Secure Scrum Notes

Mapping of agile development phases and the new secure scrum tasks.

Initial Product Backlog Creation	Identification
Product Backlog Refinement	Identification
Sprint Planning	Implementation
Daily Scrum	Implementation - Verification
Definition of Done	Verification
Sprint Review	Identification

Difficulties with secure agile

Agile sprints are tailored towards pleasing the clients wishes at after each cycle.

With pressure to produce software that meets the functional requirements the security requirements can be brushed aside. Because the security aspects are pushed back, they may not be considered until later in the SDLC.

Note: User stories - a user story is a description of a feature from a user's perspective.

Scrum roles:

Product owner - Requirements / user story master

Scrum master - leads the development using the scrum process

Development team

Back log creation - before the scrum cycle the

1)Backlog refinement/ Task review - obsolete tasks are removed

2)Task selection - The tasks for the next sprint are selected

3)Sprint planning - user stories are created for the chosen tasks

4)Scrums - Tasks are now developed and daily meetings announce task progress

5)When the time for the sprint runs out the remain tasks are returned to the back log.

6)Product demonstration - Feedback is received from 'client'

7)Sprint review - What went well? what could be improved?

Definition of done:

Essentially when how do we know when something is complete.

Definition of done usually includes Functional requirements, quality standard and non-functional requirements. A 'lower bar' for the definition of done can add technical debt to the project that will have to be 'replayed' later on.

link: HTTPs://www.scrum.org/resources/blog/done-understanding-definition-done

Security steps

- Identification component
- Implementation component
- Verification component
- Definition of Done component

The identification component is used to identify security issues during software development. Security issues are marked in the Product Backlog of Scrum.

The identification component is used during the initial creation of the Product Backlog as well as during Product Backlog Refinement, Sprint Planning, and Sprint Review. Assigning a loss value to tasks/user story's highlights where the top security concerns are. A loss value indicates the how damaging loss of said data is. A security concern can be created for recognized concerns. A 'S-tag' links a user story and a concern, multiple stories can be linked to the same concerns.

The implementation component raises the awareness of the Scrum team for security issues during a sprint. The implementation component is used in Sprint Planning, as well as during the Daily Scrum meetings. If user story is marked with a 'S-tag' then the tasks derived from the story should be marked with an 'S-mark' that links to the 'S-tag'. This allows developers to be aware of the security concerns.

The verification component ensures that team members are able to test the software with the focus on IT Security. The verification component gets managed within the Daily Scrum meeting. User stories with 'S-tags' must have the security concerns verified after completion.

The Definition of Done component enables the developers to define the Definition of Done for security related issues as postulated in standard Scrum. The developer can only mark their work as security complete if they have adequate knowledge, otherwise a dedicated task will be required.

The sprint is complete and the next sprint begins

The identification task involves finding security concerns. Security concerns should then be assigned to a task in the backlog. Identification tasks could be completed.