Scrum for Security

Organising effective security teams

SecTalks SYD0x59

Hi!  I’m Bill.

Acknowledgement of Country

I'd like to acknowledge that we are meeting on the traditional lands of the Gadigal people of the Eora nation. I pay my respects to Elders past, present and emerging, and celebrate the diversity of Aboriginal peoples and their ongoing cultures and connections to the lands and waters of NSW.

I also acknowledge and pay my respects to our Aboriginal or Torres Strait Islander people joining us this evening.

A bit about me…

- Over 15 years in Cyber
- Blue team all the way, mainly DFIR and Detection Engineering
- Moved into management about 8 years ago
- Have used scrum (in some form) in every one of these teams*


linkedin.com/in/bill-mahony-7651866


github.com/gyrospectre


medium.com/@v22bis

*Opinions are solely my own and do not express the views or opinions of my current or previous employers.

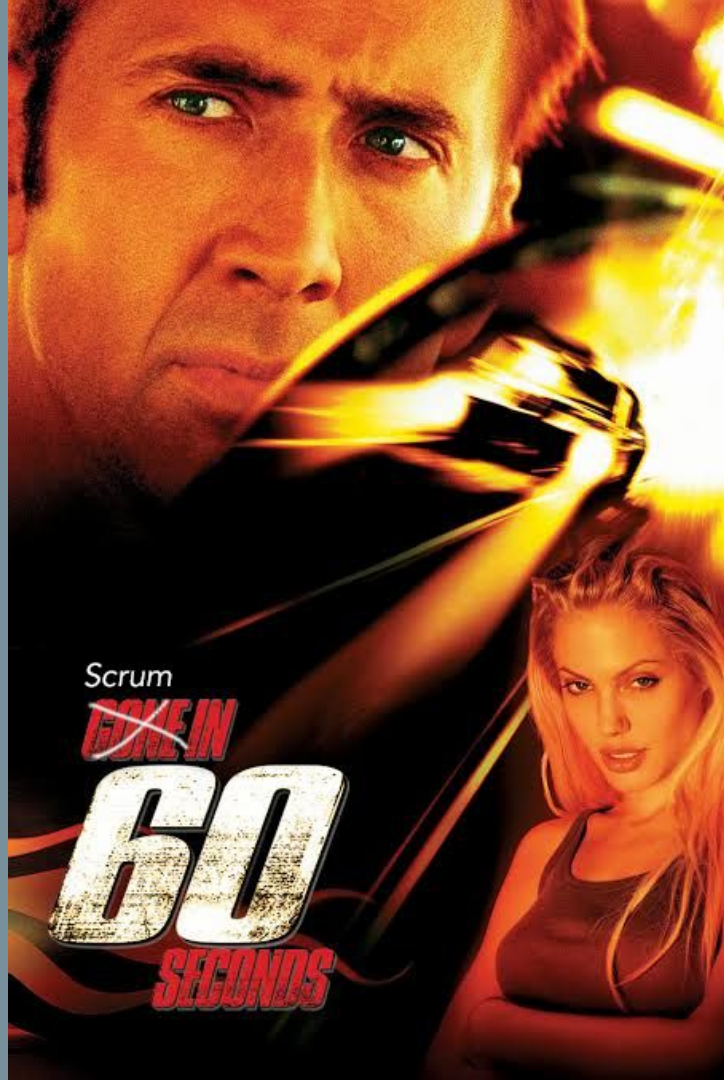
The agenda for tonight

- What is scrum and why do you care? Isn't it just for software engineers?
- Why would I consider it for my team?
- How would scrum even work for a security team?
- Some tips (informed by my past mistakes)
- Questions

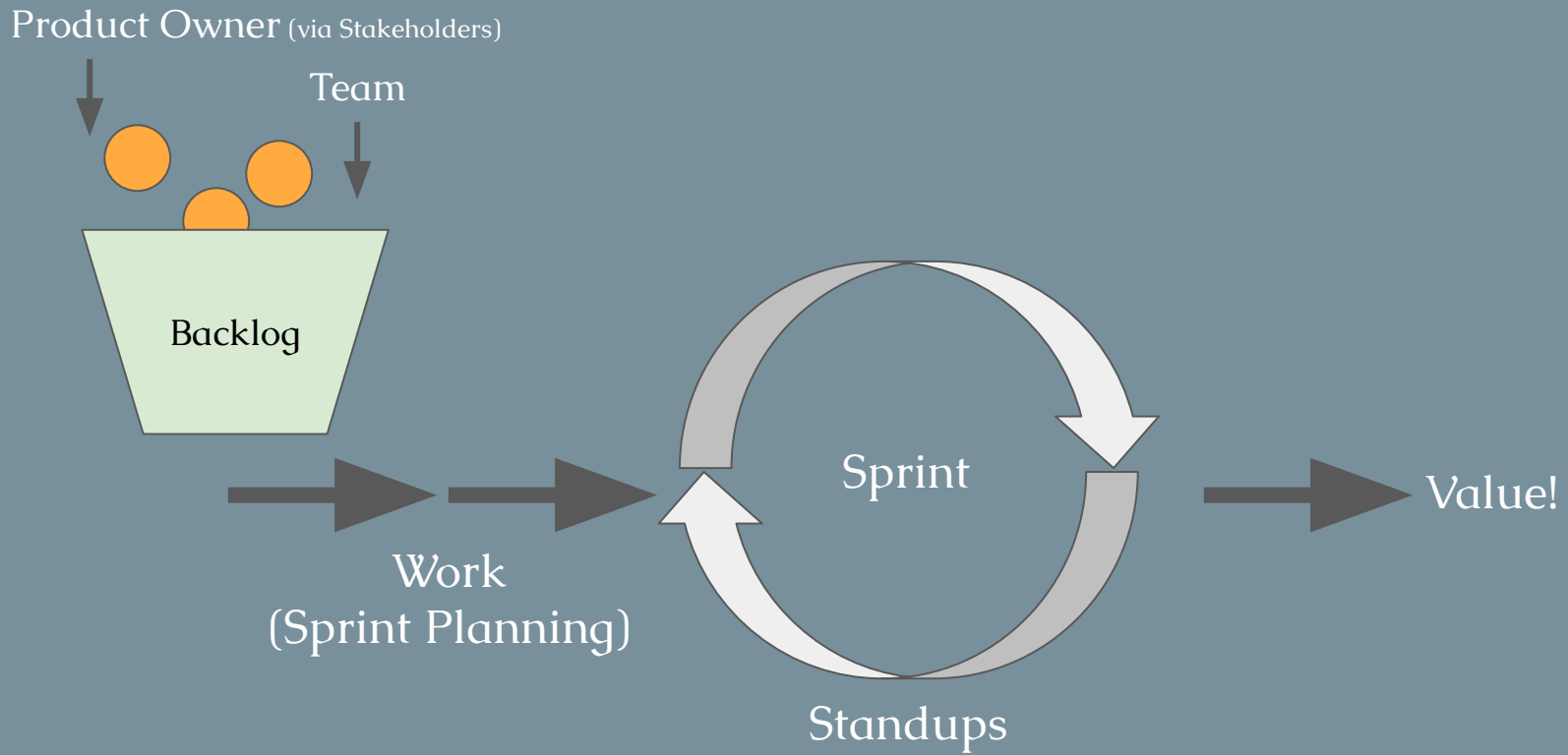
What is Scrum?

- A lightweight team organisation framework for solving complex problems.
- Empirical and iterative, evidence based
- Ordering of work into a Backlog
- Team turns a selection of this work into an Increment of value
- Inspect the results and adjust for the next Sprint
- Repeat!

https://www.atlassian.com/agile/scrum
https://scrumguides.org/scrum-guide.html



What is Scrum? (ok so > 60s)



What does this get us?

- Faster, incremental delivery
- Higher quality - Value-based prioritization = more effective delivery
- Greater flexibility to deal with the ever changing security landscape
- Increased productivity
- Better collaboration
- Better morale/engagement

Let’s look at an example.

Acme Corp Security Team

Let's take a hypothetical Security team at a small organisation, that does a wide variety of things.

- A lead/manager, and 4 ICs
- Org is in financial services, so is regulated
- Functions:
  - Intelligence collection and analysis
  - Detection Engineering and alert investigation
  - AppSec
  - GRC
  - Vuln Management
  - Incident Response
  - Threat hunting
  - Tool development
- Rotating Operations roster, 1 person per week
- They are busy! (and ineffective and burnt out)

The Plan

- Start with long term goals
- Break down into quarterly milestones
- Each quarter, the team creates backlog tickets
- 2 week sprints
- Retro/Sprint planning at the start of each
- The team adds to the backlog when additional work tasks are identified, along with an estimate
- 25% of sprint reserved to cover Operations (1 person per week)

The First Sprint

- Ops week 1 (5 days)
- 3rd Party Risk Assessment for new vendor (5 days)

- Supervise annual pen test (10 days@70%)
- Build new detection (3 days)

- Ops week 2 (5 days)
- Threat Hunt (5 days)

- Threat model customer facing app (5 days)
- Integrate scanning into CICD pipelines (5 days)

The Cycle

- Any new Stakeholder asks are captured in the backlog (protect the sprint!)
- During/at the end of sprint, next steps are captured in the backlog. e.g.
  - Threat Intel -> Threat Hunting - > Detection gaps -> New detections
  - Alert and Incident analysis/PIR -> Control gaps -> New controls
- Next sprint is planned, adjusting for stakeholder input and lessons learned
- Product owner (and team) adjusts to stay on track with longer term goals
- Do it all again!

What problems does this solve for Acme Security?

What?	*Result!*
Work is more closely tied to “value”, regular prioritisation minimises wasted effort	More efficient delivery, tighter focus on what matters most
Stakeholder expectations are better understood, the team understands “why”	Team feels more empowered and engaged
Prevents overloading the team, by avoiding changing priorities mid-sprint	Less context switching, more focus time

Convinced? A Few Tips When Getting Started

- Strong leadership and direction from Product Owner
- Don’t feel you have to implement everything at once
- Invisible work will get you, track everything

Key Takeaways

- Scrum works for all types of teams, security included
- If your team is not working as efficiency as you think it can, consider scrum
- You can start small and build up, you don’t have to do it all at once
- There are heaps of guides freely available to get you started

Questions?

scrumguides.org

Atlassian - What is scrum and how to get started