Writing Snort Rules

WRITING YOUR FIRST SNORT RULE

Matt Glass
CISSP, CEH

www.linkedin.com/in/matthewglass2

Overview

Lab setup

Why would I want to write my own rules?

Basic Snort rule structure

Writing your first rule

Test your first custom rules

Course Scenario

Globomantics

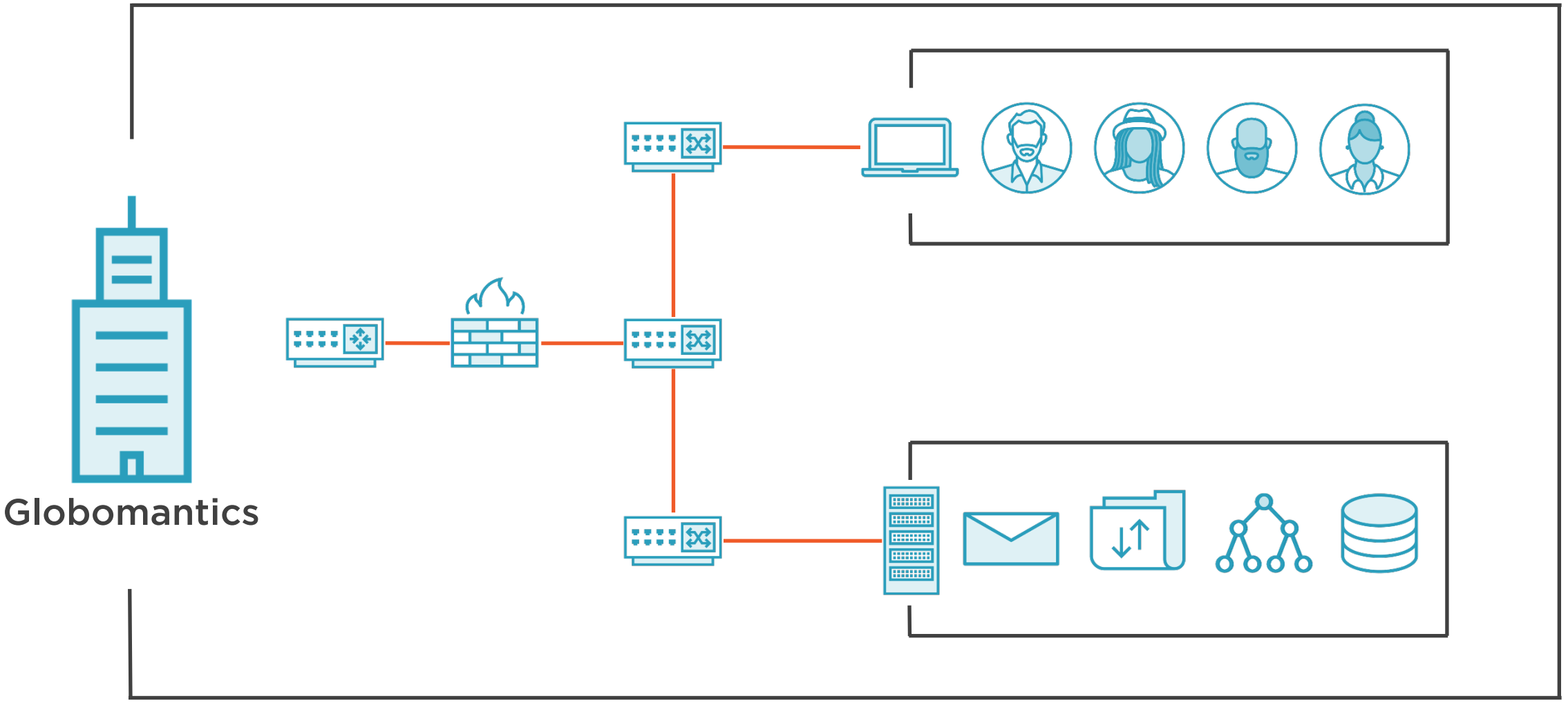
Course Scenario

Globomantics

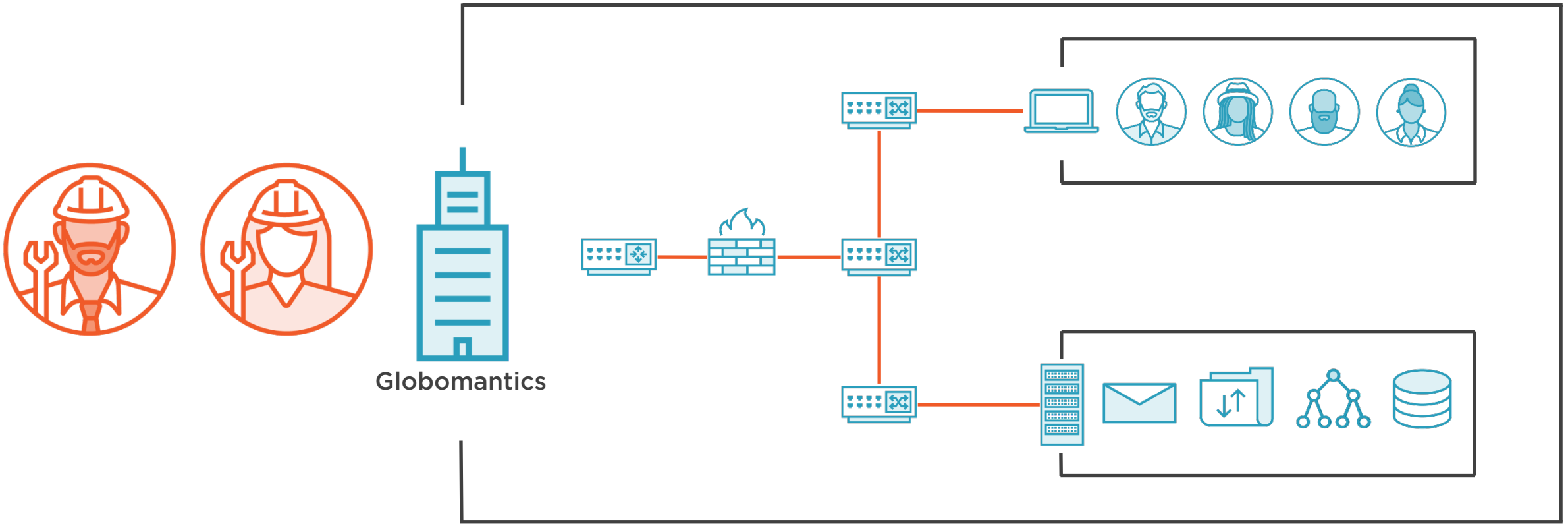
New Site 2

New Site 1

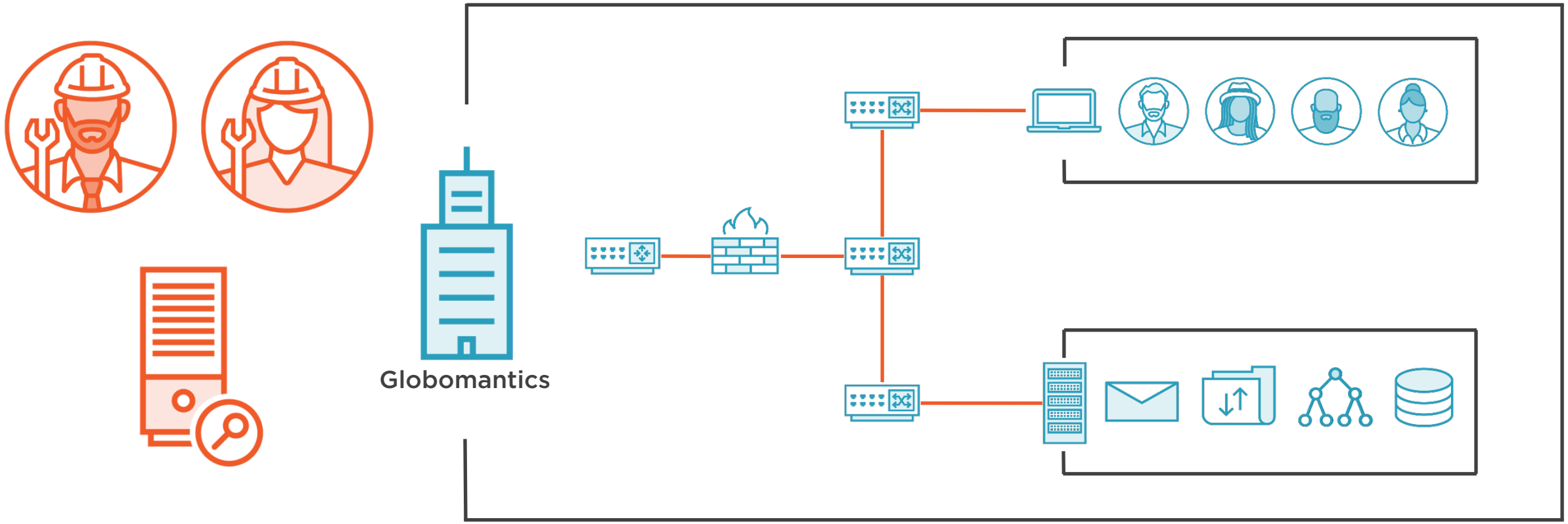
Course Scenario



Course Scenario



Course Scenario



Demo

Lab setup

Writing Your Own Snort Rules

Snort Rule Sources

Community rules available for free on snort.org

Registered rules accessed with an Oinkcode

Subscriber rules available through a regular fee

Why Would I Write My Own Rules?

Detect threats not available in the downloaded rules

Detect threats specific to your organization

Decrease false positives from downloaded rules

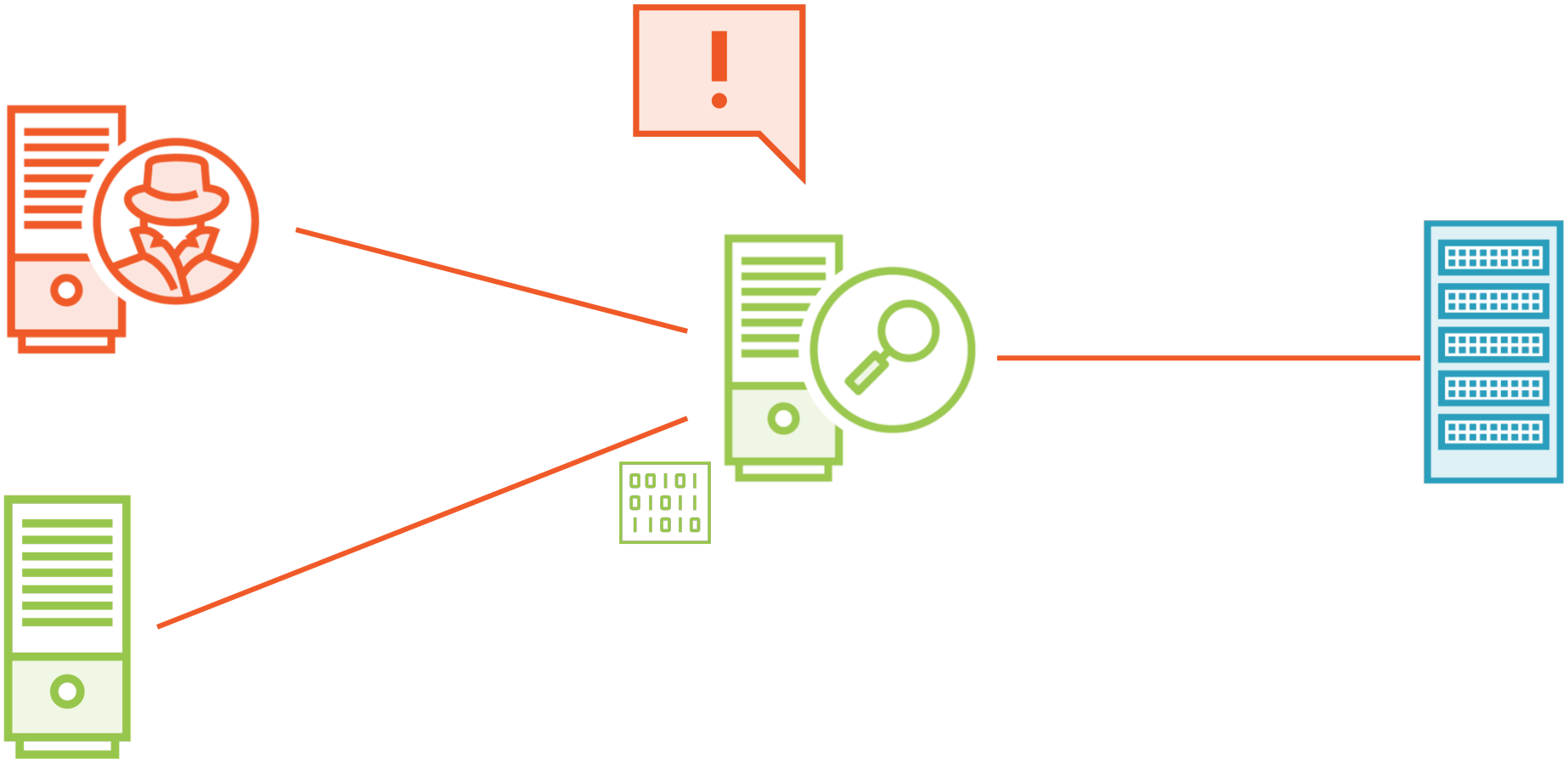
Create custom rules for internal acceptable use policies

Example Scenario

Example Scenario

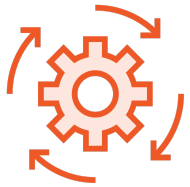
Example Scenario

Example Scenario



Example Scenario

This is an example of a false positive alert on legitimate traffic



The rule generating the alert needs to be refined

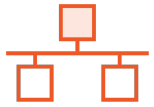
Leverage rule options to specifically target the malicious content

Writing a Basic Snort Rule

The Essential Parts of a Basic Rule

Source IP address or variable

Destination IP address or variable



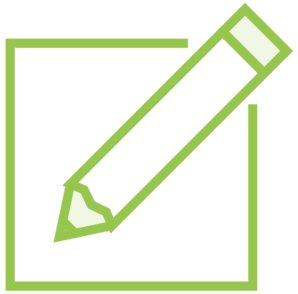
Port and protocol of the matching traffic

Action taken on the matching traffic

Direction of traffic flow

Snort Rule Actions

alert



log

pass

drop

reject

sdrop

Other Basic Rule Options

Unique ID

(sid)

Revision

(rev)

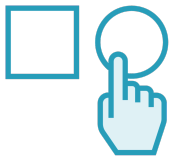
Message to print

(msg)

Additional General Rule Options

gid: specifies the source of the event within Snort

classtype: classifies traffic within predefined attack classes



priority: overwrites the default classtype priorities

metadata: embeds additional rule data

```
alert tcp any any -> 10.0.0.0/24 23 (msg:”Inbound telnet traffic detected.”;
classtype:suspicious-login; sid:1000001; rev:1;)


alert ICMP any any -> 10.0.0.0/24 any (msg:”Inbound ICMP detected.”;
classtype:ICMP-event; sid:1000002; rev:1;)
```

Example Basic Snort Rules

Alert on any inbound telnet connection attempts and classify as suspicious login

Alert on any inbound ICMP packets and classify as ICMP-event

Demo

Writing your first Snort rules

Address these security goals:

- Alert on all inbound SSH attempts from the external network
- Block and log all inbound Telnet attempts to the default port
- Reject and log all attempted RDP traffic from the external network
- Classify this traffic and assign a higher priority to telnet attempts

Test your rules

Summary

Summary

- Course scenario and lab setup
- Purpose behind writing custom rules
- Wrote our first few rules
- Tested custom rules against target traffic