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

Mis à jour le 07/05/2025

S'inscrire

Formation Certification CDSA

All-In-One : Préparation & Examen inclus au tarif

3 jours (21 heures)

Présentation

Notre formation Certification CDSA vous permettra de valider vos compétences pratiques et techniques en sécurité défensive et de devenir analyste SOC. Le rôle de l'analyste SOC est de détecter, analyser et répondre aux menaces de sécurité affectant les systèmes d'information de l'entreprise.

Notre programme de formation enseignera toutes les étapes et les techniques d'une analyse SOC et vous permettra, à l'issue de ces 3 jours, de passer l'examen de certification CDSA.

À l'issue de cette formation, vous saurez identifier, exploiter et documenter les vulnérabilités et proposer des solutions pour renforcer et d'optimiser la sécurité.

Objectifs

- Comprendre les concepts fondamentaux de la cybersécurité défensive et du fonctionnement d'un SOC.
- Maîtriser la collecte, l'analyse et la corrélation des journaux systèmes, réseaux et applicatifs.
- Identifier les activités malveillantes à partir de données issues d'un SIEM.
- Mener des investigations sur des incidents réels liés à des attaques sur Windows, Active Directory ou le réseau.
- Utiliser efficacement des outils de threat hunting, de forensique et de détection de malwares.
- Rédiger des rapports d'incidents clairs et exploitables
- Préparer et réussir l'examen officiel de certification CDSA.

Public visé

- Analyste SOC

- Analystes en cybersécurité
- Consultants en sécurité
- Administrateurs systèmes

Pré-requis

- Connaissances solides en sécurité informatique
- Avoir des notions fondamentales sur la détections de menace
- Connaissances en langages de script comme Python ou Ruby

Programme de notre Formation Certification CDSA

SOC & Gestion des Incidents

- Comprendre le rôle du SOC
- Étapes du cycle de gestion des incidents
  - NIST
  - SANS
- Techniques de triage et d’escalade d’incidents
- Utilisation d’outils de ticketing et de communication en équipe
- Rédaction des rapports d’incidents
- Simulations d'incidents en environnement contrôlé

SIEM et Analyse Tactique

- Architecture et fonctionnement d’un SIEM
- Collecte et ingestion de logs
  - Windows
  - Linux
  - Réseau
- Création de dashboards et des requêtes
- Analyse d'incidents via Splunk
- Détection de menaces via Elastic Stack
- Investigation avec corrélation de logs multi-sources

Log et Evènement D'analyse

- Identifier des comportements suspects
- Exploration des journaux d’événements Windows
- Journaux d’authentification et de connexion réseau
- Corrélation d’événements multiples
- Evtx, Sysmon, Winlogbeat pour l’analyse détaillée

Analyse Réseau & IDS/IPS

- Principes fondamentaux de l’analyse de paquets
- Analyse de PCAPs liés à des menaces réelles
- Analyse des patterns d’attaque
- Utilisation de Snort, Suricata comme IDS/IPS
- Analyse de flux NetFlow et alertes de sécurité
- Déploiement d’un environnement de détection réseau

Attaques Windows & Active Directory

- Introduction à Active Directory
- Kerberoasting, DCSync, Pass-the-Ticket
- Création de règles de détection personnalisées
- Analyse de scripts PowerShell malveillants

Analyse de Malware

- Types de malwares
  - Ransomware
  - Info-stealer
  - Droppers
- Analyse statique d’un binaire malveillant
- Désobfuscation de code JavaScript malveillant
- Sandbox et techniques d’analyse dynamique
- Extraire des Indicators of Compromise

Threat Hunting & Forensics

- Détection proactive via hypothèses
- Introduction à la forensique numérique
- Analyse de compromission post-mortem
- Création de playbooks de réponse aux menaces

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.