- Défi SEC&SI -

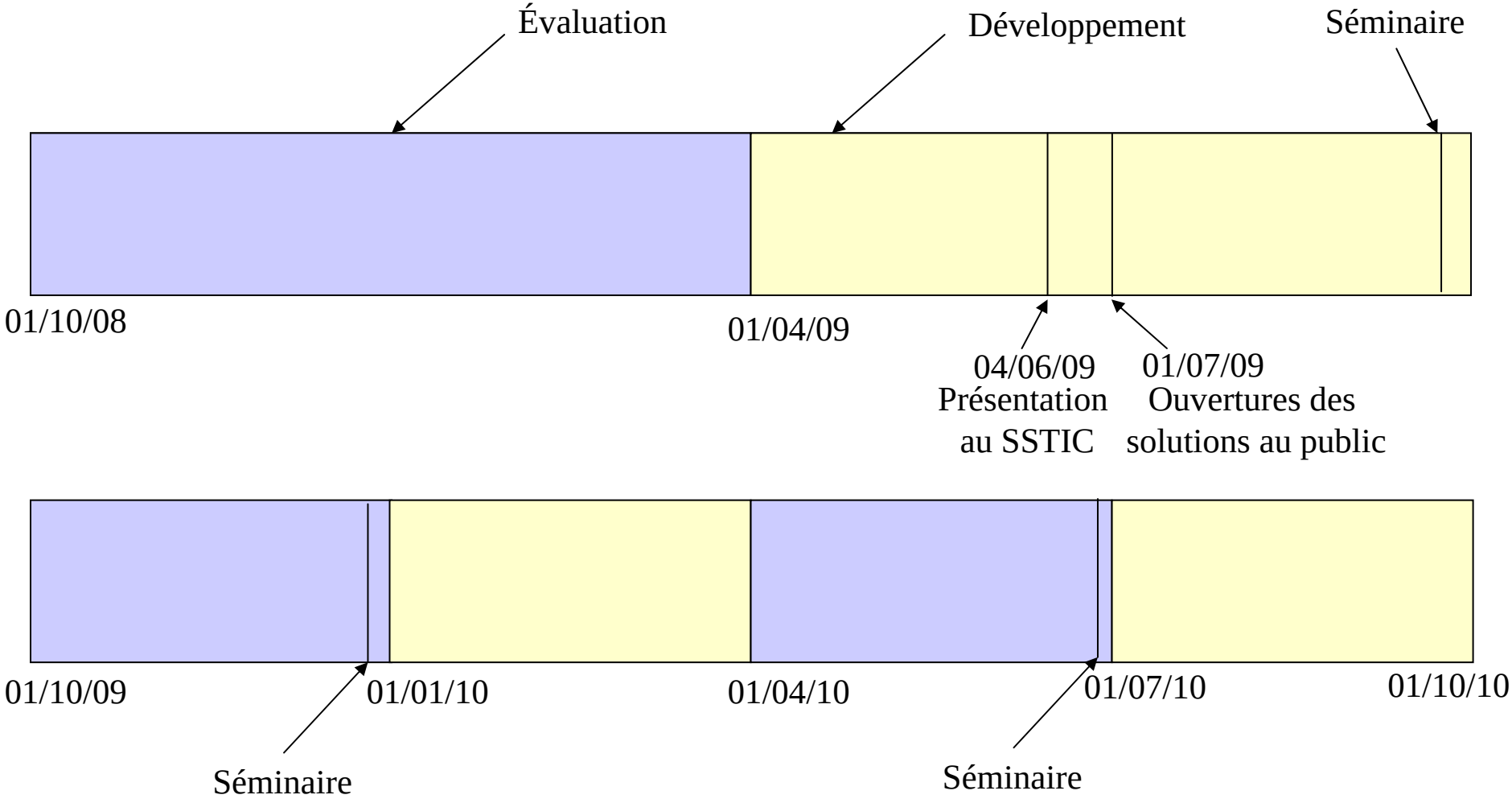
Premier séminaire: lancement de la première phase d'évaluation

ANR, 26 mars 2009

Ordre du jour

- Tour de table
- Introduction
  - Rappel du règlement de la phase d'évaluation
  - Présentation SEC&SI au SSTIC
- Présentation de OSOSOSOS
- Présentation SAFE-OS
- Présentation de SPACLik
- Questions diverses et conclusions

Rappel du calendrier



Mise à disposition des solutions

- Chaque équipe doit mettre à disposition des équipes concurrentes sa solution pour le 1er Avril 2009 au plus tard.

- Il est possible d'utiliser la forge Gforge de l'Adullact ou tout autre moyen plus approprié.

- Cette mise à disposition devra être étendue au public au plus tard le 1er juillet 2009.

Règles pour la publication des attaques (1/2)

- Toute équipe qui met en évidence une vulnérabilité dans une solution concurrente doit impérativement:
  - Prévenir le CERTA :
    - Via l'adresse suivante: reportbug-anr@certa.ssi.gouv.fr
    - Avec utilisation éventuelle (en fonction de la gravité de la vulnérabilité) de la clef GPG du CERTA
      - » http://www.certa.ssi.gouv.fr/certa/contact.html
  - Prévenir l'équipe concurrente.
  - Prévenir éventuellement les développeurs de solutions tierces impactées, en prévenant impérativement le CERTA de toute procédure de ce type engagée.
  - Signaler au jury la découverte d'une vulnérabilité (sans détails).

Règles pour la publication des attaques (2/2)

- Le CERTA communique au jury les premiers éléments d'analyse technique liés à la vulnérabilité mise en évidence, ce qui permettra au jury de coter la vulnérabilité selon le barème décrit dans le règlement.
- Le jury maintient à jour (chaque mois et demi) un classement et un tableau récapitulatif des vulnérabilités découvertes et non corrigées pour chaque solution.
  - http://secsi.adullact.net
- Toute vulnérabilité non corrigée fait perdre des points à l'équipe concernée tous les 15 jours. Il sera donc nécessaire d'être réactif!

- La publication d'une vulnérabilité ne peut intervenir qu'une fois que le CERTA a donné son autorisation explicite.

Premier ministre
Secrétariat général de la défense nationale

Périmètres des attaques

- Sont autorisées les attaques sur la solution elle-même uniquement.
- Aucune attaque sur un serveur réel en production (site internet) n'est bien sûr autorisée.
- Aucune attaque physique ne sera prise en compte.
- Les attaques ne portent que sur certains biens manipulés par la solution (voir règlement).
- Les décisions du jury font autorité et ne sont pas discutables.

- Le périmètre pourra être affiné à l'usage au cours de la phase d'évaluation en cas d'accord de l'ensemble des participants.

Notes et classement

- Chaque équipe se voit attribuer au départ de chaque phase un total de 100 points.
- Ce score évolue au fur et à mesure que des problèmes sont mis en évidence:
    - si l'équipe A met en évidence une vulnérabilité cotée par le jury à 5 points sur les solutions B et C, A marque 10 points tandis que B et C perdent 5 points.
- Un classement est établi à la fin de chaque phase d'évaluation à partir:
    - Des scores courants de chaque solution.
    - D'une note d'ergonomie (2 points pour la première phase)
- L'équipe gagnante est celle qui aura été la mieux classée sur l'ensemble des 3 phases.

Classement final (exemple)

Phase 1: 1. Équipe B 2. Équipe C 3 Équipe A.

Phase 2: 1. Équipe A 2. Équipe B 3 Équipe C.

Phase 3: 1. Équipe A 2. Équipe C 3 Équipe B.

Totaux des classements: Équipe A: 3+1+1=5;

Équipe B: 1+2+3=6;

Équipe C: 2+3+2=7.

Vainqueur: Équipe A.

Présentation au SSTIC

- Présentation (1h) lors du Symposium sur la Sécurité des Systèmes d'Information à Rennes:
  - Introduction (par qui?)
  - 15 minutes par solution (qui pour OSOSOSOS?)
  - Inscriptions fermées mais inscription automatique pour les orateurs.

- Fourniture d'un court papier pour les actes avant le 4 avril 2009 dernier délai.
  - Proposition: fournir le document rédigé au mois de décembre 2009.
  - Quels auteurs?

Premier ministre

Secrétariat général de la défense nationale

Présentation des trois solutions