

Unlocking the Power of Security Culture

A Journey Beyond Shifting Left

About Me



- Cyber Security professional with 10+ years of experience.
- 3A (Api, Applications, AI) Security Lead at SPH Media Ltd, Singapore.
- Interested in learning and giving back to the community.

 [Gowtham Sundar](#)

 [@gowsundar](#)

Before We Begin

- Share knowledge and experience.
- ~~Deep dive of tools or product.~~
- Not an endorsement of any company or feature.

Assumptions:

- Dedicated Security Teams
- Established process for Security (Tools, Automations).

A Short Story...



Source: [LinkedIn](#)



Key Approaches

- Tools and Automations
 - Security Dashboards
 - Maturity Models and Scorecards
- Security Partnerships
 - Security Champions
 - Empowering QA Teams
- Measuring Success
 - Metrics & KPIs
- Bonus - Quick Wins

Security Dashboards

- Holistic View of Security Posture.
- Highlights Top Identified Risks.
 - Top 5 or Top 10)
- Effective Tracking and Remediation.

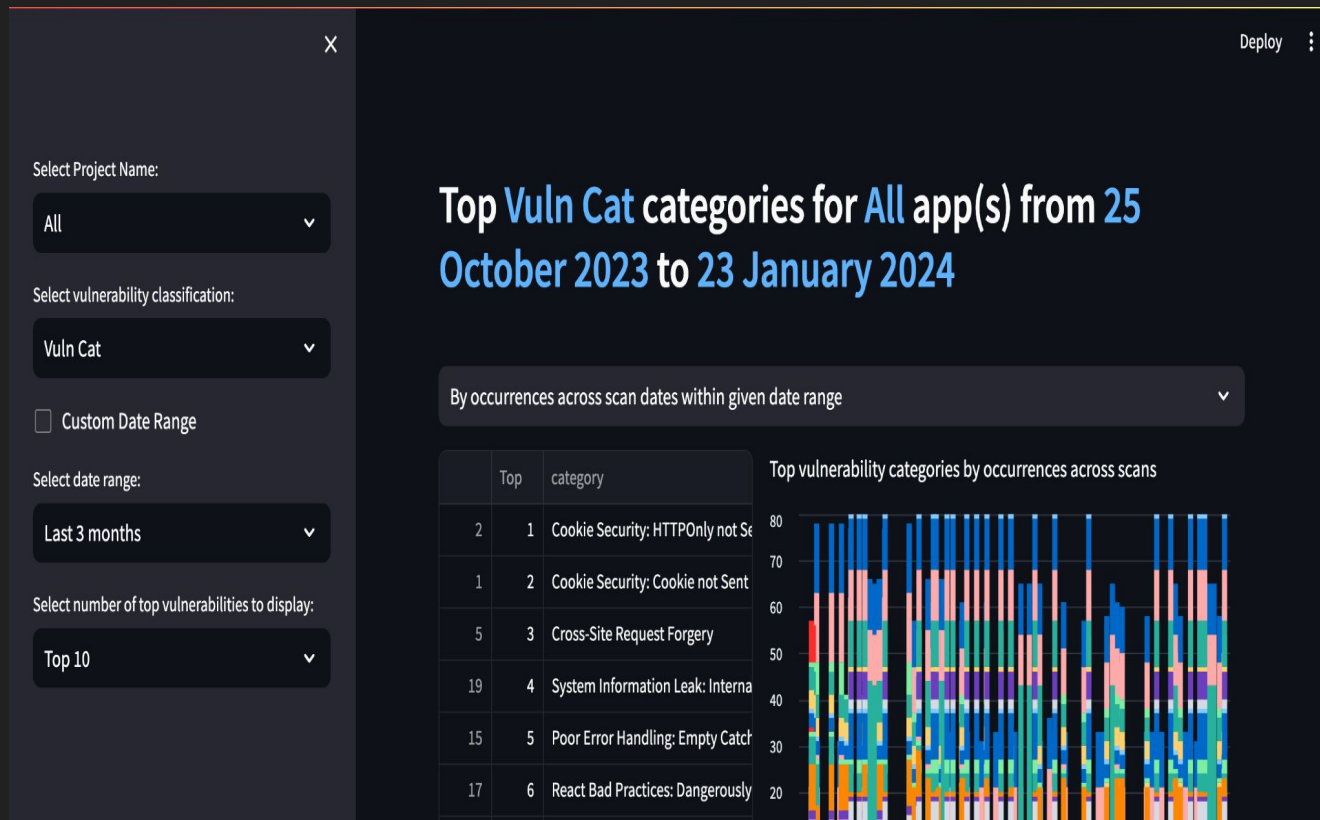
Examples:

- Total # of vulnerabilities identified in past 'N' days.
- # of vulnerabilities breached SLA.
- # of vulnerabilities based on Severity.



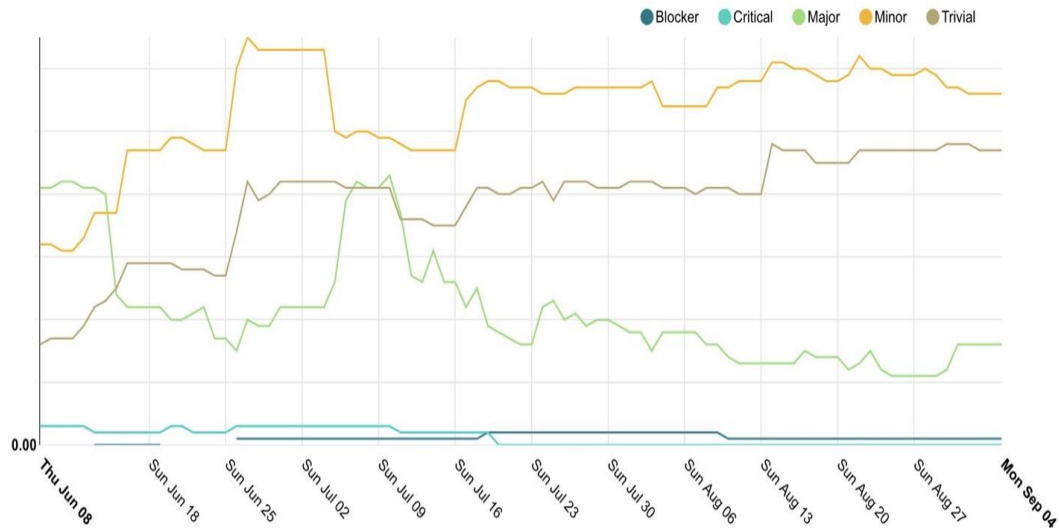
Source: Bing AI

Security Dashboards – Quick Look

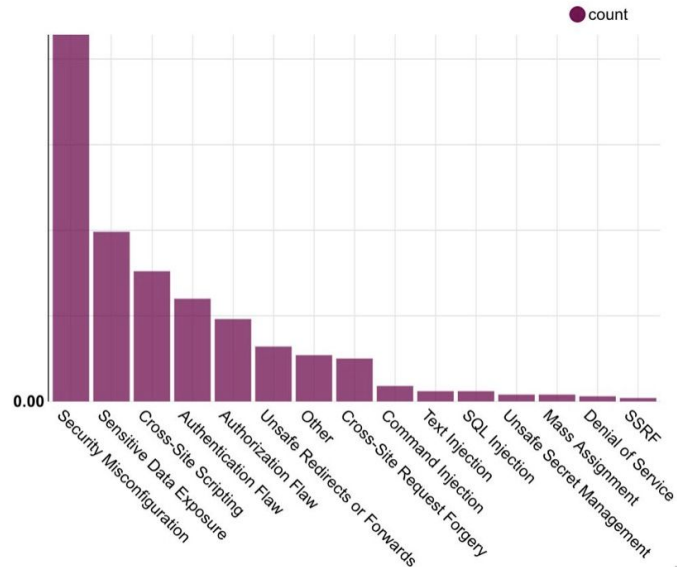


Security Dashboards - Quick Look

Open Security Vulns (by priority, last 90 days)



Vulnerability Categories (All Time)



Source: [Data Driven Bug Bounty\(Airbnb\)](#)
[\(tldrsec.com\)](#)

Security Dashboards – Success Factors

- Make dashboards accessible to **every engineering teams**.
- Walkthrough during **planning** and **grooming** meetings.
- Keep the dashboard **up-to-date**.
- Send regular **notifications** and statuses (SlackBots, Emails, etc,.).
- Feed in **multiple sources**.

Security Dashboards – Case Study

Security Dashboards

Security Dashboards are used to assess the security posture of your applications. GitLab provides you with a collection of metrics, ratings, and charts for the vulnerabilities detected by the [security scanners](#) run on your project. The security dashboard provides data such as:

- Vulnerability trends over a 30, 60, or 90-day time-frame for all projects in a group
- A letter grade rating for each project based on vulnerability severity
- The total number of vulnerabilities detected within the last 365 days including their severity

The data provided by the Security Dashboards can be used supply to insight on what decisions can be made to improve your security posture. For example, using the 365 day trend view, you can see on which days a significant number of vulnerabilities were introduced. Then you can examine the code changes performed on those particular days in order perform a root-cause analysis to create better policies for preventing the introduction of vulnerabilities in the future.

 For an overview, see [Security Dashboard](#) .

Source: [Gitlab Security](#)

Story Continues..







Maturity Models and Scorecards

- Comprehensive evaluation across multiple domains.
- Roadmap for Continuous Improvement.
- Facilitates executive buy-in for investments.
- Long Term view and growth.
- Driving Organizational Change.
- Benchmarking and Compliance.

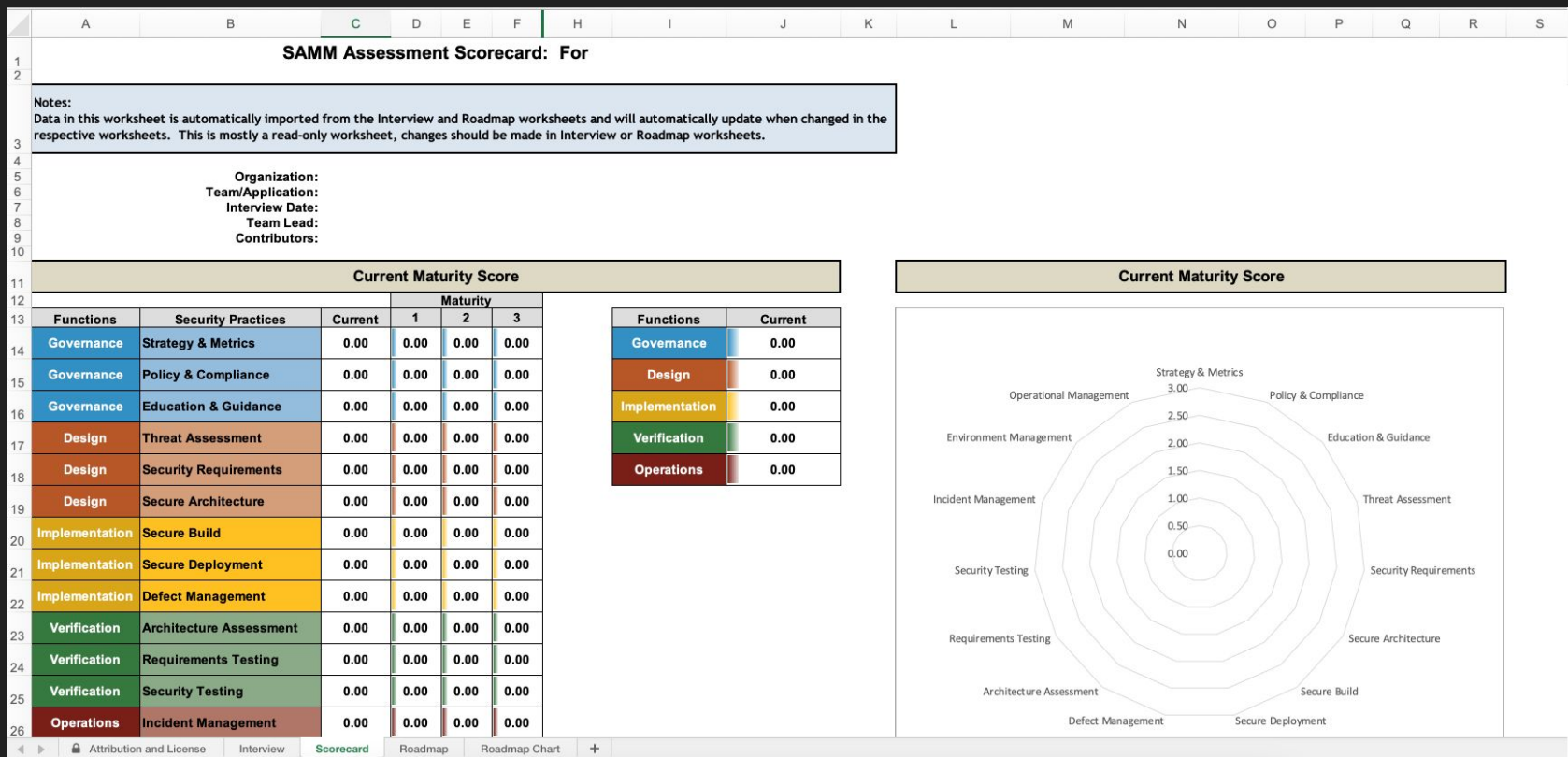
Maturity Models – References

- OWASP [SAMM](#) (Software Assurance Maturity Model)(Open Source)
- [Cybersecurity Maturity Model Certification \(CMMC\)](#) by US DoD.
- [Building Security In Maturity Model \(BSIMM\)](#) by Synopsys (proprietary model)
- [OWASP SBOM Maturity Model](#)
- [COMPARING BSIMM & SAMM](#)

Custom Maturity Model – Quick Look

Maturity Level	Category	Criteria	Score	
Level 1	Shift Security Left	Implement Security Tools in CI / CD	10	
	Training	Attend Security training and workshops	30	
	Compliance	Adherence to SLA > 75%	20	
Level 2	Shift Security Left	No Critical, High Vulnerabilities identified from security scanning	20	
	Training	Perform secure code reviews and adhere to guidelines	30	
	Compliance	Follow risk acceptance criteria	40	
Level 3	Shift Security Left	Break builds on Critical / High Findings	50	
	Training	Identified Security Champion	40	
	Compliance	Adherence to SLA > 90%	30	

SAMM Maturity Model v2.0 – Scorecard



Maturity Model – Success Factors

- Build your own maturity model levels to establish baseline security controls.
- Develop scorecarding techniques to achieve those maturity model levels.
- Use questionnaires, interviews, to identify gaps and establish controls.
- Work with product and engineering teams to achieve maturity levels.

Security Scorecards – Case Study

Security scorecards

We're focused on ensuring that security is front and center of mind across our entire product suite. To this end, we've implemented an accountability and monitoring system referred to as "product security scorecards" to measure the security posture of all products at Atlassian. This is an automated process Atlassian has created whereby we use a broad range of security-focused criteria (e.g. current vulnerabilities, training coverage, and recent security incidents) to provide an overall security score for each of our products.

This scoring process gives each of our product teams an objective view into what areas of security require attention, and identifies existing gaps that need to be addressed and actions to address these gaps. The security scorecards process also enables the Atlassian security team to easily keep track of how all products are tracking from a security perspective over time, particularly as our product suite continues to scale.

Source: [Atlassian's approach to security](#)

Story Continues..



Security Champions Program

- Dedicated **companions** for Security Teams.
- Help **Scale Security**.
- **Enablers** for security initiatives.
- **Catalysts** for cultural change.



Security Champions – Success Factors

- Identify the right stakeholders
- Define clear objectives
- Reward and Recognitions
- Continuous Feedback
- Mentoring



References:

- [Security Champion Program Success Guide](#)
- [OWASP Security Champions Guide](#)
- [Security Champions Playbook](#)

Security Champions – Case Study



[OWASP Top 10 Maturity Categories for Security Champions](#) [Lucian Corlan & Gareth Dixon](#) - Video

[Github Repo](#)

Story Continues..

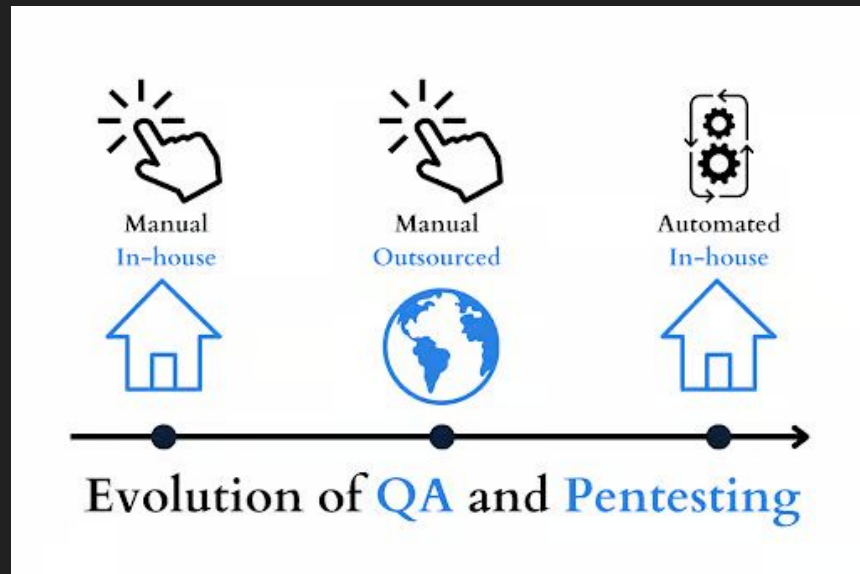
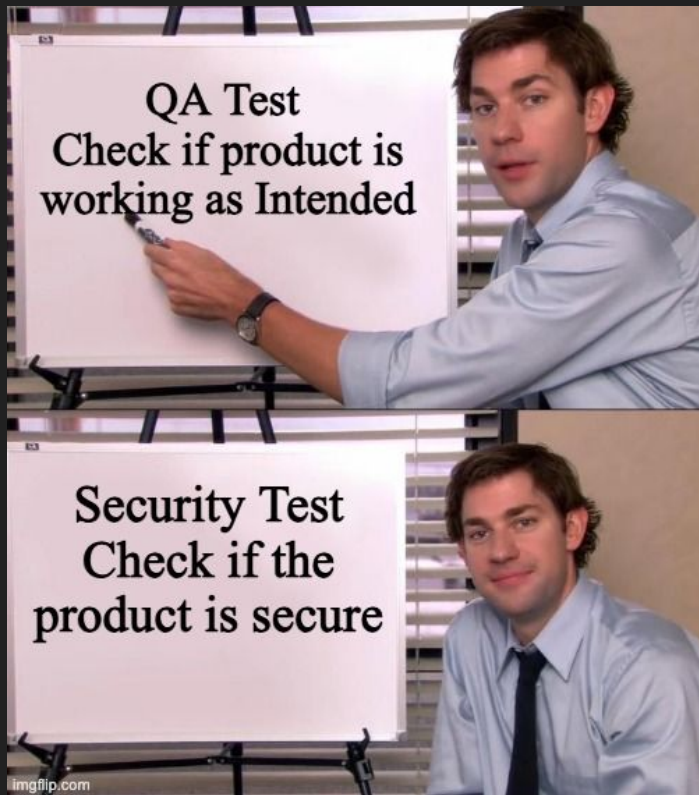


Empowering Quality Assurance Teams

Do you think QA Teams can perform Security tests ??



QA Vs Security Testing – Key Difference



Source: tldrsec.com

QA Vs Security Testing - Use Case

Test case for Insecure Direct Object Reference (IDOR)

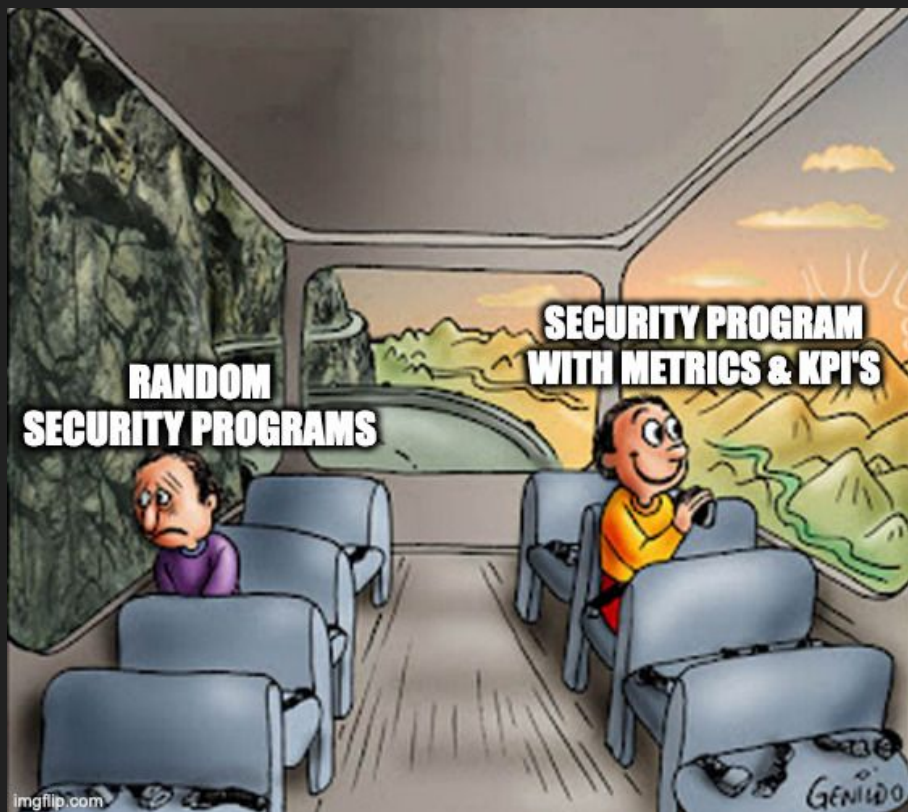
Category	Test Case ID	Test Case Description	Test Steps	Expected Output	Actual Output	Evidence	Pass / Fail
QA Test Case	TC - 01	Verify the user is able to access his profile page.	1. Login to the application with valid credentials. 2. Navigate to the profile page from settings menu.	User profile page should be displayed.			
Security Test Case	SEC - 01	Verify the user is able to access another user profile page.	1. Login to the application with valid credentials. 2. Navigate to the profile page from settings menu. 3. Modify the URL to change the "id" parameter of other user Example: owasp.com/user/profile?id={5200}	Other user profile should not be displayed unless the current user is authorized.			

Focus: Cross Site Scripting, Injection and Sensitive Information Disclosure, etc.,
Tools: Browser extensions - [Wappalyzer](#) , [Trufflehog](#).

Security Training – Success Factors

- Conduct **bespoke training** (based on Top 5 or Top 10).
- Create security test cases and include as part of their test plan / suite.
- Target **low hanging fruits** and most occurring vulnerabilities.
- Leverage **automations** to reduce time and effort.
- Target Instructor-led training sessions.
- Rewards and Recognition.

Story Continues..

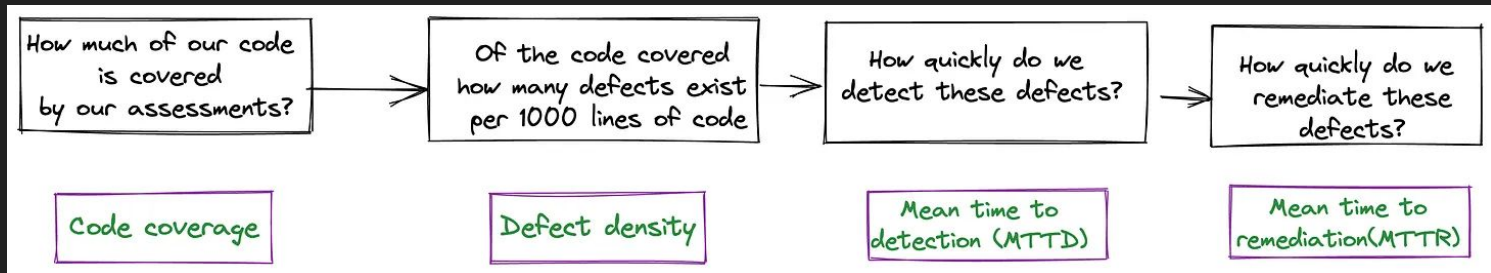


Measuring Success – Metrics & KPIs

- To determine effectiveness & progress of a program.
- Know your strength & weakness.
- Compliance and Accountability.

Measuring Success – Key Metrics (not limited to)

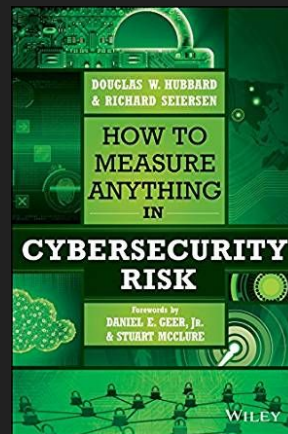
- Mean-time to Remediate (MTTR)
- Defect Density
- Training Effectiveness
- Debt Ratio
- Code / Testing Coverage



source: boringappsec.com

Metrics & KPIs – References

- [Measuring What Matters in Application Security | by James Chiappetta | better appsec](#)
- [Top 4 AppSec metrics and why they are so hard to measure](#)
- [Building Effective Security OKRs](#)

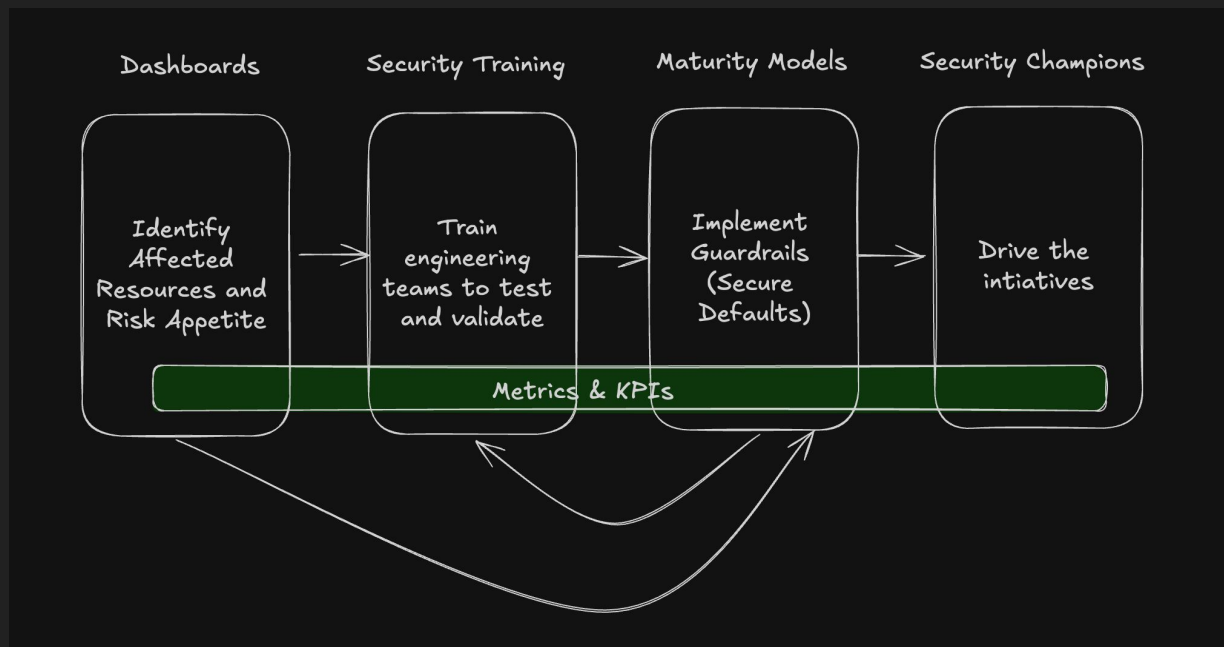


Bonus – Quick Wins

- Security Tech Talks
 - Conduct sessions to walkthrough bug bounty findings & incidents.
- Security Newsletter / Updates
- Hackathons / CTF's
- Cheat Sheet / Infographics
- Simulation Exercises



The Interlock



Dashboards are used to track Cross Site Scripting as the most common vulnerability, train engineering (QA) teams for continuous testing, and adopt Content Security Policy, driven by Security Champions who lead the effort in the engineering teams.

End of Story.



Security is everyone's responsibility.
Lead security with resilience.

Questions ??

Feedbacks ??



Linkedin QR Code

