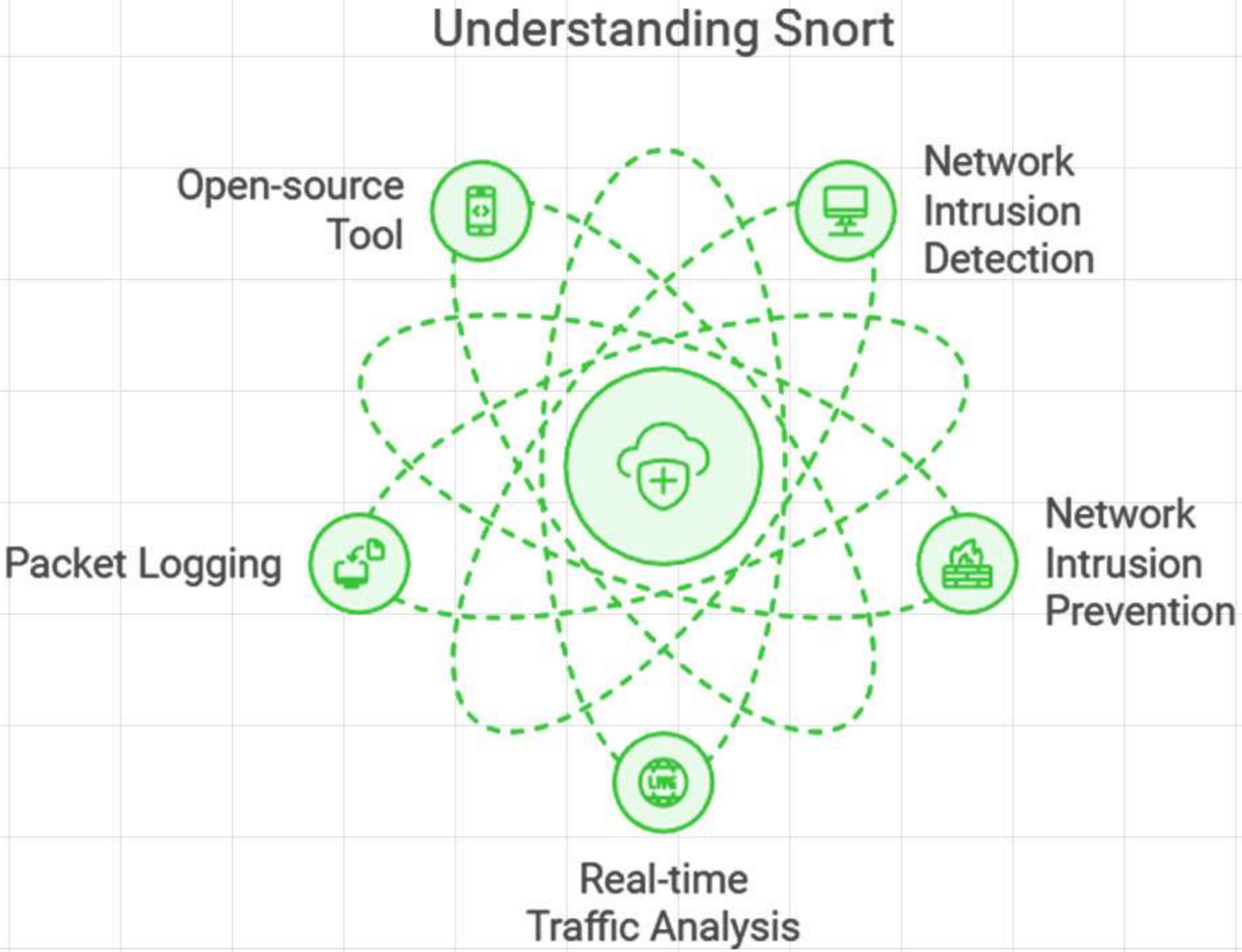
CYBERYAMI

# MASTER SNORT

The Open-Source Network Intrusion Detection System (NIDS)!

# 01

## WHAT IS SNORT?



02

# KEY FEATURES OF SNORT

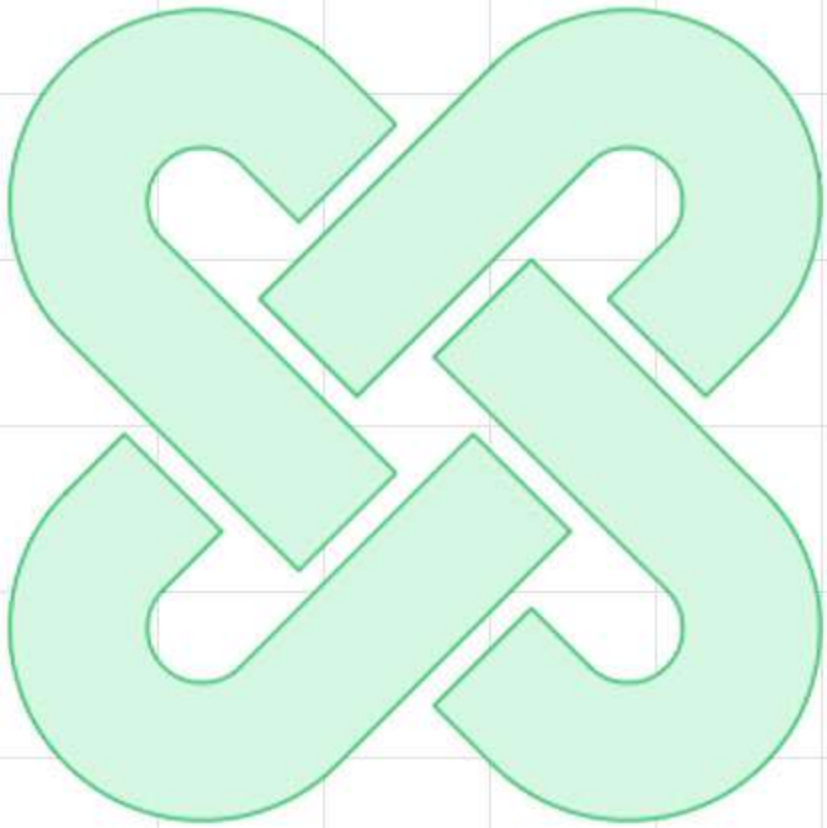
## SNORT's Core Functionalities

**Custom Rule Writing**

Write rules to detect specific attacks

**Real-time Intrusion Detection**

Detects and logs suspicious traffic



**Packet Sniffing**

Captures and analyzes network packets

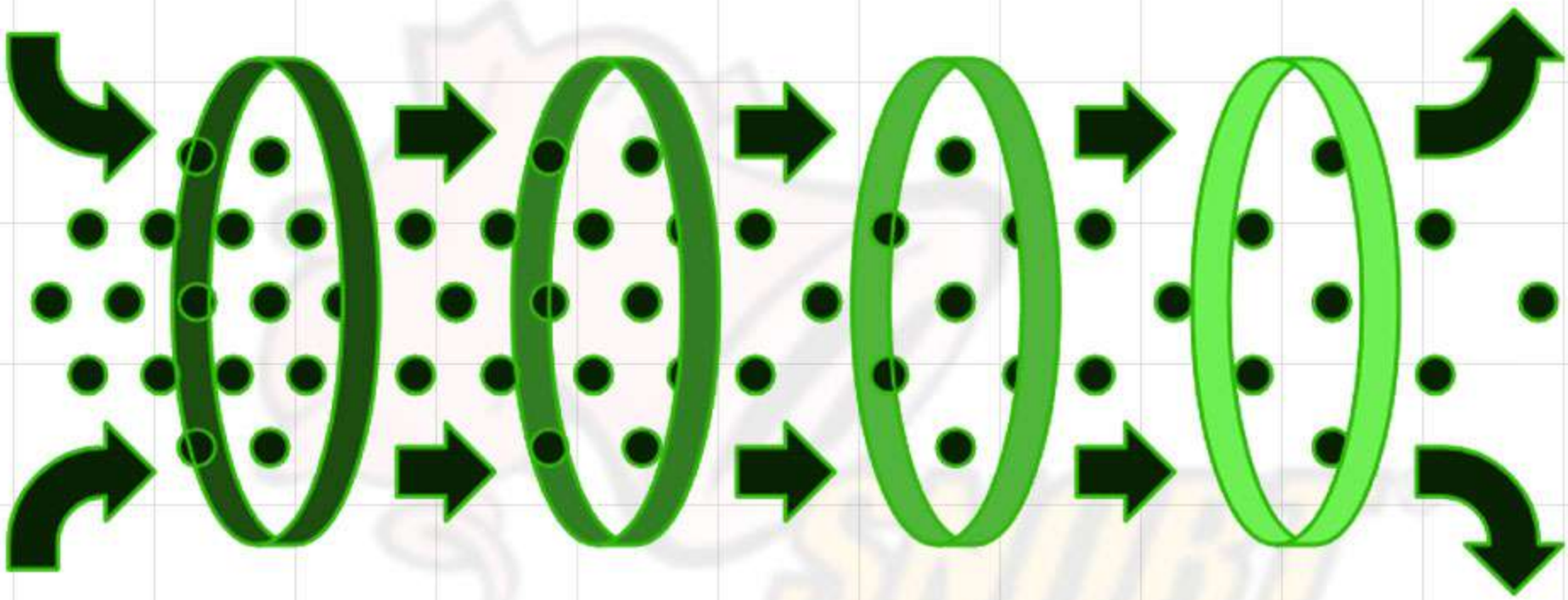
**Protocol Analysis**

Examines application layer protocols

# 03

## HOW SNORT WORKS

SNORT Intrusion Detection Process



**Packet Sniffing**

Captures and collects network data

**Preprocessing**

Normalizes data for consistent analysis

**Detection**

Applies rules to identify threats

**Logging/Alerting**

Logs events or alerts for suspicious activities

04

# INSTALLING SNORT

## Download Snort

Obtain the Snort software from the official website.

## Install Libraries

Set up necessary libraries like libpcap for Snort to function.

## Configure Snort

Adjust the Snort configuration file to suit your needs.

## Run Snort

Execute Snort in IDS mode using the command line.

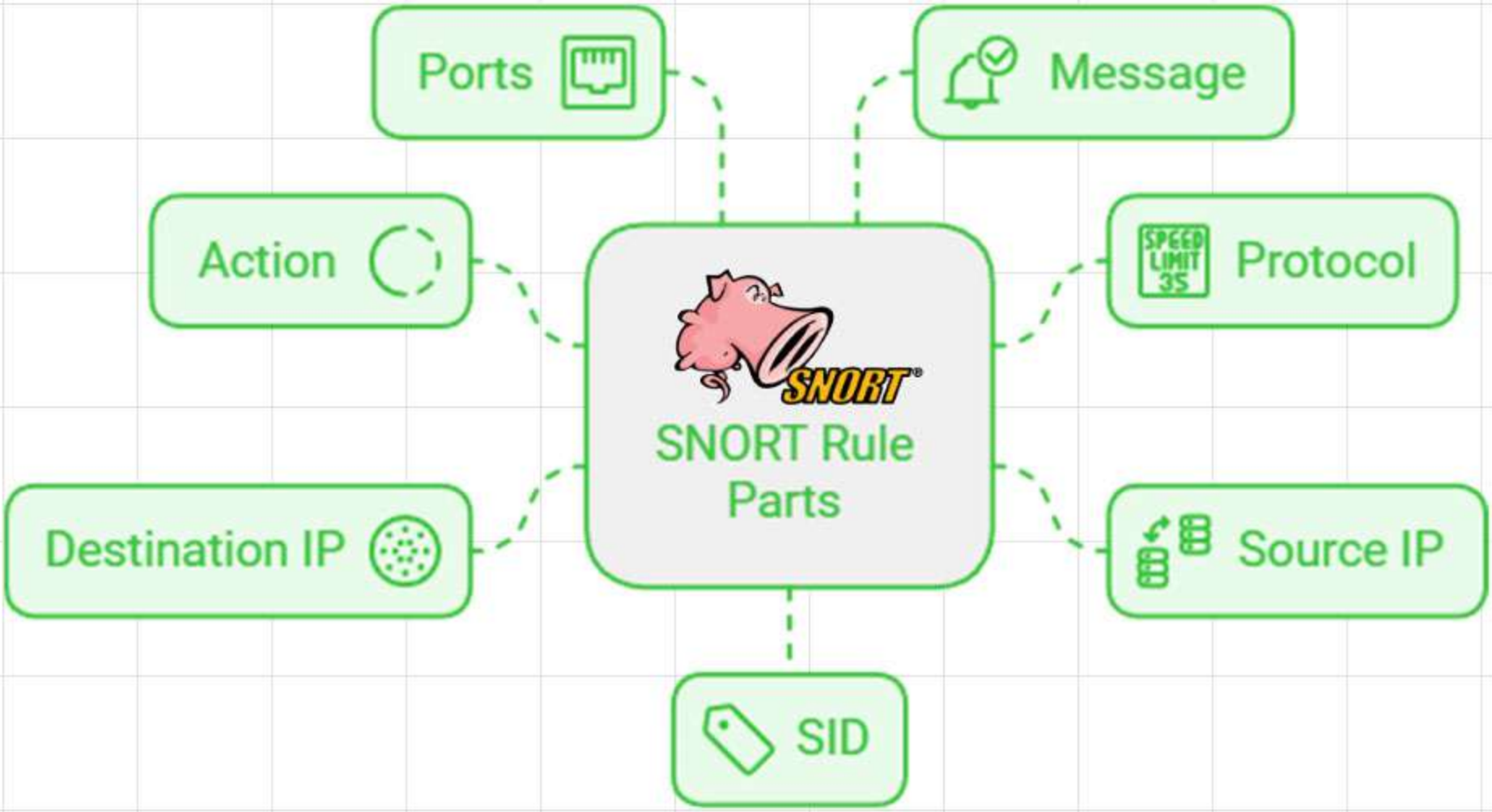
# 05

## SNORT RULE BASICS

**SNORT rules are written in a specific syntax to detect different types of traffic.**

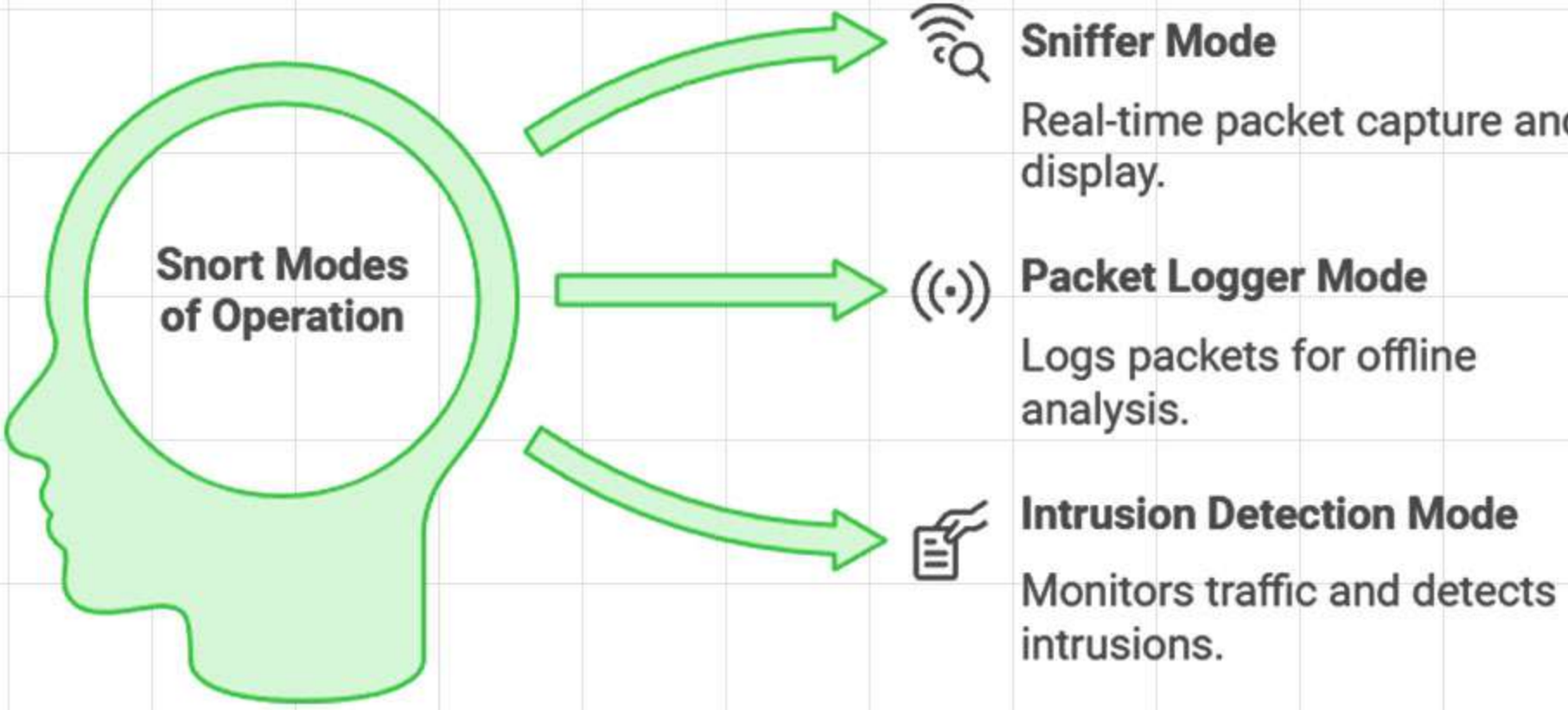
**Basic rule structure:**

alert tcp any any -> 192.168.1.0/24 80 (msg:"Test Rule"; sid:1000001; rev:1;)



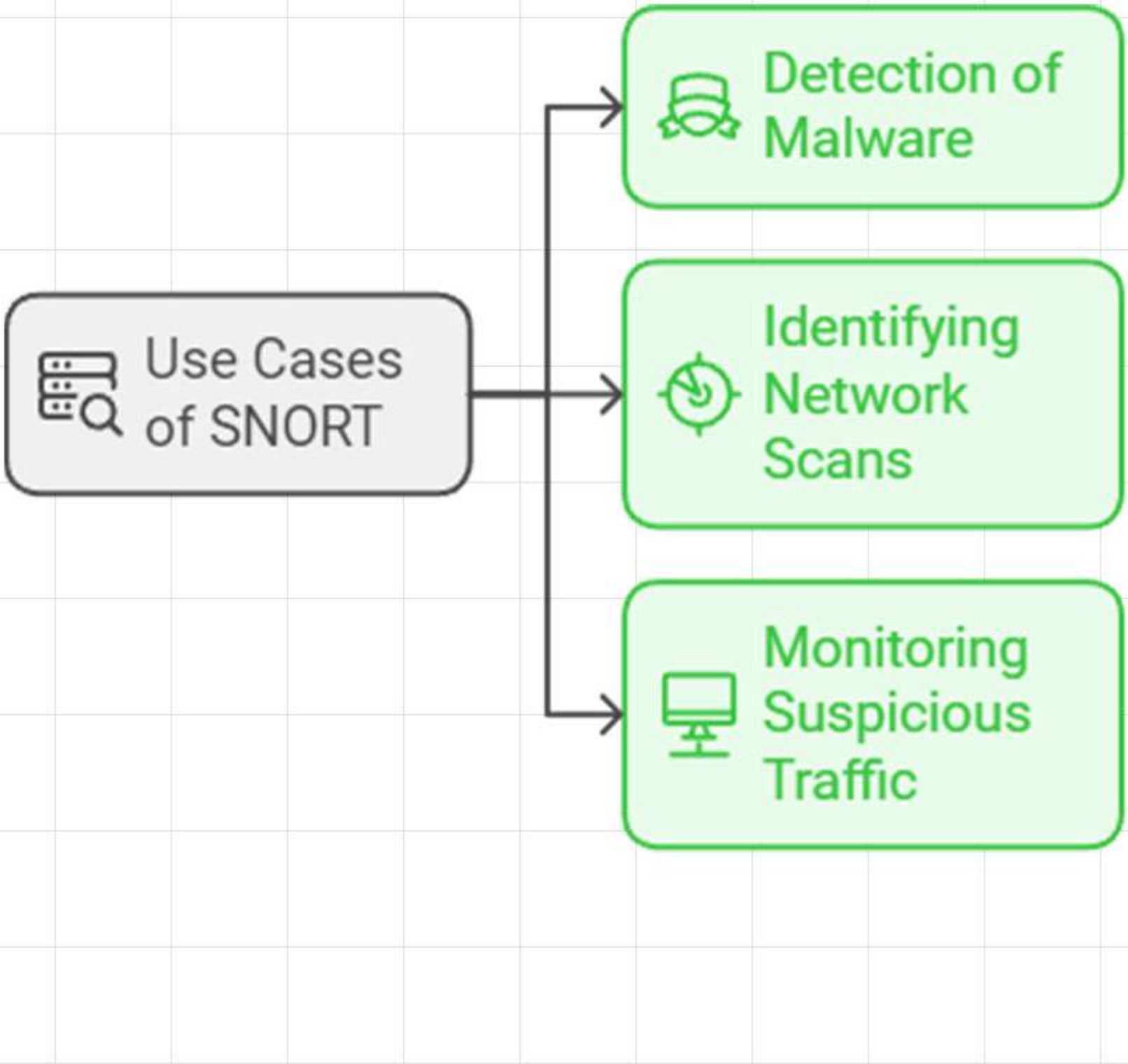
# 06

## SNORT MODES OF OPERATION



# 07

## USE CASES OF SNORT



08

# WRITING CUSTOM SNORT RULES FOR SPECIFIC THREATS

Crafting SNORT Rules for Threat Detection

**Brute-Force Login Attempts**

Prevents unauthorized access attempts

**Zero-Day Vulnerabilities**

Detects newly discovered security flaws

**Emerging Threats**

Identifies evolving cyber risks

# 09

## TAKE YOUR NETWORK SECURITY TO THE NEXT LEVEL WITH SNORT!

Join the SNORT Tool Bootcamp to master network defense techniques! Follow us for more cybersecurity tips!

# WAS IT HELPFUL?

FOLLOW FOR MORE