Besoins LOT 10

Gestion par un opérateur intermédiaire (tiers) de la fourniture de prestations de transfert de compétences de haut niveau d'expertise sur environnements virtualisés variés

Description du profil attendu pour les formateurs pour le cas des classes virtuelles (synchrones)

1. Expérience professionnelle requise

- **Plusieurs années d'expérience** dans les domaines abordés lors des formations.
- Pratique démontrable dans les domaines abordés lors des formations.
- Pratique professionnelle dans les domaines abordés lors des formations.

2. Compétences techniques indispensables

- Maîtrise du **fonctionnement technique** dans les domaines abordés lors des formations.
- 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** dans les domaines abordés lors des formations.
- Capacité à enseigner la manipulation des techniques lors des TP.
- Capacité à guider les apprenants dans mise en œuvre pratique.

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	Plateforme identifiée au moment du lancement de la consultation
TC10/01	Pentest web avancé et revue de code en profondeur	**Objectif pédagogique** : Appréhender le pentest web avancé et la revue de code en profondeur. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - **Maîtrise pratique du pentesting web et de la sécurité applicative** : exercices pratiques (labs) permettant d'apprendre à trouver et exploiter des vulnérabilités réelles (tel que XSS, SQLi, JSON Web Tokens, authentification/autorisation, etc.) et à comprendre les failles au niveau du code ou de la logique d'application. - **Approche technique basée sur des technologies et cas réels** : technologies variées, manipulation de protocoles web, exploitation de vulnérabilités tirées de CVE réels, revue de code, et concepts de sécurité modernes (JWT, TLS, cryptographie vulnérable). - **Labs et travaux pratiques interactifs dans un environnement web** : en ligne via un navigateur, sans nécessité de configurer des machines virtuelles. - **Vidéos et soutien pédagogique** : vidéos approfondies et support expert. - **Certification de progression** : certificats de réalisation pour valoriser les compétences acquises.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 an pour l'accès en distanciel.	PENTESTERLAB (https://pentesterlab.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/02	Pentesting, évaluation web, analyse des menaces et réponse aux incidents	**Objectif pédagogique** : Appréhender le pentesting, l'évaluation web, l'analyse des menaces et réponse aux incidents à un niveau avancé et reconnu. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Acquérir des compétences pratiques reconnues en **cybersécurité offensive et défensive** - Préparer les certifications reconnues : OSCP+, OSEP, OSWE, etc. couvrant des domaines comme le pentesting, l'évaluation web, l'analyse des menaces et la réponse aux incidents. - Maîtriser des techniques d'attaque et de défense dans des environnements simulés proches du réel : scénarios avancés de tests d'intrusion et de sécurité web, réseaux, exploitation avancée.	Travaux pratiques sur l'ensemble des méthodes et outils présentés, avec des labs réalistes.	Durée 1 an pour l'accès en distanciel.	OFFENSIVE SECURITY (https://www.offsec.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/03	CTF progressif avec scénarios offensifs et défensifs	**Objectif pédagogique** : Développer des compétences opérationnelles en cybersécurité grâce à une plateforme interactive orientée pratique**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Proposer un apprentissage orienté hands-on avec des labs interactifs, des environnements virtuels et des Capture-The-Flag (CTF) permettant aux apprenants d'acquérir des compétences techniques concrètes en sécurité offensive et défensive, sans configuration locale complexe. - Proposer des chemins d'apprentissage progressifs allant du débutant à des compétences avancées, facilitant la montée en expertise des équipes. - Intégrer une culture de cybersécurité en impliquant les équipes dans des exercices interactifs gamifiés, soutenus par une communauté active de praticiens et d'apprenants, favorisant l'échange et l'amélioration continue des connaissances techniques. - Préparer les certifications reconnues THM	Travaux pratiques sur l'ensemble des méthodes et outils présentés, avec des scénarios réalistes.	Durée 1 an pour l'accès en distanciel.	TRYHACKME (https://tryhackme.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/04	Pratiques en DevSecOps et sécurité des environnements cloud-native	**Objectif pédagogique** : Développer des compétences techniques pratiques en DevSecOps et sécurité des environnements cloud-native**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Proposer des formations orientées pratique couvrant les technologies Kubernetes, Docker, Linux, Cloud, CI/CD et des thématiques de sécurité associées. - Aborder des outils et stacks utilisés en entreprise (Kubernetes, Docker, Helm, Terraform, Cloud providers, pipelines CI/CD). - Proposer des labs intégrés, permettant aux apprenants de manipuler directement des environnements techniques réels (Kubernetes, conteneurs, systèmes Linux, cloud) sans installation locale.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 an pour l'accès en distanciel.	KODEKLOUD (https://kodekloud.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/05	Sécurité Kubernetes	**Objectif pédagogique** : Comprendre les fondamentaux de la sécurité Kubernetes en environnement professionnel Linux Foundation**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Fournir une compréhension structurée des concepts clés de sécurité Kubernetes, incluant la gestion des accès (RBAC), la sécurité des clusters, des workloads et des composants critiques, en autonomie. - Les contenus s'appuient sur les technologies Kubernetes officielles et les standards reconnus de l'écosystème cloud-native, en lien avec les recommandations de la Cloud Native Computing Foundation (CNCF) et les pratiques de sécurité actuelles).	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 an pour l'accès en distanciel.	LINUX FOUNDATION (https://www.linuxfoundation.org/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/06	Linux Kernel Internals	**Objectif pédagogique** : Comprendre en profondeur l'architecture et le fonctionnement interne du noyau Linux**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Fournir une compréhension détaillée des mécanismes internes du noyau Linux, incluant la gestion des processus, de la mémoire, des interruptions, du scheduling et des appels système, afin de maîtriser le comportement du système au plus bas niveau. - Intégrer des travaux pratiques permettant d'explorer le code source du noyau, de compiler un kernel personnalisé, d'écrire et charger des modules noyau, et d'analyser le fonctionnement interne à l'aide d'outils dédiés (Linux Foundation).	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 4 à 5 jours pour l'accès en distanciel synchrone.	LINUX FOUNDATION (https://www.linuxfoundation.org/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/07	Sécurité du Linux Kernel	**Objectif pédagogique** : Approfondir la compréhension des mécanismes de sécurité du noyau Linux**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Maîtriser les concepts et composants de sécurité intégrés au noyau Linux, notamment les modèles de permissions, les capacités, les mécanismes de contrôle d'accès et les surfaces d'attaque au niveau kernel. - Couvrir les fonctionnalités de sécurité spécifiques au noyau Linux (frameworks de sécurité, contrôles d'accès obligatoires, isolation, protections mémoire), avec une approche technique orientée compréhension et usage en environnement réel (Linux Foundation).	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 4 à 5 jours pour l'accès en distanciel synchrone.	LINUX FOUNDATION (https://www.linuxfoundation.org/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/08	Entrainement au pentest	**Objectif pédagogique** : Appréhender le test d'intrusion avec une approche méthodologique complète sur des labs professionnels**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Aborder des technologies clés du pentesting (réseaux, systèmes, Active Directory, applications web, protocoles, élévation de privilèges, mouvements latéraux), avec un focus sur l'exploitation des vulnérabilités et la compréhension approfondie des mécanismes sous-jacents. - Formation académique et instance d'environnement d'entrainement (pro labs). - Préparer les certifications reconnues HTB CPTS	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 an pour l'accès en distanciel.	HACK THE BOX (https://www.hackthebox.com/°

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/09	Cybersécurité défensive (Blue Team).	**Objectif pédagogique** : Développer des compétences opérationnelles en cybersécurité défensive (Blue Team)**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Aborder la détection, l'analyse et la réponse aux incidents de sécurité, en permettant aux apprenants de se former aux métiers de la Blue Team à travers des scénarios concrets de cyberattaques et d'activités malveillantes. - Proposer des labs basés sur des traces réelles (logs, alertes, fichiers, artefacts système) permettant de pratiquer l'investigation numérique, l'analyse d'incidents, la détection de compromission et la réponse aux attaques. - Aborder des technologies et concepts clés tels que l'analyse de logs, les SIEM, la détection d'intrusion, la forensique, la threat hunting et l'analyse de malwares.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 an pour l'accès en distanciel.	BLUE TEAM LABS ONLINE (https://blueteamlabs.online/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/10	Opérations Blue Team avancée.	**Objectif pédagogique** : Développer une expertise avancée en cybersécurité défensive et opérations Blue Team**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Acquérir les compétences techniques nécessaires à la détection, l'investigation et la réponse à des incidents de sécurité complexes, en s'adressant à des profils ayant déjà une expérience opérationnelle en cybersécurité défensive. - Couvrir des domaines clés tels que l'analyse de logs, la détection avancée, la threat hunting, la forensique numérique et la réponse à incident, avec une approche orientée pratiques professionnelles et environnement SOC. - Préparer les certifications reconnues BTL2	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 an pour l'accès en distanciel.	SECURITY BLUE TEAM (https://www.securityblue.team/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/11	Opérations Red Team avancée.	**Objectif pédagogique** : Développer une expertise avancée en opérations de Red Team en conditions réelles**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Conduire des opérations offensives complètes, en reproduisant les tactiques, techniques et procédures utilisées par des attaquants réels dans des environnements d'entreprise. - Couvrir les environnements Active Directory, les attaques réseau, la post-exploitation, les mouvements latéraux, l'évasion des mécanismes de détection et les techniques utilisées lors d'opérations de Red Team. - Préparer les certifications reconnues BTL2	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 an pour l'accès en distanciel.	ZERO POINT SECURITY (https://www.zeropointsecurity.co.uk/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/12	Data engineering.	**Objectif pédagogique** : Maîtrisez le Data Warehouse, le calcul distribué et le temps réel dans un contexte Big Data**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Préparation au Big Data, stockage de données, Hadoop, Spark, flots de données en temps réel. - Automatisation et déploiement d'applications, construire des DAGs en Python. - Analyse en temps réel, automatisation des pipelines, calcul distribué.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 an pour l'accès en distanciel.	BLENT AI (https://blent.ai/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/13	Devops engineering.	**Objectif pédagogique** : Maîtrisez le cycle de vie des applications, l'approche GitOps et l'automatisation des infrastructures**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Préparation au DevOps, maitrise des concepts du cloud, Déploiement d'applications et GitOps. - Infrastructure as Code, Terraform, Ansible, monitoring avec Prometheus, Grafana. - Mise en place d'une stratégie de déploiement de mise à jour Canary sur Kubernetes, Exécution d'un cluster Kafka résilient.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 an pour l'accès en distanciel.	BLENT AI (https://blent.ai/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/14	ANDROID KERNEL FUZZING.	**Objectif pédagogique** : Mettre en place des environnements spécifiques de fuzzing du noyau Android**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Mécanismes de sécurité du noyau Android : MAC, SELinux, verified boot, KASLR, CFI, protection pile. - Analyse et exploitation des vulnérabilités : débogage : adb, kgdb, analyse dmesg, exploitation UAF et Race Conditions, syzkaller Android, utilisation kcov, Kernel Sanitizers. - Durcissement et stratégies de mitigation.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 3 à 5 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/15	FUZZING IOS & MACOS KERNEL	**Objectif pédagogique** : Découvrir des vulnérabilités d'escalade de privilèges dans le noyau d'iOS et macOS**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Mécanismes de sécurité Apple : Sandbox et Seatbelt, Secure Boot, BootROM, et Secure Enclave Processo - Analyse et exploitation : utilisation de LLDB et KDP, fuzzing du noyau iOS, adaptation de syzkaller et usage de kcov, KASAN - Durcissement et défense : configurations de sécurité recommandées (PAC, KASLR), rôle du SEP et d'iBoot.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 3 à 5 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/16	APPLIED AI/LLM FOR ANDROID REVERSING	**Objectif pédagogique** : Exploiter l'IA et les LLM pour accélérer la rétro ingénierie Android**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Analyse statique assistée par l'IA, LLM pour l'audit de code, reverse engineering d'APKs, annotation du code décompilé par l'IA - Analyse dynamique et automatisation par l'IA : génération de scripts Frida par l'IA, générer des harnais de fuzzing (Java/Native), intégration avec AFL++ ou libFuzzer, création de modèles Nuclei générés par l'IA.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 à 2 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/17	AI/LLM FOR VULNERABILITY RESEARCH	**Objectif pédagogique** : Intégrer l'IA dans un workflow de recherche de vulnérabilités**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - OSINT et CTI : extraction et structuration des indicateurs de compromission (IOC) à partir de sources non structurées - Reverse engineering : assistance par IA pour l'annotation de code - Identification de vulnérabilités : analyse statique augmentée par LLM pour identifier des schémas de code dangereux ou des sink non protégés, fuzzing.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 à 2 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/18	AI/LLM FOR PENTESTING	**Objectif pédagogique** : Exploitez les modèles d'IA et de LLM pour automatiser et améliorer les phases d'un test d'intrusion**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Outils et frameworks pour le pentesting basé sur l'IA : API OpenAI, extensions Burp Suite - Détection de vulnérabilités assistée par l'IA - Analyse dynamique et génération d'exploits avec l'IA - Génération d'e-mails et de messages de phishing convaincants - Automatisation avec l'IA de l'escalade de privilèges et du mouvement latéral.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 à 2 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/19	AI, ML & LLM FOR REVERSING	**Objectif pédagogique** : Améliorer l'analyse de binaires avec des outils basés sur l'IA et les LLM**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Outils et frameworks pour la rétro ingénierie pilotée par l'IA : OpenAI Codex, BinaryAI et scripts d'IA personnalisés - IA pour l'analyse statique, la compréhension du code obfusqué, reconnaissance des motifs malveillants - IA pour l'analyse dynamique, analyse de la mémoire, traçage d'exécution - IA pour l'analyse des firmwares et des systèmes embarqués	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 à 2 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/20	REVERSING eBPF Linux	**Objectif pédagogique** : Améliorer les techniques de rétro engineering spécifiques à eBPF**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Types de programmes eBPF : XDP, TC, tracepoints, kprobes, uprobes, format du bytecode eBPF - Outils de compilation : de C vers eBPF avec LLVM, désassemblage de bytecode eBPF - Helpers eBPF, exploiter les faiblesses de l'analyse statique - Analyse dynamique : tracer l'exécution de programmes eBPF avec ftrace et perf, fuzzing, audit de sécurité d'applications eBPF.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 à 2 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/21	REVERSING RISC-V APPLICATION	**Objectif pédagogique** : Maîtriser la rétro engineering de RISC-V**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Jeu d'instructions RISC-V : format des instructions, encodage, pseudo-instructions, ABI RISC-V, compilateurs GCC/LLVM, assembleur, éditeur de liens, format binaire - Émulation et simulation : QEMU, Spike, TinyEMU, radare2, objdump, Ghidra - Analyse statique : reconstruction de flux, identification des structures de contrôle, reverse de firmware embarqué - Cryptographie, Side-channels, fuzzing d'applications RISC-V	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 à 2 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/22	PRACTICAL NETWORKS FUZZING	**Objectif pédagogique** : Maîtriser le fuzzing de protocoles réseau pour identifier des failles de sécurité Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Fuzzing workflow pour les applications réseau - Analyse et débogage des résultats de fuzzing : analyse des crashes et débogage - Fuzzing de protocoles : HTTP, SIP, SMTP; structure-Aware Fuzzing - Exécution symbolique et concolique, fuzzing différentiel et personnalisé.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 2 à 4 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/23	PRACTICAL FUZZING FOR VULNERABILITY RESEARCH	**Objectif pédagogique** : Maîtriser la méthodologie de fuzzing de bout en bout pour la recherche de vulnérabilités Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Architecture des fuzzers modernes : mutation, génération, feedback et couverture de code - AFL++, LibFuzzer et honggfuzz, harnais de fuzzing - Dictionnaires et grammaires, optimisation de la vitesse d'exécution, fuzzing distribué - Windows fuzzing : WinAFL, Winafl – cmin - Debugging : GDB, WinDbg, LLDB, fuzzing avec QEMU, Frida, DynamoRIO.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 3 à 5 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/24	DOCKER SECURITY AUDIT	**Objectif pédagogique** : Maitriser les audits de sécurité sur les environnements Docker Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Bases du Dockerfile, principes du moindre privilège - Scanning de vulnérabilités : trivy, images signées - Mécanismes d'isolation Linux : Namespaces, cgroups, capabilities, AppArmor - Durcissement : docker.sock, namespaces.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 à 3 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/25	KUBERNETES SECURITY AUDIT	**Objectif pédagogique** : Auditer les environnements Kubernetes pour identifier et corriger les mauvaises configurations et les vulnérabilités de sécurité Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Pods, Controllers : Deployments, StatefulSets, ReplicaSets, Services, Ingress, et rôle de kube-proxy - Identité, réseau et contrôle d'accès : Kubeconfig, certificats client, RBAC, Pod Network, Cluster IP, NodePort, LoadBalancer - Reconnaissance et énumération : kubectl, apiservers, kubelets, - Obtenir un accès cluster-admin	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 à 3 jours pour l'accès en distanciel.	FUZZING LABS (https://fuzzinglabs.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/26	Red Team et Blue Team	**Objectif pédagogique** : Comprendre les rôles et objectifs respectifs des équipes Red Team et Blue Team**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Appréhender les outils offensifs et défensifs, en lien avec les tests d'intrusion, la surveillance des systèmes, l'analyse des incidents et la protection des infrastructures. - Évaluer le niveau de sécurité d'un système d'information, améliorer la résilience des organisations et renforcer les capacités des équipes internes. - Faire collaborer les équipes offensives et défensives afin d'optimiser la posture de sécurité et de favoriser une amélioration continue face aux menaces cyber	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 1 an pour l'accès en distanciel.	DIATEAM (https://www.diateam.net/fr/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/27	Prédire et décider avec l'IA	**Objectif pédagogique** : Acquérir les bases de la compréhension et de l'exploitation des données**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Aborder les principes fondamentaux de structuration des données, incluant la qualité, la cohérence et l'organisation des informations, afin de faciliter leur analyse et leur interprétation. - Apprendre à lire et interpréter des données à l'aide d'indicateurs, de représentations simples et de raisonnements analytiques, dans une logique d'aide à la décision. - Formation sous forme de modules en ligne combinant vidéos, activités pédagogiques et évaluations, permettant une progression autonome et structurée des apprenants	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 4 à 5 jours en distanciel.	FUN MOOC (https://www.fun-mooc.fr/fr/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/28	Rétro-ingénierie	**Objectif pédagogique** : Acquérir les bases de la rétro-ingénierie pour analyser des fichiers**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Analyse de documents et de scripts malveillants. - Architecture et format des binaires. - Analyse statique avancée, analyse dynamique - Projet pour valider la micro certification FUN MOOC	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée 4 à 5 jours en distanciel.	FUN MOOC (https://www.fun-mooc.fr/fr/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/29	Développement de malwares Windows	**Objectif pédagogique** : Acquérir une expertise technique en développement de malwares Windows**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Maîtriser les principes du développement de malwares sur les systèmes Windows, en se concentrant sur le fonctionnement interne de l'OS, les API Windows et les mécanismes utilisés par les logiciels malveillants modernes. - Développer pas à pas des composants de malwares (payloads, loaders, shellcode). - Couvrir des techniques telles que l'injection de code, l'exécution en mémoire, l'obfuscation, l'évasion des mécanismes de détection et l'analyse des comportements défensifs.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée sans limite en distanciel.	MALDEV ACADEMY (https://maldevacademy.com/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/30	Kubernetes et les fondamentaux DevOps	**Objectif pédagogique** : Maîtriser Kubernetes et les fondamentaux DevOps en environnement de production**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Docker intensif, Fondamentaux Kubernetes, Packaging d'applications pour K8s. - Comprendre et maîtriser Kubernetes ainsi que les principes DevOps associés, afin de déployer, administrer et exploiter des applications conteneurisées. - Manipuler des clusters Kubernetes, de déployer des workloads, de gérer les ressources, les configurations et les cycles de vie applicatifs.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée entre 5 et 7 jours en distanciel.	ENIX (https://enix.io/fr/)

Ref	Libellé	Description	Travaux pratiques	Durée envisagée	Plateforme identifiée au moment du lancement de la consultation
TC10/31	L'IA au service de la cyber	**Objectif pédagogique** : Comprendre les apports de l'intelligence artificielle en cybersécurité**.** Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - L'IA Générative dans un contexte Cybersécurité (gouvernance, analyse technique). - La Cybersécurité confrontée à l'IA : défis, opportunités et risques liées à l'IA. - Usages de l'IA en lien avec les domaines de défense et d'attaque.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée entre 2 et 3 jours en distanciel.	NEOSOFT (https://www.neosoft.fr/)