Maturing Your AppSec Program

Tanya Janca

Semgrep

SheHacksPurple

What are we going to talk about today?

Common AppSec Models

What are we going to talk about today?

Why They Fail

What are we going to talk about today?

How to do better

How I conducted my research

Tanya Janca

- Head of Community at Semgrep
- AKA @SheHacksPurple
- Author: Alice and Bob Learn Secure Coding & Alice and Bob Learn Application Security
- 28+ years in tech, Sec + Dev
- Founder: We Hack Purple, OWASP DevSlop, #CyberMentoringMonday, WoSEC
- Advisor: Katilyst
- Faculty: IANs Research

Let’s Talk *Maturity*

Application Security Models

OWASP SAMM

BSIM

NIST

Onto the models!

Note: Spot the AI *weirdness* in the images!

Model 1:
Just PenTest The Important Stuff

Extremely common

Everyone doing their own thing

No formal SDLC

Mixed Tech Stack

Code all over the place

Why this model is bad

How to Mature Model 1

1. Secure Coding Training

How to Mature Model 1

2. No Budget Plan

1. Use a free tools like Zap or Burp for DAST, and Semgrep OSS, Brakeman, Bandit, Find Bugs, for SAST
2. Create a secure coding guideline
3. Create a list of security requirements for all new projects
4. Consolidate your code, scan it!
5. Push for a real SDLC, centralization, and standardization

How to Mature Model 1

2. No Budget Plan

6. Threat model your super important app(s)
7. Share information on past incidents
8. Scan your codebase for secrets
9. Put a free WAF in front of *terrible* apps
10. You still PenTest the important apps, but now the results don’t embarrass you!

How to Mature Model 1

3. If you have Budget

3.1 Hire an AppSec Person

3.2 Paid next-gen SAST

3.3 Continue with free-ish DAST

All of Step 2 (the no budget plan)

Model 2:
Tools, tools, and more tools

The Most Common Model

Partially rolled out tools

Inconsistent program

Little-to-no documentation

SAST + DAST

Lots of bug reports,

but few fixed bugs

“Why won’t the developers fix the bugs?”

why this model is bad

How to Mature Model 2

1. Do all the stuff from the previous Maturity model.

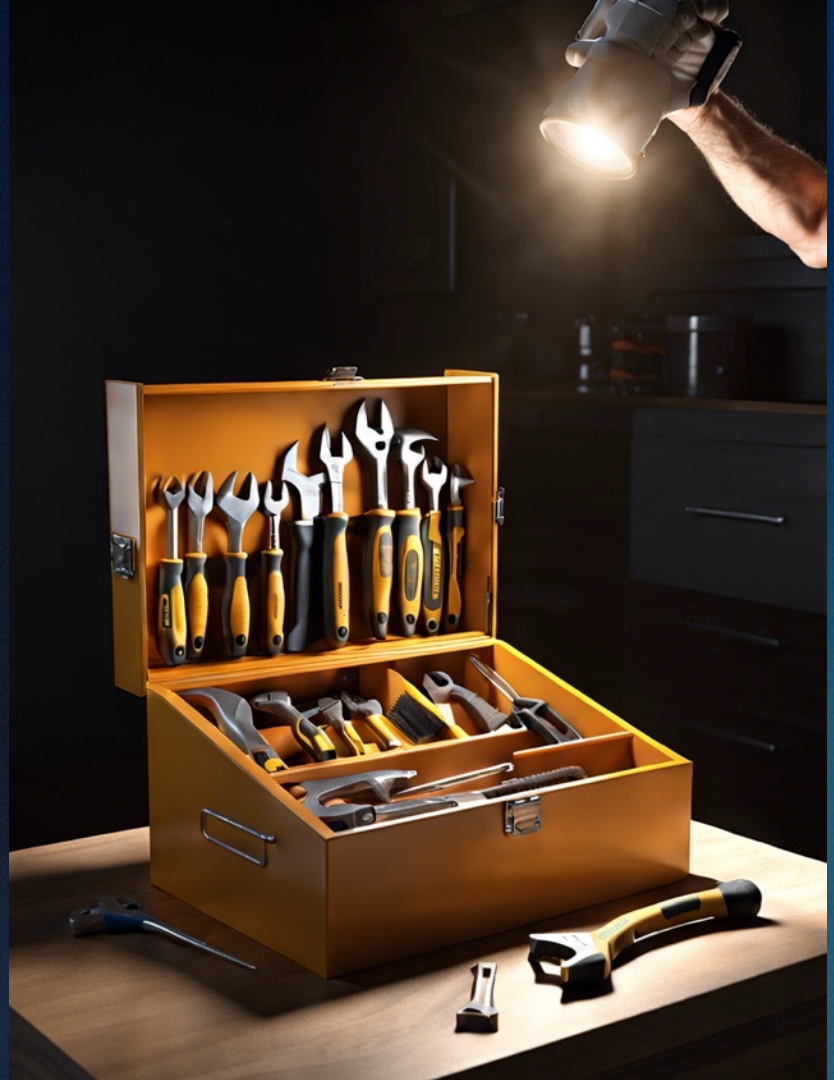
How to Mature Model 2

2. Hire more AppSec folks

Semgrep

How to Mature Model 2

3. Reassess Your Tools



How to Mature Model 2

4. Ensure your Rollout is Complete

How to Mature Model 2

5. Provide Advice and Support

How to Mature Model 2

6. Start to Manage Incidents, Properly

6.1 Create a way to report incidents

6.2 Incident Training for Devs

6.3 Incident Response Process

Semgrep

Model 3:
Strangle Hold + Giant Spend

ALL THE TOOLS

GIANT SPEND

Constant friction

No interaction between Dev and Sec

Security Posture Not Satisfying

Strangle hold governance

Why this model is bad

How to Mature Model 3

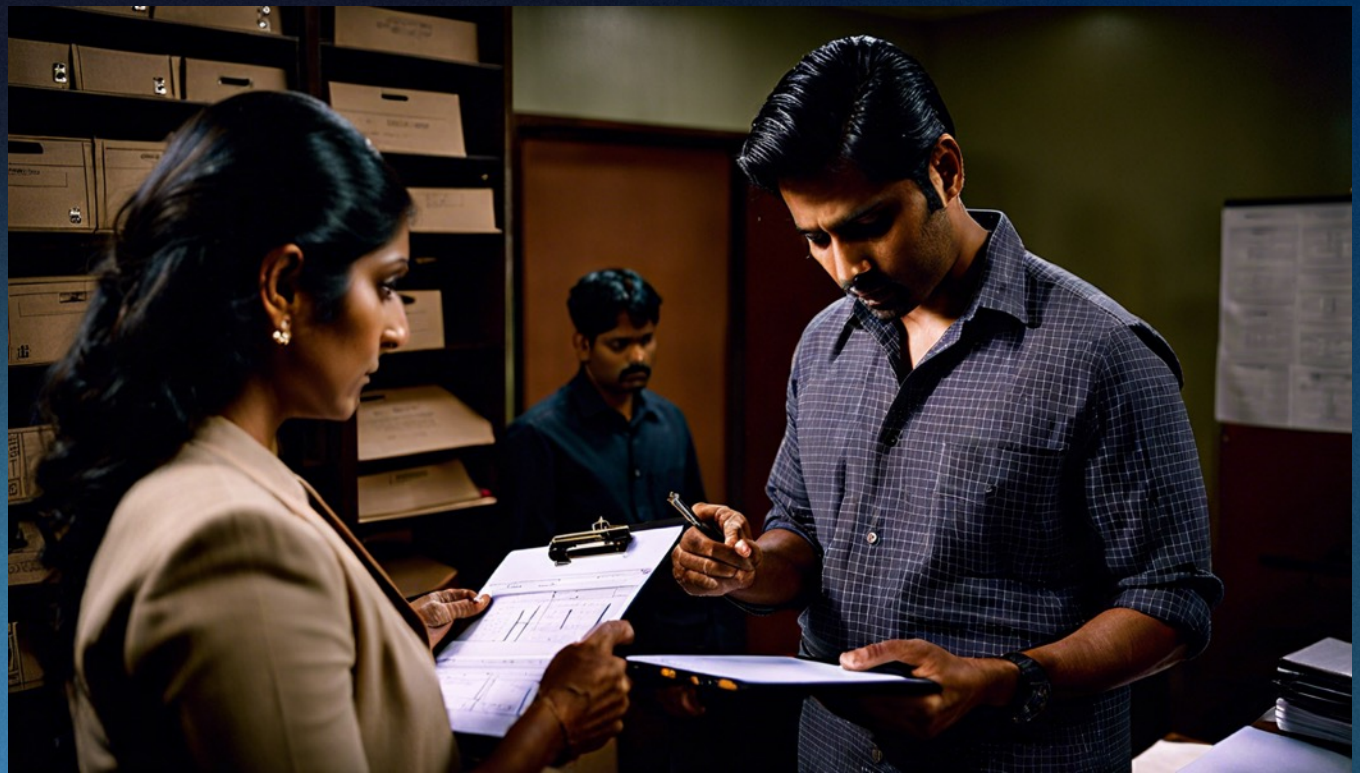
1. Scale with more AppSec or Champs

How to Mature Model 3

2. If not champs, use advocacy

How to Mature Model 3

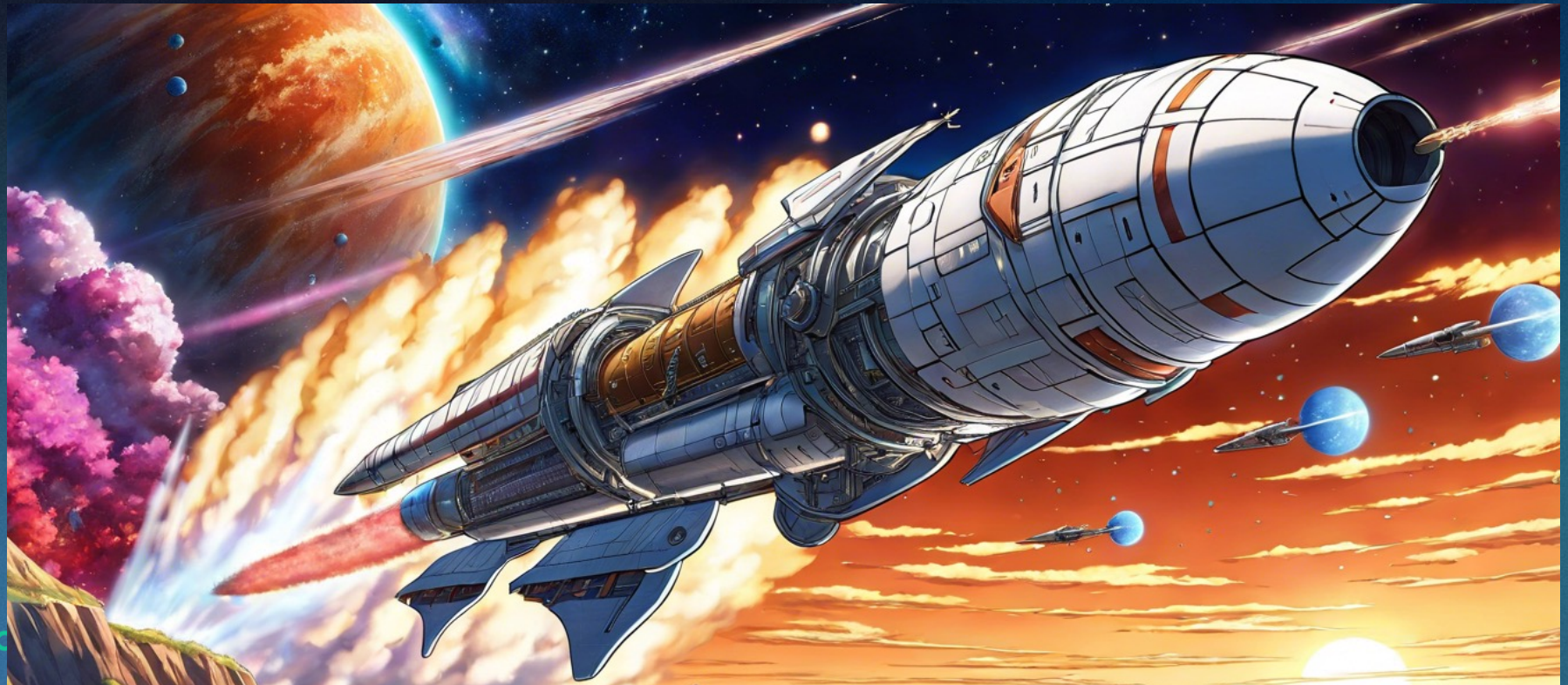
3. Make it a standard



Semgrep

How to Mature Model 3

4. Make your tools go fast!



How to Mature Model 3

5. Examine your APIs

Semgrep

How to Mature Model 3

6. Embrace Threat Modelling

How to Mature Model 3

7. Company-wide Secret Management

Semgrep

How to Mature Model 3

8. Continuous Scanning

Semgrep

How to Mature Model 3

9. Training that Doesn’t Suck

How to Mature Model 3

10. WAF -> RASP or IAST

How to Mature Model 3

11. AppSec Incident Response

How to Mature Model 3

12. Data Driven Approach

Conclusion

We Learned:

- 3 common AppSec Program Models
- How to identify the models
- How to mature the models
- How to build an awesome AppSec Program!

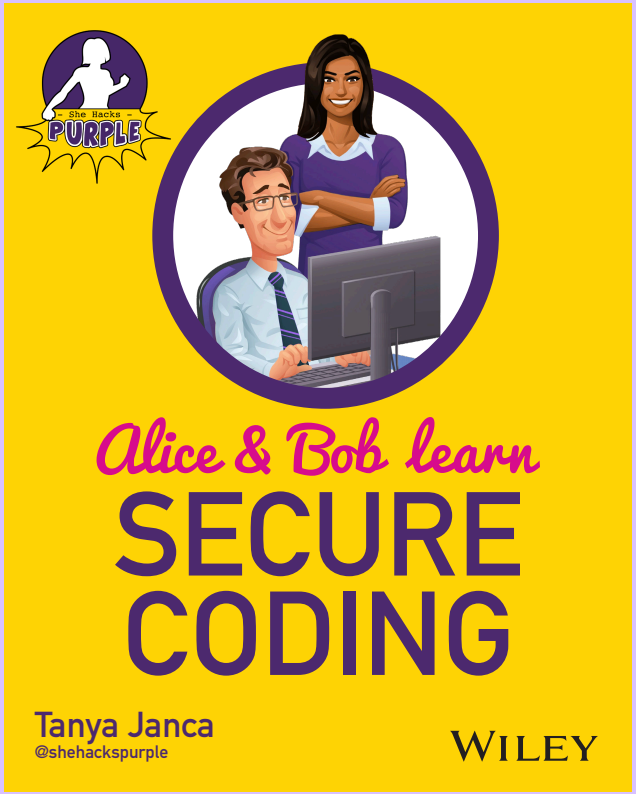
Resources

Semgrep Academy!

https://academy.semgrep.dev/

Learn something new, for free!

My books!



https://aliceandboblearn.com

#CyberMentoringMonday

Every Monday

tl;dr sec

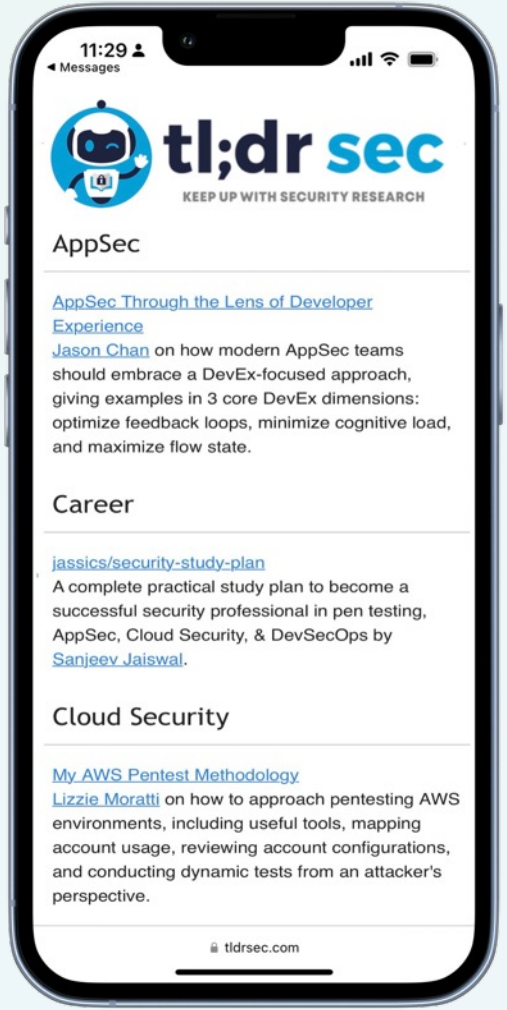
Keep up with security research

The best security tools, talks, and resources in your inbox every week.

Join 50,000+ hackers and CISOs from Google, Microsoft, AWS...

"Absolute gold."
Caleb Sima, ex CSO Robinhood

"I love tl;dr sec."
Jason Chan, ex VP, Netflix



Resources: Meeeeeeeee!

@SheHacksPurple

Twitter/TikTok/Mastodon/GitHub/Instagram/etc.

YouTube.com/SheHacksPurple

https://SheHacksPurple.ca

https:// SheHacksPurple.ca/blog

https://Newsletter.SheHacksPurple.ca

Tanya Janca
Community @ Semgrep
SheHacksPurple.ca