Implementing Cisco Cybersecurity Operations

Formation Informatique / Réseaux et Sécurité / Cisco

Il s'agit du deuxième cours du programme Cisco CCNA Cyber Ops et il est conçu pour permettre aux stagiaires de comprendre le fonctionnement d'un centre d'opérations de sécurité - Security Operations Center (SOC) et d'acquérir les connaissances requises dans cet environnement. Ce cours se concentre sur les compétences de base nécessaires à un analyste SOC. Plus précisément, il s'agit de comprendre l'analyse de base des menaces, la corrélation des événements, l'identification des activités malveillantes et la façon d'utiliser un guide pour répondre aux incidents. Le suivi de cette formation permet de valider un total de 30 crédits dans le cadre du programme d'Education Continue Cisco (CCE) pour les professionnels qui souhaitent renouveler leur titre de certification.

OBJECTIFS

- Définir un SOC et les différents rôles dans un SOC
- Comprendre les outils et systèmes d'infrastructure du SOC
- Apprendre l'analyse de base des incidents pour un SOC centré sur la menace
- Explorer les ressources disponibles pour aider à une investigation
- Expliquer la corrélation et la normalisation de base des événements
- Décrire les vecteurs d'attaque courants
- Apprendre à identifier les activités malveillantes
- Décrire et expliquer un manuel de suivi des incidents
- Définir les types de metriques du SOC
- Comprendre le système de gestion des flux de travail et l'automatisation de SOC

PUBLIC

Les personnes intéressées par une carrière dans la cybersécurité, ou cherchant à mieux comprendre les opérations de cybersécurité, ou souhaitant obtenir leur certification CCNA Cyber Ops.

PRE-REQUIS

- Compétences et connaissances équivalentes à celles acquises dans le cadre du cours Cisco Certified Network Associate (CCNA)
- Des compétences et des connaissances équivalentes à celles acquises dans le cadre du Comprendre les fondamentaux de la cybersécurité Cisco (SECFND)
- Connaissance pratique du système d'exploitation Windows
- Connaissance pratique des réseaux et des concepts de Cisco IOS

PROGRAMME

Vue d'ensemble du SOC

Définition du Security Operations Center
Comprendre les outils et les données du MNS
Comprendre l'analyse des incidents dans un SOC centré sur la menace
Identifier les ressources pour chasser les cybermenaces
Investigations sur les incidents de sécurité
Comprendre la corrélation et la normalisation des événements
Identifier les vecteurs d'attaque courants
Identifier les activités malveillantes
Identifier les modèles de comportements suspects

Mener des enquêtes sur les incidents de sécurité
Opérations du SOC

- Description du Playbook du SOC
- Comprendre les métriques du SOC
- Comprendre le WMS et l'automatisation du SOC
- Description du plan d'intervention en cas d'incident
- Annexe A - Description de l'équipe d'intervention en cas d'incident de sécurité informatique

Annexe B - Comprendre l'utilisation de VERIS
Travaux pratiques :

- Explorer les outils de surveillance de la sécurité des réseaux
- Etude de la méthodologie des hackers
- Traquer les trafics malveillants
- Corréler les journaux d'événements, les PCAP et les alertes d'une attaque
- Travailler sur les attaques basées sur les navigateurs
- Analyser les activités DNS suspectes
- Travailler sur les activités suspectes à l'aide de l'oignon de sécurité
- Travailler sur les menaces persistantes avancées

A retenir

Durée : **5 jours** soit 35h.
Réf. **SECOPS**

01 42 93 52 72

Dates des sessions

Cette formation est également proposée en formule INTRA-ENTREPRISE.

Inclus dans cette formation

Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100% SATISFACTION GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.

- Travailler sur les playbooks SOC

Horaires, Planning et Déroulement de cette formation

Horaires

• Formation de 9h00 (9h30 le premier jour) à 17h30.
• Deux pauses de 15 minutes le matin et l'après-midi.
• 1 heure de pause déjeuner

DEROULEMENT

• Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
• Une attestation de suivi de formation vous sera remise en fin de formation.
• Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

Réussir la Certification Gestion de Projet PMP du PMI
Réussir la Certification PRINCE2 Foundation
Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner
Réussir la Certification ITIL Foundation
Réussir la Certification Agile certifié SCRUM Master
Réussir les Certifications TOGAF Certified et TOGAF Foundation

Retrouvez cette formation sur notre site :
Implementing Cisco Cybersecurity Operations