Leveraging OWASP Projects and Tools to Transform Your SDLC

John DiLeo (@gr4ybeard)

Datacom and OWASP NZ

September 2024

About Me

- Past lives
  - Simulation developer and system analyst
  - University lecturer - Math, Comp Sci, IT, *et al.*
  - J2EE developer and architect
- Full-time in AppSec since 2014
- Moved from US to New Zealand late 2017

About My Day Job

Gallagher Security – Application Security Lead

- Manage Threat Modelling Program
- AppSec Maturity Uplift
- Feature Security Reviews
- In-House AppSec Training

About My *Other* 'Job'

Chapter Leader, OWASP New Zealand

- Hamilton Meetup
- Regional Training Days

Chair, OWASP New Zealand Day Conference, 2019-2024

Chair, OWASP Global AppSec-Auckland, 1-5 Sept 2025

OWASP SAMM Project – Core Team

Launched SAMMwise and State of AppSec Survey Projects

What You Can Expect to Hear

- My thoughts about Software Assurance
- Some information about the OWASP Software Assurance Maturity Model (SAMM)
- The names of *dozens* of OWASP Projects
- A few thoughts on leveraging OWASP Projects

What You Shouldn't Expect to Hear

- An in-depth treatment of SAMM
- Information about *every* OWASP project
  - There are 225 "active" OWASP projects*
  - I'll mention only 30 or so by name
  - I'll provide *overviews* of fewer than 20

* 15 Flagship, 8 Production, 34 Lab, 126 Incubator, and 42 "need website update" (new or dormant)

Reasons to Love OWASP Projects

- Developed and maintained by passionate volunteers…who happen to be experts
- Supportive community of users and contributors
  - OWASP Slack (https://owasp.org/slack/invite)
  - Project channels (e.g., #project-samm)
  - Topical channels (e.g., #threat-modeling)
- Open-source – Public repos on GitHub
- Project deliverables are FREE (as in ‘freedom’ *and* as in ‘free beer’)

Software Assurance

"Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle and that the software functions in the intended manner."

- [US] National Information Assurance (IA) Glossary, April 2010

And, by that you mean…?

- Attain and maintain high **stakeholder confidence** in successful delivery of the features you **intended** to deliver
- Prevent, detect, and remove **vulnerabilities**
- Improve **reliability** and **resilience** of the production system

SO MUCH MORE than code reviews or 11th-hour penetration tests

Software Assurance Maturity Model

Flagship Project

What is SAMM?

An open framework that provides an **effective** and **measurable** way for all types of organizations to **analyze** and **improve** their software security posture.

https://owaspsamm.org

What is SAMM?

The resources provided by SAMM aid in:

- evaluating an organization's existing software security practices;
- building a balanced software security assurance program in well-defined iterations;
- demonstrating concrete improvements to a security assurance program; and
- defining and measuring security-related activities throughout an organization.

SAMM Model Structure

- Five Business Functions
- 15 Practice Areas
- 2 Activity Streams per Practice Area
- 3 Activities in each Stream – 90 Activities total

Governance	Design	Implementation	Verification	Operations
Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Education & Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management

Source: https://owaspsamm.org

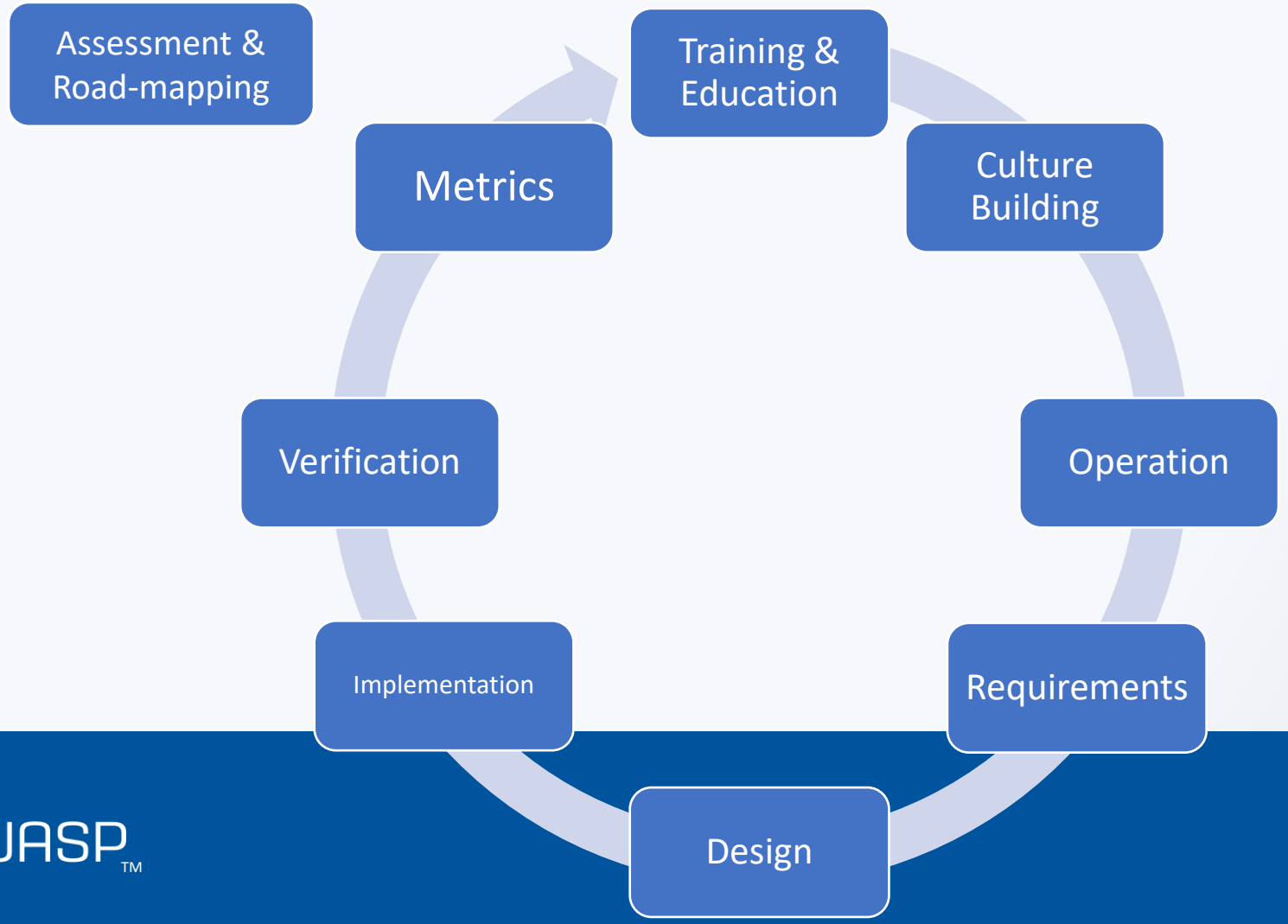
SAMM Maturity Levels

Within an Activity Stream, Activities represent progressive maturity levels:

- Level 0 – Practice unfulfilled
- Level 1 – *Ad hoc* / best-effort / inconsistent
- Level 2 – Defined / documented / standardized
- Level 3 – Measured and optimized

AppSec Program Elements

Ref: OWASP Integration Standards Project



Training and Education

Awareness:

- AppSec Awareness Campaigns
- **OWASP Top 10 Family**

Board Game:

- Snakes & Ladders

Broadcasts:

- DevSlop Show
- Podcast Series

Training Platforms/Applications:

- Cyber Scavenger Hunt
- TimeGap Theory

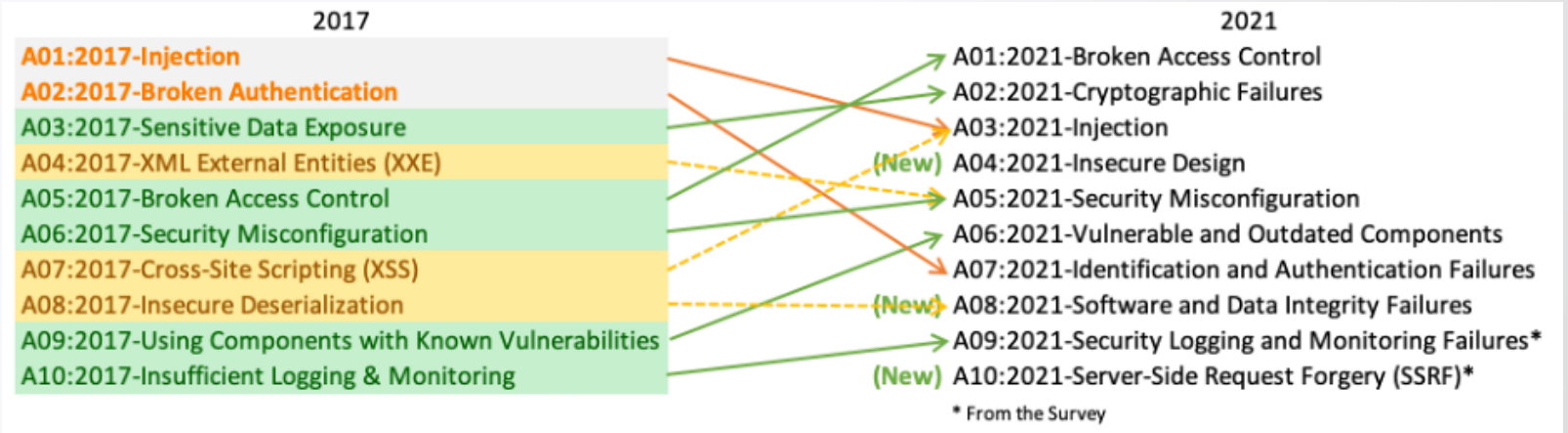
Intentionally Vulnerable WebApps:

- **Juice Shop**
- Security Shepherd
- WebGoat / PyGoat
- WrongSecrets

OWASP Top 10

Flagship Project

- Standard awareness document for developers and web application security
- Represents broad consensus about the most critical security risks to web apps
  - Current version: 2021
  - Next version: 2024?



The OWASP Top Ten

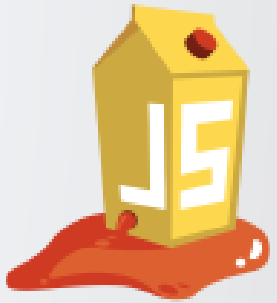
Flagship Project

25 Other OWASP Projects in the Top Ten “family”:

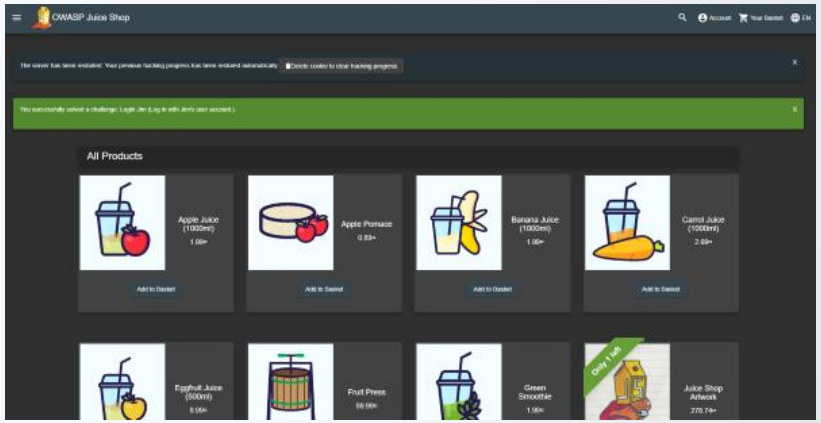
- **Lab:** Machine Learning, Mobile, CI/CD, LLM, Low-Code/No-Code, Privacy
- **Incubator:** AI, Cloud-Native AppSec, Data Security, Desktop App Security, DevSecOps, Docker, Kubernetes, Operational Technology (OT), Serverless, Thick Client, Client-Side Security, Drone Security, Maritime, Insider Threats, “in XR”
- **Inactive:** Internet of Things (IoT), Open-Source Software, Smart Contract, Solana

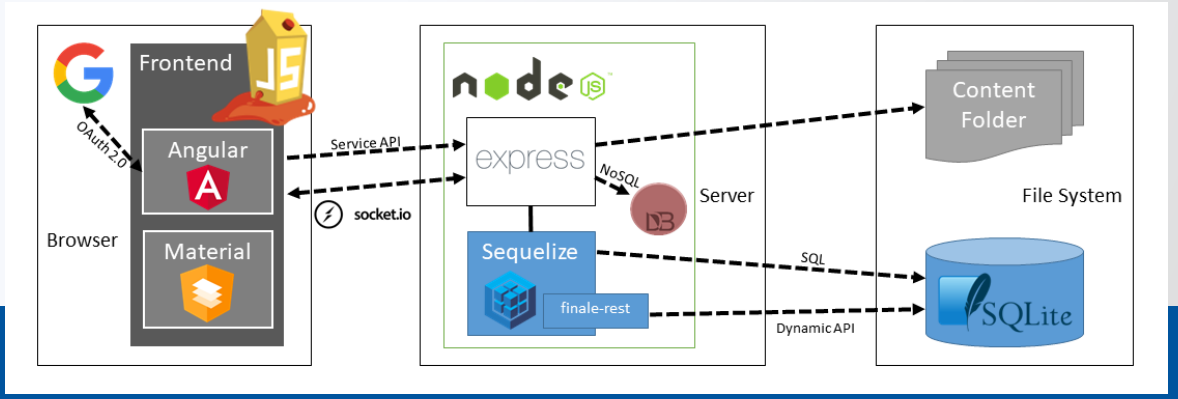
Juice Shop

Flagship Project



- World's most modern and sophisticated insecure web application!
- Exhibits vulnerabilities from the entire OWASP Top Ten, and lots more
- Useful for:
  - Security training
  - Awareness demos
  - Capture the Flag events (CTFs)
  - Target app for security tools



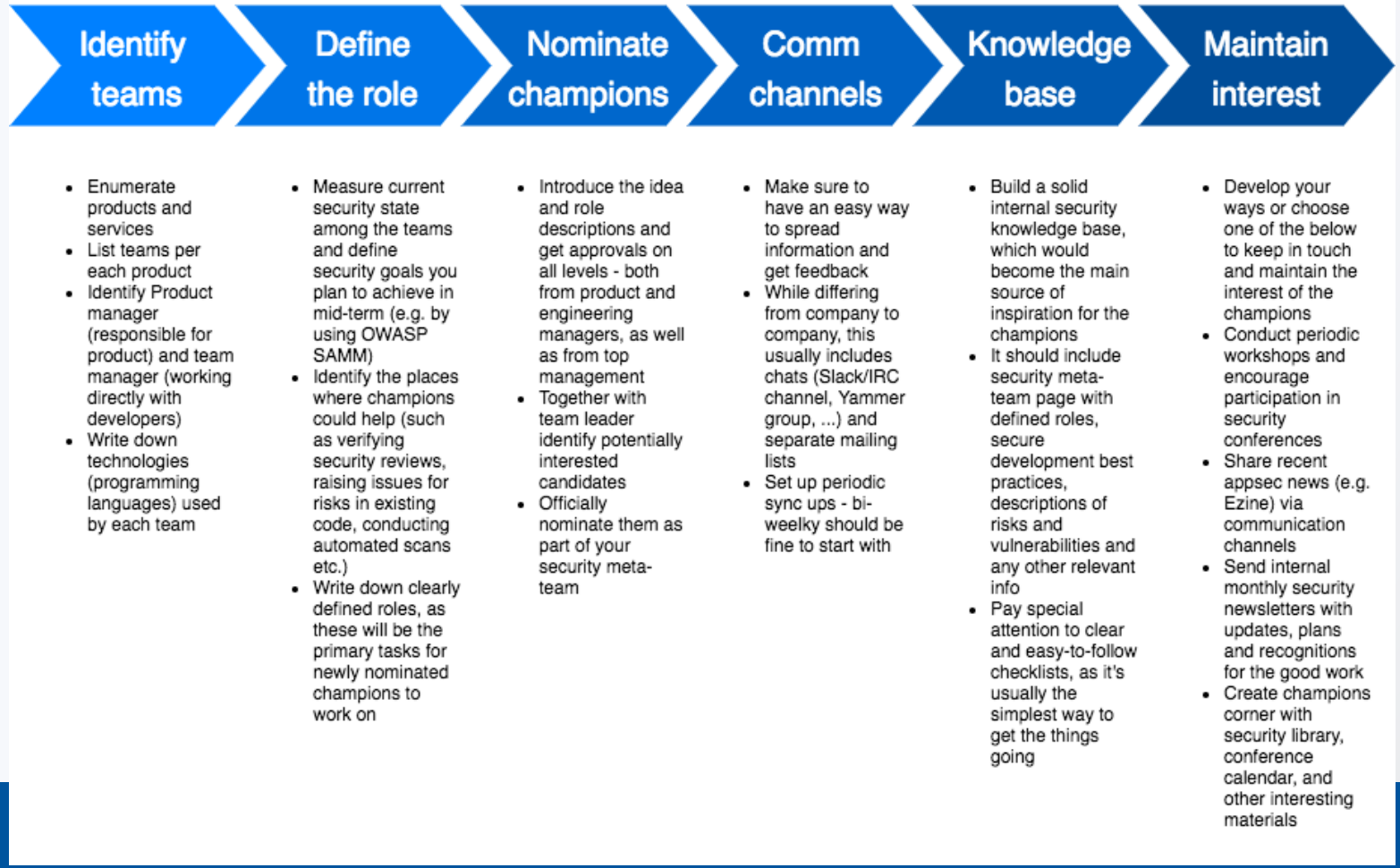


Culture Building

- Security Champions Playbook
- Security Culture

Security Champions Guide

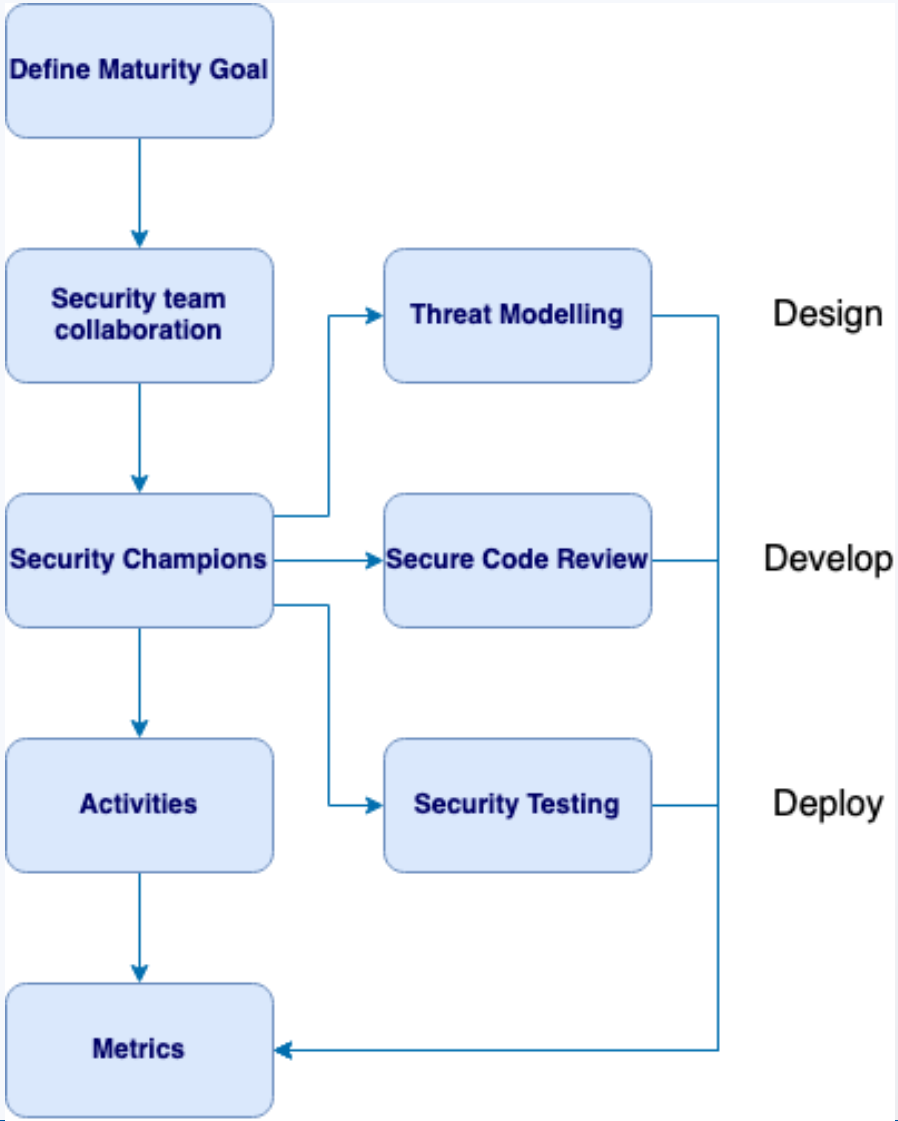
Incubator Project



(Legacy Artifact)

Security Culture

Incubator Project



Operation

- Core Rule Set (CRS)
- Coraza Web Application Firewall (WAF)

Core Rule Set (CRS)

Flagship Project

- Set of generic attack detection rules for use with ModSecurity or compatible web application firewalls
- Sims to protect web applications from a wide range of attacks, including the OWASP Top Ten, with a minimum of false alerts.
- Provides protection against many common attack categories

OWASP CRS

THE 1ST LINE OF DEFENSE

Coraza Web Application Firewall (WAF)

Production Project

- golang enterprise-grade Web Application Firewall framework
  - Supports Modsecurity's seclang language
  - 100% compatible with OWASP CRS
- Enrich your web application's security with powerful rules that comprehensively enforce good cybersecurity behavior.

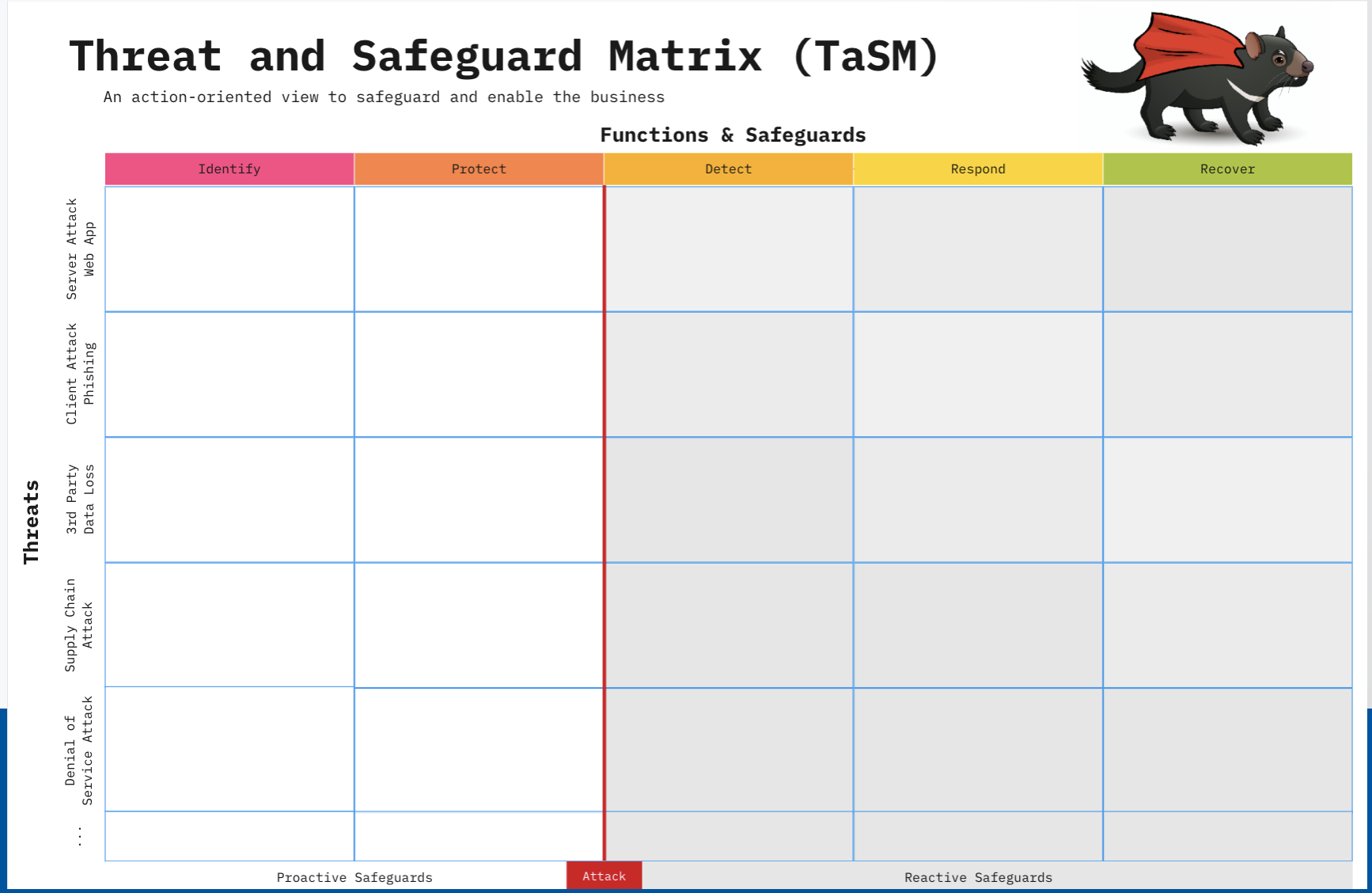
coraza
WEB APPLICATION FIREWALL

Requirements

- Application Security Verification Standard (ASVS)
- Threat and Safeguard Matrix (TaSM)
- Mobile Application Security – Verification Standard (MASVS)
- **SecurityRAT**

Threat and Safeguard Matrix (TaSM)

Incubator Project



SecurityRAT

Incubator Project

Security Requirement Automation Tool (SecurityRAT) focuses on automating the generation and management of security requirements

1. You specify the type of software artifact.
2. SecurityRAT tells you which requirements you should fulfill.
3. You decide how to handle those desired requirements.
4. You persist the artifact state in an issue tracker and create tickets for the requirements where an explicit action is necessary.
5. You document relevant changes in requirement compliance whenever appropriate.

Demo instance (usually) at https://securityrat.org

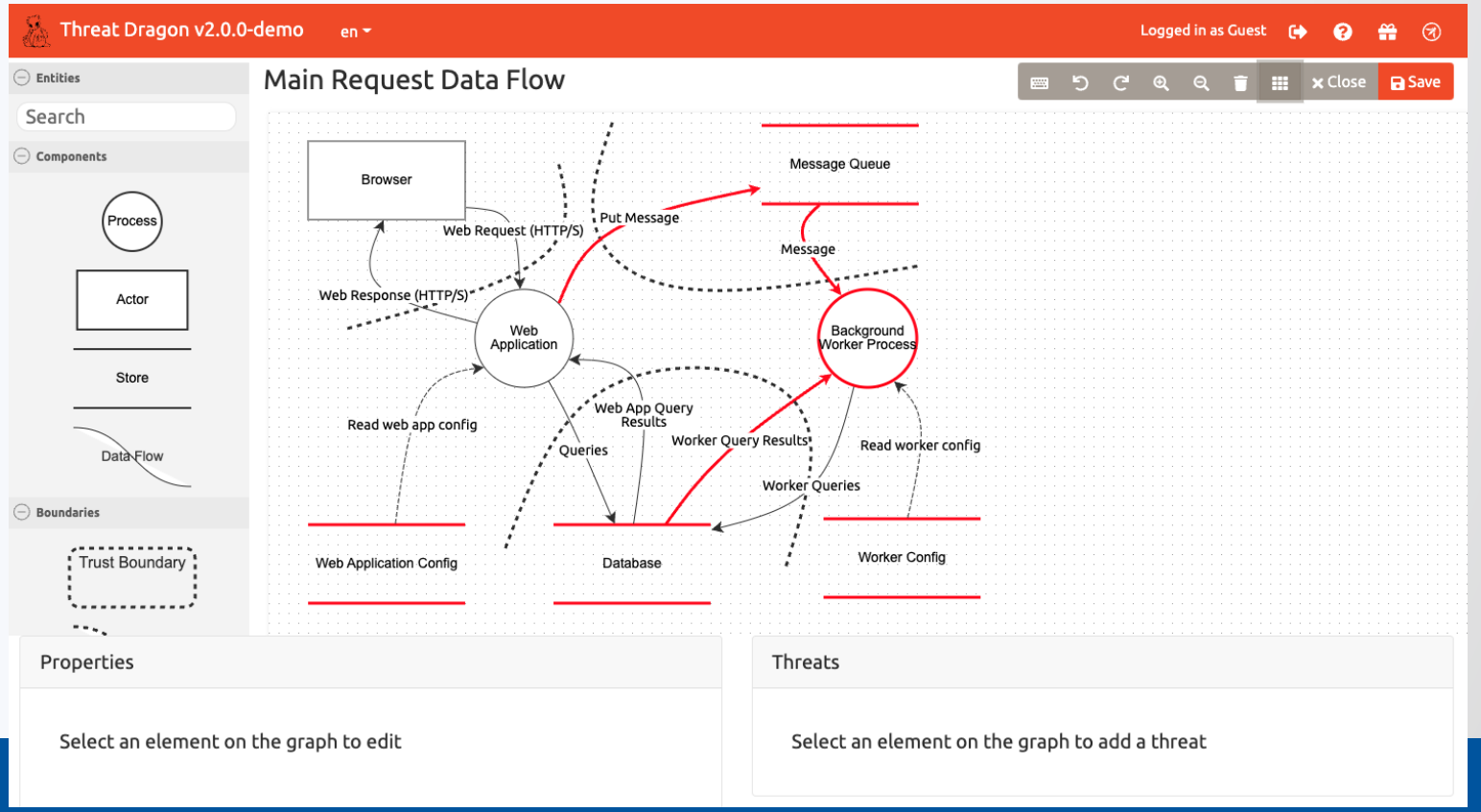
Design

- Cheat Sheet Series
- **Cornucopia**
- Ontology Driven Threat Modeling Framework (OdTM)
- **PyTM**
- **Threat Dragon**
- Threat Modeling Playbook (OTMP)

Threat Dragon

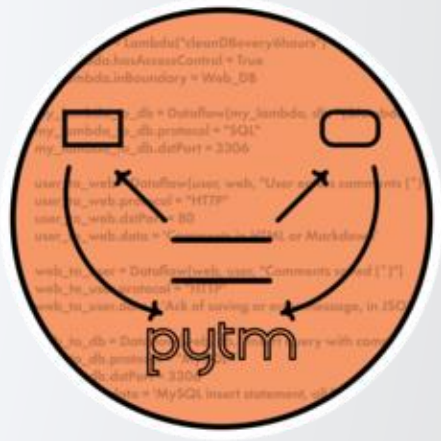
Lab Project

- Open-source threat model diagram creation tool
- Runs as desktop app or web app



PyTM

Lab Project



- A ‘Pythonic’ framework for threat modeling
- Define your system *in Python*, using the elements and properties described in the pytm framework
- Can generate Data Flow Diagram (DFD) or Sequence Diagram views of system and threats

Cornucopia – Website App Edition

Lab Project

- Card game to support secure coding design, similar to *Elevation of Privilege (EoP)*
- Based on Secure Code Practices (SCP) – Quick Reference Guide
- Six suits:
  - Data validation and encoding
  - Authentication
  - Session management
  - Authorization
  - Cryptography
  - Cornucopia
- Download card images and print locally
- Play online at: https://copi.securedelivery.io/

Cornucopia – Mobile App Edition

Lab Project

- Card game to support secure coding design, similar to *Elevation of Privilege (EoP)*
- Based on Secure Code Practices (SCP) – Quick Reference Guide
- Six suits:
  - Platform & Code
  - Authentication & Authorization
  - Network & Storage
  - Resilience
  - Cryptography
  - Cornucopia
- Download card images and print locally
- Play online at: https://copi.securedelivery.io/

Implementation

Documentation:

- **Proactive Controls**
- Go Secure Code Practices (SCP) Guide
- Cheat Sheet Series

Software Composition Analysis (SCA):

- Dependency-Check
- **Dependency-Track**

Libraries:

- Enhanced Security API (ESAPI)
- CSRFGuard

Proactive Controls for Developers

Lab Project

Describes the most important control and control categories that **every architect and developer** should absolutely, 100% include in every project

- C1: Define Security Requirements
- C2: Leverage Security Frameworks and Libraries
- C3: Secure Database Access
- C4: Encode and Escape Data
- C5: Validate All Inputs
- C6: Implement Digital Identity
- C7: Enforce Access Controls
- C8: Protect Data Everywhere
- C9: Implement Security Logging and Monitoring
- C10: Handle All Errors and Exceptions

Dependency-Track

Flagship Project

- Intelligent Supply Chain Component Analysis platform
- Leverages capabilities of Software Bill of Materials (SBOM)

Verification

Documentation:

- Web Security Testing Guide
- Mobile Security Testing Guide

Frameworks:

- Glue
- Dracon

Tools:

- Attack Surface Detector
- **Amass**
- **Code Pulse**
- Offensive Web Testing Framework (OWTF)
- Nettacker
- **DefectDojo**

Amass

Flagship Project

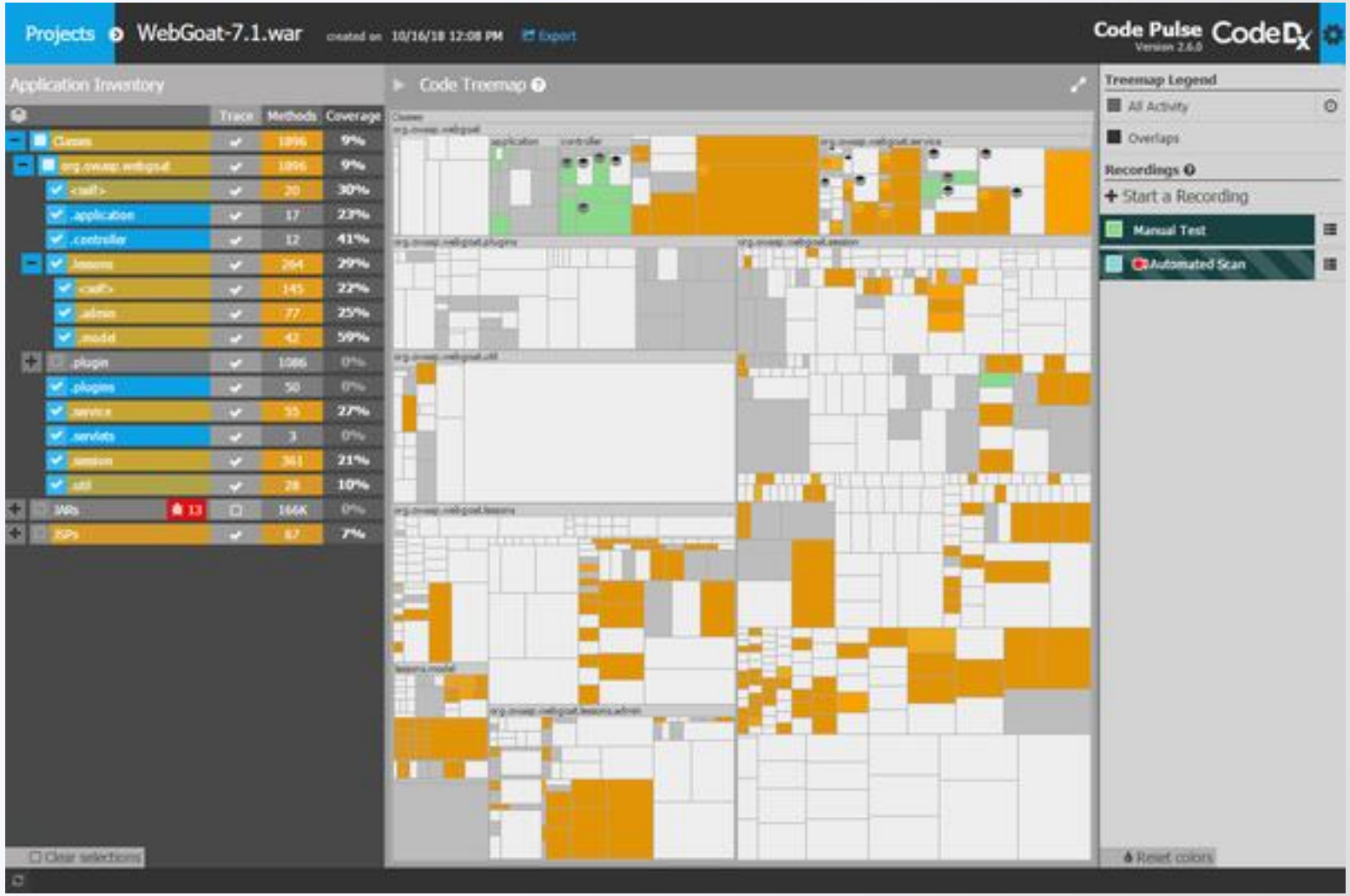
Our Goal - In-depth DNS Enumeration, Attack Surface Mapping and External Asset Discovery!

- Mapping of network attack surfaces
- External asset discovery
- Open-source information gathering and active reconnaissance techniques

Code Pulse

Lab Project

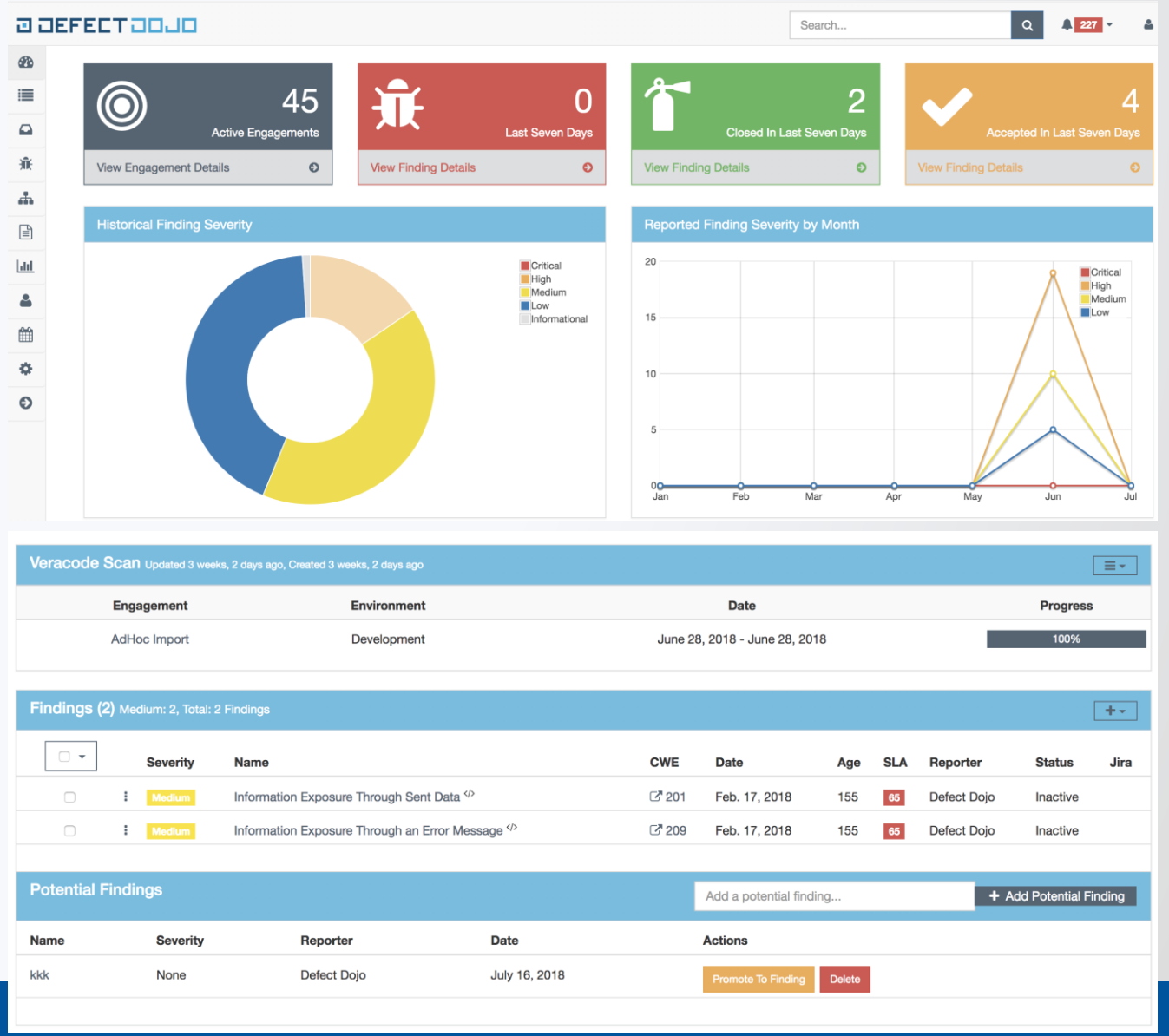
- Provides insight into the real-time code coverage of black box testing activities
- Cross-platform desktop application
- Agent-based runtime monitoring



DefectDojo

Flagship Project

- Open-source vulnerability management tool
- Streamlines the testing process
  - Templating
  - Report generation
  - Metrics



Some Closing Thoughts

- Don’t oversell – “free” tools aren’t *really* free
  - Be honest and realistic about total cost of ownership: instance charges, admin hours, etc.
- Use the right tool for your use case
  - When the OWASP tool isn’t the right one, it can still provide a cost-effective proof-of-concept
- Don’t be too proud to ask for help
  - OWASP community
  - Local AppSec community
  - Internal Security Team (if you have one)
  - External consultants and trainers

Resources

- OWASP: https://owasp.org
- OWASP Integration Standards Project: https://owasp.org/www-project-integration-standards/
- OWASP SAMM: https://owaspsamm.org/
- Security Champions Playbook: https://github.com/c0rdis/security-champions-playbook
- Join the OWASP Slack: https://owasp.org/slack/invite

Questions?

Connect / Reach out

- Email:
  - Day job: *john.dileo@gallagher.com*
  - "Other job": *john.dileo@owasp.org*
- Twitter (rarely): *@gr4ybeard*
- LinkedIn: *john-dileo*
- OWASP Slack *https://owasp.org/slack/invite*

OWASP

NEW ZEALAND DAY 2024

owasp.org.nz