Analyste des opérations de sécurité Microsoft SC-200

SYSTÈMES RÉSEAUX ET SÉCURITÉ

Objectifs	Le cours SC-200 (Security Operations Analyst) a pour but de former les professionnels de la sécurité (analystes SOC, ingénieurs sécurité, etc.) à détecter, investiguer, répondre et chasser les menaces dans des environnements Microsoft / cloud hybride / on-prem. À l'issue du cours, le participant doit être capable de : Configurer et utiliser Microsoft Sentinel pour la détection, l'analyse, le reporting des incidents - Utiliser le Kusto Query Language (KQL) pour requêter, créer des alertes, investiguer des incidents - Configurer et gérer Microsoft Defender XDR, Defender for Endpoint, Defender for Cloud (Azure), Defender pour Microsoft 365 etc., pour la protection et la remédiation des menaces - Répondre aux incidents de sécurité : triage, investigation, prise de contre-mesures, automatisation des réponses lorsque possible - Améliorer la posture de sécurité organisationnelle (politiques, détection, protection, conformité), conseiller sur les meilleures pratiques - Chasser activement les menaces (threat hunting), y compris dans les environnements cloud/hybrides, et faire usage de l'intelligence des menaces.
Participants	Analystes des opérations de sécurité Microsoft - Toute personne impliquée dans la sécurité informatique ou la gestion des risques - Administrateurs de solutions de sécurité - Membres des équipes SOC (Security Operations Center) ou CERT (Computer Emergency Response Team) - Gestionnaires de la sécurité informatique - Utilisateurs avancés des solutions Microsoft de sécurité
Prérequis	Avant de suivre ce cours (et pour tirer pleinement avantage), il est recommandé d'avoir : Une compréhension de base de Microsoft 365 (utilisation des services Microsoft 365) - Une connaissance fondamentale des produits de sécurité, conformité (compliance), et d'identité chez Microsoft (Azure AD / Entra, Defender, etc.) - Une familiarité/intermédiaire avec les systèmes d'exploitation Windows (et souvent aussi Linux ou mobiles selon les environnements) - Familiarité avec les services Azure : machines virtuelles, stockage (Azure Storage), base de données SQL Azure, réseau virtuel etc - Concepts réseau de base (protocoles, logs, authentification, etc.) - Notion de scripts ou automatisation peut être utile (surtout pour certaines parties, playbooks, automatisation de réponse).
Moyens pédagogiques	1 poste par participant - 1 Vidéo projecteur - Support de cours fourni à chaque participant - Ateliers Individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et Evaluation des acquis tout au long de la formation.
Méthodes pédagogiques	Exposés théoriques et démonstrations Questions-réponses et échanges d'expériences Mises en situation et travaux dirigés Accompagnement personnalisé du formateur avec des tests de positionnement.
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
Tarif inter-entreprise	2720 € HT
Durée	4 jours (28 heures)

Code : NCI_10LH57J

Programme :

Atténuer les menaces à l'aide de Microsoft 365 Defender

Présentation de la protection contre les menaces Microsoft 365
Atténuer les incidents à l'aide de Microsoft 365 Defender
Protéger les identités avec Azure AD Identity Protection
Corriger les risques avec Microsoft Defender pour Office 365
Protéger un environnement avec Microsoft Defender pour Identity
Sécuriser les applications et services cloud avec Microsoft Defender pour les applications cloud
Répondre aux alertes de prévention des pertes de données à l'aide de Microsoft 365
Gérer les risques internes dans Microsoft 365.

Atténuer les menaces à l'aide de Microsoft Defender for Endpoint

Se protéger contre les menaces avec Microsoft Defender for Endpoint
Déployer l'environnement Microsoft Defender pour Endpoint
Implémenter les améliorations de sécurité de Windows
Effectuer des enquêtes sur les appareils
Effectuer des actions sur un appareil
Effectuer des enquêtes sur les preuves et les entités
Configurer et gérer l'automatisation
Configurer les alertes et les détections
Utiliser la gestion des vulnérabilités

Atténuer les menaces à l'aide de Microsoft Defender pour le cloud

Planifier les protections des charges de travail cloud à l'aide de Microsoft Defender pour le cloud
Connecter les actifs Azure à Microsoft Defender pour le Cloud
Connecter des ressources non Azure à Microsoft Defender pour le cloud
Gérer la gestion de votre posture de sécurité cloud
Expliquer les protections de charge de travail cloud dans Microsoft Defender pour le cloud
Corriger les alertes de sécurité à l'aide de Microsoft Defender for Cloud.

Créer des requêtes pour Microsoft Sentinel à l'aide du langage de requête Kusto (KQL)

Construire des instructions KQL pour Microsoft Sentinel
Analyser les résultats des requêtes à l'aide de KQL
Créer des instructions multi-tables à l'aide de KQL
Travailler avec des données dans Microsoft Sentinel à l'aide du langage de requête Kusto.

Configurer votre environnement Microsoft Sentinel

Présentation de Microsoft Sentinel
Créer et gérer des espaces de travail Microsoft Sentinel
Interroger les journaux dans Microsoft Sentinel
Utiliser des listes de surveillance dans Microsoft Sentinel
Utiliser les renseignements sur les menaces dans Microsoft Sentinel.

Connecter les journaux à Microsoft Sentinel

Connecter des données à Microsoft Sentinel à l'aide de connecteurs de données
Connecter les services Microsoft à Microsoft Sentinel
Connecter Microsoft 365 Defender à Microsoft Sentinel
Connecter des hôtes Windows à Microsoft Sentinel
Connecter les journaux Common Event Format à Microsoft Sentinel
Connecter des sources de données Syslog à Microsoft Sentinel
Connecter des indicateurs de menace à Microsoft Sentinel.

Créer des détections et effectuer des investigations à l'aide de Microsoft Sentinel

Détection des menaces avec Microsoft Sentinel Analytics
Automatisation dans Microsoft Sentinel
Réponse aux menaces avec les playbooks Microsoft Sentinel
Gestion des incidents de sécurité dans Microsoft Sentinel

WEDO 365 by NCI

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon
Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille
www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20