Cybersecurity Specialization: Incident Handler

Durée: 2 Jours **Réf de cours: GK840101** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Acquérir les connaissances et compétences nécessaires pour gérer et réduire efficacement les incidents de cybersécurité.

Ce cours est conçu pour fournir aux professionnels de la cybersécurité les connaissances et compétences essentielles nécessaires pour gérer et réduire efficacement les incidents de cybersécurité.

Apprenez les différentes composantes et phases des cadres de réponse aux incidents, explorez des outils et techniques de pointe, et participez à des exercices pratiques pour perfectionner vos capacités de réponse aux incidents.

À la fin de ce cours, les étudiants auront acquis une expérience pratique avec des outils et techniques efficaces utilisés dans l'analyse des logiciels malveillants, la réponse aux incidents et la chasse aux menaces. Ils seront équipés des outils, techniques et méthodologies nécessaires pour protéger leur organisation contre les menaces cybernétiques en constante évolution et assurer une posture de cybersécurité résiliente.

Nos cours de spécialisation en cybersécurité suivent les 9 piliers de la cybersécurité, fournissant les compétences clés nécessaires pour réussir en tant que professionnel de la cybersécurité

Mise à jour : 10/12/2024

Public visé:

Ce cours de niveau intermédiaire à avancé est conçu pour :
Analystes en sécurité informatique, Analystes Forensic, Administrateurs réseau, Membres de l'équipe du Centre des opérations de sécurité (SOC), Responsables de la sécurité de l'information, Consultants en cybersécurité, Membres de l'équipe de réponse aux incidents

Compétences techniques solides (Minimum plus de 2 ans d'expérience en sécurité).

Objectifs pédagogiques:

- À l'issue de la formation, les participants seront capables de :
- Identifier les composants clés et les phases des cadres de réponse aux incidents avancés.
- Lister les outils et techniques utilisés dans l'analyse des logiciels malveillants, la réponse aux incidents et la chasse aux menaces.
- Expliquer l'importance et la fonction de chaque phase dans un cadre de réponse aux incidents.
- Décrire le processus et les méthodologies derrière l'analyse statique et dynamique des logiciels malveillants.
- Démontrer l'utilisation d'outils avancés comme SIEM, EDR et les logiciels d'analyse médico-légale dans la gestion des incidents de cybersécurité.
- Réaliser des exercices de chasse aux menaces en utilisant des outils et techniques standards de l'industrie.
- Analyser des scénarios d'incidents complexes pour déterminer la cause profonde et l'impact.
- Comparer différents cadres de réponse aux incidents et leur application dans divers contextes organisationnels.
- Évaluer l'efficacité des stratégies et cadres de réponse aux incidents en utilisant des métriques prédéfinies.
- Évaluer les menaces émergentes et les tendances pour déterminer leur impact potentiel sur les défenses en cybersécurité.
- Concevoir un cadre de réponse aux incidents personnalisé adapté aux besoins spécifiques de l'organisation.
- Développer des rapports d'incidents complets et une documentation basée sur des simulations d'incidents réels

Pré-requis:

Pour assister à cette formation, il est recommandé pour les candidats de:

- Connaissances de base des concepts de cybersécurité et des outils de sécurité
- Avoir des compétences fondamentales du réseau.
- Avoir une expérience avec les systèmes d'exploitation.
- Avoir les connaissances de base de la gestion des incidents et en analyse des logiciels malveillants

Avoir suivi la formation "Cybersecurity Foundation" ou posséder les connaissances équivalentes.

https://www.globalknowledge.com/fr-fr/formation/security/cybersec/9701

- 9701 - Cybersecurity Foundations

Contenu:

JOUR 1

Cadres de réponse aux incidents et techniques avancées

- Cadres de réponse aux incidents avancés
- Approches progressives d'analyse des incidents cybernétiques
- Pratiques de pointe en analyse des logiciels malveillants
- Chasse aux menaces et défense proactive
- Atelier pratique:
- Exercice avancé d'analyse des logiciels malveillants
- Exercice de chasse aux menaces
- Études de cas : Discussion sur des scénarios complexes de réponse aux incidents et les leçons apprises

JOUR 2

Outils de gestion des incidents et tendances émergentes

- Outils avancés de gestion des incidents
- Menaces et tendances émergentes
- Automatisation et orchestration de la réponse aux incidents
- Métriques et rapports de réponse aux incidents
- Atelier pratique :
- Exercice d'automatisation de la réponse aux incidents
- Exercice de rapport d'incidents

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.

Un support de cours électronique sera remis aux participants.
Suivi de cette formation à distance depuis un site client équipé. Il suffit d'avoir une bonne connexion internet, un casque avec micro et d'être dans un endroit au calme pour en profiter pleinement

Une fiche explicative est adressée en amont aux participants pour leur permettre de vérifier leur installation technique et de se familiariser avec la solution technologique utilisée.

L'accès à l'environnement d'apprentissage, ainsi qu'aux feuilles d'émargement et d'évaluation est assuré.
En savoir plus : https://www.globalknowledge.com/fr-fr/solutions/methodes-d'apprentissage/classe-a-distance

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement