Besoins LOT 9

Fourniture de prestations de transfert de compétences de haut niveau d'expertise en recherche de vulnérabilités et rétroconception - environnements variés

Description du profil attendu pour les formateurs

1. Expérience professionnelle requise

- **Plusieurs années d'expérience** en recherche de vulnérabilités ou en audit de logiciels binaires.
- Pratique démontrable dans la mise en œuvre de **campagnes de fuzzing** ou **audit d'applications**.
- Pratique professionnelle dans l'analyse statique et dynamique d'applications.
- Expérience d'outils d'analyse bas niveau.

2. Compétences techniques indispensables

- Maîtrise du **fonctionnement global du système d'exploitation concerné**.
- Connaissance approfondie des techniques abordées en formation.
- Maîtrise des TP réalisés en formation.
- Très bonne compréhension des **mécanismes de sécurité** abordés en formation.
- Usage confirmé des mécanismes abordés en formation.

3. Savoirs et savoir-faire attendus

- Capacité à expliquer les **mécanismes internes et leurs interactions**.
- Capacité à enseigner la manipulation des techniques lors des TP.
- Capacité à guider les apprenants dans mise en œuvre pratique d'analyses avancées.

4. Éléments différenciants (facultatif)

- Diplômes ou certifications spécialisés dans le domaine.
- Formations récentes reçues en cybersécurité.
- Expérience dans des scénarios réels proches de ceux enseignés.
- Contributions open-source.
- Participation à des conférences, CTF ou publications techniques avancées.

Description détaillée des prestations attendues

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC09/01	Fuzzing	**Objectif pédagogique** : Appréhender les méthodologies de fuzzing de logiciel. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Recherche de vulnérabilités et fuzzing. - Outillage et fuzzing de fichiers exécutables, QBDI, Honggfuzz, optimisation. - Emulation : Qemu, AFL++, unicorn. - Exécution symbolique : BV, array, concolic fuzzer.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 4 à 5 jours pour le cours en présentiel.

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC09/02	Retro-ingénierie logicielle	**Objectif pédagogique** : Appréhender les méthodes et techniques de rétro-ingénierie logicielle. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Analyse statique, architectures, assembleur, formats PE et ELF. - Analyse dynamique : x84dbg, IDA, Frida, pyQBDI - Protection des binaires : obfuscation, anti-VM.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 4 à 5 jours pour le cours en présentiel.

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC09/03	Android sécurité	**Objectif pédagogique** : Appréhender les mécanismes des applications utilisées sous Android. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - SDK Android, APK, storage, outillage. - Frida, injection de code, recherche vulnérabilité sur un APK - Analyse d'applications protégées - Internals : bootloader, firmware, kernel, trutzone	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 4 à 5 jours pour le cours en présentiel.