Besoins LOT 5

Fourniture de prestations de transfert de compétences de haut niveau d'expertise en administration avancée des systèmes d'information en expertise Linux

Description du profil attendu pour les formateurs

1. Expérience professionnelle requise

- **Plusieurs années d'expérience** en administration et sécurisation de systèmes Linux.
- Pratique démontrable sur des environnements Linux ou SELinux en production.
- Pratique professionnelle de la mise en œuvre de mesures de sécurité sur serveurs Linux ou SELinux.
- Expérience dans l'analyse et la correction de faiblesses de configuration Linux.

2. Compétences techniques indispensables

- Maîtrise des **fondamentaux 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 de sécurité abordés en formation.

3. Savoirs et savoir-faire attendus

- Capacité à **implémenter des mécanismes de sécurité défensifs** dans le système d'exploitation concerné.
- Capacité à enseigner la manipulation des techniques lors des TP.
- Capacité à guider les apprenants dans l'**implémentation opérationnelle des bonnes pratiques de sécurité Linux ou SELinux**.

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
TC05/01	Sécurité Linux	**Objectif pédagogique** : Gérer en profondeur les problèmes de sécurité liés aux systèmes Linux. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Cryptographie : SSH, DNSSEC, GnuPG, X509. - Sécurité Hôte : Grub, Syslog, AIDE, détection de rootkit. - Contrôle d'accès : droits, ACL, SELinux, etc. - Sécurité Réseau : tcpdump, nmap, netfilter, OpenVPN	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
TC05/02	Comprendre SELinux et savoir modifier la politique de sécurité	**Objectif pédagogique** : Comprendre les mécanismes du fonctionnement de SELinux. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Présentation SELinux. - booléens : getsebool, setsebool - Gestion d'une politique de sécurité : setfiles, restorecon, fixfiles, chcon, newrole, runcon, semanage, apol, audit2why, audit2allow - modification d'un politique de sécurité	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 2 à 3 jours pour le cours en présentiel.