```
sudo apt install -y \
  build-essential cmake make gcc g++ autoconf libtool pkg-config \
  libpcap-dev libpcre3-dev zlib1g-dev \
  libdumbnet-dev \
  luajit libluajit-5.1-dev \
  libhwloc-dev liblzma-dev \
  openssl libssl-dev libnghttp2-dev \
  libunwind-dev libmnl-dev \
  bison flex git
```

Build and install libdaq

```
sudo apt install -y libpcre2-dev
```

Build and install libdaq

```
cd ~
git clone https://github.com/snort3/libdaq.git
cd libdaq
./bootstrap
./configure
make -j$(nproc)
sudo make install
sudo ldconfig
```

Build and install Snort 3

```
cd ~
git clone https://github.com/snort3/snort3.git
cd snort3
rm -rf build
./configure_cmake.sh --prefix=/usr/local
cd build
make -j$(nproc)
sudo make install
sudo ldconfig
```

Verify Snort installed correctly

```
snort -V
```

Local Packet capture example

```
snort -c /etc/snort/snort.lua -i eth0
```

This command starts Snort using the specified configuration file and captures packets on the eth0 interface, allowing you to monitor network traffic in real time for suspicious activity. Adjust the interface name as needed to match your system's network setup.

Analyze local pcap

```
snort -r file.pcap -c /etc/snort/snort.lua
```

This command reads packets from the specified pcap file and analyzes them using Snort according to the provided configuration, helping you review past network traffic for signs of intrusion or anomalies.

Log traffic to pcap and read pcap with snort

tcpdump

```
tcpdump -i <interface> -w <filename.pcap>
```

snort

```
snort -r <filename.pcap> -c /etc/snort/snort.lua
```

Example 2

```
sudo snort -c /etc/snort/snort.lua --daq-dir /usr/local/lib/daq -i eth0 -l /var/log/snort
```

This command runs Snort with the specified configuration file, using the DAQ library directory and monitoring the eth0 interface, while saving logs to /var/log/snort for later analysis. Adjust parameters to match your environment and logging preferences.

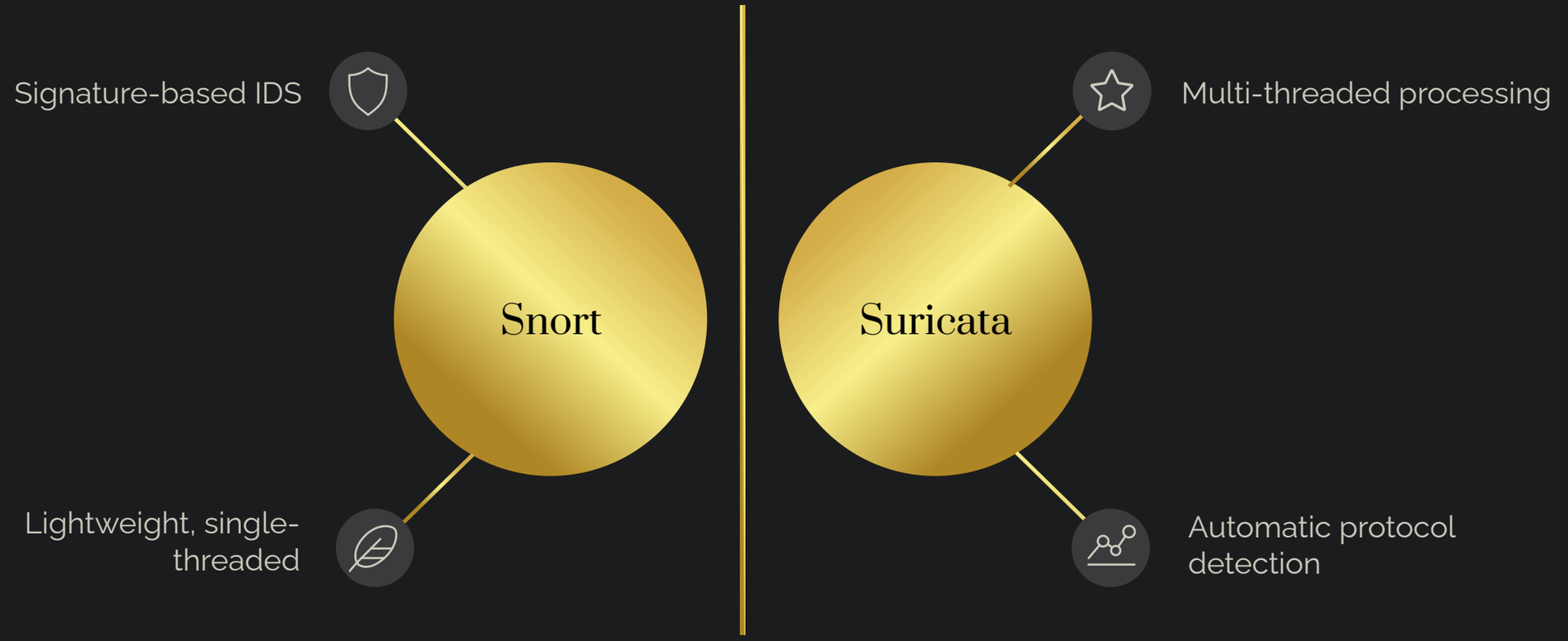
snort documentation

docs.snort.org

Getting Started with Snort 3 – Snort 3 Rule Writing Guide

The section will walk you through the basics of building and running Snort 3, and also help get you started with all things Snort 3. Specifically, this section contains information on building Snort 3, running Snort 3 for the first time, configuring Snort's detection engines,...

Example 2 Suricata



docs.suricata.io

Suricata User Guide — Suricata 6.0.10 documentation

Suricata Setup

```
sudo apt update && sudo apt upgrade -y
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
sudo apt install suricata -y
```

X

```
sudo vim /etc/suricata/suricata.yaml
```

Paste in the below

```
af-packet:
  - interface: eth0
    threads: 4
    cluster-id: 99
    cluster-type: cluster_flow
    defrag: yes
```

Rules Example

```
sudo vim /etc/suricata/rules/suricata.rules
```

```
alert udp any any -> any 53 (msg:"SURICATA DNS Query to a Suspicious *.ws Domain"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|02|ws|00|"; nocase; sid:2500003; rev:1;)
alert http any any -> any any (msg:"SURICATA HTTP Request to a Suspicious *.ws Domain"; flow:established,to_server; content:".ws"; http_host; isdataat:!1,relative; sid:2500004; rev:1;)
alert udp any any -> any 53 (msg:"SURICATA DNS Query to a Suspicious *.to Domain"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|02|to|00|"; nocase; sid:2500005; rev:1;)
alert http any any -> any any (msg:"SURICATA HTTP Request to a Suspicious *.to Domain"; flow:established,to_server; content:".to"; http_host; isdataat:!1,relative; sid:2500006; rev:1;)
alert http any any -> any any (msg:"SURICATA HTTP Request to a Suspicious *.onion.to Domain"; flow:established,to_server; content:".onion.to"; http_host; isdataat:!1,relative; sid:2500007; rev:1;)
alert http any any -> any any (msg:"SURICATA HTTP Request to a Suspicious *.onion.city Domain"; flow:established,to_server; content:".onion.city"; http_host; isdataat:!1,relative; sid:2500008; rev:1;)
alert http any any -> any any (msg:"SURICATA HTTP Request to a Suspicious *.onion.cab Domain"; flow:established,to_server; content:".onion.cab"; http_host; isdataat:!1,relative; sid:2500009; rev:1;)
alert http any any -> any any (msg:"SURICATA HTTP Request to a Suspicious *.onion.direct Domain"; flow:established,to_server; content:".onion.direct"; http_host; isdataat:!1,relative; sid:2500010; rev:1;)
alert http any any -> any any (msg:"SURICATA HTTP Request to a Suspicious *.onion.* Domain"; flow:established,to_server; content:".onion."; http_host; isdataat:!1,relative; sid:2500011; rev:1;)
alert udp any any -> any 53 (msg:"SURICATA DNS Query to a Suspicious *.onion Domain"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|02|onion|00|"; nocase; sid:2500012; rev:1;)
alert tls any any -> any any (msg:"SURICATA SSL session to suspicious *onion.to"; tls.subject:"CN=*.onion.to, OU=Domain Control Validated"; sid:2500013; rev:1;)
```

Testing Suricata

```
sudo suricata -T -c /etc/suricata/suricata.yaml
```

```
┌─[us-vip-1]─[10.10.14.64]─[spsand1@htb-fa3fpr6t7j]─[~]
└──╼ [★]$ sudo suricata -T -c /etc/suricata/suricata.yaml
12/11/2025 -- 18:12:45 - <Info> - Running suricata under test mode
12/11/2025 -- 18:12:45 - <Info> - Configuration node 'af-packet' redefined.
12/11/2025 -- 18:12:45 - <Notice> - This is Suricata version 6.0.10 RELEASE running in SYSTEM mode
12/11/2025 -- 18:12:45 - <Notice> - Configuration provided was successfully loaded. Exiting.
```

Hybrid Intrusion Detection System

Network Data

Traffic patterns across all segments

Host Information

Device-level system logs and files

Enhanced Accuracy

Fewer false positives, better threat detection

Integrated Analysis

Combined intelligence for comprehensive view

Example: Prelude IDS integrates host and network data to detect sophisticated, multi-vector attacks

IDS Detection Methods

Signature-Based Detection

How it works: Matches traffic against known attack patterns

✓ Fast and reliable

 Misses new threats

Anomaly-Based Detection

How it works: Detects deviations from normal behavior baselines

✓ Catches unknown attacks

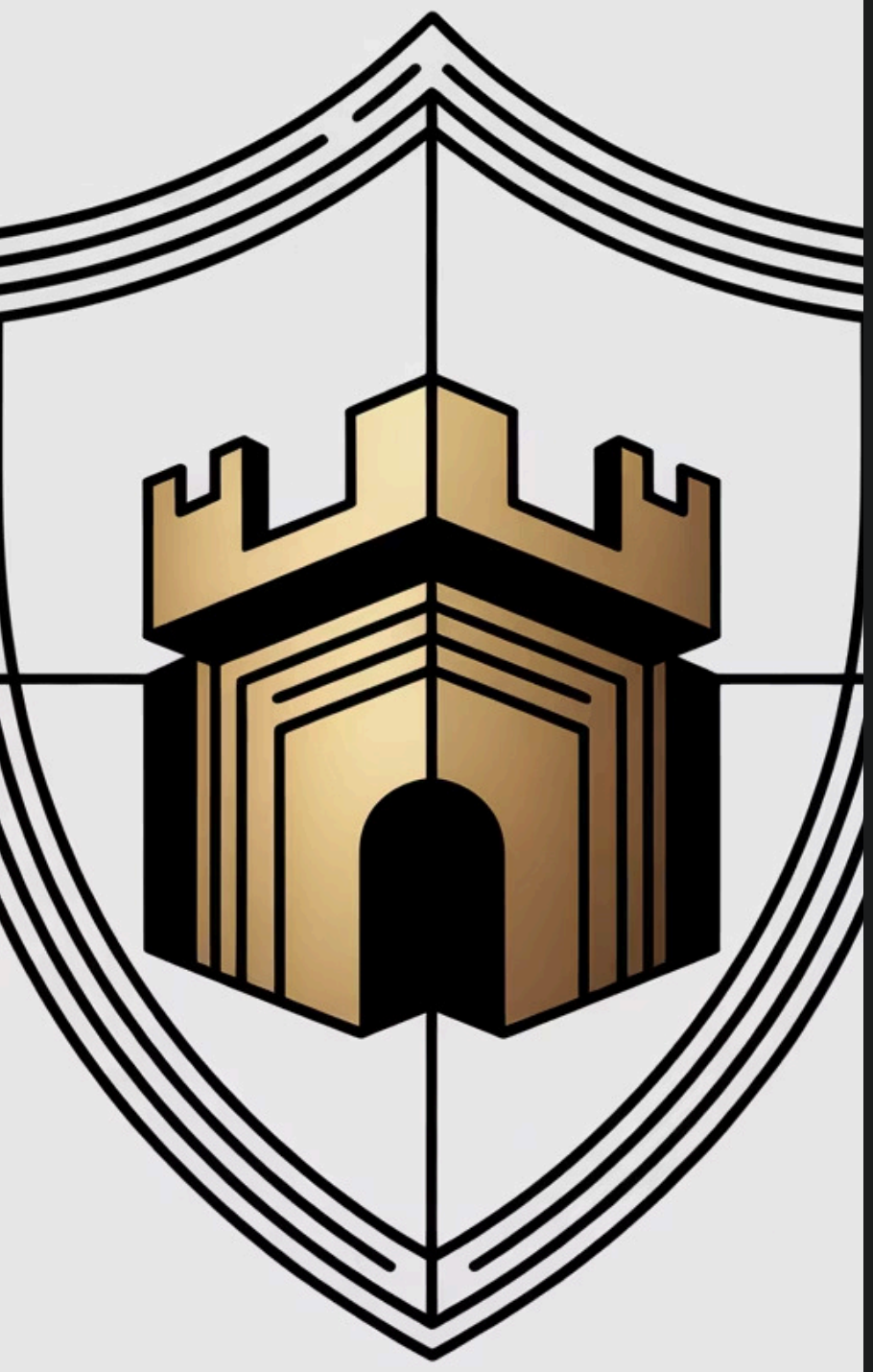
 Higher false alarm rate

Hybrid Detection

How it works: Combines signature and anomaly methods

✓ Balanced accuracy

✓ Comprehensive protection



IDS: Essential Cybersecurity Sentinels

1

Critical Early Warnings

IDS provide the first line of defense with real-time threat detection

2

Tailored Selection

Choose IDS type and detection method based on your environment and risk profile

3

Continuous Vigilance

24/7 monitoring and rapid response keep you ahead of evolving threats

4

Strategic Investment

Protect digital assets, maintain infrastructure trust, and ensure business continuity