Analyste des opérations de sécurité Microsoft

Réf : SC200

OBJECTIFS DE LA FORMATION

Apprendre à enquêter, répondre et rechercher les menaces en utilisant Microsoft Azure Sentinel, Azure Defender, et Microsoft 365 Defender.
Savoir comment atténuer les cybermenaces à l'aide de ces technologies.
Configurer et utiliser Azure Sentinel et le Kusto Query Language (KQL) pour effectuer la détection, l'analyse et la création de rapports.

PROGRAMME

ATTÉNUER LES MENACES À L'AIDE DE MICROSOFT DEFENDER POUR ENDPOINT

Se protéger contre les menaces avec Microsoft Defender pour Endpoint.
Déployer l'environnement Microsoft Defender pour Endpoint.
Mettre en oeuvre les améliorations de sécurité de Windows 10 avec Microsoft Defender pour Endpoint.
Gérer les alertes et les incidents dans Microsoft Defender pour Endpoint.
Effectuer des enquêtes sur les appareils dans Microsoft Defender pour Endpoint.
Effectuer des actions sur un appareil à l'aide de Microsoft Defender pour Endpoint.
Effectuer des enquêtes sur les preuves et les entités à l'aide de Microsoft Defender pour Endpoint.
Configurer et gérer l'automatisation à l'aide de Microsoft Defender pour Endpoint.
Configurer les alertes et les détections dans Microsoft Defender pour Endpoint.
Utiliser la gestion des menaces et des vulnérabilités dans Microsoft Defender pour Endpoint.
Travaux pratiques : déployer Microsoft Defender pour Endpoint. Atténuer les attaques à l'aide de Defender for Endpoint.

ATTÉNUER LES MENACES À L'AIDE DE MICROSOFT 365 DEFENDER

Introduction à la protection contre les menaces avec Microsoft 365.
Atténuer les incidents à l'aide de Microsoft 365 Defender.
Protéger vos identités avec Azure AD Identity Protection.
Remédier aux risques avec Microsoft Defender pour Office 365.
Protéger votre environnement avec Microsoft Defender for Identity.
Sécuriser vos applications et services cloud avec Microsoft Cloud App Security.
Répondre aux alertes de prévention des pertes de données (DLP) avec Microsoft 365.
Gérer les risques liés aux initiés dans Microsoft 365.
Travaux pratiques : mise en application : atténuer les menaces avec Microsoft 365 Defender.

ATTÉNUER LES MENACES À L'AIDE DE AZURE DEFENDER

Planifier les protections des charges de travail cloud à l'aide de Azure Defender.
Expliquer les protections des charges de travail cloud dans Azure Defender.
Connecter les ressources Azure à Azure Defender.
Connecter les ressources non-Azure à Azure Defender.
Corriger les alertes de sécurité à l'aide d'Azure Defender.
Travaux pratiques : déployer Azure Defender. Atténuer les attaques avec Azure Defender.

CRÉER DES REQUÊTES POUR AZURE SENTINEL AVEC LE KUSTO QUERY LANGUAGE

Construire des instructions Kusto Query Language (KQL) pour Azure Sentinel.
Analyser les résultats des requêtes en utilisant Kusto Query Language (KQL).

La formation est accessible aux personnes à mobilité réduite et toute demande d'adaptation peut être étudiée en amont de la formation en fonction du besoin des personnes. Nous contacter pour plus d'informations

Lieu : Site de Metz : JCD FORMATION - 193 rue Metman - 57070 METZ - 03 87 37 97 70
Site de Pompey : KAPEDIA – 132 Rue Léonard de Vinci – 54340 POMPEY – 03 83 49 80 80

4 jours soit 28h

Nous contacter

2590 HT / participant

Public / Prérequis

Public :
Analystes sécurité, ingénieurs sécurité.

Prérequis
Connaissances de base : Microsoft 365.
Bonnes connaissances de Windows 10, des services Azure (Azure SQL, stockage Azure), des machines virtuelles Azure et des réseaux virtuels, etc.

Méthodes et Moyens pédagogiques

Alternance continuelle entre apport de connaissances et manipulation des outils. Fourniture de documents et supports de cours qui restent la propriété des stagiaires.

Salles équipées : vidéoprojecteur, paperboard, ordinateur individuel, support de cours papier ou électronique, outils de prise de note

Validation

Attestation de stage

Profil intervenant

Professionnel et expert en informatique

Suivi et Évaluation de l'action

Compte rendu de fin de formation et analyse interne

Questionnaire « évaluation de la formation » rempli par le stagiaire.

Document mis à jour le 16/12/2022

Analyste des opérations de sécurité Microsoft

Réf : SC200

OBJECTIFS DE LA FORMATION

Préparer les étudiants avec une expertise en conception et en évaluation des stratégies de cybersécurité dans les domaines suivants :

- confiance zéro,
- risques conformité en matière de gouvernance (GRC),
- opérations de sécurité (SecOps),
- données et applications,
- conception d'architecture de solutions à l'aide de principes de confiance zéro,
- savoir spécifier des exigences de sécurité pour l'infrastructure cloud dans différents modèles de service (SaaS, PaaS, IaaS)

PROGRAMME

Construire des instructions multi-tables à l'aide de Kusto Query Language (KQL).
Travailler avec des données dans Azure Sentinel en utilisant Kusto Query Language (KQL).
Travaux pratiques : construire des instructions KQL de base. Analyser les résultats des requêtes à l'aide de KQL. Construire des requêtes multi-tables en utilisant KQL. Travailler avec des données de type chaîne à l'aide d'instructions KQL.

CONNECTER LES JOURNAUX À AZURE SENTINEL

Connecter des données à Azure Sentinel à l'aide de connecteurs de données.
Connecter les services Microsoft à Azure Sentinel.
Connecter Microsoft 365 Defender à Azure Sentinel.
Connecter les hôtes Windows à Azure Sentinel.
Connecter les journaux Common Event Format (CEF) à Azure Sentinel.
Connecter des sources de données syslog à Azure Sentinel.
Connecter les indicateurs de menace à Azure Sentinel.
Travaux pratiques : connecter les services Microsoft à Azure Sentinel. Connecter les hôtes Windows à Azure Sentinel.
Connecter les hôtes Linux à Azure Sentinel.
Connecter les renseignements sur les menaces à Azure Sentinel.

CRÉER DES DÉTECTIONS ET EFFECTUER DES ENQUÊTES À L'AIDE D'AZURE SENTINEL

Détecter des menaces avec les analyses de Azure Sentinel.
Répondre aux menaces avec les manuels Azure Sentinel.
Gérer les incidents de sécurité dans Azure Sentinel.
Utiliser l'analyse du comportement des entités dans Azure Sentinel.
Interroger, visualiser et surveiller les données dans Azure Sentinel.
Travaux pratiques : Créer des règles analytiques. Modéliser les attaques pour définir la logique des règles. Atténuer les attaques à l'aide de Azure Sentinel. Créer des classeurs dans Azure Sentinel.

EFFECTUER LA CHASSE AUX MENACES DANS AZURE SENTINEL

Chasse aux menaces avec Azure Sentinel.
Chasse aux menaces à l'aide de notebooks dans Azure Sentinel.
Travaux pratiques : chasse aux menaces dans Azure Sentinel. Chasse aux menaces à l'aide de notebooks.

4 jours soit 28h

Nous contacter

2590 HT / participant

Public / Prérequis

Public :
Analystes sécurité, ingénieurs sécurité.

Prérequis
Connaissances de base : Microsoft 365. Bonnes connaissances de Windows 10, des services Azure (Azure SQL, stockage Azure), des machines virtuelles Azure et des réseaux virtuels, etc.

Méthodes et Moyens pédagogiques

Alternance continuelle entre apport de connaissances et manipulation des outils. Fourniture de documents et supports de cours qui restent la propriété des stagiaires.

Salles équipées : vidéoprojecteur, paperboard, ordinateur individuel, support de cours papier ou électronique, outils de prise de note

Validation

Attestation de stage

Profil intervenant

Professionnel et expert en informatique

Suivi et Évaluation de l'action

Compte rendu de fin de formation et analyse interne

Questionnaire « évaluation de la formation » rempli par le stagiaire.

La formation est accessible aux personnes à mobilité réduite et toute demande d'adaptation peut être étudiée en amont de la formation en fonction du besoin des personnes. Nous contacter pour plus d'informations

Lieu : Site de Metz : JCD FORMATION - 193 rue Metman - 57070 METZ - 03 87 37 97 70
Site de Pompey : KAPEDIA – 132 Rue Léonard de Vinci – 54340 POMPEY – 03 83 49 80 80

Document mis à jour le 16/12/2022