EATING THE ELEPHANT
APPLICATION SECURITY WHEN YOU AREN’T A START-UP

Stephen Morgan – Westpac New Zealand
• Westpac New Zealand – Security Assurance Manager
  • Find and fix all the (security) things
  • Risk stuff
  • Annoy the SecOps team
  • Secure Development Initiatives

• Background:
  • Penetration Testing
  • Software Development
  • Risk and Policy
OUTLINE

• What is Good?
• The Reality
• Secure Development Menu
• Lessons Learnt
WHAT IS GOOD?

The Current Dogma:

• Application Security Engineers

• DevSecOps
WHAT IS GOOD?

Application Security Engineers

• Pros:
  • A security team’s snake in the grass
  • Catch issues early
  • Passively upskills the rest of the squad
  • Very popular with large tech companies

• Cons:
  • Don’t exist or are gold plated
  • Large tech companies practically have constantly open vacancies
  • Seriously these people are unicorns (and probably all in this room)
WHAT IS GOOD?

- Automated Security Testing
- Pull Requests
- Fresh Image
- Latest Dependencies
- Minimal Docker
- Scale Out
- Zero Access
THE REALITY

Automated Security Testing
Pull Requests
Fresh Image
Scale Out
Latest Dependencies
Minimal Docker
Friend approved
Version pinned?
Dependency happy dev's
But full image is easier
Encryption is hard
Except for Dave

People

Or just Testing

Version pinned?
Encryption is hard
Friend approved
But full image is easier
Dependency happy dev's
Latest Dependencies
Minimal Docker
Automated Security Testing
Or just Testing
We can solve this with basic principles:

- Education and Awareness
- Visibility

If you can’t have an App Sec Engineer
And you can’t commit to DevSecOps…
SECURE DEVELOPMENT MENU

Education and Awareness:

- Introduction to Secure Development - OWASP Top 10
- Secure Code Warrior
- Introduction to Penetration Testing – OWASP Juice Shop
- Capture the Flag – FBCTF
- Help with Remediating Findings
Visibility:
- Attend Stand-Ups
- Threat Modelling – Elevation of Privilege
- Pull Requests
- Static Code Analysis – HP Fortify, OWASP SonarQube (findsecbugs)
- Dependency Scanning – JFrog X-Ray / OWASP dependency check (maven, node) / snyk
- Vulnerability Scanning - Nessus
- Compliance Scanning – Chef Automate; authenticated VMS
LESSONS LEARNT

• Iterate – don’t try it all at once
• Let squads pick and choose

• Build rapport – Previous encounters with Security team may not have gone well
• Build trust - Squads may be scared of you
• Track it
THANKS

• Special mention to O’Reilly Agile Application Security