

## *Why do Programmers Do What they Do? – Interview Questions*

### **Participant Background**

- What is your role within your organisation/teams?
- Please describe any security education you got before working at your current job?
- What prior work experience do you have with security and privacy protocols?
- Would you like to tell me anything more about your background/experience in the industry?

### **Current Work**

- What security protocols do you regularly use and adopt?
- Can you give brief overviews of the security protocols for someone who may have never used them before?
- How do you choose what security practices to use and disregard? What factors are taken into consideration?
- Are you adding to the protocols in any way?
- Do you give other teams/individuals feedback on their security practices?
- Do you change languages based on the security practice you use? Why?
- What decision makings and actions have arisen surrounding security in your programming from covid19/working from home.
- Does your work provide any training, or is it expected that you know how to program “securely”?
- How did you learn about your chosen practices in order to adopt them?
- If you have obtained training, has that continued? How has it changed since when you first started.
- How are the security practices you have used/are using been tested?
- Do your security practices have any influences from OWASP. If not, why? If yes, how?
- How well do your teams chosen methods fit your current work?
- Please share if you and your team have adapted any of the approaches to suit your work better?
- How well do your team's security practices fit into the organisations overarching practices?

- What changes over time, if any, has your team enacted? Why?
- How important would you consider security needs to be for the quality/success of your work?
- What practices have been extremely valuable?
- What are some difficulties in joining a team with an established process? What was the induction process like?
- Do security practices change based on the requirements of the project? How are they identified?
- How are security requirements prioritised in relation to functional requirements?
- What work do you do in a project on a day-to-day basis to ensure system security? Or if not daily, how often is attention given to security?
- At what stages of the project/how often is attention given to security? What approaches/techniques are used at each stage?
  - Planning
  - Requirement Gathering
  - Design/Development
  - Testing
  - Implementation
  - Iterations

### **Experience-Based**

- What recommendations would you generally give to teams looking to adopt your security practice of choice?
- What differences do you see between new and experienced teams?
- What common “mistakes” do you see?
- What factors contribute to a successful education on how to use security practices?
- What difficulties did the teams you have worked with share? Which ones were unique? Why?
- What changes have you observed in the security programming landscape in New Zealand?

### **Impacts**

- For your current particular languages and security used, how has it impacted the projects you have worked on?
- Have there been successes of using some security practices over others?

- Have there been any lessons learned in your own personal projects and style?
- What have been problems in projects due to choosing specific protocols?
- How have your chosen practices affected your ability to deliver within constraints?

**Any other issues or comments?**