

Manage Suricata Rule Sets and Rule Sources

Understanding Suricata Rule Sets and Sources



Matt Glass
CISSP, MCSE

<https://mattglass-it.com/>



Overview



Course scenario

Lab setup

Open-source rule sets

Suricata rule sets and sources

Managing rule sets and sources

Emerging Threats rule set



Course Scenario



Globomantics



Course Scenario



Globomantics



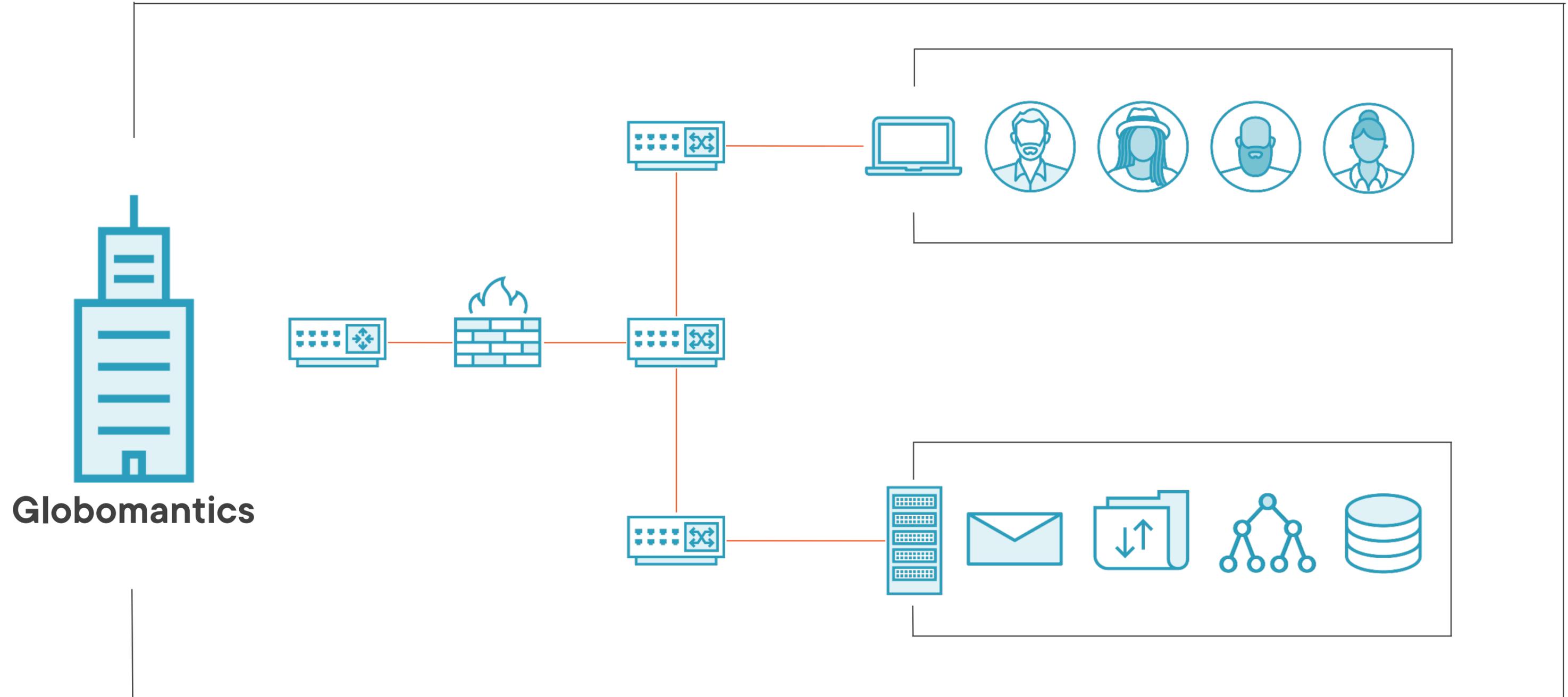
New Site 2



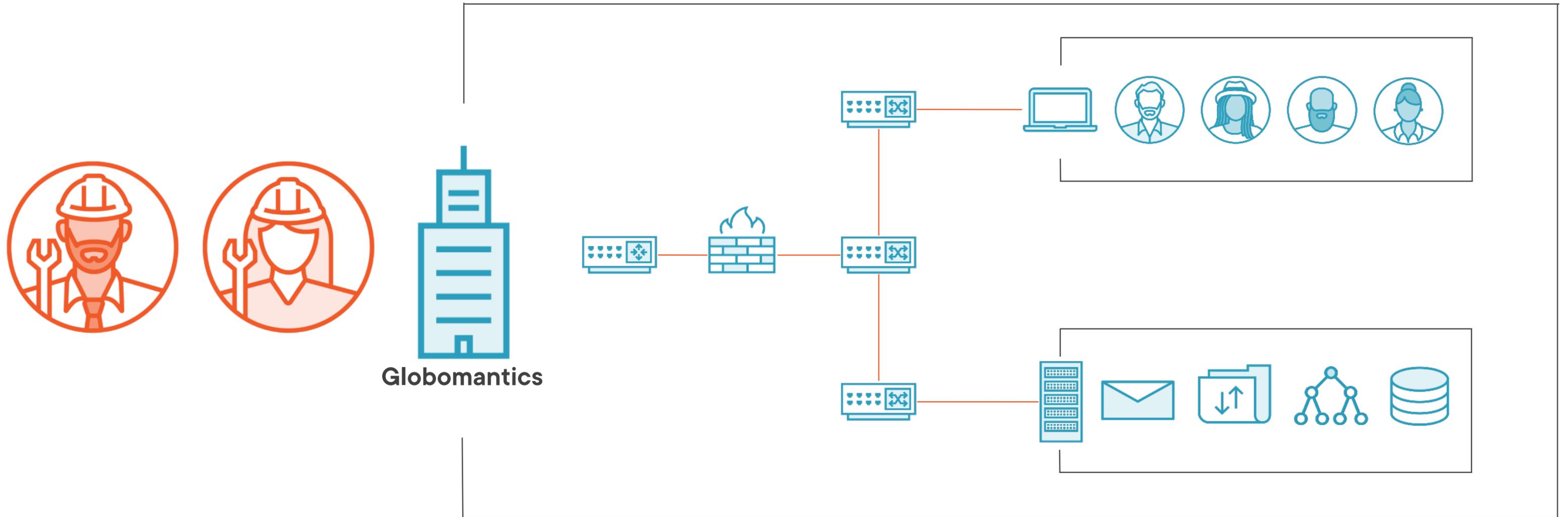
New Site 1



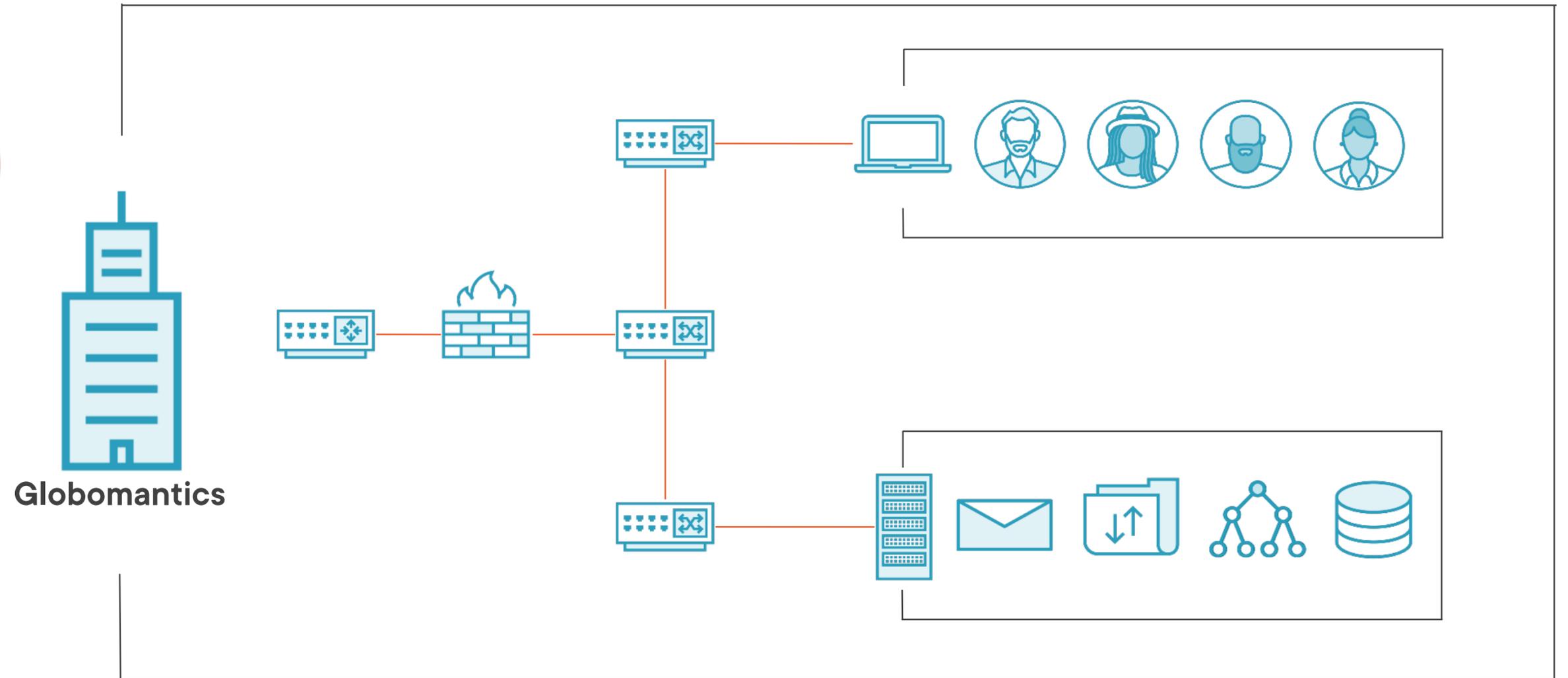
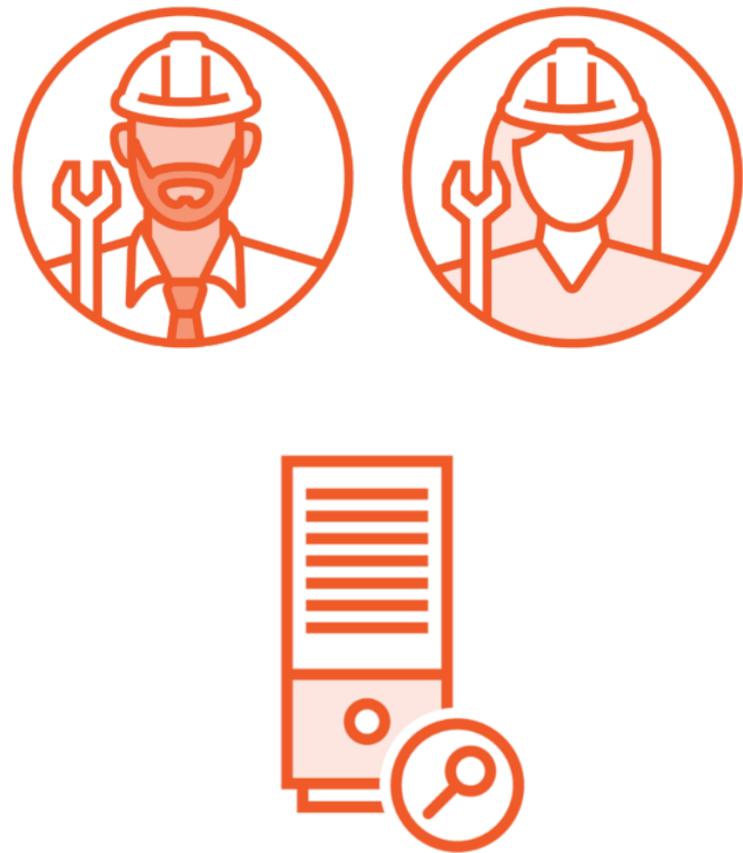
Course Scenario



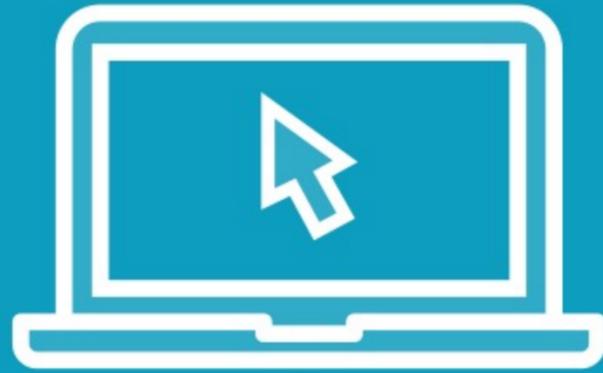
Course Scenario



Course Scenario



Demo



Lab setup



The Vagrant files require
modification to fit your
environment.



Suricata Rule Sets and Sources



Rule Sets and Sources



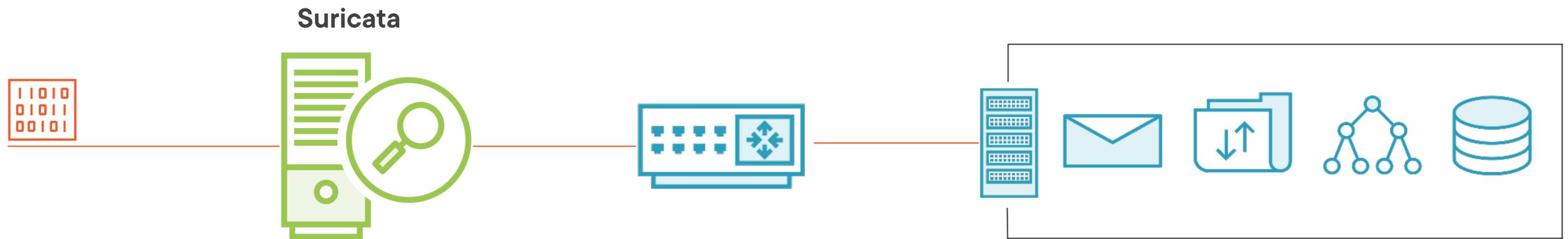
Suricata rule sets are pre-written lists of Suricata rules that take a pre-determined action on traffic.



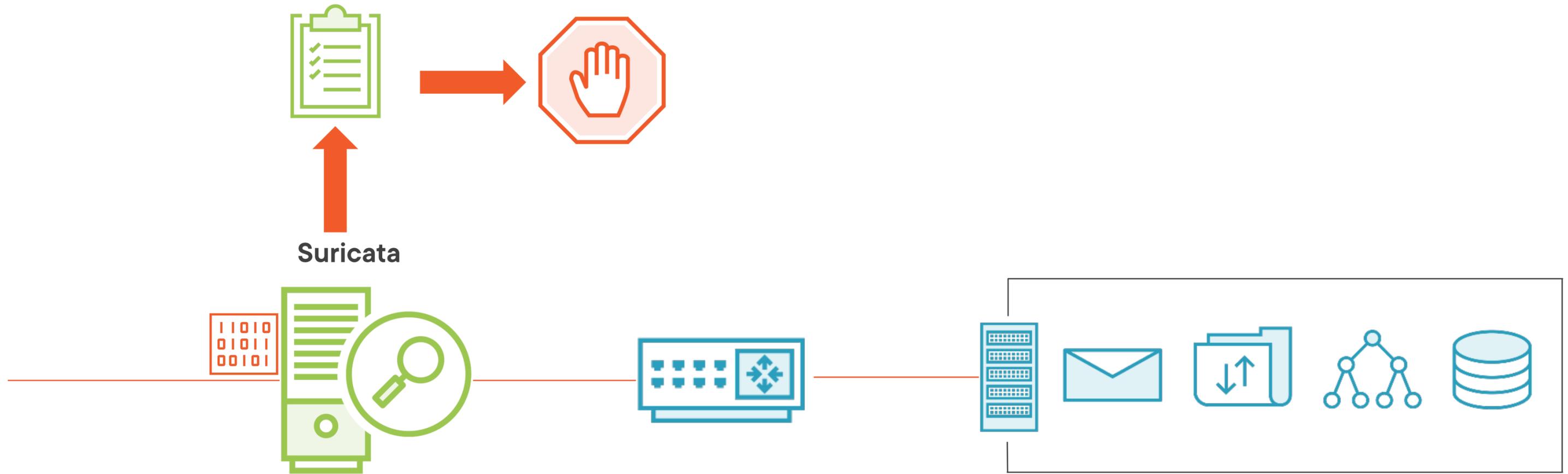
Suricata rule sources are the locations of rule sets written for Suricata and managed by external organizations.



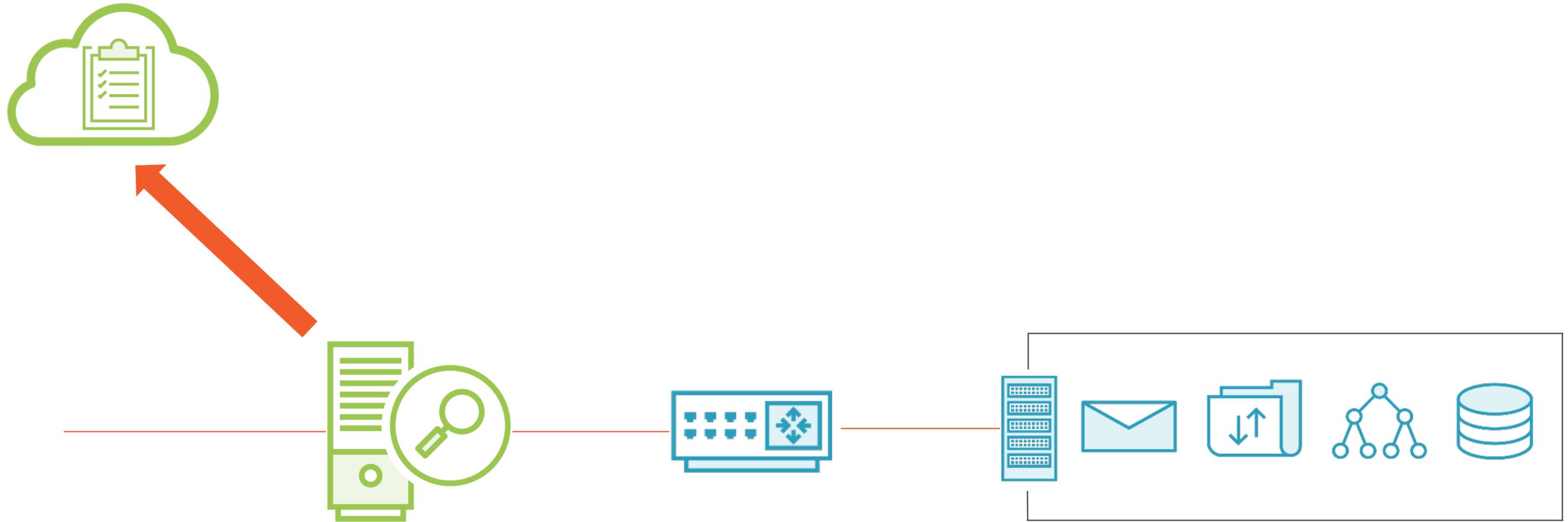
Suricata Rule Sets



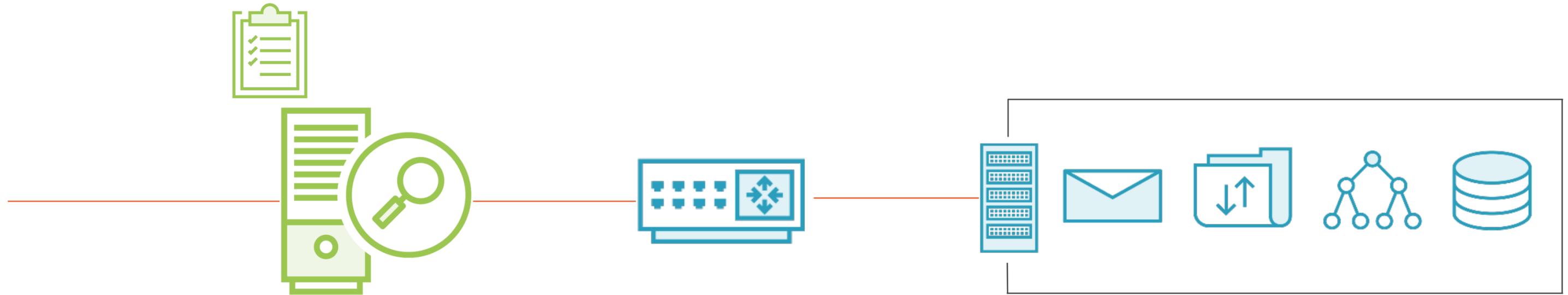
Suricata Rule Sets



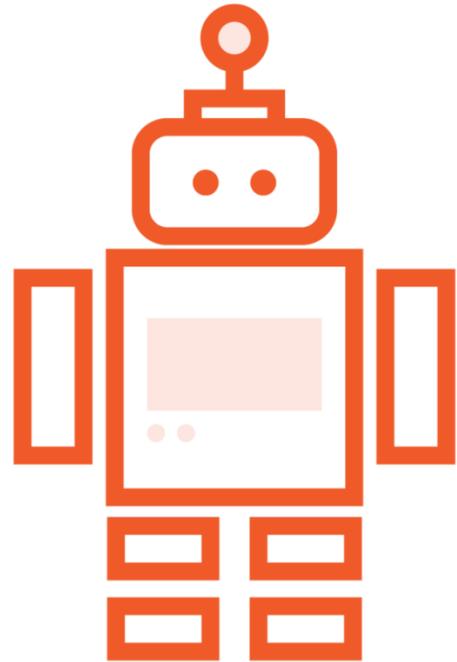
Suricata Rule Sources



Suricata Rule Sources



Managing Suricata Rule Sets and Sources



**Automated using tools
like suricata-update**



**Manual configuration by
updating local rules files**



**Combination of both
automated and manual**



Open-Source Rule Sets



What are Open-Source Rule Sets?



Rule sets pre-written by information security organizations



Available for download from rule sources



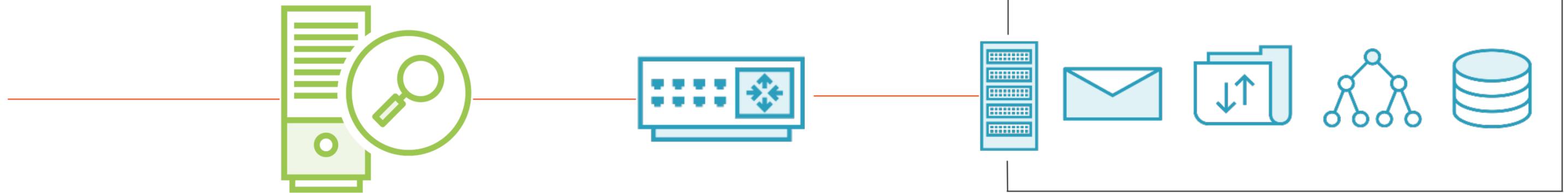
Free for use and modification to fit your environment



Leveraging Open-Source Rules



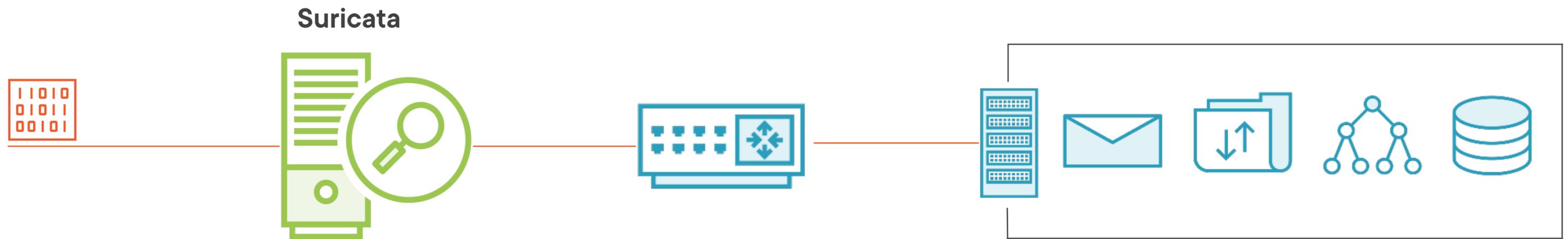
Suricata



Leveraging Open-Source Rules



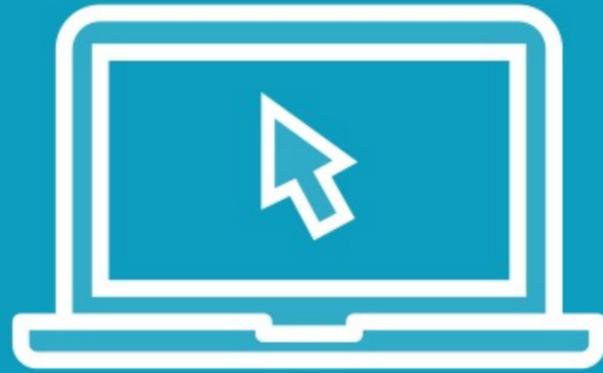
Leveraging Open-Source Rules



Leveraging Open-Source Rules



Demo



Explore the Emerging Threats rules

- Emerging Threats rules were installed in **Suricata: Getting Started**
- Explore the rule set on our **Suricata server**



Summary



Summary



Explored open-source rule sets

Evaluated the Emerging Threats rule set

Discovered applicable rules

