OWASP
Open Web Application Security Project

State of AppSec in New Zealand 2022

John DiLeo (@gr4ybeard)

OWASP New Zealand and Datacom

July 2022

Thank You to Our Sponsors and Hosts!

OWASP
NEW
ZEALAND
owasp.org.nz

QUANTUM
SECURITY

AUT

CyberCX

DATACOM

snyk

auth0

Checkmarx

HCL AppScan

kordia

LATERAL
SECURITY

MICRO
FOCUS

Pulse Security
www.pulsesecurity.co.nz

RedShield

Flux

SEQA
Information Security

Cobalt

LACEWORK

SecureFlag

Without them, OWASP New Zealand Day couldn't happen

About Me

- Past lives
  - Simulation developer and system analyst
  - University lecturer - Maths, Comp Sci, IT, *et al.*
  - J2EE developer and architect
- Moved to Application Security, 2014
- Moved to New Zealand, late 2017
- OWASP Leadership
  - New Zealand Chapter
  - Author, Software Assurance Maturity Model (SAMM)
  - AppSec Curriculum Project

Where I Work and What I Do

Datacom's AppSec Services team

- Software Assurance Lead
- Advise on Software Assurance
  - SAMM-based maturity assessments
  - Maturity improvement guidance
  - GRC, Training, Tooling, DevSecOps
- Within Datacom: Help improve Software Assurance maturity of Digital Engineering teams

We're (about to be) hiring…and we're here, so…

Agenda

- Motivation
- Survey Design
- Data Collection
- Responses and Insights So Far
- Future Work

Motivation

- There are lots of “State of XXX Security” reports out there
  - Most either US-focused or broadly global
  - “New Zealand’s different…”
- Consulting *is* my day job
  - Looking for “evidence” things are as bad as I think
  - But, also…that they can *and do* get better

Support for Current Effort

- Datacom is supporting this effort, through in-kind contributions
  - Release time to work on it
  - Use of resources
- But…the report *is not* a Datacom product
  - Publications are OWASP documents
  - CC Attribution-ShareAlike 4.0 license

Deliverables

- A publicly available whitepaper
  - Summary statistics only
- On request: a ‘customised’ version of the whitepaper, with the requesting organisation’s responses highlighted
  - “You Are Here”

Survey Design

Why not anonymous?

- We want to report on “organisations” as our population
  - Need to identify multiple responses for orgs
- SurveyMonkey isn’t ‘smart’…unless you pay more
  - Every “false start” is a separate response
  - No support for editing your submitted response
    - That’s a feature at a higher ‘tier’ of the service
  - Need to identify duplicate/replacement responses
- Organisation needed for ‘customised’ report

Survey Design
Why so complicated?

- There are *lots* of ways for orgs to "do AppSec"
  - For some, *many* questions are irrelevant
- Flow keyed on four 'tiers' of development
  - No bespoke software at all
  - Outsource dev, deployment, and operations
  - Outsource dev, in-house deploy/ops
  - In-house dev, deployment, and operations

Survey Design

Question Groups (Survey Pages)

- Application Inventory
- Governance, Risk, and Compliance
- OWASP “Awareness” and Use
- Penetration Testing
- Cloud Security
- Skills and Hiring
- Organisation’s attitude toward AppSec
- Formalisation / Funding of AppSec Efforts
- Secure Coding
- Security Defect Management
- Security Testing
- Security Training
- Logging and Monitoring
- Security Requirements
- Supplier Security

Survey Design
Example Flow

- “We use only ‘off-the-shelf’ commercial software”
  1. Application Inventory
  2. Governance, Risk, and Compliance
  3. OWASP “Awareness” and Usage
  4. Penetration Testing
  5. Cloud Security
  6. Skills and Hiring
  7. Organisation’s Priority for AppSec

Data Collection

- Respondents self-select…with encouragement
- SurveyMonkey
- Promotion
  - Chapter mailing list
  - NZ Slack workspaces (InfoSecNZ, NZITF)
  - Personal networks
  - Social media…kinda

Data Collection
…is still underway

- We've held the response window open
  - All submissions received through 22nd July will be included in the 2022 results (two more weeks)
- SurveyMonkey

  https://www.surveymonkey.com/r/L2B8X6L

Responses

- As at 15th June: 54 Responses
- Development ‘Tier’ (Path) Distribution:
  - COTS Only: 5 9%
  - All outsourced: 6 11%
  - Outsourced Dev / In-House Ops: 4 7%
  - In-House Dev: 36 67%
  - No response: 3 6%

Responses

What is your approach to penetration testing?

• We don't do any:	2	4%
• On an *ad-hoc* basis:	3	6%
• Only for new applications:	3	6%
• Only if required for compliance:	5	9%
• On a regular cadence:	21	39%
• No response:	20	37%

Responses

What do you do with pen test results?

• Nothing:	1	2%
• Remediate only if critical:	13	24%
• Remediate enough to pass audit:	3	6%
• Pass to dev team for RCA:	7	13%
• Remediate all findings:	7	13%
• No response:	23	43%

Responses

Do you feel there is a technical skills shortage in New Zealand?

		Total	Not Skipped
• Yes:	36	67%	95%
• No:	2	4%	5%
• No response:	16	29%	

Some Observations

- Most questions were optional
  - Not everyone has enough information to answer every question for their organisation
  - To get *statistically significant* results for *all* questions, the response pool needs to be **much** bigger
- Question (and response) design was done by a homogeneous group, with similar 'agendas'
  - To get more *meaningful* results, questions must be de-biased

Future Work

- Ensure this really is the *first annual* survey
  - Quality Improvements
  - Grow Responses
- Develop trend metrics
  - We'll have three data points (for some) in 2024
- Create OWASP Project
  - Go Global!

    ...with a National Survey

    No…really

Opportunities for Improvement

- Engage experts to identify and reduce bias in question design
- A more intentional data collection effort
- Better promotion and messaging
- Invite other perspectives into design

Questions?

Thank You!

Want to chat some more?

Looking for help?

Reach out!

OWASP: *john.dileo@owasp.org*

Day job: *john.dileo@datacom.co.nz*

Twitter: *@gr4ybeard*

LinkedIn: *@john-dileo*