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

Mis à jour le 17/09/2024

S'inscrire

Formation Certification OSTH™

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

3 jours (21 heures)

PRÉSENTATION

Vous souhaitez centraliser et optimiser la gestion de vos processus métiers ? Avec notre préparation à la certification OSTH il est totalement possible d'intégrer des outils de suivi ou la gestion et analyse. Cela favorisera la fluidité des opérations et l'automatisation des tâches répétitives pour gagner en efficacité.

Durant la formation OSTH™, vous apprendrez à utiliser des fonctionnalités comme la gestion des workflows, l'automatisation des tâches, la surveillance des performances en temps réel ainsi que l'intégration avec d'autres systèmes d'information.

Divers sujets seront abordés tels que la personnalisation des interfaces, les outils de reporting avancés, et l'accès à une plateforme collaborative qui permet de mieux coordonner les équipes. Nous explorerons aussi les mécanismes de sécurité intégrés pour protéger les données.

Grâce à cette formation, vous acquerrez des compétences en gestion de projets, en automatisation des processus métiers et en analyse de données.

Après avoir effectué notre préparation, vous pourrez prétendre au passage à la certification OSTH™.

OBJECTIFS

- Mettre en œuvre et gérer les mesures de sécurité en garantissant que les systèmes et les réseaux restent sécurisés contre les menaces
- Maîtriser les concepts fondamentaux de la chasse aux menaces
- Identifier les motivations et techniques des acteurs de la menace
- Rédiger et communiquer efficacement les rapports de chasse aux menaces
- Analyser et détecter les menaces à partir de données réseau

- Utiliser les IoCs pour identifier les activités malveillantes

PUBLIC VISÉ

- Testeurs d'intrusion Web
- Hackers éthiques
- Spécialistes sécurité informatique
- Analystes SOC

Pré-requis

- Base solide en matière de réseaux TCP/IP
- Connaissance des systèmes d'exploitation Linux et Windows
- Compréhension de base des concepts de cybersécurité

Pré-requis logiciels

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

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

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSTH™

Concepts et pratiques de la chasse aux menaces

- Introduction à la chasse aux menaces
- Les bases de la cyberdéfense proactive
- Cycle de vie de la chasse aux menaces
- Outils et technologies couramment utilisés
- Stratégies de détection des menaces
- Études de cas : exemples réels de chasse aux menaces

Vue d'ensemble du paysage des acteurs de la menace

- Typologies et motivations des acteurs de la menace
- Techniques d'attaque courantes utilisées par les cybercriminels
- Études des groupes APT (Advanced Persistent Threats)
- Analyse des tendances actuelles en matière de cybermenaces
- Cartographie des menaces et techniques MITRE ATT&CK

Communication et rapports pour les chasseurs de menaces

- Importance de la communication dans la chasse aux menaces
- Rédaction de rapports techniques pour les équipes de sécurité
- Présentation des résultats aux parties prenantes
- Collaboration avec les équipes internes et externes
- Pratiques de documentation des enquêtes de chasse aux menaces
- Utilisation d'outils de reporting automatisés

La chasse aux données réseau

- Introduction à l'analyse de données réseau pour la chasse aux menaces
- Surveillance et collecte des journaux réseau
- Détection des anomalies dans le trafic réseau
- Techniques de détection des comportements malveillants
- Utilisation de solutions comme Wireshark, Zeek, et Suricata
- Exercices pratiques sur la détection d'attaques réseau

La chasse sur les points finaux

- Identification et analyse des menaces sur les endpoints
- Techniques d'investigation sur les endpoints (EDR, XDR)
- Collecte des artefacts : journaux, processus, mémoire
- Détection des attaques fileless et persistance
- Techniques d’analyse de logiciels malveillants sur les endpoints
- Exemples pratiques et études de cas

La chasse aux menaces avec les IoCs

- Introduction aux Indicateurs de Compromission (IoCs)
- Sources d’information sur les IoCs : CTI, Threat Intelligence Platforms
- Intégration et corrélation des IoCs avec les outils de sécurité
- Méthodes de détection basées sur les IoCs
- Utilisation des IoCs dans la chasse proactive
- Études de cas : chasse aux menaces avec des IoCs en temps réel
-
-

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.