

Formation

Cybersécurité Opérationnelle

SecOps

Durée : 4 jours – 28h

Face à des cyberattaques toujours plus sophistiquées, la formation SecOps vise à doter les participants des compétences essentielles pour détecter, anticiper et répondre efficacement aux menaces de cybersécurité.

L'objectif de la formation est de d'entraîner les apprenants aux gestes clés en matière de cybersécurité grâce une double approche :

- Offensive - comprendre comment procèdent les attaquants
- Défensive - apprendre à protéger efficacement les solutions

Cette formation combine théorie et applications pratiques sur notre plateforme de simulation CyberRange, avec 16 exercices basés sur des attaques réelles.

Public visé : Techlead, Ops, Administrateurs, architectes et experts techniques

Prérequis : Ops (administration et environnement Cloud)

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, le stagiaire est en capacité de :

- ♦ Expérimenter les techniques des attaquants pour mieux s'en protéger
- ♦ Mettre en place des stratégies et des outils de prévention et de défense
- ♦ Apprendre à détecter et analyser les attaques
- ♦ Identifier et remédier les failles de sécurité dans les configurations serveurs et Cloud
- ♦ Suivre les normes et les réglementations de sécurité informatique et de protection des données

PROGRAMME

1. Les responsabilités du techlead & l'application des standards :

- Concepts fondamentaux de la sécurité
- Identifier un risque et les responsabilités
- Application des standards de l'entreprise

Travaux pratiques :

Approche défensive : Analyser les risques cyber d'une solution

Approche défensive : Gérer une crise cyber

2. Sécuriser les composants :


- Le risque des composants obsolètes
- Renforcer les configurations par défaut
- Sécuriser les composants et services tiers

Travaux pratiques :


Approche offensive : Détecter une CVE avec un scanner et exploiter la vulnérabilité


Approche défensive : Analyser les problématiques de sécurité avec Trivy


Informations pratiques


 **Durée :** 4 jours – 28h

 **Ressources**
Supports de cours
70% d'exercices pratiques

 **Tarifs 2026**
En intra : contactez-nous pour un devis

 **Modalités**
Sur inscription
Contact et information par mail
Session de 8 stagiaires minimum

 **Lieu**
Sur site Client, LUIPSE
ou distanciel

 **Accessibilité aux personnes en situation de handicap**
Contactez-nous pour étudier la faisabilité de votre demande.

Taux de satisfaction



Compétences des formateurs

Nos formateurs sont des spécialistes certifiés de la cybersécurité avec une expérience terrain dans la sécurité des systèmes d'information. Ils ont été validés par notre équipe pédagogique sur le plan des connaissances métiers et sur celui de la pédagogie, et sont évalués régulièrement. Une veille permanente ainsi qu'une pratique régulière dans leur domaine garantit leur niveau d'expertise.

Modalités d'évaluation des stagiaires

Les objectifs sont régulièrement évalués tout au long de la formation moyen de quizz, de mises en situation et de travaux pratiques et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur

Le participant complète un test de positionnement en amont et en aval de la formation pour valider les compétences acquises.

Moyens techniques et pédagogiques

Aides audiovisuelles, environnement de formation en ligne, support de cours et exercices, études de cas ou présentation de cas réels, sessions de questions-réponses.



contact@lupise.fr

Suite =>

3. Contrôler les accès techniques

- Gérer des secrets
- L'application du triple A A A
- La gestion des accès de comptes utilisateurs

Travaux pratiques :

Approche offensive : Exploiter une mauvaise configuration des accès par une attaque par bruteforce

Approche défensive : Déploiement d'un honeypot

4. Gérer et superviser les accès techniques

- Exploiter une mauvaise configuration des accès par une attaque par bruteforce
- Gérer ses logs pour assurer une supervision efficace
- Filtrer les accès réseaux

Travaux pratiques :

Approche défensive : Comment investiguer les traces d'une attaque cyber

6. Protéger les environnements docker

- Identifier les problématiques d'isolation des droits
- Bonnes pratiques des configurations

Travaux pratiques :

Approche offensive : Hacking d'un environnement complet

Approche défensive : Sécuriser les environnements docker

7. Sécuriser les flux

- Interception de données : modèle d'attaque MITM
- Durcir les protocoles et chiffrer les flux

Travaux pratiques :

Approche offensive : Exploiter une attaque de type Man in the middle pour analyser les trames d'un protocole FTP non chiffré

Approche défensive : Outil d'analyse des protocoles de chiffrements des flux

8. Gérer les secrets

- Quels sont les risques des secrets hardcodés ?
- Rechercher les secrets hardcodés
- Implémenter les coffres-forts de secrets

Travaux pratiques :

Approche offensive : Jouer le rôle d'un hacker qui utilise la force d'indexation Google à la recherche de secrets exposés

Approche défensive : Implémenter un coffre-fort de secret

9. Validation des acquis

Travaux pratiques :

Approche offensive : Dans la peau d'un hacker, exploiter différentes situations

Approche défensive : Dans la peau d'un SecOps, implémenter les solutions pour améliorer la sécurité dans différentes situations

Informations complémentaires

▪ Matériel nécessaire

Les stagiaires devront être munis d'un PC pendant la formation.

▪ Evaluation et validation de la formation

À la fin de chaque formation, les participants complètent un questionnaire d'évaluation qui est analysé par nos équipes pédagogiques.

Une feuille d'émargement par demi-journée de présence est signée par le stagiaire. A l'issue de la formation, un certificat de réalisation de formation est remis au stagiaire si celui-ci a bien assisté à la totalité de la session.

contact@lupise.fr