OPEN SECURITY SUMMIT

June | 2020

Beating the 1:100 Odds - Team Topologies for Security

Organisers:
Manuel Pais
Mario Platt

Beating the Odds

Some text

- With bullets….

Raw format - for guidance

This document includes headings you may use to describe your session outcomes. Rearrange the headings as necessary to ensure coherence and clarity.

Please use any additional headings that will improve the outcomes.

NOTE: *The italic text in this page/document is used for explanation only. Replace it with other useful content.*

Outcomes/Deliverables (recommend)

The outcomes are the results produced from a session regardless of the session type. These can be:

- *Diagrams*
- *Documents or Books*
- *Playbooks*
- *Roadmaps (for next meeting)*
- *Wiki pages (namely on owasp.org)*
- *Code*
- *Statement or Position (signed by the Working Sessions Participants)*
- *Security Review (or a particular application or api)*
- *Lessons Learned*

Raw format - for guidance

```
Notes taken during the session
```

Main challenge being on ratio of 1:100 in terms of Devs to Security and how we can organise to make that less of a constraint in implementing security

Just adding more security people isn't going to be an easy solution, or palatable to the business

Team Topologies is about general IT teams, but how can we show teams on how teams can evolve as opposed to adoption of static team models
Product teams optimise for faster feedback and that should include security

How can we support teams in getting the knowledge they need to do things securely in their context. How can we create team topologies to enable this to happen more consistently

Enabling teams is the default way of enabling that, by having a tem of security experts to detect and help bridge gaps

Enabling purpose also geared towards reducing dependencies on security experts by teaching rather than doing the work (like a Platform team), and jointly agree when more collaboration is needed (on a per-team basis)

Enabling team isn't there to fix all problems (security practices, lack of prioritisation or unsecure coding)

Raw format - for guidance

Notes taken during the session

This team also needs to have time to stay on top of their practice (strategies, practices, tools, frameworks, threats etc)

BDD security (BDD type frameworks) to create scenarios about security, to explore possible threats

Aim to have Strea-aligned teams to do 80% of work, with all else done by the security expert teams.
Start by thinking about OWASP Top 10, but aim to do that. Even this is hard, so ability to focus on particular types of threats is more beneficial

Orbiting - Iterative and working closely with particular teams (time bound) to improve security around defaults for instance

Platform provides self-service capabilities, and allow lower level services that several stream aligned teams will need, ad develop better abstractions to make it easier to consume

Aim to have security domain knowledge around compliance checks into self-service APIs in platform

General pattern - discover useful platform with stream aligned teams then push to the platform (sense for evolution)

Airbnb security talk (get link from Manuel)

Move from in-flow execution based team dependencies to out of flow capability based team dependencies

Raw format - for guidance

Notes taken during the session

We need help from different teams to create these capabilities

We need to help security people on how to be good mentors and coaches to the other teams

Raw format - for guidance (Contd)

Synopsis and Takeaways (recommend)

- Security teams need to be more deliberate about their interaction modes
- Team Topologies book can be leveraged to think and develop the security capabilities within organisations and how security experts can interact with Stream-aligned and Platform teams
- We can use Team Topologies to also think and develop interaction modes between different teams within InfoSec

Identified Questions

- How can we be more deliberate and consider evolving relationships within Infosec teams ?

Important Conclusions

Make a simple list of conclusions that were taken at the session.

Working Materials (recommend)

- https://docs.google.com/presentation/d/1dZKaMmkeCHExIOVgXCE_w9mYe8j2lHlFKVoEVLDldTk/edit#slide=id.p

References (recommend)

- www.teamtopologies.com

https://www.amazon.co.uk/Team-Topologies-Organizing-Business-Technology/dp/1942788819/ref=sr_1_1?dchild=1&keywords=team+topologies&qid=1592827530&sr=8-1

Raw format - for guidance (contd)

```
### Additional/External References

*Make a bullet list with additional references that might be useful*

* *Link 1 Title: URL 1*

* *Link 2 Title: URL 2*

* *Link 3 Title: URL 3*
```