AppSec Program

in an agile environment

Agenda

- Introduction
- Definitions: Application Security
- Definitions: Agile Practices
- Proactive Approaches
- Reactive Approaches

Introduction

Mert Coskuner, MSc, Security Engineer at Amazon

OSCP, OSCE, eCPTX, eWPTX, eMAPT

Bunch of conference talks about red team, threat int. and appsec

We are hiring! https://www.amazon.jobs/en-gb/jobs/1419513/senior-security-engineer

Opinions expressed are solely my own

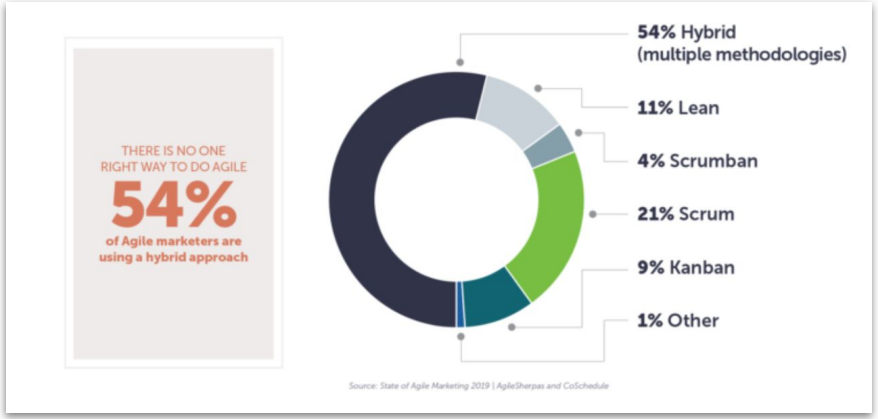
and do not express the views or opinions of my employer

Application Security

"Application security encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities."

Agile Practices

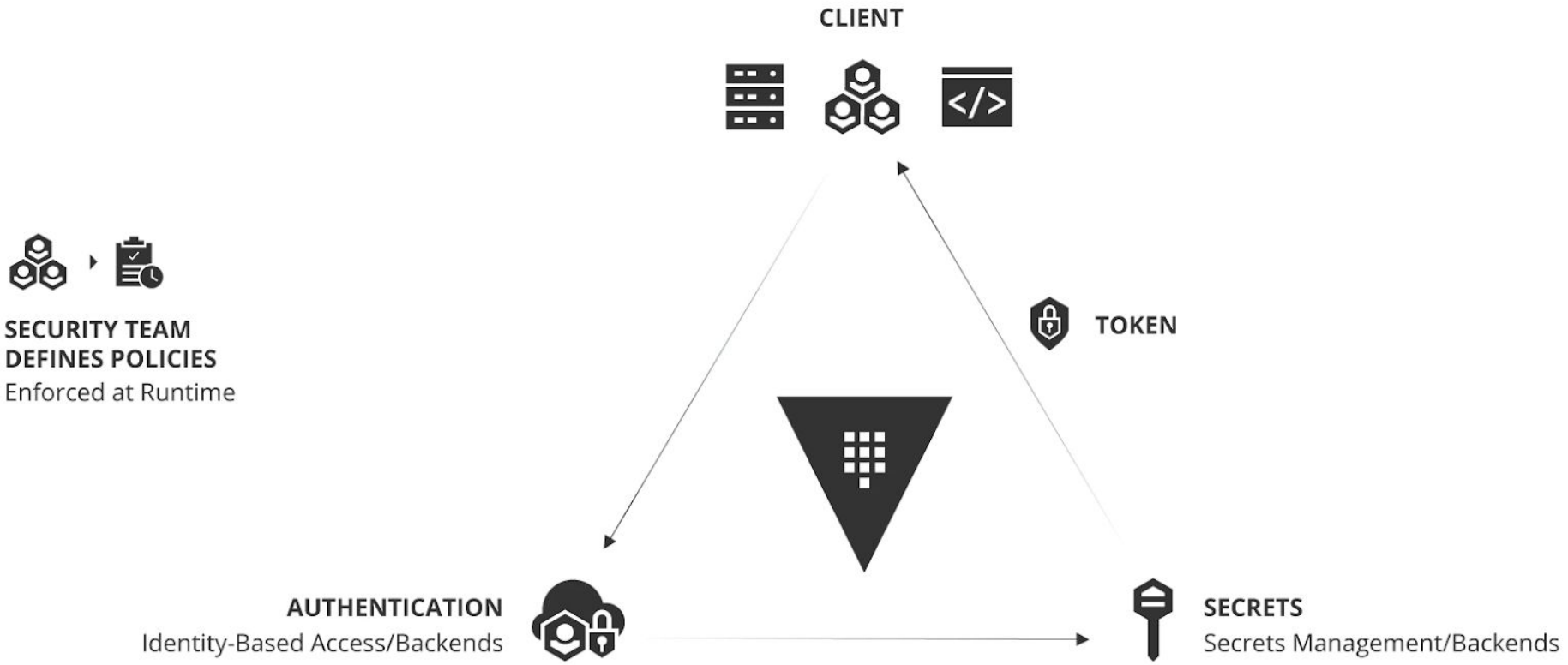
“Successful practices include keeping teams small, sticking to short iterations, getting rapid feedback from customers, setting value-based business priorities and engaging users in refining requirements. It is the core values and guiding principles for how people work together that make Agile methods sustainable.”



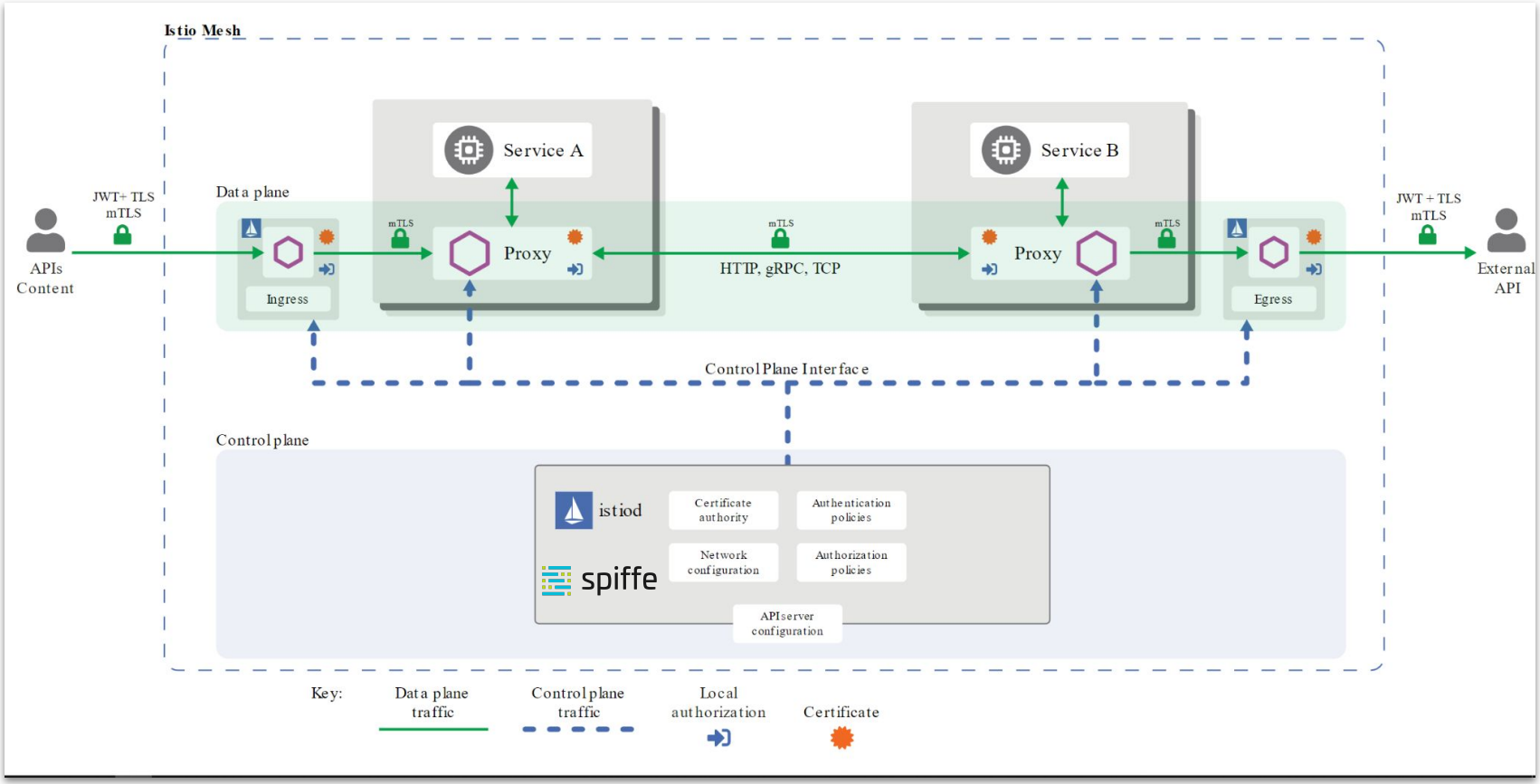
Proactive Approaches

- Security practices for developers
  - Meetups
  - Threat modeling sessions
  - Code review sessions
  - Onboarding newcomers
- SAST, DAST and container scan at CI/CD
- Risk scoring and maturity measurement
  - Risk based on data criticality
  - Maturity based on mean time to fix and vulnerability count
- Abstract features for developers
  - Secret management
  - Authentication, authorization logic

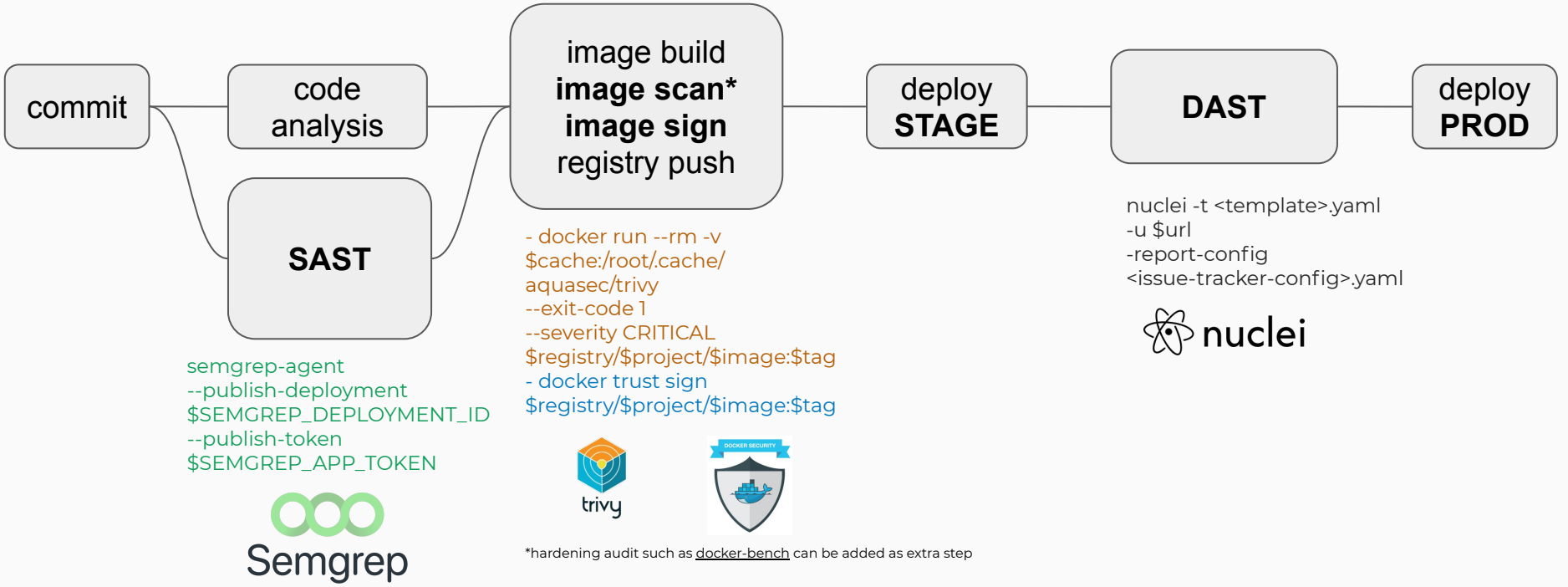
Secret management



AuthN/Z using service mesh



Sample pipeline



Reactive Approaches

- Penetration testing
  - Before production deployment
- Vulnerability scanning
  - Scheduled scans to support CI/CD practices
- Bug bounty program
  - Start with a private program
  - Move towards a public program as you mature

Contact

linkedin.com/in/mcoskuner

We are hiring!
https://www.amazon.jobs/en-gb/jobs/1419513/senior-security-engineer