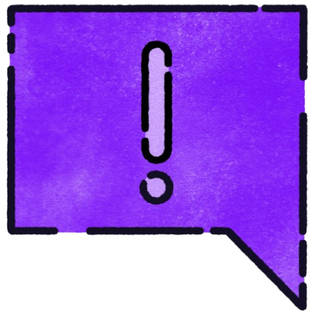
Respond to Security Incidents

Antonio J. Piedra
Senior DevOps Engineer

www.linkedin.com/in/ajpiedra

Why Monitor Suspicious Activities?

Threats can arise from many sources



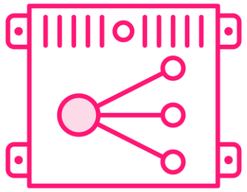
Be informed when abnormal activity happens

Take rapid action to minimize impact

Types of Activities to Monitor

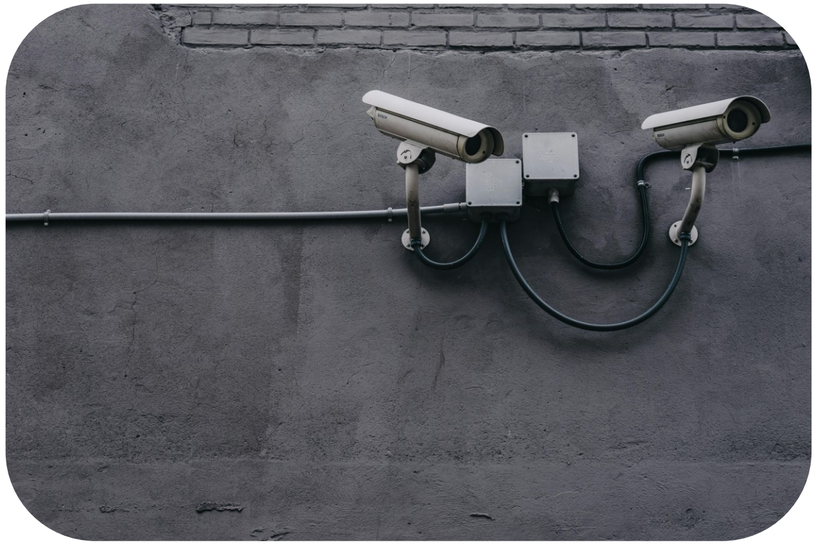
Unauthorized shell access

Privilege scalation



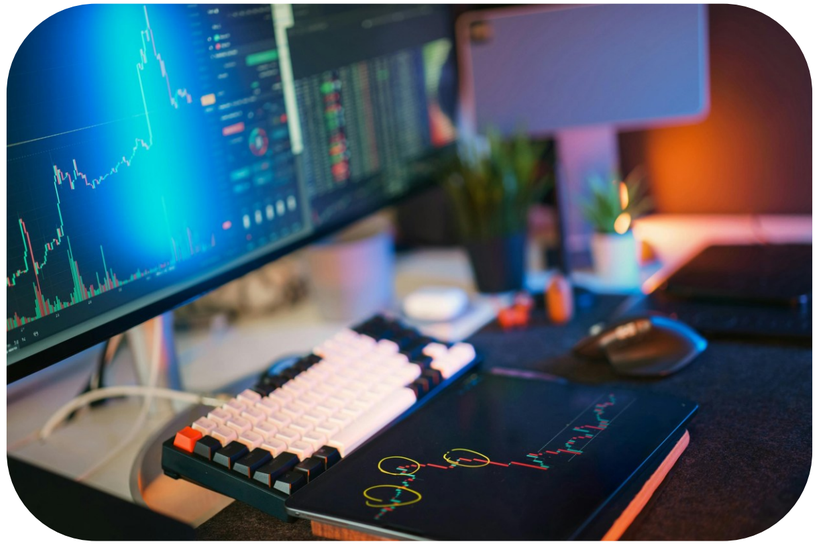
Unexpected network behavior

Open-source Tools for Monitoring Suspicious Activity



Falco

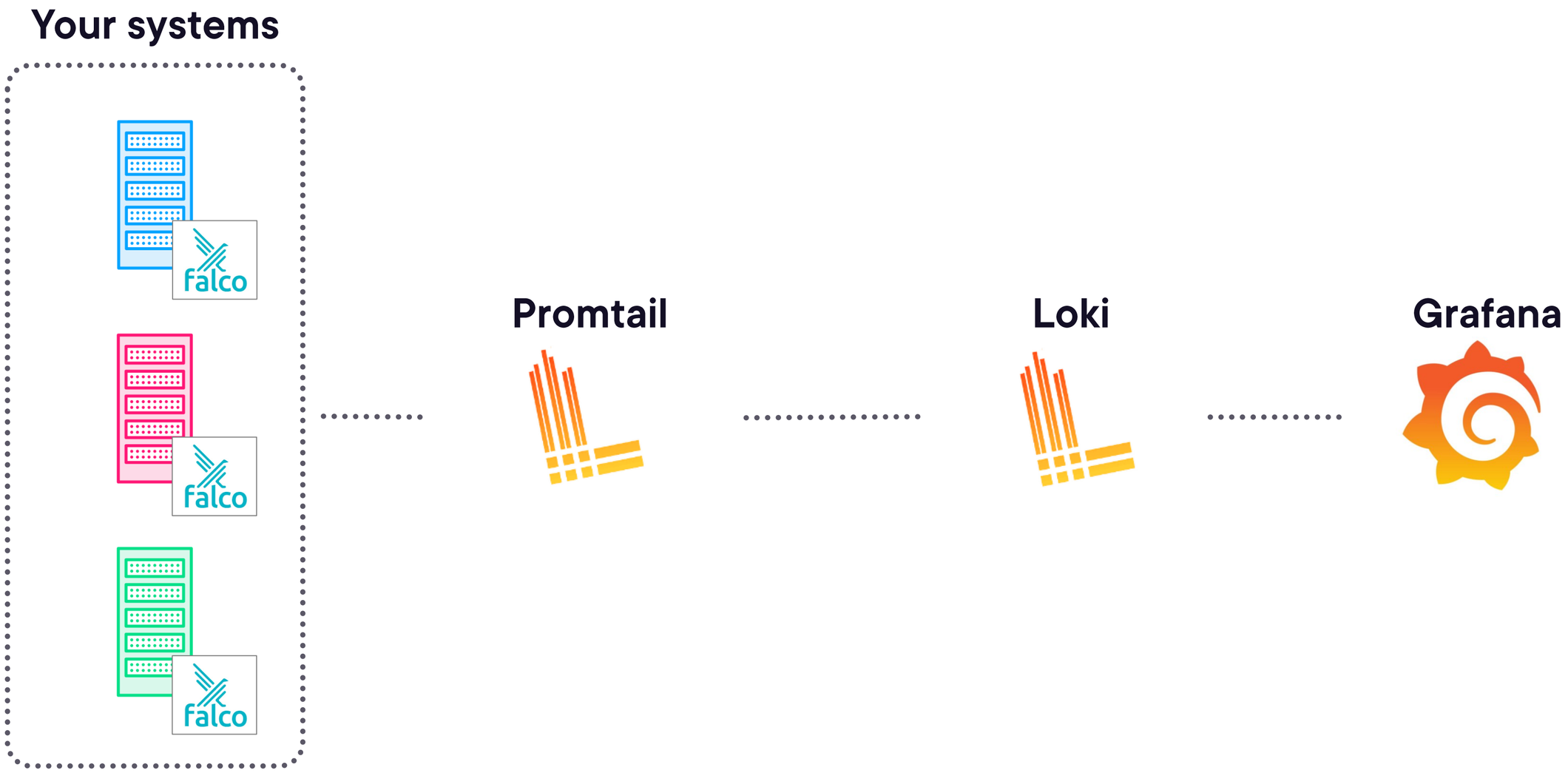
Real-time container runtime threat detection



Promtail, Loki and Grafana

Collect, store and visualize security events

Sample Monitoring Diagram



Demo: Install and Configure Falco

Monitor runtime security and detect anomalous container behavior

Demo: Install and Configure Loki

For storing and indexing log data

Demo: Install and Configure Promtail

Scrapes and pushes logs them to Loki

Demo: Install and Configure Grafana

Monitor security events and analyze logs in real time

Demo: Review Suspicious Activity

Identify and respond to security incidents

Thank you for your time!

www.linkedin.com/in/ajpiedra