Let us know what you think

Click ‘engage’ to rate session.

Rate 12 sessions to get the supercool GOTO reward

Join the conversation gotoldn
When devops meets security

Michael Brunton-Spall
"I'm from the Government and I'm here to help"
"I'm from security and I'm here to help"
Government Digital Service
Simpler, Clearer, Faster
The state of information security in 2015
ISO27001:2005
Approval to operate
Accreditation
Certification
PCI
What does this look like?
Traditional model
How do we deal with changes?
Agile changes everything
Only do what's needed now
Release It!
MVP and iterate
Focus on flow and cycle time
A security nightmare!
A brave new world for security
Security needs to be an enabler
We reviewed agile projects across government
Biggest consistent finding?
There is no consistency
Most teams don't know how to do this
So what can we do?
Principles over rules
The UK Government published 8 principles
1 - Accept uncertainty
2 - Security as part of the team
3 - Understand the risks
4 - Trust decision making
5 - Security is part of everything
6 - User experience is important
7 - Audit decisions
8 - Understand big picture impact
But what does that mean?
Imagine a new project
Choose security model that's appropriate
At project inception
Understand the threats
Educate decision makers to risks
Make risk decisions, per story, in the team
What do you do about it?
Avoid
Transfer
Accept
Mitigate
Temporarily Accept
What sort of controls might we use?
Active countermeasures
Deter, Detect, Prevent
Reactive countermeasures
Correct, Respond, Recover
Traditional security people understand this
But there's more
Anti-personas
Misuse cases
Attack trees
Component

- Design
- Produce
- Distribute
  - Loading Dock
    - Trust
    - Guard
    - Subvert guard or evade detection
  - Truck
  - Depot
- Use
- Discard

Red teams
Automated penetration testing
Automated
Integrated
Repeatable
Please remember to rate this session.

Thank you!
Thanks !