Online Survey Questionnaire: Security Practices in Agile Software Development

Background Questions

1a. Name: _____

1b. Email: _____

1c. Current Company: _____

1d. Current Role: _____

1e. Total years of experience: _____

2. In your opinion, how important is software security for your team?
- □ Not at all important
- □ Slightly important
- □ Moderately important
- □ Very important
- □ Extremely important

3. Do you use Agile software development methodology in your organization?
□ Yes □ No

4. How much do you agree with the statement: "Software developed through Agile methods are relatively less secure when compared to software developed through sequential software development life-cycle processes like Waterfall"
- □ Strongly Disagree
- □ Disagree
- □ Neither agree nor disagree
- □ Agree
- □ Strongly agree

5. Does your team include any security activities in the Agile process?
□ Yes □ No

6a. What are these security practices used in your Agile process? (*Optional*)

_____

_____

6b. What is your take on these security practices used in your team? (*Optional*)

_____

_____

6c. How has the inclusion of these security practices affected the team productivity? (*Optional*)

_____

_____

6d. How has the involvement of these security practices affected the software product? (*Optional*)

_____

_____

6e. How has the inclusion of these security practices affected the organization? (*Optional*)

_____

_____

6f. How has the involvement of these security practices affected your day-to-day activities? (*Optional*)

_____

_____

6g. How was the sprint velocity affected? (*Optional*)

_____

_____

7. After using these security practices are you more confident in the security of the software you are building?
- □ Not confident at all
- □ Slightly confident
- □ Somewhat confident
- □ Fairly confident
- □ Completely confident

How effective would each security practice be in increasing the security and robustness of the software, if your team would include it in the Agile software development process.

8a. Addressing security from early iterations with requirements and testing
- □ Not at all effective
- □ Slightly effective
- □ Moderately effective
- □ Very effective
- □ Extremely effective

8b. Clearly stating security requirements, that are expected to be in the production software.
- □ Not at all effective
- □ Slightly effective
- □ Moderately effective
- □ Very effective
- □ Extremely effective

8c. Adding a Security specialist or Security master to your team.
- □ Not at all effective
- □ Slightly effective
- □ Moderately effective
- □ Very effective
- □ Extremely effective

8d. Assigning additional points or weight to a ticket, considering the level of impact the ticket will have on software security.
- □ Not at all effective
- □ Slightly effective
- □ Moderately effective
- □ Very effective
- □ Extremely effective

8e. Iterative and incremental vulnerability and penetration testing.
- □ Not at all effective
- □ Slightly effective
- □ Moderately effective
- □ Very effective
- □ Extremely effective

8f. Iterative and incremental security static analysis.
- □ Not at all effective
- □ Slightly effective
- □ Moderately effective
- □ Very effective
- □ Extremely effective

8g. Iterative and incremental risk analysis, countermeasure graphs.
- □ Not at all effective
- □ Slightly effective
- □ Moderately effective
- □ Very effective
- □ Extremely effective

8h. Automatic testing adding vulnerabilities analysis, risk assessment into the deployment pipeline
- □ Not at all effective
- □ Slightly effective
- □ Moderately effective
- □ Very effective
- □ Extremely effective

How willing are you to include each security practice in your Agile software development process?

9a. Addressing security from early iterations with requirements and testing
- □ Not at all willing
- □ Slightly willing
- □ Moderately willing
- □ Very willing
- □ Extremely willing

9b. Clearly stating security requirements, that are expected to be in the production software.
- □ Not at all willing
- □ Slightly willing
- □ Moderately willing
- □ Very willing
- □ Extremely willing

9c. Adding a Security specialist or Security master to your team.
- □ Not at all willing
- □ Slightly willing
- □ Moderately willing
- □ Very willing
- □ Extremely willing

9d. Assigning additional points or weight to a ticket, considering the level of impact the ticket will have on software security.
- □ Not at all willing
- □ Slightly willing
- □ Moderately willing
- □ Very willing
- □ Extremely willing

9e. Iterative and incremental vulnerability and penetration testing.
- □ Not at all willing
- □ Slightly willing
- □ Moderately willing
- □ Very willing
- □ Extremely willing

9f. Iterative and incremental security static analysis.
- □ Not at all willing
- □ Slightly willing
- □ Moderately willing
- □ Very willing
- □ Extremely willing

9g. Iterative and incremental risk analysis, countermeasure graphs.
- □ Not at all willing
- □ Slightly willing
- □ Moderately willing
- □ Very willing
- □ Extremely willing

9h. Automatic testing adding vulnerabilities analysis, risk assessment into the deployment pipeline
- □ Not at all willing
- □ Slightly willing
- □ Moderately willing
- □ Very willing
- □ Extremely willing

Note: Question 6 and its part were optional. Questions 8 & 9 were presented to survey participants in a grid format