Besoins LOT 4

Fourniture de prestations de transfert de compétences de haut niveau d'expertise dans le domaine de la protection et de la sécurité informatique défensive - méthodes et technologies variées

Description du profil attendu pour les formateurs

1. Expérience professionnelle requise

- **Plusieurs années d'expérience** en sécurité défensive ou analyse de risque.
- Pratique démontrable dans des environnements en production.
- Pratique professionnelle en environnement lié à la sécurisation des SI.
- Expérience en **sécurité du système concerné ou pilotage d'analyse de risque**.

2. Compétences techniques indispensables

- Maîtrise complète de la méthodologie à appliquer dans le domaine concerné.
- Connaissance approfondie des techniques abordées en formation.
- Maîtrise des TP réalisés en formation.
- Usage confirmé des mécanismes de sécurité abordés en formation.

3. Savoirs et savoir-faire attendus

- Capacité à **implémenter des mécanismes de sécurité défensif** dans le système concerné ou capacité à **former des participants à l'autonomie**.
- Capacité à enseigner la manipulation des techniques et des bonnes pratiques lors des TP.
- Capacité à guider les apprenants dans l'**implémentation complète d'un scénario**.

4. Éléments différenciants (facultatif)

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

Description détaillée des prestations attendues

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC04/01	EBIOS RM 2018 Risk Manager	**Objectif pédagogique** : Appréhender la réalisation d'une analyse des risques selon la méthodologie EBIOS 2018 Risk Manager. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Les bases de la gestion de risques. - Déroulement de la méthode : 5 ateliers - Mise en application des concepts sur un cas d'étude.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 2 à 4 jours pour le cours en présentiel.

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC04/02	Analyse inforensique avancée	**Objectif pédagogique** : Appréhender la corrélation des évènements, retro-concevoir des protocoles de communications, analyser des systèmes de fichiers corrompus, connaître et analyser la mémoire volatile des systèmes d'exploitation. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - inforensique réseau, analyse post-mortem réseau, IOC - mémoire volatile, analyse des processus, shellcode, handles, windbg - FileSystem NTFS, artefacts, timestomping - trace d'exécution et mouvement latéraux, eventID - cas d'utilisation timesketch.	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
TC04/03	Audit sécurité d'applications mobiles Android et iOS	**Objectif pédagogique** : Appréhender les problématiques sécurité des applications mobiles, savoir effectuer une analyse statique et dynamique, intercepter le trafic d'une application mobile Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - écosystème iOS et analyse statique d'applications - écosystème Android et analyse statique d'applications - Analyse des données d'applications iOS - Analyse dynamique d'applications iOS et Android - Sécurité des communications des applications iOS et Android - Instrumentation d'applications Android avec Frida.	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
TC04/04	Sécurisation des infrastructures Windows	**Objectif pédagogique** : Appréhender le durcissement d'un serveur Windows, administrer de façon sécurisée, sécuriser les postes de travail, auditer une infrastructure. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Durcissement système et réseau : journalisation, cloisonnement, parefeu, IPSec. - Administration sécurisée : TTP, AD, GPO, etc. - Sécurité du poste de travail : bitlocker, isolation, secure boot, VBS, WDAC. - Auditer son infrastructure : chemins d'attaque, BloodHound, simulation.	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
TC04/05	Sécurité des Architectures	**Objectif pédagogique** : Appréhender les problématiques liées à l'architecture des réseaux complexes, connaître les solutions associées, savoir auditer une architecture, développer un plan d'évolution sécurisée d'une architecture. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Réseaux et Flux : VLAN, Diode, filtrage, authentification. - Architecture de base : risques, administration, DNS, VPN - Architectures spécifiques : virtualisation, wifi, cloud, SCADA, GTB, IoT.	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
TC04/06	ISO 27005 Risk Manager	**Objectif pédagogique** : Acquérir une compréhension globale des concepts, de la norme, des méthodes et des techniques de gestion des risques, mettre en œuvre la méthode ISO 27005. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Norme ISO 27005, PDCA, gestion du processus de management du risque, évaluation du risque, risque résiduel, communication du risque - Mise en situation avec une étude de cas.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 2 à 4 jours pour le cours en présentiel.

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC04/07	Cybersécurité des systèmes industriels	**Objectif pédagogique** : Appréhender la cybersécurité des systèmes industriels par une approche pragmatique et pratique, développer un plan de sécurisation, auditer les SI industriels, initier la préparation de plans de réponse à incident. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Architectures des SI industriels, ISA/IEC 62443 - Protocoles ModBus, détection, filtrage - Incidents représentatifs et évolutions, cloud industriel - Référentiels sur la sécurité des systèmes d'information industriels, guide ANSSI, IEC, NIST, ISO - Réponse à incident sur un système industriel, IOC, artefacts industriels.	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
TC04/08	Sécurité des environnements cloud	**Objectif pédagogique** : Appréhender le fonctionnement et les risques de sécurité inhérent aux solutions de développement agile, identifier les points faibles de ce type d'infrastructures, exploiter les faiblesses afin d'en évaluer l'impact, comprendre les solutions de remédiations les plus efficaces. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Environnements Agiles, outils DevOPS et CI/CD - Infrastructure As Code, terraform - Services du Cloud, IAM, roles, SCP, VPC, serverless - Elévation de privilèges, kubernetes, RBAC	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
TC04/09	Tests d'intrusion des objets connectés	**Objectif pédagogique** : Evaluer et renforcer la sécurité des dispositifs IoT, mettre en place des stratégies efficaces pour défendre ces dispositifs contre les attaques. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Concepts de base de l'Internet des objets - Reverse Engineering Hardware, I2C, UART, timing attack - Récupérer et Analyser le Firmware, port JTAG, extraction SWD - Reverse Software, ghidra, overflow sur UART - Attaques par Faute, exploitation, STM32, glitch compteur - Radio IoT, WiFi, Bluetooth/BLE	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
TC04/10	Tests d'intrusion des systèmes industriels	**Objectif pédagogique** : Comprendre le fonctionnement des SI industriels, découvrir les outils et les méthodologies pour les tests d'intrusion. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - SI industriels, modèle CIM, composants - Tests d'intrusion : principes, metasploit - Active Directory, powerview, crackmapexec - Vulnérabilités en environnement industriel, protocoles modbus S7 OPC, supervision de sécurité, correctifs - Sureté de fonctionnement - Tests d'intrusion sur API, web, FTP, protocoles pripriétaires - Sécurisation des SI industriels : cloisonnement, diode	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
TC04/11	Sécurité des systèmes d'intelligence artificielle	**Objectif pédagogique** : Comprendre le fonctionnement des systèmes d'IA, encadrer et gouverner les usages de l'IA. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Cartographie des usages de l'IA en entreprise - Objectifs et enjeux de sécurité de l'IA - Conformité et cadre réglementaire de l'IA - Gestion des risques de l'Intelligence Artificielle - Sécurité de l'IA et gestion de projet - Résilience des systèmes d'IA : IA Act	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
TC04/12	Audit des systèmes d'intelligence artificielle	**Objectif pédagogique** : Préparer et réaliser un audit de sécurité approfondi d'un système d'IA. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Vulnérabilités du modèle : attaques antagonistes, injection de prompt, empoisonnement des données d'entrainement. - Vulnérabilités applicatives : injection via les sorties du modèle, fuite de données sensibles, élévation de privilèges via le modèle, attaque sur RAG. - Mesures défensives et bonnes pratiques : Méthodes de préparation et de restitution d'un audit de sécurité IA, gestes à adopter en cas d'attaque, considérations juridiques et protection des données.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 2 à 4 jours pour le cours en présentiel.