+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 15/10/2024

S'inscrire

Formation OSIR™ (IR-200)

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS IR-200

5 jours (35 heures)

PRÉSENTATION

Vous souhaitez améliorer la gestion des incidents de sécurité et renforcer les défenses de votre organisation face aux cyberattaques ? Avec notre préparation à la certification OSIR™ (OffSec Incident Response), vous pourrez développer des compétences essentielles pour détecter, analyser, contenir, éradiquer et récupérer des incidents de sécurité, tout en réduisant les risques pour votre organisation.

Durant la formation OSIR™, vous apprendrez à utiliser des outils de réponse aux incidents, tels que les systèmes de détection d'intrusions (IDS), les solutions de gestion des événements de sécurité (SIEM) et les outils forensic.

Vous serez également formé à la gestion des communications pendant une crise de sécurité, à la rédaction de rapports techniques, et à la coordination des efforts au sein des équipes.

Divers sujets seront abordés, tels que l'analyse des malwares, la sécurisation des points d'accès réseau, la gestion des artefacts suspects, et la restauration des systèmes compromis. Nous explorerons également les meilleures pratiques en matière de surveillance post-incident pour éviter les récidives.

Grâce à cette formation, vous acquérez des compétences en gestion de la réponse aux incidents et en défense active, tout en vous préparant efficacement pour l'examen OSIR™.

Après avoir terminé cette formation, vous serez prêt à passer la certification OSIR™ et à mettre en pratique vos compétences dans un environnement professionnel.

OBJECTIFS

- Comprendre le cycle de vie de la réponse aux incidents
- Identifier et analyser les cyberattaques courantes
- Utiliser les outils forensic pour la gestion des incidents
- Éradication des menaces et restauration des systèmes compromis
- Rédiger des rapports techniques et communiquer efficacement

PUBLIC VISÉ

- SOC Analysts
- Blue Team Specialists
- Incident Responders

Pré-requis

- Solides bases en réseaux TCP/IP
- Connaissances des systèmes d'exploitation Linux et Windows
- Compréhension des concepts de cybersécurité, y compris la gestion des menaces et vulnérabilités

Pré-requis logiciels

- **Kali Linux** --> Téléchargeable ici

Note : Ambient IT n’est pas propriétaire de OSIR™, cette certification appartient à OffSec ® Services LLC.

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSIR™

Concepts et pratiques de la réponse aux incidents

- Introduction à la réponse aux incidents
- Principes fondamentaux de la cyberdéfense
- Cycle de vie de la réponse aux incidents
- Outils couramment utilisés pour la réponse aux incidents
- Stratégies de détection des incidents
- Études de cas : incidents réels

Vue d'ensemble du paysage des cyberattaques

- Typologies des cyberattaques (phishing, ransomware, etc.)
- Motivations des attaquants : Hacktivisme, cybercriminalité, espionnage industriel

- Techniques d’attaque courantes : attaques par force brute, injections SQL, et exploitation des vulnérabilités
- Études des groupes APT (Advanced Persistent Threats) : Comprendre les tactiques et les méthodes des groupes APT
- Analyse des tendances actuelles en cybersécurité : Évolution des menaces, nouveaux vecteurs d’attaque
- Cartographie des attaques avec MITRE ATT&CK : Utilisation du cadre MITRE

Analyse des incidents et gestion des preuves

- Investigation des incidents : Collecter, préserver et analyser les preuves numériques
- Techniques d'analyse des journaux et artefacts : Analyse des logs système, réseau, et application pour tracer les incidents
- Outils forensic : Utilisation d’outils tels que Autopsy, FTK Imager, pour les investigations post-incident
- Méthodologie d'analyse des malwares : Détecter, analyser, et neutraliser les malwares en activité
- Évaluation de l'impact des incidents : Mesurer la portée des attaques sur les actifs critiques
- Documentation des investigations : Techniques de rédaction

Éradication des menaces et restauration des systèmes

- Nettoyage et suppression des malwares
- Analyse des points d’entrée exploités
- Scripts d’éradication et automations
- Test post-éradication
- Récupération des données compromises
- Prévention des incidents futurs

Récupération et retour à l’opérationnel

- Restaurer les systèmes affectés
- Vérification des mises à jour de sécurité
- Surveillance post-récupération
- Communication post-incident
- Évaluation des impacts économiques et réputationnels
- Plan d'amélioration continue

Pratiques de communication et rapport d'incidents

- Importance de la communication dans la réponse aux incidents
- Rédaction de rapports techniques
- Présentation des résultats aux parties prenantes
- Collaboration avec des équipes internes et externes
- Documentation des incidents
- Utilisation d'outils de reporting

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.