Examining Rule Set Effects

Matt Glass
CISSP, MCSE

https://mattglass-it.com/

Overview

Evaluate the effects of a rule set

Capture traffic to a PCAP file

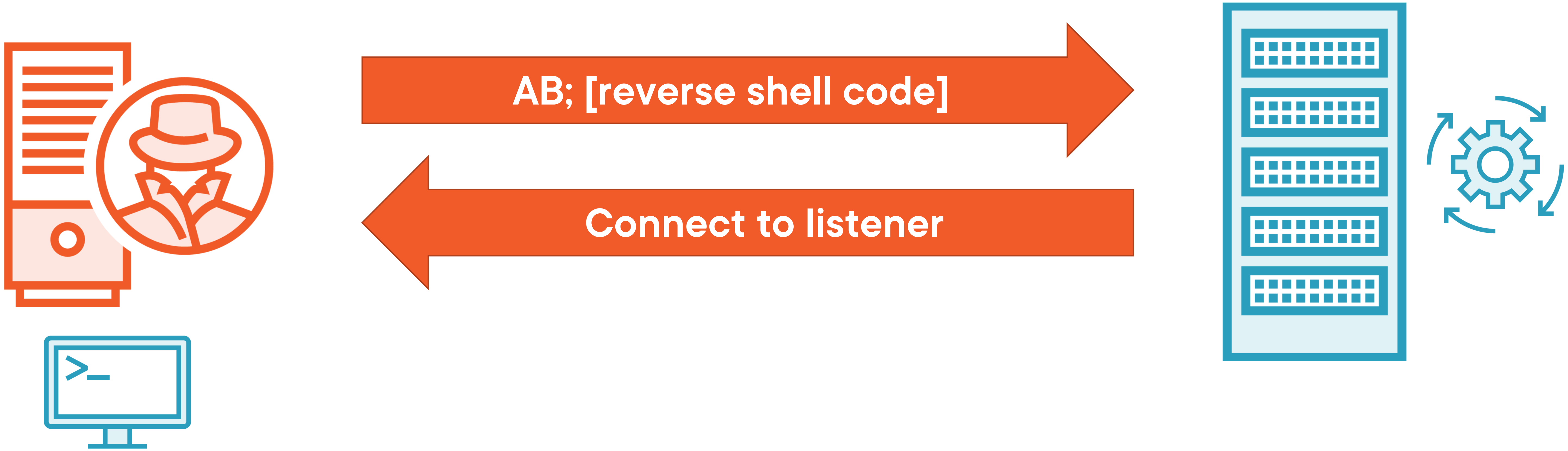
Simulate unauthorized traffic

Enable the rule sources

Test rule set application through traffic replay

Detecting Specific Threats

UnrealIRCd Backdoor



AB; [reverse shell code]

Connect to listener

Evaluating Potential Rule Sets

Emerging Threats chat rules

Threat hunting rules

Custom rule source

Using PCAP Capture and Replay

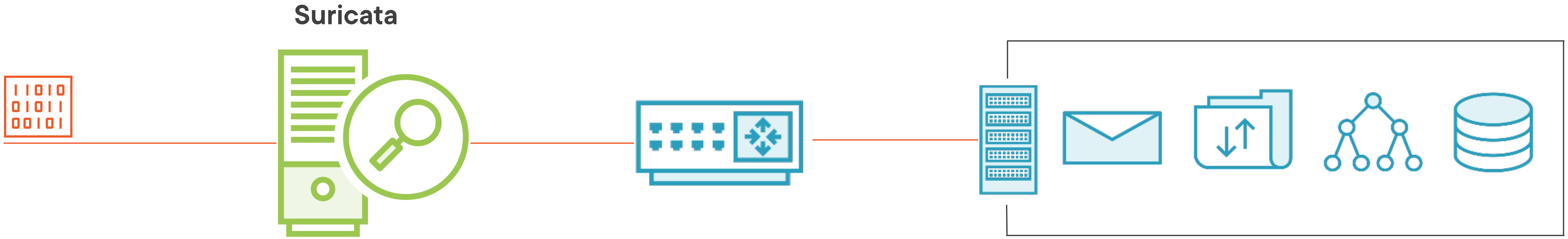
What is PCAP?

PCAP stands for packet capture

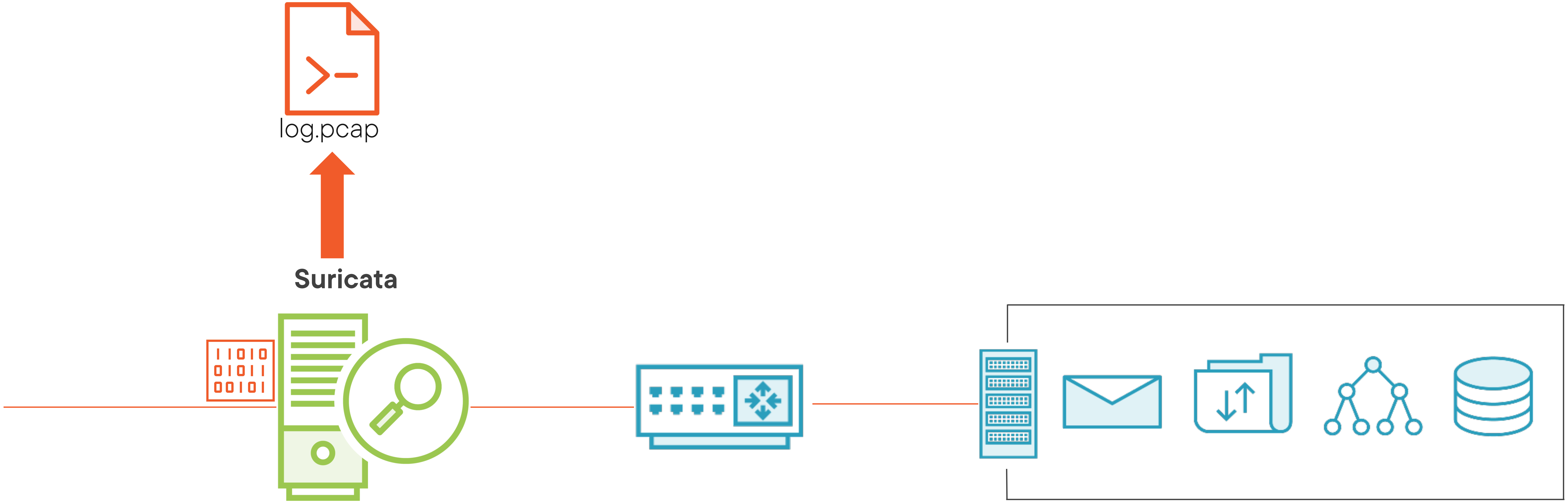
Files that contain packets from traffic passing through Suricata

Stored for additional analysis, replay, or use with other tools

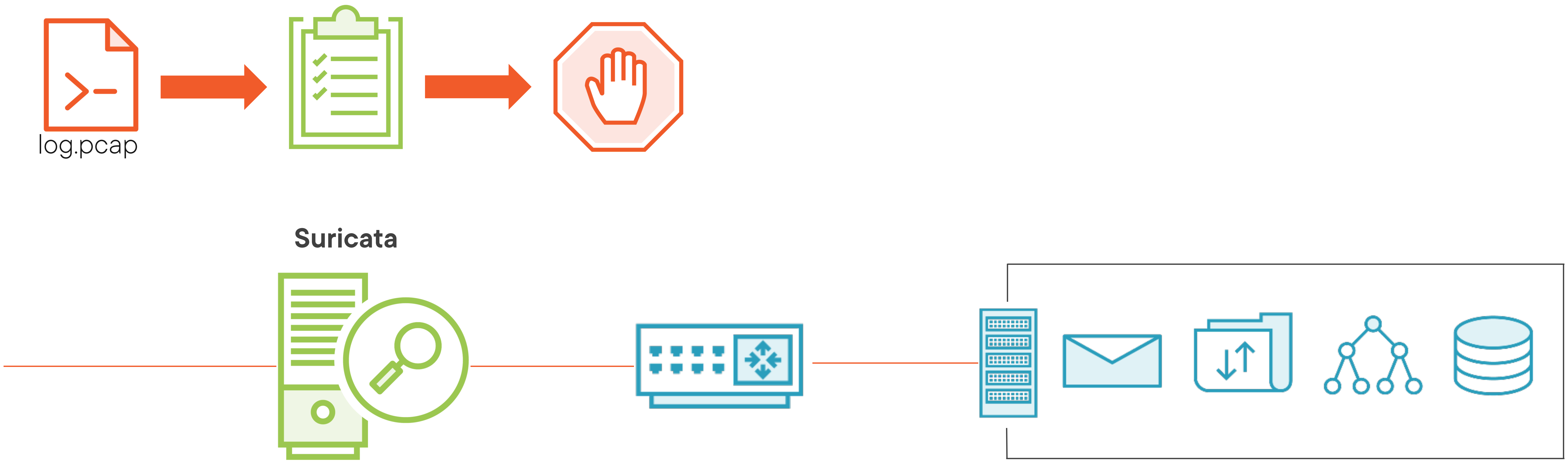
Capturing Traffic to PCAP File



Capturing Traffic to PCAP File



Replaying PCAP Traffic



Demo

Capturing traffic to PCAP for replay

Globomantics Goals:

- Capture traffic simulating the potential threat
- Test the PCAP replay to ensure its use for evaluating rule sets

Demo

Test the new rule set with PCAP replay

Globomantics Goals:

- Select an appropriate rule sources and sets to detect the UnrealIRCd exploit
- Evaluate the new rules through PCAP replay
- Ensure the threat is detected with the new rule set

Summary

Summary

Captured traffic to PCAP for future use and evaluation

Obtained rules to detect specific threats

Examined rule set effects using PCAP replay