Security Vulnerability Management:

OWASP DefectDojo

Augsburg, 24.04.2025

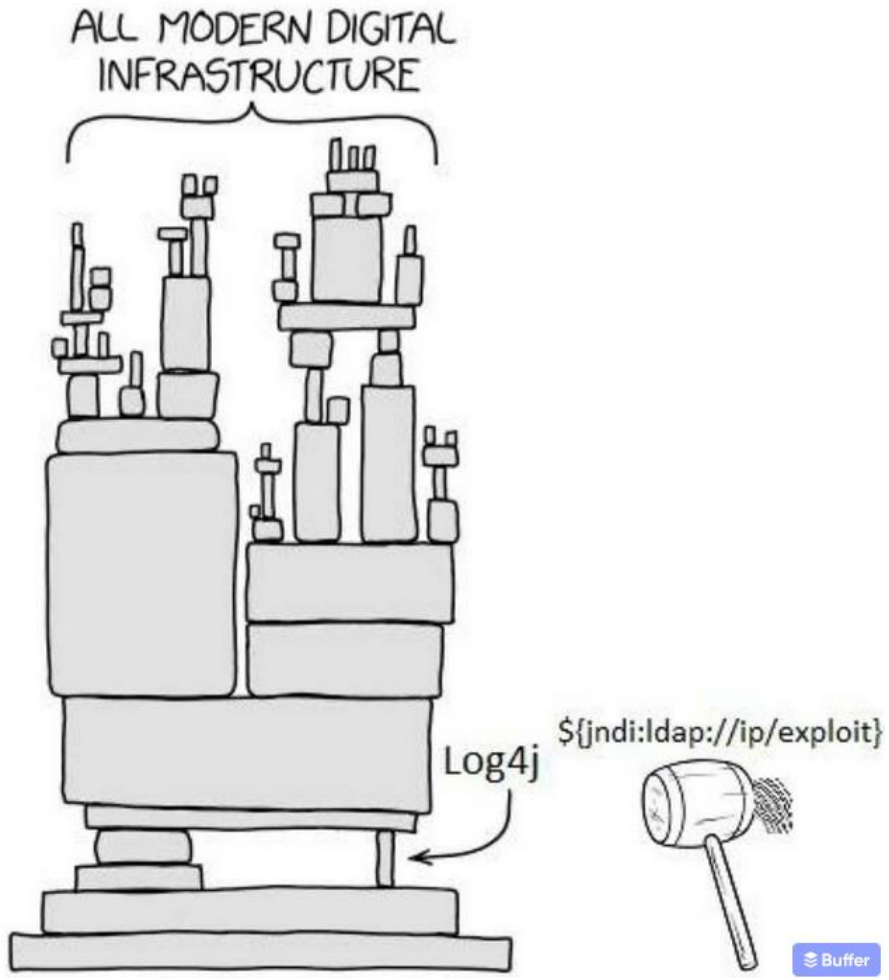
About me

- Born in Augsburg, living in Nürnberg
- Bachelor 2011 & Master 2024 at TH Augsburg
- Software Engineer for 10 years
- AppSec Consultant at secureIO
- More info: https://mwager.de/

- Agenda:
  - Intro: SSDLC, AppSec-Programs & DevSecOps
  - The Problem: Scanner Overload
  - What is OWASP DefectDojo?
  - Live-Demo
  - DevSecOps Automation in Action

Intro

- Example: Log4J
- SSDLC, AppSec-Programs, DevSecOps
- Regulations: ISO/IEC 27001, NIS2, Cyber Resilience Act



The Problem: Scanner Overload

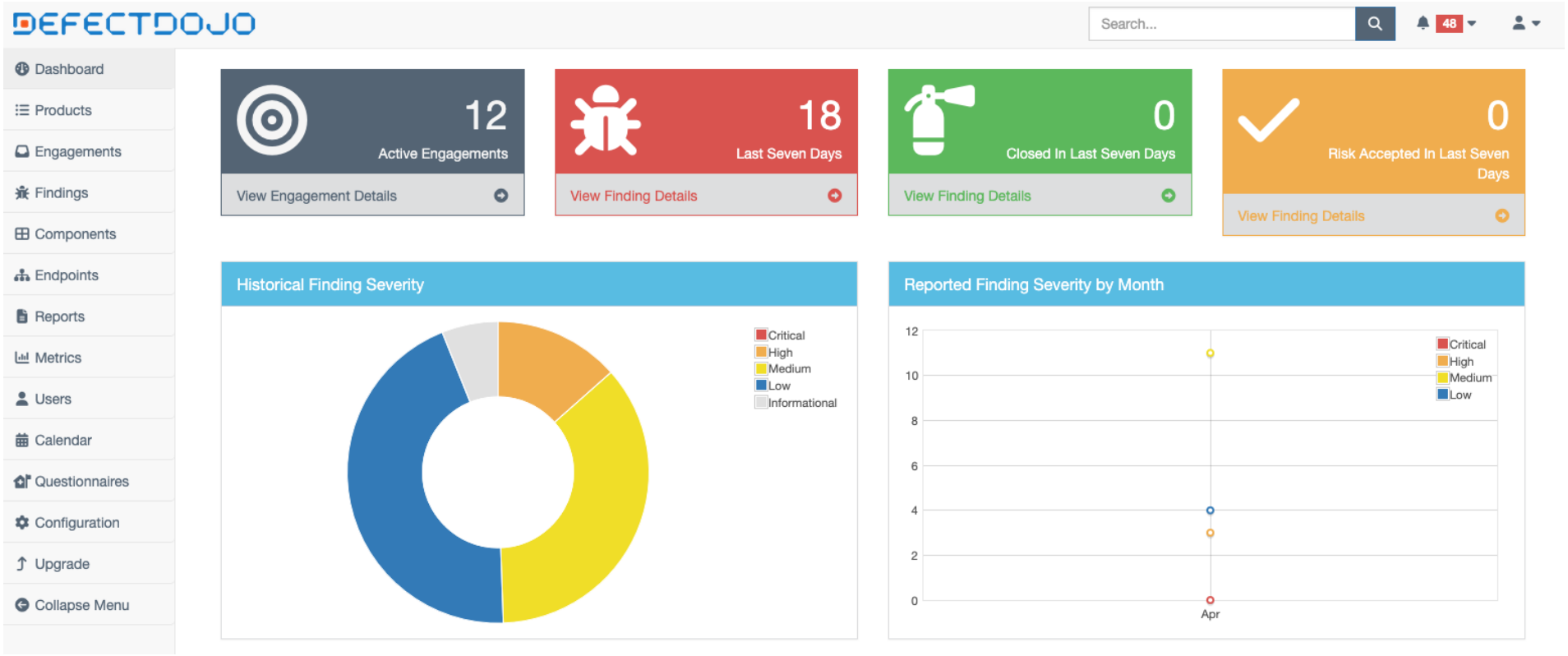
- What is security scanning?
- Tracking of results?
- Policy requirements
- Reporting & Transparency

OWASP DefectDojo

- OWASP
  - *Open Web Application Security Project*
  - OWASP Top 10 (E.g. Injection, supply chain)
  - But there is more! Tools, Projects, Standards, Chapters (e.g. OWASP Augsburg Stammtisch)
  - Community-driven & free
- DefectDojo
  - Open-source vulnerability management tool by OWASP
  - Central platform to track, deduplicate, and triage findings across multiple applications, teams, and scan types
  - Supports automation, reporting, and integrations (Jira, CI/CD, API) to streamline AppSec programs

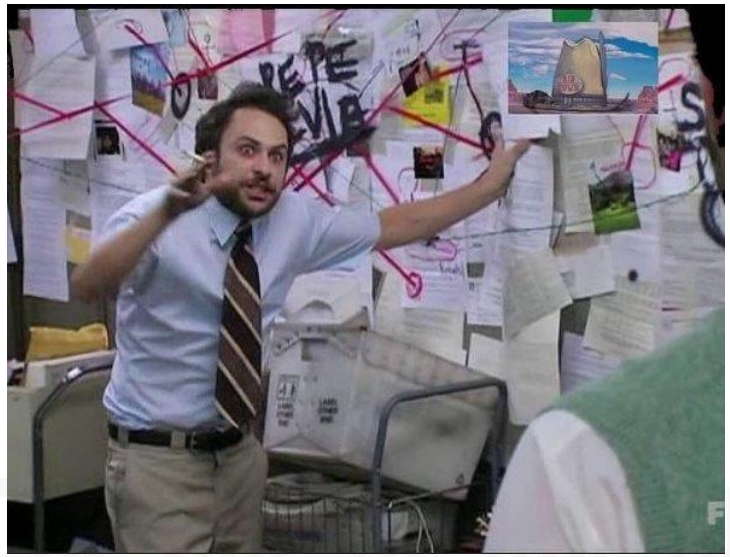
Demo

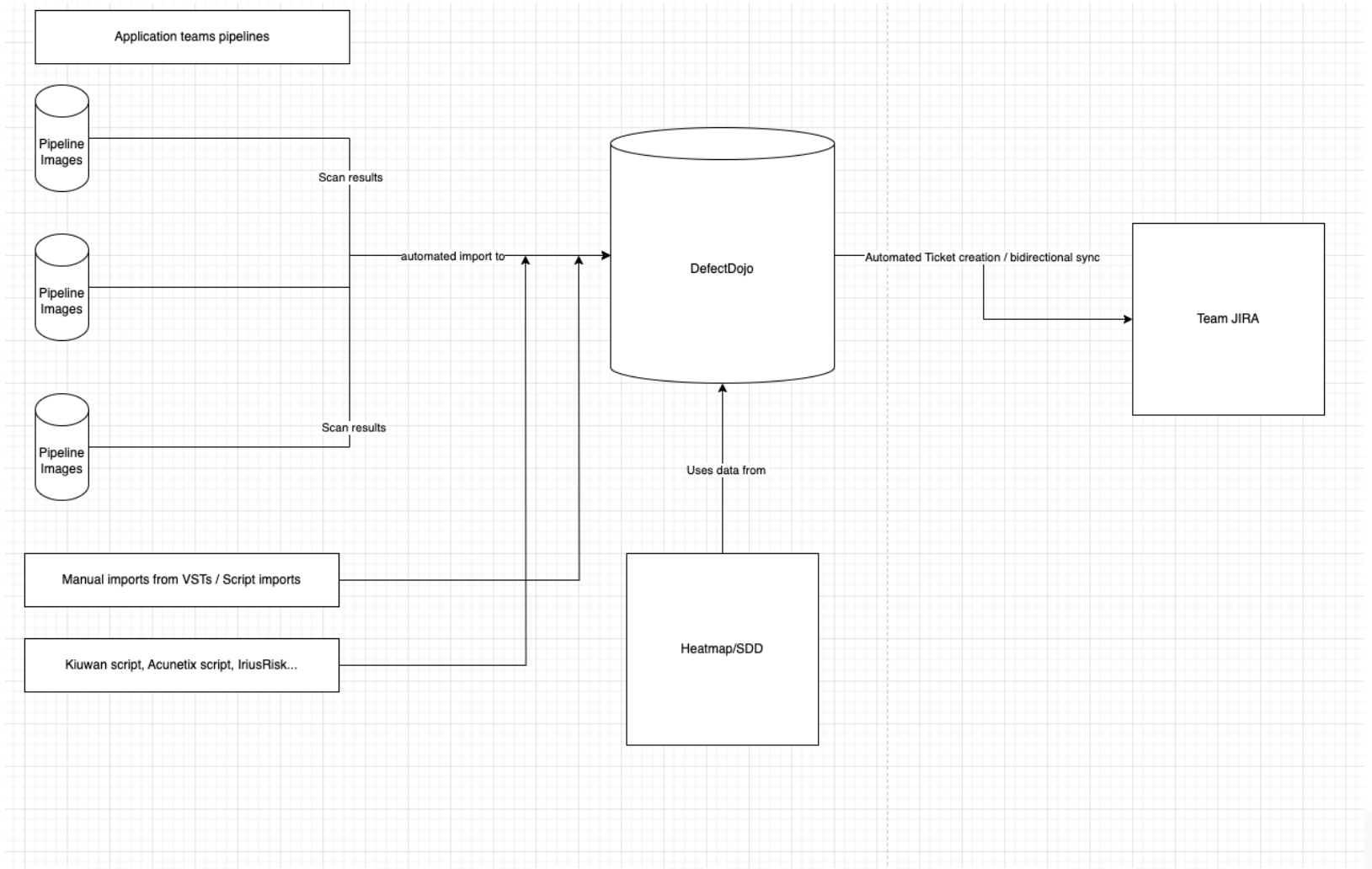
https://demo.defectdojo.org/



DevSecOps Automation in Action

- Standardization of Scanning in CI/CD Pipelines
- Centralized Management with DefectDojo
- Ticket Automation & Feedback Loop





Discussion