Nouvelle méthode EBIOS

Réunion courante

3 mai 2018

État d'avancement du projet

Développement

- Méthode : commentaires du Club EBIOS étudiés
- Bases de connaissances : premiers livrables pour fin mai
- Outil : la méthode sera outillée

Accompagnement

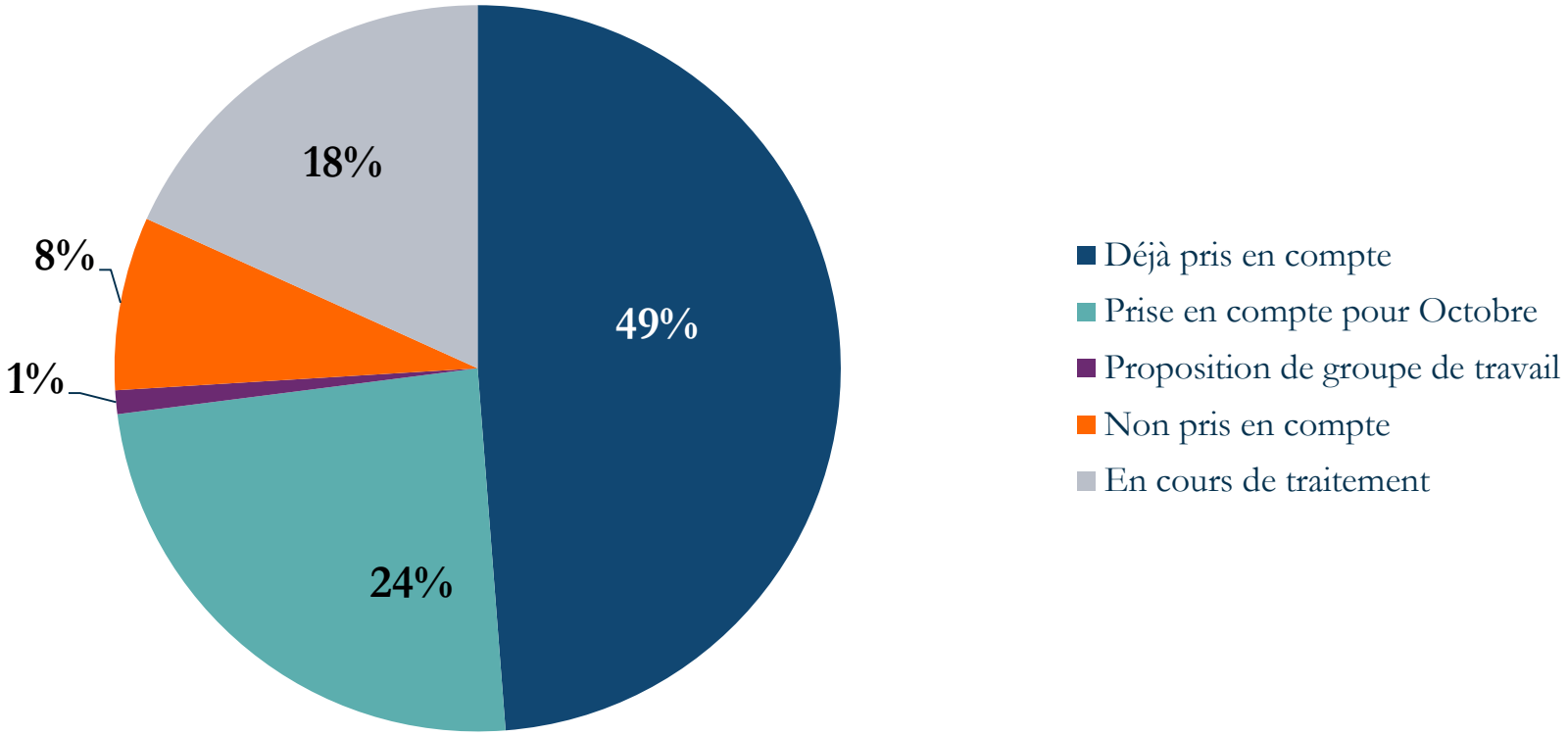
- Formation : référentiel de formation + squelette de support de formation
- Portail Club EBIOS et *Community Manager* : échange avec l'équipe COM ANSSI en mai au sujet de la stratégie de communication

Promotion

- Présentations à des entreprises, au CLUSIR Nord-de-France…
- Accompagnement de l'agence EU-LISA sur la nouvelle méthode
- Groupe de travail sur le *risk management* au Conseil de l'UE
- Publication prévue en Octobre 2018 (FR+EN) : possible de faire des retours sur la méthode et son applicabilité pendant 1 an

Prise en compte des commentaires du Club EBIOS

285 commentaires formulés par le Club EBIOS :



Focus sur les commentaires dans les pages suivantes

Les commentaires acceptés

- **Reformulation** de tournures de phrases peu ou pas claires
- **Précisions** sur des notions (objectif de sécurité, scénarios pratiques vs scénarios de risques, appréciation des risques plutôt que analyse de risques, etc.)
- La notion d'objectif adverse devient **objectif visé** (pour se mettre dans la position de l'attaquant)
- Réintégration de la **notion d'évènement redouté**, élément clé de la méthode et de son lien avec les objectifs visés
- Lien entre scénarios de risque **stratégiques** (atelier 3) et **pratiques** (atelier 4)

Précisions suite à certains commentaires

- « Les durées des ateliers sont proposées à titre indicatif. Elles **n'incluent pas le travail de formalisation à réaliser en amont ou en aval** des différents ateliers »

- Les étapes de construction de scénarios **ne visent pas la recherche de l'exhaustivité** (d'où la présence d'indications volumétriques comme le nombre de valeurs métiers ou le nombre de couples Source de risque/Objectifs visés généralement suffisants pour la suite de l'étude)

- Logique de *dissuasion* dans le traitement des risques : « C'est-à-dire que l'objectif est de complexifier la tâche de la source de risque pour **rendre son retour sur investissement défavorable, voire insupportable**, et le lui faire comprendre. »

Propositions de GT à mener par le Club EBIOS

- Elaboration des scénarios pratiques : quelles autres méthodes que l'utilisation d'une *cyber kill chain* ?
- *Cyber kill chain* : créer une base de connaissances de modes d'actions élémentaires
- Besoins de sécurité : comment les utiliser de bout-en-bout dans l'analyse de risques ?
- Compatibilité entre EBIOS et les grands standards (NIST, IEC 62443, ISO)

Un vote pourra être proposé sur la plateforme du Club pour identifier les GT qui suscitent l'intérêt