Security Event Management Process

Dated: April 2013
Approved: April 2013
Version: 1.0

	**SOG-IS Recognition Agreement** **Joint Interpretation Library Working Group** **Policies and Procedures**

Document ID: JIL-Security-Event-Management-Processs-V1-0
Subject: Security Event Management Process

Introduction

1 The Common Criteria standard includes several assurance requirements about the conformity of the product and its development environment to its security target definition. These assurance requirements are typically the class dealing with development activities (class ADV), functional testing (class ATE), life cycle definition (class ALC)… The Common Criteria also include a specific assurance requirement related to the efficiency evaluation of the product security functions. This assurance requirement is the vulnerability analysis (class AVA). In particular, this class requires till its first level that any publicly known attack shall not be applicable to the Target Of Evaluation (TOE).

2 The AVA class is a challenge for all on-going evaluation, particularly when a new type of attack, relevant for the product undergoing an evaluation, becomes publicly known before the certification issuance. The challenge concerns all roles involved in the product evaluation and certification:

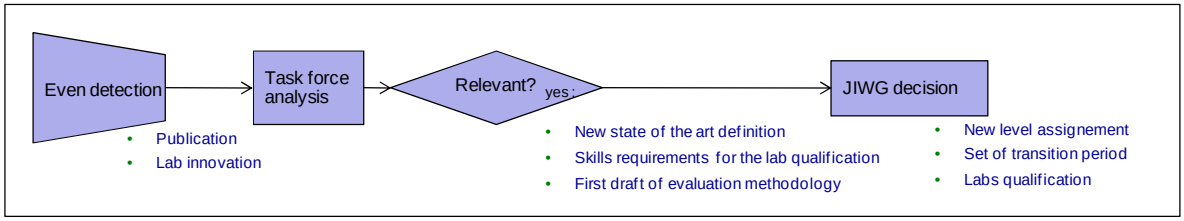
- the Certification Body, that has to be sure that this new type of attack will be taken into account by the evaluation facility within the ongoing evaluation before issuing any certification, even if this was not identified at the startup of the evaluation,
- the evaluation facility, that may not have the necessary skills, knowhow and equipments to check this new type of attack on the product undergoing a common criteria evaluation, and may not have planned the necessary workload to include this new attack into its test plan,
- the developer of the product, who may not have expected this new technical possibility of attack in the security architecture of the product,
- the sponsor of the evaluation, who may have to negotiate a supplement to the evaluation workload with the lab, and may be delayed in its business program if the certificate is delayed.

3 The goal of the process described in this document is to set a framework shared between SOGIS qualified participants[1], allowing monitoring, analyzing and ending with a common conclusion on any new attack or any new event that may impact Common Criteria evaluations. The objective of this process is to allow an efficient and common reaction, analysis and response.

Process description

General process

4 A task force is defined by the JIL sub groups (JTEMS, JHAS …). When an event occurs that might impact Common Criteria evaluations for a specific technical domain, the associated task force investigates the case and provides a technical analysis with a proposal of conclusion about the impact for Common Criteria evaluations. The trigger for the task force to start the investigation might come from the JIWG, the JIL Sub Group, or the task force itself. In the latter case the JIWG have to be informed by the task force about the security event. This process is summarized in the following picture:

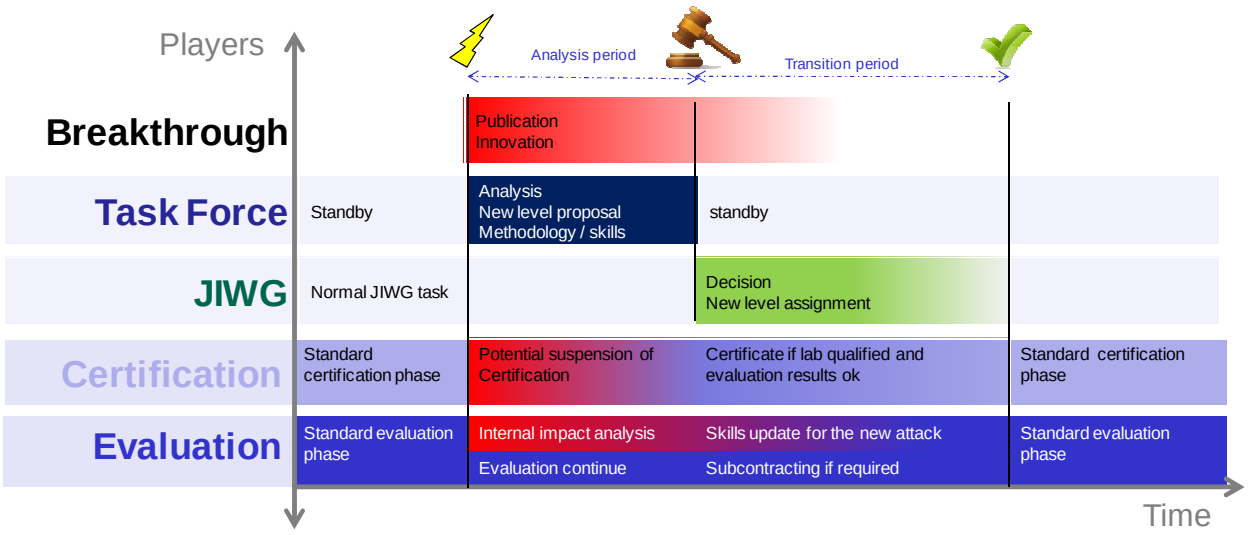


5 Two main phases are to be considered in this process:

- The analysis period, necessary for the task force to analyze the event and provides conclusion,
- The transition period, set by the JIWG when the event has an impact and needs to be implemented by the Certification Body.

[1] Mutual Recognition Agreement of Information Technology Security Certificates, version 3.0 8 Jan. 2010

6 The impacts of each phase per actor are summarized in the following picture and detailed below:



Analysis period

7 If possible, the analysis period should not exceed one month. It is up to the task force to shorten it as much as possible.

Breakthrough

8 An event can be detected by any member of the certification ecosystem. The chair of the task force shall be notified immediately. In such a case, the chair informs the JIWG chairperson about the event and proposes to mobilize the task force on the matter.

Task force

9 Following the JIWG acknowledgement, the chair of the task force will immediately propose an action plan to its member. The action plan may include:

- Publication review,
- Meeting with the organization/people responsible for the event,
- Meeting with technical organization involved to get further elements.

10 After agreement of the task force members, the action plan is executed.

11 The deliverable of the task force is a written document sent to the JIWG chairperson and containing:

- The action plan
- Minutes of meeting/discussions including technical details
- Analysis and conclusions
- Proposal to JIWG.

Certification

12 For on-going or just achieved evaluations, the certification body will analyze the issue on its own and may decide to issue a certificate before getting the conclusion of JIWG, depending on the context, the skills of the evaluation facility, and architecture consideration on the product. He will however not issue a certificate if he does not have the appropriate conclusions or the assurance that the evaluation facility handles the issue correctly. This is due to the Common Criteria assurance requirement (AVA class) that requires any publicly known attack to be considered within the evaluation.

Evaluation

13 The evaluation is not stopped in case of an event. All evaluation tasks continue as planned in order to minimize the impact on the planning. This does not prevent the evaluation facilities to perform their own impact analysis to anticipate the possible conclusion of the task force, and to provide their own rational for the ongoing evaluation to their certification body.

Transition period

14 The duration of the transition period may depend on a lot of factors. No limits can be defined.

JIWG

15 When the chairperson of JIWG receives the report from the task force, he distributes it to the JIWG members and asks for a consensus on the task force proposal.

- *Agreement:* if all members agree, the proposal is adopted. It is then up to each certification body to implement the proposal.
- *Disagreement:* The JIWG members organize a meeting to adjust the proposal with their own rational.

16 Any business consideration can be raised at the JIWG level by any actor or association of the certification ecosystem, through its preferred Certification Body or by a formal request to the chairperson of JIWG.

17 A transition period is defined and agreed, to allow the implementation of the proposal by the Certification Scheme.

Certification

18 Each Certification Body shall implement the proposal adopted or modified by JIWG. The CB shall make sure that relevant labs are able to perform the new attacks.

Evaluation

19 In order to be able to continue to perform evaluations after the transition period, the evaluation facility needs to demonstrate to the CB that he is able to perform the new attack.

Task force composition

Organization and membership

20 The task force members shall be identified at least for one year, on a voluntary basis. A chair of the task force shall be identified. The chair of the task force maintains a record with the contact details of each member of the task forces. The JIWG will assist the chair of the task force in selecting the members of the task force.

21 The task force shall be made of the following representatives:

- At least two representatives from evaluation facilities,
- At least one representative of a Certification Body (SOGIS qualified participant),
- At least one representative of the end-users (certificate consumer involved in Risk Management).

22 When an event occurs, each member of the task force may mandate an external recognized expert or a relevant developer to assist and participate to the analysis, particularly when the technical domain of the event required specific high level skills.

Profile requirement

23 The goal of the task force is to perform a technical analysis. Therefore, its members shall have a technical profile (expert, architect, evaluator), or at least shall be able to evidence a technical background. Business or “time to market” consideration shall not undermine the technical analysis of the task force. This kind of consideration shall be raised directly at the JIWG level.