

How do you ensure evaluators are competent?

[ICCC 2010]

Zarina Musa *CISSP, GCUX*

Evaluator

CyberSecurity Malaysia MySEF,
Malaysia

21 September 2010

Little bit about myself

- An evaluator in CyberSecurity Malaysia MySEF (Malaysian Security Evaluation Facility) since 2008.
- Given responsibility to assist in planning and implementing training for all MySEF staff.
- Previous work – involved in IT security since 1995 doing audits and consultations.

Outline

- Objective
- Introduction
- Our strategies for ensuring our evaluators competency
- Recommendations

Objective

To impart our experiences in ensuring that our evaluators are competent and have the necessary skills to perform Common Criteria evaluations

Introduction

- Representing CyberSecurity Malaysia MySEF
- The first project of Ninth Malaysian Plan for CyberSecurity Malaysia established the requirements for the Malaysian Common Criteria (MyCC) Scheme.
- Aims
 - to increase Malaysian competitiveness in quality assurance of information security using the CC standard,
 - to build consumer confidence in Malaysian information security products and systems.

Introduction

- So, in 2007, CyberSecurity Malaysia commenced a project to establish the MyCC scheme beginning with the development of the scheme strategy and its associated implementation plan.
- In response, CyberSecurity Malaysia MySEF was established, and it was the one and only Common Criteria evaluation facility in Malaysia.
- Once established, we started on a few pilot projects and then proceed to shadow evaluation projects as we aim to fulfill the requirements to be an authorizing member of the CCRA.

Introduction

- As we are looking at increasing number of products coming in for evaluation, a large number of new evaluators are hired.
- Who are they?
 - IT and engineering graduates
 - some of our requirements - good performers in college, good attitude, high achievers
 - most important : they must be interested in becoming an evaluator – lots of documentations.

Introduction

- They also
 - must have a basic level of knowledge in IT security.
- Some of them are fresh graduates and have no working experience.
- Almost all do not have any exposure and have not attended any formal training on Common Criteria.

How do we ensure our evaluators are competent?

- Our challenge :
 - for a newly set-up evaluation facility, and with a number of new evaluators in our hands, we have to ensure that they have the necessary skills within an acceptable time-frame.
- Proper planning is needed.
- We will share what we have been doing, our approach and experience.

Strategies for ensuring competency

- First - we need to ensure they have good knowledge of IT security.
- Internal trainings on various subjects related to IT, IT security and specific product trainings in order to
 - provide fundamental knowledge and build the competency level of MySEF new evaluators
 - and also to ensure their correct and common understanding of the subject.

Trainings (internal & external)

- Conducted a series of internal trainings - cryptography, VPN, network security, access control, Unix security, web application security, biometrics, wireless etc.
- From time to time, send to more advanced and specialized trainings.

Knowledge Sharing Sessions

- Ensure evaluators are
 - aware of new technologies and are up-to-date with current aspects of the IT security.
 - used from time to time to refresh the evaluator's understanding of the main principles of IT security.
- Evaluators who went for external trainings, share knowledge with other evaluators in these sessions. Done within one month after training.
- Frequency depends on availability of presenters and evaluators, aim for once in every two weeks.

Penetration testing class

- Need to continuously update and refresh on penetration testing techniques.
- Conduct demos on penetration testing among the evaluators.
- Hands-on classes, so all evaluators can be involved and can try executing the steps themselves.
- Classes conducted weekly, depending on the availability of presenter and evaluators.

Competency in MyCC Scheme evaluation functions

To increase competency in MyCC Scheme evaluation functions, we have a few programs :

- a) Formal CC Training
- b) Hands-on CC Training
- c) Mentor-mentee program

Formal CC Training

- Uses MyCC Scheme expertise to provide up to working level of competency in Common Criteria evaluation.
- New evaluators must attend formal MyCC scheme training conducted by senior staff from the MyCB and MySEF.

Formal CC Training

- Training modules provide basic and working level competency in IT security evaluations and the MyCC Scheme, Security Targets, Protection Profiles, functionality and assurance requirements (supported by a case study).
- Competency will be verified by question and answer sessions with the students.
- A MyCC Scheme Common Criteria examination will be administered to the students, and passing it demonstrates their mastery of the subject matter.

Hands-on training

- Apart from formal training, we also conduct a one week hands-on evaluation training.
- We prepared exercises for ASE, ADV, AGD, ALC, ATE evaluation phases and divided the training class into several groups.
- Each group will work on one evaluation phase and discussions and presentations will be held which involve all participants in the class.

Mentor-mentee program

- Our next strategy for ensuring competency is implementing a mentor-mentee program.
- Necessary for new evaluators. Each new evaluator is attached to a senior MySEF evaluator who will become his/her mentor.
- One-to-one or one-to-two instead of one-to-many training. This personal training enables more focused and flexible environment.
- Pace is depending on mentor, as long as it is within the allocated timeframe.

Mentor-mentee program

- Consists of hands-on evaluation exercise. The exercise will be done on a prepared Target of Evaluation (TOE) which will be evaluated for EAL1+ assurance level.
- Evaluations will be done under the guidance of each assigned mentor using
 - Part 1, Part 2 and Part 3 of Common Criteria
 - Common Evaluation Methodology for Information Technology Security Evaluation
 - and in conformance with MyCC Scheme Policy

Mentor-mentee program

- There will be 6 modules involved in this program and they are required to be completed as an exercise before the mentees can conduct any actual evaluation works.
- The modules cover all classes - ASE, AGD, ADV, ALC, ATE and AVA evaluation.

Mentor-mentee program

- At the beginning of the program, a briefing will be given by a senior MySEF evaluator, which gives an overview of the whole training program such as the modules involved and the schedule.
- We have a tentative schedule which specifies the allocated timeframe for each module
- Mentors are responsible to ensure the training completion is according to schedule.

Mentor-mentee program

- Mentor's responsibilities are to :
 - provide their mentees with relevant evidence documents and workbooks at the beginning of each module
 - coach and provide guidance to their mentees during the evaluation exercises
 - ensure that their mentee completes the assigned module according to schedule
 - perform a peer review on the completed workbooks, discuss the findings with their mentee and share the correct evaluation verdict.

Mentor-mentee program

- Mentee's responsibilities are to :
 - perform evaluation exercises and complete workbook
 - complete the assigned module according to schedule
 - discuss findings with their mentor and find out the correct evaluation verdict

Mentor-mentee program

- Before the start of the ATE and AVA evaluation, a briefing will be done by a senior MySEF evaluator.
- Ensure the mentees have sufficient knowledge and understanding in order to perform ATE and AVA evaluations.
- Briefing will cover topics like :
 - Drafting a Test Plan for Functional, Independent Testing and Vulnerability Assessment
 - Mapping between Test Script and TSFI
 - Choosing the right tools for Vulnerability Assessment

Mentor-mentee program

Upon completion of each training module :

- Mentees are required to fill in Section A of CyberSecurity Malaysia MySEF Common Criteria Training Evaluation Form to assess their own understanding of the evaluation work.
- Mentors are required to assess their mentee's evaluation performance and efficiency level by filling in Section B of the form. Scores are given for each module together with comments.

Mentor-mentee program

After all modules have been assessed :

- a total score of 70% and above can be used to show that the mentee is able to perform the evaluation work.
- mentors should also state in the form whether :
 - the training meets its objectives,
 - the mentee is competent,
 - the mentee is recommended to attend further trainings to increase their competency.

Intermediate and advanced CC training

- We engage with known CC practitioners – recently had one with Mr. Wouter Slegers of Your Creative Solutions to provide intermediate and advanced CC training to our evaluators.
- The trainings not only involved theory, but also hands-on exercises and discussions.
- These kind of trainings enable us to go deep in discussions and also get proven methods and approach from experienced and knowledgeable people.

How do we ensure our evaluators are competent?

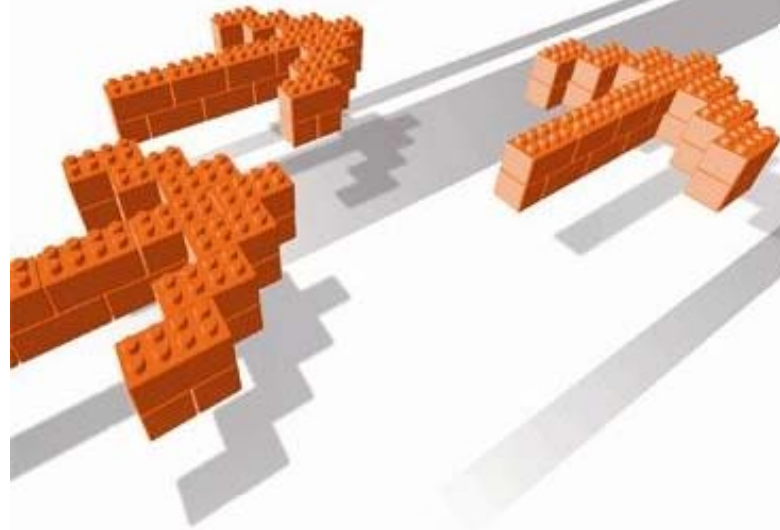
- These strategies are what CyberSecurity Malaysia MySEF implements in order to ensure our evaluators are competent.
- For now, we find that they are effective, but we hope to get feedbacks and recommendations from the floor.
- Sometimes faced with some constraints such as unavailability of budget for trainings.
- Most importantly, there is no specific place for us to get assistance and advice in our effort of increasing our evaluators' level of competency.

Recommendation

- Recommend that an institute for CC training is established in order to provide CC training, especially for young schemes like MyCC.
- Recommend a mechanism is introduced whereby senior evaluation facilities can provide assistance to newly established evaluation facilities.
- May help speed up the learning curve and provide solution for the constraints I mentioned which might be faced by some other new evaluation facilities too.
- We also hope to encourage discussions and recommendations on this topic.

References

- 1) CyberSecurity Malaysia MySEF Training Plan
- 2) CyberSecurity Malaysia MySEF CC Training Module
- 3) CyberSecurity Malaysia MySEF Common Criteria Training Evaluation Form



Corporate Office:
CyberSecurity Malaysia,
Level 8, Block A,
Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

Tel. +603 8946 0999

Fax. +603 8946 0888

Hotline. +1 300 88 2999

www.cybersecurity.my

Thank You



Q & A

Send questions or feedbacks to
nina@cybersecurity.my