Analyste des opérations de sécurité Microsoft

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Systèmes et Réseaux

Action collective : Non

Filière : Systèmes et réseaux Microsoft

Rubrique : Sécurité des systèmes

Code de formation : MSSC200

PRÉSENTATION

Objectifs & compétences

Être capable d'expliquer comment Microsoft Defender pour Endpoint peut remédier aux risques dans votre environnement Savoir créer un environnement Microsoft Defender pour Endpoint Apprendre à configurer les règles de réduction de la surface d'attaque sur les appareils Windows 10 Comprendre comment effectuer des actions sur un appareil à l'aide de Microsoft Defender pour Endpoint Savoir construire des instructions KQL Savoir gérer un espace de travail Azure Sentinel

Public visé

Analystes sécurité Ingénieurs sécurité

Pré-requis

ompréhension de base de Microsoft 365 Compréhension fondamentale des produits de sécurité, de conformité et d'identité Microsoft Compréhension intermédiaire de Windows 10 Familiarité avec les services Azure, en particulier les bases de données Azure SQL et le stockage Azure Connaissance des machines virtuelles Azure et des réseaux virtuels Compréhension de base des concepts de script

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 la 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

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 les identités avec Azure AD Identity Protection
- Remédier aux risques avec Microsoft Defender pour Office 365
- Protéger son environnement avec Microsoft Defender for Identity
- Sécuriser ses applications et services cloud avec Microsoft Cloud App Security
- Répondre aux alertes de prévention de la perte de données à l'aide de Microsoft 365
- Gérer les risques internes dans Microsoft 365

€ Tarifs

Prix public : 2620 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 28 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

ATTÉNUER LES MENACES À L'AIDE D'AZURE DEFENDER

- Planifier les protections de la charge de travail cloud à l'aide d'Azure Defender
- Expliquer les protections des charges de travail cloud dans Azure Defender
- Connecter les actifs Azure à Azure Defender
-Connecter des ressources non-Azure à Azure Defender
- Corriger les alertes de sécurité à l'aide d'Azure Defender

CRÉER DES REQUÊTES POUR AZURE SENTINEL À L'AIDE DU LANGAGE DE REQUÊTE KUSTO (KQL)

- Construire des instructions KQL pour Azure 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 Azure Sentinel à l'aide du langage de requête Kusto

CONFIGURER VOTRE ENVIRONNEMENT AZURE SENTINEL

- Introduction à Azure Sentinel
- Créer et gérer des espaces de travail Azure Sentinel Requête des journaux dans Azure Sentinel
- Utiliser des listes de surveillance dans Azure Sentinel
- Utiliser l'intelligence des menaces dans Azure Sentinel

CONNECTER LES JOURNAUX À AZURE SENTINEL

- Connecter les 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 du format d'événement commun à Azure Sentinel
- Connecter les sources de données Syslog à Azure Sentinel
- Connecter les indicateurs de menace à Azure Sentinel

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

- Détection des menaces avec l'analyse Azure Sentinel
- Réponse aux menaces avec les playbooks Azure Sentinel
- Gestion des 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

EFFECTUER UNE RECHERCHE DE MENACES DANS AZURE SENTINEL

- Chasse aux menaces avec Azure Sentinel
- Traquer les menaces à l'aide de blocs-notes dans Azure Sentinel

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.