Getting Started with Snort

CAPTURING YOUR FIRST PACKETS WITH SNORT

Matt Glass
CISSP, CEH

www.linkedin.com/in/matthewglass2

Overview

- What is Snort?
- Snort 2.0 vs 3.0
- Lab setup
- Capturing your first packets
- Configuration files
- Rules files
- Starting IDS mode

Course Scenario

Globomantics

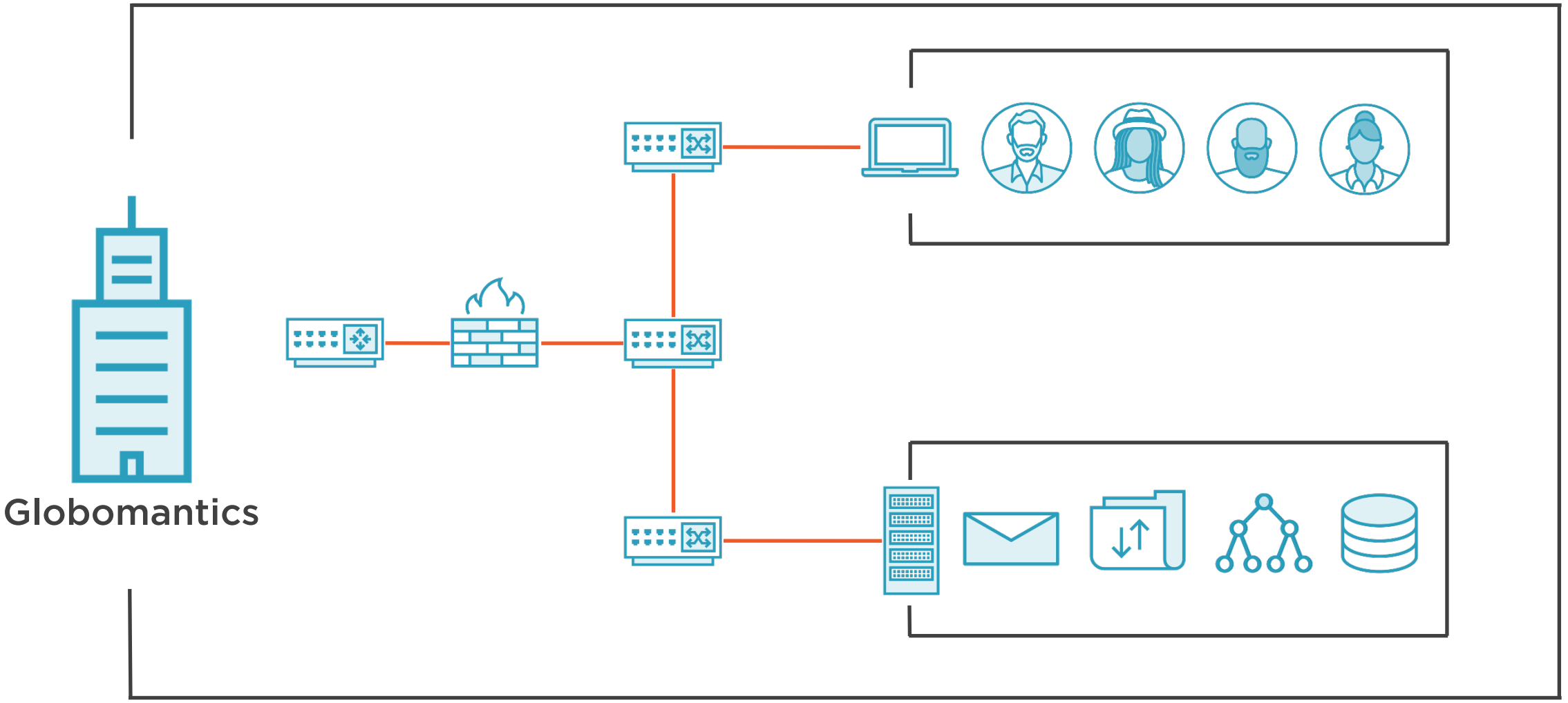
Course Scenario

Globomantics

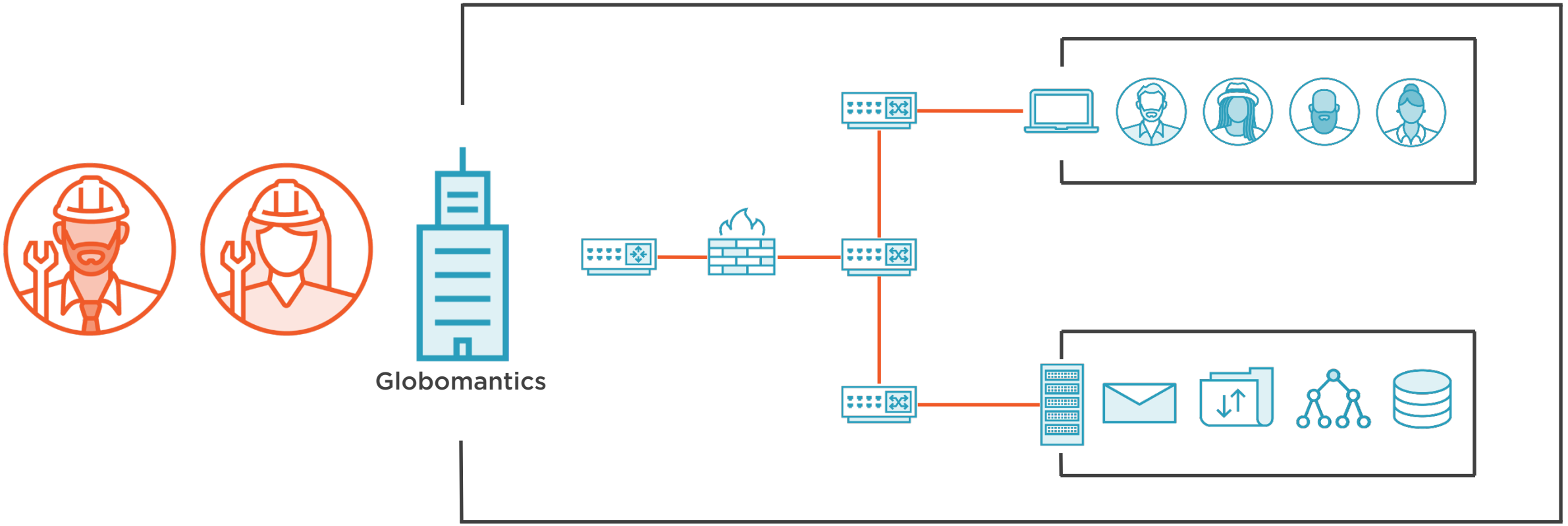
New Site 2

New Site 1

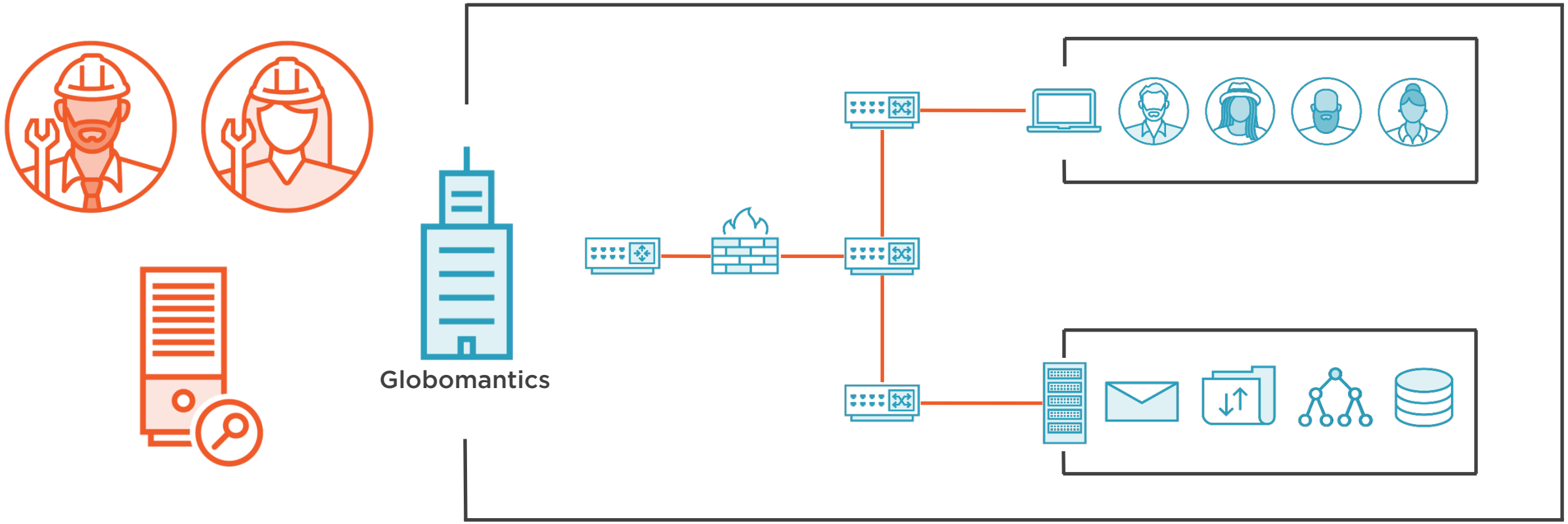
Course Scenario



Course Scenario



Course Scenario



Introduction to Snort

Signature-based IPS

Detects attacks through specific patterns and malicious sequences

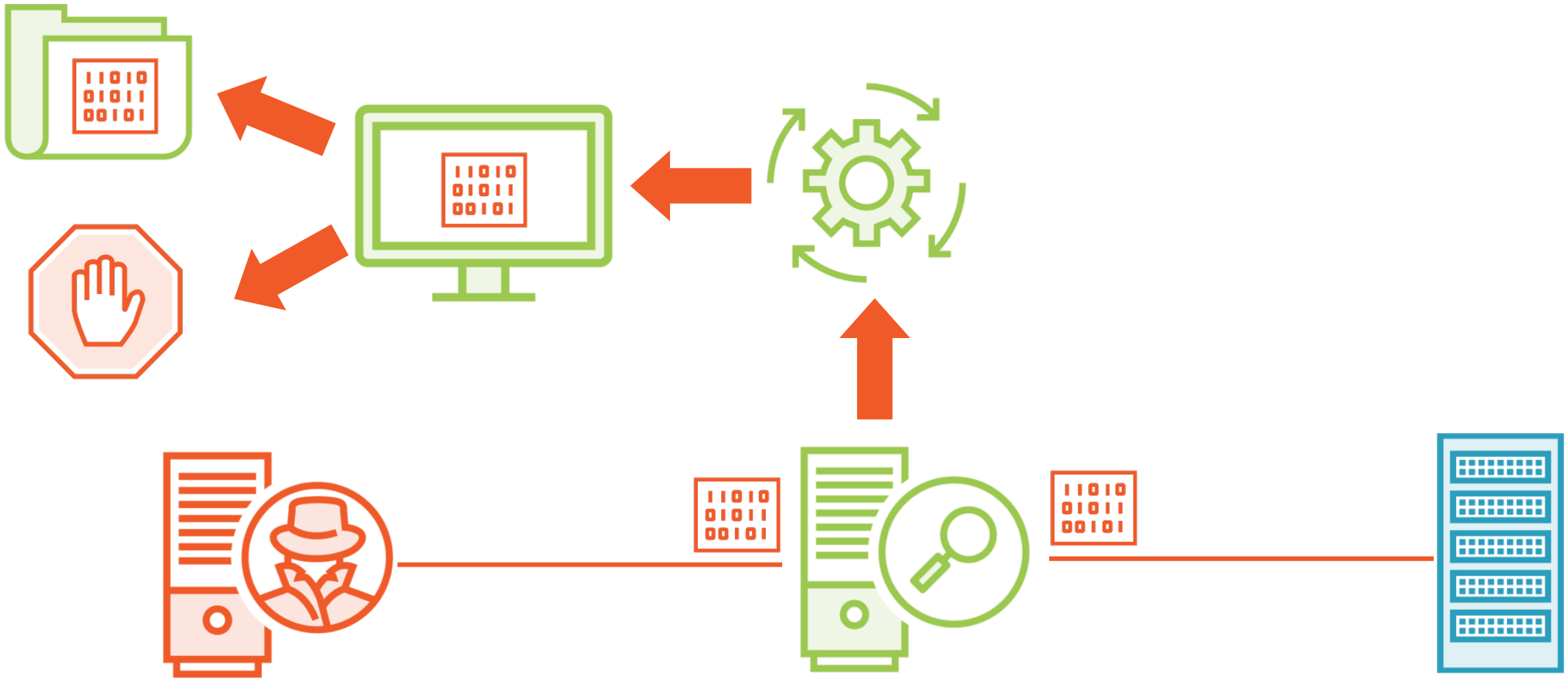
Snort uses tools to reassemble and normalize packet content

Rules are configured to match traffic patterns and take an action

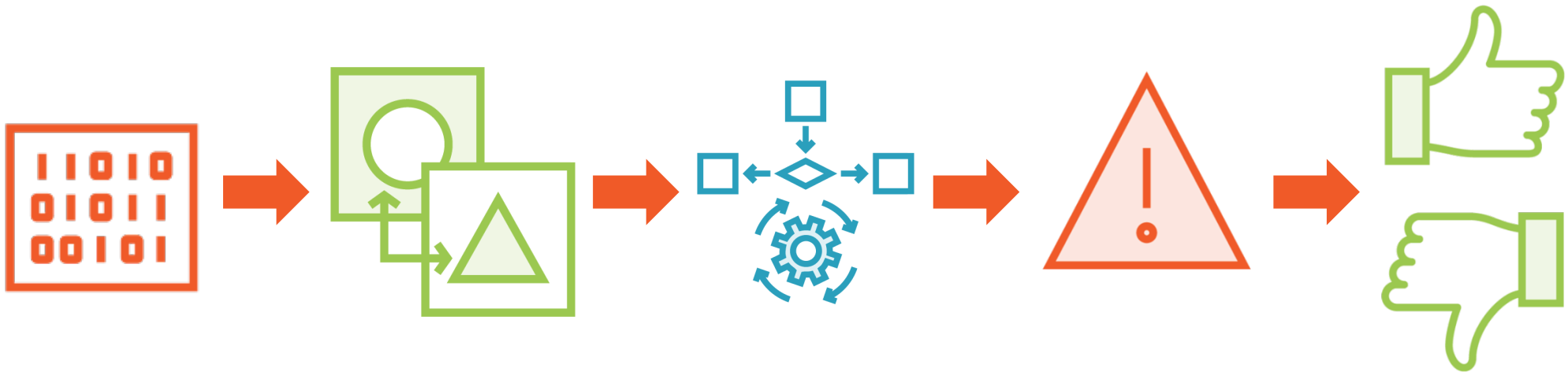
Snort has community rules and paid subscription options

High Level Processing Flow

High Level Processing Flow



High Level Processing Flow

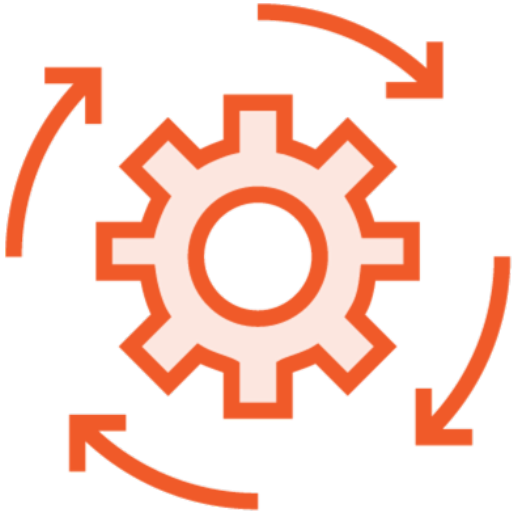


Snort Inline Server Placement

Snort Port-Mirroring Server Placement

Snort 2 vs Snort 3

Some New Features in Snort 3.0



Processing of raw files (ex. PDF)

Configurable port scan with the ability to block

More extensive help from the command line

Over 200 plugins available

Compatibility Issues with Snort 2

Use of Lua programming language for the configuration file

Uses plugin modules instead of preprocessors

Rule configuration is different from Snort 2

Snort2Lua

Converts the Snort 2 configuration file to a Lua file compatible with Snort 3

Can convert some rule files, but not all options are supported in Snort 3

Demo

Lab setup

Demo

Running Snort in IDS mode

Identify potential threats and violations

- Detect internal Facebook usage
- Detect all pings to internal devices
- Detect inbound HTTP traffic

Configuration and Rules Files

Snort Configuration File

Template snort.lua included with Snort 3.0 installation

Written in the Lua programming language

Used to configure over 200 modules

Lua Configuration File

This excerpt is the first section where HOME_NET and EXERNAL_NET are set

```
---------------------------------------------------------------------
-- 1. configure defaults
---------------------------------------------------------------------

-- HOME_NET and EXTERNAL_NET must be set now
-- setup the network addresses you are protecting
HOME_NET = 10.0.0.0/24

-- set up the external network addresses.
-- (leave as “any” in most situations)
EXTERNAL_NET = ‘any’

include ‘snort_defaults.lua’
include ‘file_magic.lua’

---------------------------------------------------------------------
-- 2. configure inspection
---------------------------------------------------------------------
```

Snort Rules Files

Local rules files configured by you

Community rules downloaded from Snort.org

Registered rules downloaded from Snort.org with oinkcode

Subscriber rules downloaded with paid subscription to Snort.org

Example Rules

These are example rules from the builtin rules file

```
alert ( msg:"DECODE_NOT_IPV4_DGRAM"; sid:1; gid:116; rev:1; metadata:rule-type
decode; classtype:protocol-command-decode; )

alert ( msg:"DECODE_IPV4_INVALID_HEADER_LEN"; sid:2; gid:116; rev:1; metadata:rule-
type decode; classtype:protocol-command-decode; )

alert ( msg:"DECODE_IPV4_DGRAM_LT_IPHDR"; sid:3; gid:116; rev:1; metadata:rule-type
decode; classtype:protocol-command-decode; )
```

This is the example rule to test configuration by detecting a ping

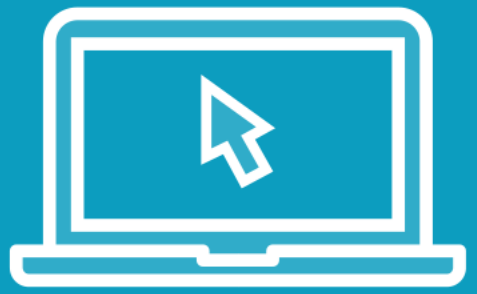
```
alert icmp any any -> any any (msg:"ICMP Traffic Detected";sid:10000002;)
```

Demo

Snort configuration file

Changing the HOME_NET variable

Demo



Obtaining and enabling community rules

Obtaining and enabling registered rules

Summary

Summary

- Snort placement and configuration
- High level process flow
- Differences between Snort 2.0 and 3.0
- Captured packets using Snort 3.0
- Introduction to the configuration file
- Obtained and enabled rules