
Realising benefit and value from CC evaluations

23 September 2008

- NATA accredited
- Common Criteria evaluations under the Australasian Information Security Evaluation Program (AISEP)
- Lab based in Canberra, Australia
- About me
 - AISEF evaluator for 2 years
 - Various evaluations of differing levels

- Common Criteria has developed a reputation of being:
 - Difficult
 - Irrelevant
 - Time consuming
 - Costly

- Difficulties associated with initial evaluations occur as a result of:
 - Developers needing to
 - Understand the criteria, and apply it to the development process
 - Develop required documentation
 - Evaluators needing to understand the TOE, its boundaries, implementation and integration within the environment

Irrelevant



- After the product is developed and released:
 - In the majority of cases, only minor issues can be fixed
 - Changes are usually implemented in the ST and guidance rather than in the TOE

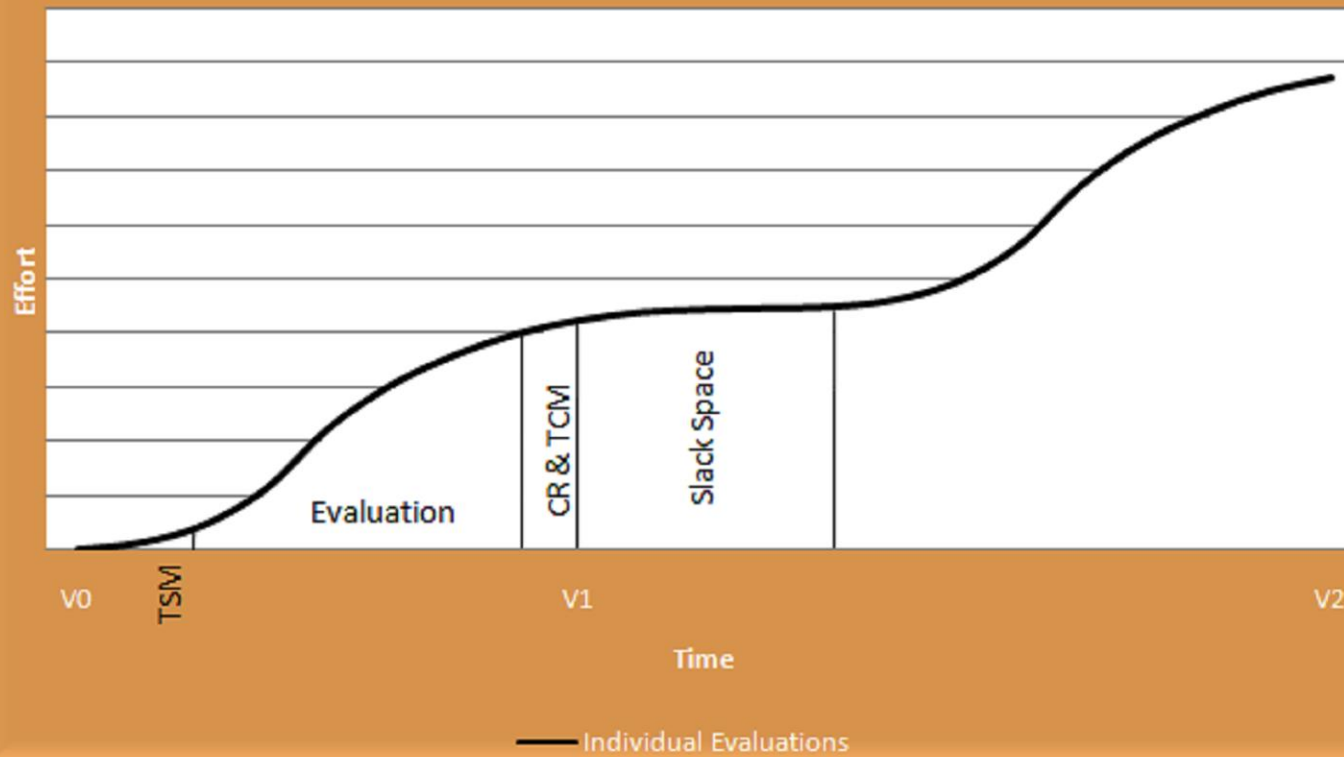
- Rather than creating design documentation during the development of the TOE, developers often struggle to produce accurate documentation after the TOE is released
- Developers who worked on the TOE are often unavailable during the evaluation as they have moved on to the next project
- Developer's experience with the formal IT security evaluation process is often limited

Costly



- The cost of evaluations is often quite high as a result of:
 - The current documentation set for a product being non-compliant with the Common Criteria requirements
 - A poor understanding from developers regarding Common Criteria requirements resulting in multiple resubmissions of documents
 - The steep learning curve for both evaluators and developers
 - Some issues raised could be extremely costly to fix

Evaluation Effort - Major Release



It doesn't have to be this way!

- A lab partnership involves:
 - Long-term arrangement between a lab and developer
 - Building on the initial baseline, minor versions are “re-evaluated” or accepted under maintenance
 - Maintenance of assurance for future releases of the product
 - Working with a lab over the life of a product

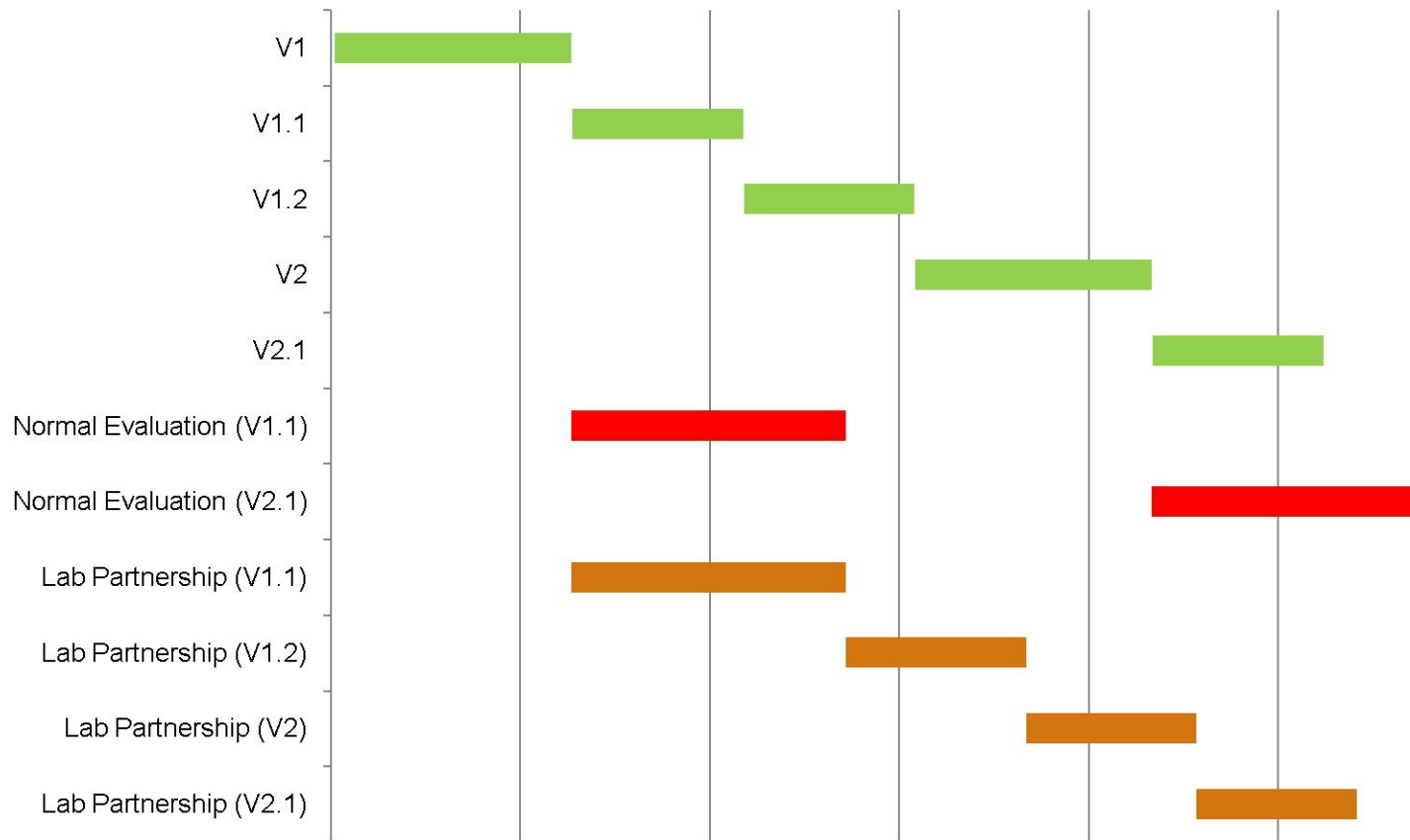
What are the benefits?



- Reduced learning curve for developers and evaluators
- Partner labs can assist with assurance maintenance
- Minor documentation updates are only required for each re-evaluation
- Detection of issues during development, resulting in CC evaluations becoming more relevant to the secure development of the product

- Improved usability of TOEs in their evaluated configuration
- Re-evaluations have a lower cost, as the effort is reduced
- You have the marketing edge!

Development Life Cycle





- Common Criteria does not have to be difficult, irrelevant, time consuming and costly
- By partnering with a lab and building evaluation into the development roadmap a more efficient and streamlined evaluation process can be established

Questions



Any questions?

Contact Details



stratsec lab

Email: lab@stratsec.net

Ph: +61 2 62608878

Fax: +61 2 62608828

Thank you