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

Mis à jour le 22/04/2024

S'inscrire

Formation et préparation à la Certification OSDA™

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS EXP-301

3 jours (21 heures)

PRÉSENTATION

La certification OSDA™ est un moyen essentiel de prouver vos compétences en matière de sécurité des opérations et d'analyse défensive.

Elle atteste de votre maîtrise des principes fondamentaux de la sécurité informatique et de votre capacité à détecter, analyser et répondre aux menaces de sécurité de manière efficace.

L'examen OSDA™ est composé de plusieurs modules couvrant un large éventail de sujets, notamment :

- les réseaux d'entreprise
- Les attaques côté serveur et client
- L'escalade de privilèges

Chaque module teste vos connaissances et compétences dans des domaines spécifiques de la sécurité des opérations et de l'analyse défensive.

Notre formation OSDA™ offre une préparation complète à l'examen, en fournissant un contenu pédagogique approfondi et des exercices pratiques pour renforcer votre compréhension des concepts.

Nous couvrons chaque aspect du programme de certification, en mettant l'accent sur les compétences pratiques et les meilleures pratiques de l'industrie.

La formation OSDA™ est constamment mise à jour pour refléter les dernières tendances et évolutions dans le domaine de la sécurité informatique.

OBJECTIFS

- Comprendre les principes de la Cyber Kill-Chain de Lockheed-Martin
- Acquérir les compétences nécessaires pour analyser les journaux d'événements Windows et Linux
- Maîtriser l'utilisation des scripts et commandes non graphiques
- Identifier et évaluer les artefacts de journalisation des attaques côté serveur et client
- Développer des compétences avancées en matière d'escalade de privilèges sur les systèmes Windows

PUBLIC VISÉ

- Testeurs d'intrusion Web
- Chercheurs en sécurité
- Analysts SOC

Pré-requis

- Une expérience préalable dans le domaine de la sécurité des opérations ou de l'analyse défensive est préférable
- Des connaissances de base sur les systèmes d'exploitation Windows et Linux
- Une familiarité avec les outils de détection et de journalisation des événements
- Une expérience pratique avec des outils de sécurité informatique courants est un plus
- Une compréhension des principes de base de la rétro-ingénierie et de l'analyse de logiciels malveillants serait un atout

Pré-requis logiciels

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

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

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSAD™

Introduction aux fondamentaux de la sécurité et de l'analyse défensive

- Compréhension des réseaux d'entreprise et de la DMZ
- Étude des environnements de déploiement
- Différenciation entre les périphériques réseau principaux et périphériques de bord
- Analyse des réseaux privés virtuels (VPN) et des sites distants
- Exploration des étapes de la Cyber Kill-Chain de Lockheed-Martin
- Application de la Cyber Kill-Chain à des exemples de malware
  - Cryptominage
  - Ransomwares

- Introduction aux classifications du Framework MITRE ATT&CK
- Analyse de cas de campagnes OilRig, APT3 et APT28 avec le Framework MITRE ATT&CK

Fondamentaux des Endpoints Windows

- Compréhension des processus Windows et des services
- Exploration de la structure et des types de valeurs du Registre Windows
- Utilisation des scripts et commandes non graphiques pour interagir avec Windows
- Création de scripts batch, de scripts Visual Basic et de fonctions PowerShell personnalisés
- Introduction aux journaux d'événements Windows
- Analyse des journaux d'événements à l'aide de l'Observateur d'événements Windows et de PowerShell

Attaques côté serveur Windows

- Analyse des abus d'identifiants et des attaques sur les applications web
- Évaluation des artefacts de journalisation des attaques par injection de commandes
- Compréhension des attaques binaires
  - via les débordements de tampon et des artefacts générés
- Étude de l'utilisation de Windows Defender Exploit Guard
- Évaluation des artefacts de journalisation générés par Windows Defender Exploit Guard

Attaques côté client Windows

- Analyse des attaques via des logiciels Microsoft Office
- Utilisation de techniques de social engineering et de spearphishing
- Évaluation des artefacts de journalisation générés par des attaques de phishing
- Surveillance de PowerShell pour détecter les attaques et les activités suspectes
- Compréhension des capacités de logging étendues de PowerShell

Escalade de privilèges Windows

- Compréhension des niveaux d'intégrité Windows et de l'UAC
- Détection des tentatives d'escalade de privilèges
- Évaluation des artefacts de journalisation créés par les techniques de bypass UAC
- Utilisation de techniques d'escalade de privilèges vers SYSTEM
- Analyse des permissions de service pour l'escalade de privilèges

Introduction aux Endpoints Linux

- Compréhension des applications et daemons Linux
- Exploration de l'infrastructure Syslog et du journal daemon
- Analyse des logs web sous Linux
- Automatisation de l'analyse défensive à l'aide de scripts
- Utilisation d'outils DevOps pour étendre les capacités de scripting
- Application des compétences acquises dans un scénario de chasse réel

Détection des attaques réseau et des évasions

- Compréhension de la segmentation réseau
- Utilisation d'iptables pour la mise en œuvre de la segmentation
- Détection des tentatives de contournement d'egress
- Compréhension du tunneling et du forwarding de ports
- Utilisation d'outils pour détecter les tentatives de tunneling
- Application de règles Snort pour détecter les attaques et les communications C2

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.