Besoins LOT 6

Fourniture de prestations de transfert de compétences de haut niveau d'expertise sur la détection des incidents de sécurité

Description du profil attendu pour les formateurs

1. Expérience professionnelle requise

- **Plusieurs années d'expérience** en sécurité des systèmes d'information.
- Pratique démontrable en détection d'incidents de sécurité en environnement opérationnel.
- Pratique professionnelle de la surveillance des systèmes et des réseaux.
- Expérience dans l'analyse d'événements de sécurité et la qualification d'incidents.

2. Compétences techniques indispensables

- Maîtrise des **principes de la détection des incidents de sécurité**.
- 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 de détection abordés en formation.

3. Savoirs et savoir-faire attendus

- Capacité à expliquer les **enjeux et objectifs de la détection des incidents**.
- Capacité à enseigner la manipulation des techniques lors des TP.
- Capacité à guider les apprenants dans les mécanismes de détection par des **cas pratiques et scénarios réalistes**.

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
TC06/01	Détection des incidents de sécurité	**Objectif pédagogique** : Acquérir des méthodologies avancées d'analyse et de détection de comportements malveillants pour assurer une protection proactive face aux cybermenaces. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Panorama de la détection système. - Kill chain / Mitre attack. - Techniques de détection pour Windows : journaux, powershell, persistance, élévation de privilèges. - Linux : auditd, wazuh, ossec	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours pour le cours en présentiel.

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC06/02	Détection et réponse aux incidents de sécurité	**Objectif pédagogique** : Apprendre à détecter et répondre aux incidents de sécurité. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Phases d'une attaque, kill chain. - Architecture de détection : IDS, IPS, SIEM, endpoints - Outils et techniques : wireshark, Bro, détection - SOC, CSIRT	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours pour le cours en présentiel

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC06/03	Détection et réponse aux incidents de sécurité avancée	**Objectif pédagogique** : Enrichir une infrastructure de détection en place. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Recherche de canaux de communication avec l'infrastructure de l'attaquant. - Détection des persistances et Détection d'exfiltration par USB - Recherche d'événement typique d'une exploitation de chemins de contrôle Active Directory - Réponse à incident : outil de collecte, large parc.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours pour le cours en présentiel