Baking Security In

An AppSec ‘Critical Path’ for Developers

John DiLeo (@gr4ybeard)

Gallagher Security and OWASP NZ

September 2025

Thank You to Our Sponsors and Hosts!

Without them, this conference couldn't happen.

About Me

- Past lives
  - LONG-time student (4.9 degrees)
  - Simulation developer / analyst
  - University lecturer
  - Web developer and architect (J2EE)
- Doing Application Security (AppSec) since 2014
- Moved to New Zealand in 2017

About My Day Job

Application Security Lead

- Lead Cybersecurity Services Team
- Threat Modelling Program
- Product Security Risk Management
- AppSec Maturity Uplift
- Cybersecurity & Privacy Impact Assessments (CPIAs)
- In-House AppSec Training
- AppSec Evangelist

About My *Other* 'Job'

Chapter Leader, OWASP New Zealand

- Hamilton Meetup
- Regional Training Days

Chair, OWASP New Zealand Day Conference, 2019-2025

OWASP SAMM Project – Core Team

Launched SAMMwise and State of AppSec Survey Projects

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

Software Assurance

- 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

OWASP SAMM

Software Assurance Maturity Model

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

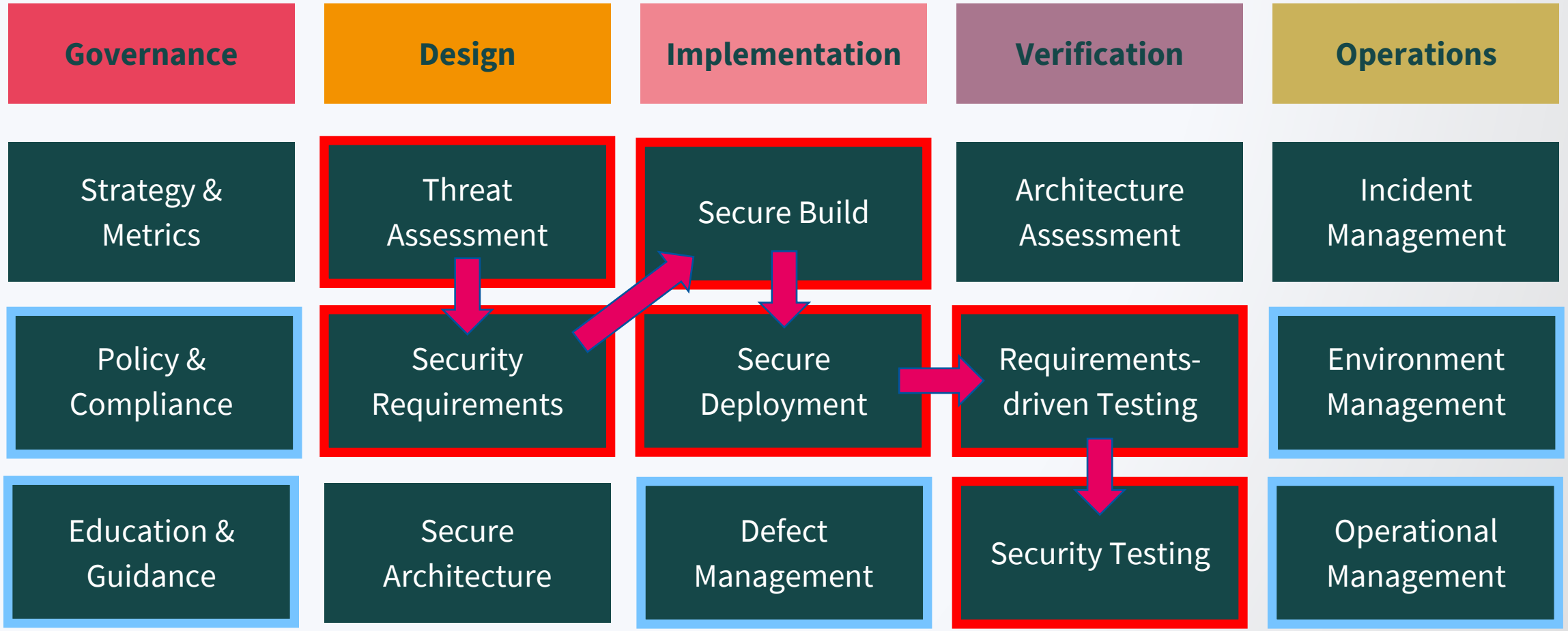
SAMM Structure

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

The “Critical Path”

SAMM Structure



Source: https://owaspsamm.org

Threat Assessment

Application Risk Profiles

Use standard risk profile instrument to understand risk of each application

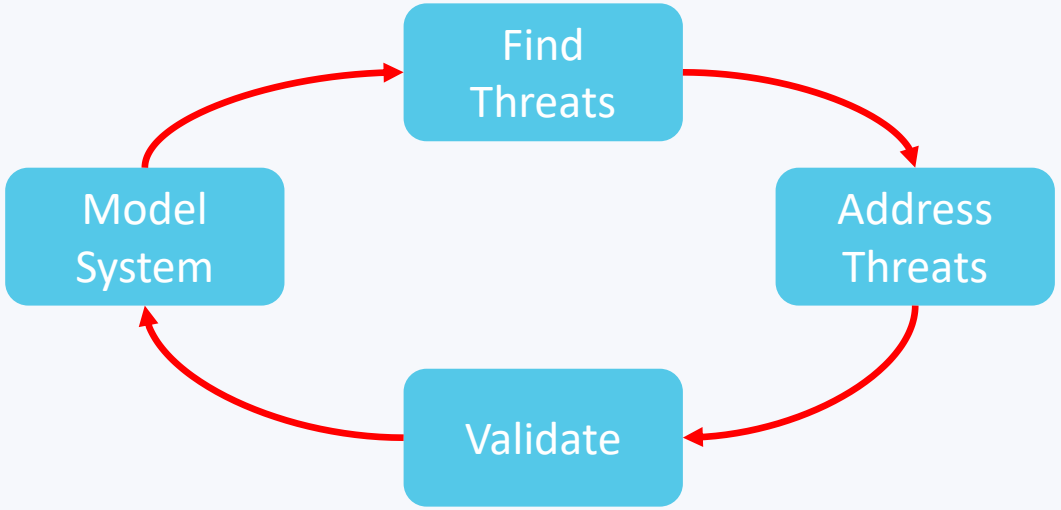
Cross-portfolio catalog / dashboard

Threat Modeling

Use consistent, repeatable technique to identify threats to applications, and capture mitigation approach

Threat Modelling

General Approach



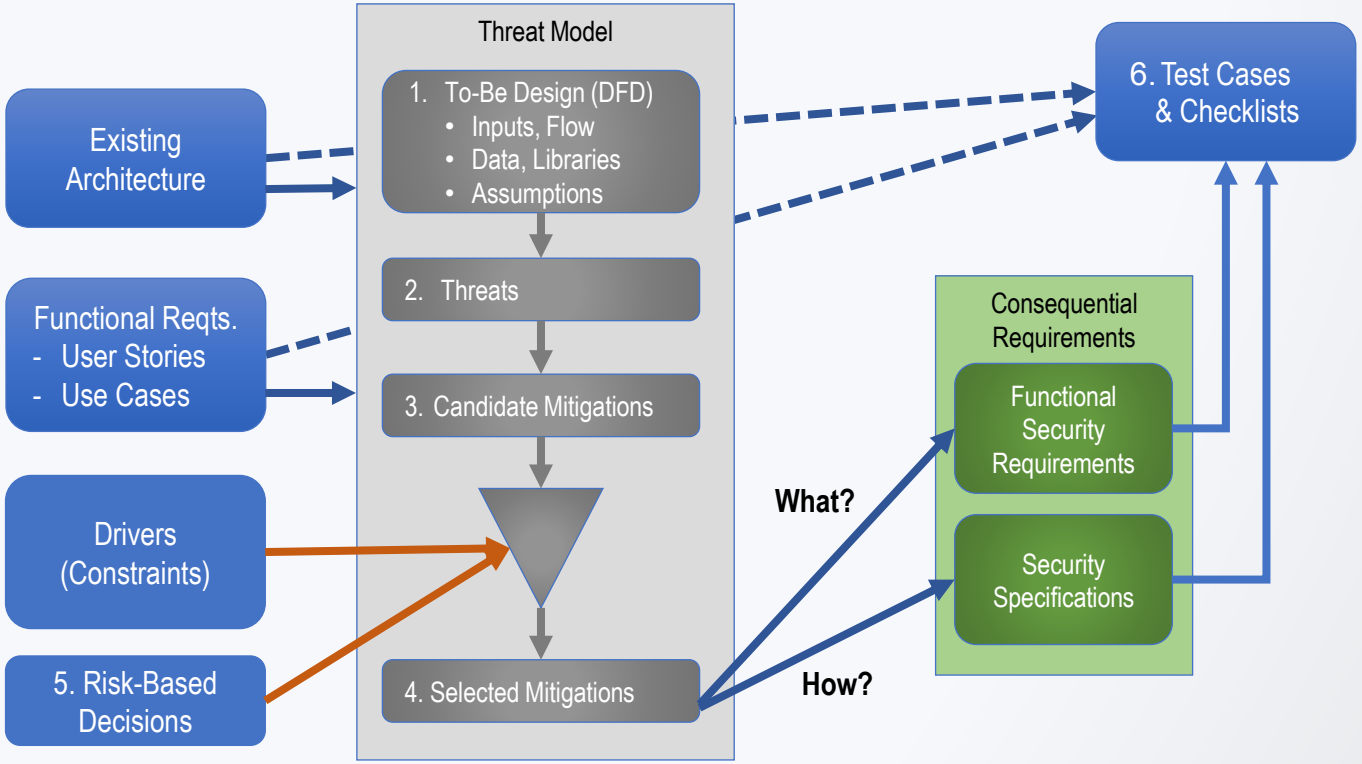
"DiLeo's Seven Questions"

Expanding on the classic "Four Questions" (Shostack)

1. What are we building? (Draw DFD)
2. What can go wrong? (STRIDE Analysis)
3. What *could* we do about it? (Identify)
4. What *will* we do about it? (Select)
5. Have all residual risks been accepted?
   - If 'no,' repeat #4 until 'yes.'
6. How will we know it works? (Verify)
7. Is our model correct? (Validate)

Threat Modeling

"Baked in" to the SDLC



Security Requirements

Software Requirements

Incorporate *consequential* ('yes, and…') security requirements into backlog, with links to features that depend on them

Supplier Security

- Supplier security assessment
- Security SLAs in agreements

Requirements-Driven Testing

Control Verification

- QA and regression test cases for functional security requirements
- Verification checklists/scripts for non-functional requirements

Misuse/Abuse Testing

- “Fuzz” testing, where relevant
- Extend QA and regression testing to “abuse cases”
- Security stress testing

Secure Build

Build Process

- Automated, repeatable builds
- Security *of* the build process
- Security testing in pipeline

Technology Management

Use Software Composition Analysis (SCA) to identify vulnerable/outdated library dependencies

Secure Deployment

Deployment Process

- Automated, repeatable deploys
- Secure processes
- Managed environment promotion

Secret Management

- Protect production secrets
- Automated secret deployment
- Managed refresh lifecycle

Security Testing

Automated Testing

Security *in* the build process

- Static App Security Testing (SAST)
- Dynamic App Security Testing (DAST)
- Dependency Analysis (SCA)

Penetration Testing

- Engage third-party testers to verify application's security posture
- Base frequency on application risk and compliance drivers

Key Artifacts

1. Application Risk Ratings
2. Threat Models
3. Security Test Cases
4. Verification Procedures
5. Risk Acceptances, as needed

The Five Pillars

Essential support from other Practices

Education and Guidance

Awareness and Training

- Basic awareness training for all
- Progressive, role-specific training program for developers and all adjacent roles
- Continual learning around secure development

Security Culture

- Security Champions program
- Software Security Group (SSG)
- Build software security culture

Operational Management

Data Protection

- Data catalogue
- Data Protection Policy
- Compliance monitoring

System Decommissioning / Legacy Management

- Retire unused systems
- Manage end-of-life for third-party and own-built components and app versions

Environment Management

Configuration Hardening

- Consistent hardening standards, “secure” images
- Active monitoring to detect non-conforming changes

Patching and Updating

- Regular patching
- Monitor information feeds for out-of-cycle patches

Defect Management

Defect Tracking

- Track security defects
- Tie remediation timelines to severity
- Integrate with other tooling

Metrics and Feedback

- Monitor defect patterns across the portfolio
- Prioritize initiatives to prevent common defects

Policy and Compliance

Policy and Standards

- Build comprehensive, “light” policy/standard framework
- Measure and monitor program/project compliance

Compliance Management

- Understand all relevant compliance drivers
- Align policies, processes, etc., to “result in” full compliance

What about the other SAMM Practices?

If only we had more time…

Questions?

Connect / Reach out

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

OWASP NEW ZEALAND DAY 2025

owasp.org.nz