Besoins LOT 8

Fourniture de prestations de transfert de compétences de haut niveau d'expertise en investigation Windows

Description du profil attendu pour les formateurs

1. Expérience professionnelle requise

- **Plusieurs années d'expérience** sur les environnements Microsoft Windows à un niveau bas système.
- Pratique démontrable dans l'analyse des fonctionnements internes de Windows.
- Pratique professionnelle en analyse de malwares en environnement réel.
- Expérience d'outils d'analyse bas niveau sur Windows.

2. Compétences techniques indispensables

- Maîtrise du **fonctionnement global du système d'exploitation Windows**.
- 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 sous Windows abordés en formation.

3. Savoirs et savoir-faire attendus

- Capacité à expliquer les **mécanismes internes de Windows 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 sous Windows.

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
TC08/01	Mécanismes internes de Windows	**Objectif pédagogique** : Comprendre le fonctionnement interne du système d'exploitation Microsoft Windows. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Processus : gestion mémoire, format PE, isolations. - WinDBG, noyau : appels système, IoManager, IRQL, APC, DPC. - Modèle de contrôle d'accès : token, security descriptor, privilèges. - WMI, ETW, WoW64.	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
TC08/02	Analyse forensique sous Windows	**Objectif pédagogique** : Appréhender l'analyse forensique sur systèmes Windows, à des fins d'investigation sur cyber-attaque. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Anatomie d'une attaque ciblée avancée. - Espace mémoire, processus, threads Windows - Analyse de malwares : API Win32, persistance, analyse statique et dynamique, signatures yara et suricata. - Investigation, méthodologie, traces d'exécution.	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
TC08/03	Analyse malware avancée sous Windows	**Objectif pédagogique** : Appréhender l'analyse de codes malveillants complexes ayant des interactions avancées avec le système d'exploitation Windows. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Analyse d'un malware utilisé lors d'APT. - Reverse Engineering avec Ghidra : anti analyse, anti debug - Désobfuscation et unpacking avec Python. - Noyau Windows : DES bypass, patchGuard, rootkits.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 4 à 5 jours pour le cours en présentiel.