Understanding Cisco Cybersecurity Operations Fundamentals

Durée: 5 Jours **Réf de cours: CCNACBR** **Version: 2.0**

Résumé:

La formation « **Understanding Cisco Cybersecurity Operations Fundamentals** » (CCNACBR) permet d'acquérir une compréhension des équipements d'infrastructure réseau, des opérations et des vulnérabilités de la suite de protocoles TCP/IP, ainsi que des concepts fondamentaux de la sécurité de l'information, des opérations courantes et des attaques visant les applications réseau, des systèmes d'exploitation Windows et Linux, et des types de données utilisées pour enquêter sur les incidents de sécurité. À l'issue de cette formation, vous disposerez des connaissances de base nécessaires pour occuper le poste d'analyste en cybersécurité de niveau associé au sein d'un centre d'opérations de sécurité (SOC) axé sur les menaces.
Cette formation vous prépare à l'examen 200-201 CCNACBR v1.2. Si vous le réussissez, vous obtiendrez la certification Cisco Certified Network Associate (CCNA) Cybersecurity et pourrez occuper le poste d'analyste junior ou débutant en opérations de cybersécurité au sein d'un SOC. Cette formation vous permet également d'obtenir 28 crédits de formation continue (CE) valables pour le renouvellement de votre certification.
Mise à jour : 13/07/2026

.

Public visé:

Cette formation s'adresse aux analystes en cybersécurité de niveau Associate.

Objectifs pédagogiques:

- À l'issue de cette formation, les participants seront capables de :
- Expliquer les principes fondamentaux des SOC, notamment leurs différents types, les rôles clés et les indicateurs essentiels permettant de mesurer leur efficacité
- Appliquer les principes fondamentaux de sécurité et les concepts de gestion des risques afin d'évaluer et de protéger les actifs de l'organisation
- Comparer et appliquer différents modèles de contrôle d'accès afin de sécuriser les ressources réseau et de faire respecter les politiques de l'organisation
- Différencier les différents modèles de déploiement et de services Cloud et expliquer le principe de responsabilité partagée en matière de sécurité dans les environnements Cloud
- Expliquer les concepts fondamentaux de la cryptographie, différencier les différents algorithmes cryptographiques et expliquer comment les principes cryptographiques sont appliqués dans les protocoles et systèmes réels, notamment pour l'échange de clés, les signatures numériques et SSL/TLS
- Identifier et décrire les composants fondamentaux et les aspects opérationnels du système d'exploitation Windows dans le cadre d'une analyse de sécurité
- Identifier et décrire les composants fondamentaux et les aspects opérationnels du système d'exploitation Linux dans le cadre d'une analyse de sécurité
- Utiliser les interfaces en ligne de commande (CLI) pour les interactions système de base, la gestion des fichiers et les
- Décrire les techniques fondamentales d'attaque réseau exploitant les vulnérabilités des protocoles
- Décrire les vecteurs d'attaque avancés et les menaces émergentes dans le paysage actuel de la cybersécurité
- Identifier et expliquer les différents types de données de surveillance de la sécurité réseau (NSM) et leur rôle dans l'investigation des incidents
- Identifier et interpréter différentes sources de données de journaux provenant des systèmes d'exploitation, des équipements réseau et des outils de sécurité
- Expliquer le fonctionnement de NetFlow et son utilisation comme outil de sécurité pour la surveillance du réseau et la détection des anomalies
- Décrire les attaques courantes visant les applications Web et leurs méthodes d'exploitation
- Appliquer des techniques avancées d'analyse des journaux afin d'interpréter les données de sécurité et d'identifier des schémas de comportement suspects
- Effectuer une analyse des captures de paquets et appliquer des processus d'investigation numérique afin d'analyser les incidents de sécurité. Se concentrer sur les 5 éléments du 5-tuple et les horodatages afin d'établir des corrélations avec d'autres journaux, ceux-ci constituant des éléments essentiels pour l'investigation réseau
- Expliquer les résultats issus de l'analyse des logiciels malveillants et appliquer les frameworks de renseignement sur les menaces dans

tâches liées à la sécurité dans les environnements Windows et Linux

- Expliquer le fonctionnement des principaux protocoles réseau et identifier leurs implications en matière de sécurité
- Décrire et différencier différents mécanismes de sécurité réseau et leur utilisation pour protéger l'infrastructure réseau
- Différencier les différents systèmes de détection et de prévention des intrusions (IDS/IPS) et interpréter leurs résultats dans le cadre de la surveillance de la sécurité
- Décrire et comparer différentes solutions de sécurité des terminaux et leur efficacité face aux menaces courantes
- Identifier et catégoriser les différents acteurs de la cybermenace en fonction de leurs motivations, de leurs capacités et de leurs tactiques habituelles
- Expliquer les différentes phases du modèle classique Cyber Kill Chain et identifier les actions des attaquants au sein de chacune de ces phases
- Appliquer le framework MITRE ATT&CK pour analyser et cartographier les cybermenaces, expliquer sa structure et son utilisation, et l'exploiter afin d'améliorer la détection des menaces, la réponse aux incidents et la communication au sein d'un environnement d'opérations de sécurité
- Identifier et décrire les différents vecteurs d'attaque liés à l'ingénierie sociale, y compris ceux renforcés par l'IA générative

le cadre des investigations de sécurité

- Expliquer l'architecture, les fonctions principales et les bonnes pratiques de mise en œuvre des solutions SIEM afin d'assurer une surveillance efficace de la sécurité
- Expliquer les fonctionnalités et les cas d'utilisation courants des plateformes SOAR pour automatiser et rationaliser la réponse aux incidents
- Expliquer la plateforme Cisco XDR, ses fonctions principales, ses fonctionnalités et ses composants permettant une détection et une réponse unifiées aux menaces
- Différencier les recommandations historiques et modernes du NIST en matière de réponse aux incidents (publications spéciales NIST SP 800-61 Rev. 2 et NIST SP 800-61 Rev. 3), décrire les principaux composants de la réponse aux incidents conformément au framework NIST CSF 2.0 et identifier comment ces pratiques répondent aux exigences CMMC applicables à la Defense Industrial Base (DIB)
- Décrire les rôles, les catégories et les services opérationnels des équipes de réponse aux incidents de sécurité informatique (CSIRT)
- Expliquer le concept de playbooks de surveillance de la sécurité et leurs composants afin de standardiser la réponse aux incidents
- Appliquer différentes méthodologies de recherche proactive de menaces (Threat Hunting) afin d'identifier et de réduire les menaces dissimulées au sein d'un réseau

Pré-requis:

Il n'y a pas de prérequis pour cette formation. Toutefois, il est recommandé de disposer des connaissances et compétences suivantes avant de suivre cette formation :

- Connaissance des réseaux Ethernet et TCP/IP
- Connaissance pratique des systèmes d'exploitation Windows et Linux
- Connaissance des principes fondamentaux de la sécurité des réseaux
- CCNA - Mettre en oeuvre et administrer des solutions réseaux Cisco

Test et certification

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- *None recommended*

Contenu:

Programme de la formation

- Opérations de sécurité
- Principes de sécurité
- Modèles de contrôle d'accès
- Modèles de sécurité Cloud
- Cryptographie pour les opérations de sécurité
- Principes fondamentaux du système d'exploitation Windows
- Principes fondamentaux du système d'exploitation Linux
- Interfaces en ligne de commande (CLI) dans le domaine de la sécurité
- Protocoles réseau
- Contrôles de sécurité réseau
- Systèmes IDS et IPS
- Sécurité des terminaux
- Acteurs de la menace
- Modèle Cyber Kill Chain
- Framework MITRE ATT;CK
- Attaques par ingénierie sociale
- Principes fondamentaux des attaques réseau
- Panorama des menaces avancées
- Données de surveillance de la sécurité réseau (NSM)
- Sources de données de journaux
- NetFlow pour la surveillance de la sécurité
- Attaques contre les applications Web
- Analyse avancée des journaux
- Capture de paquets et investigation numérique
- Logiciels malveillants et renseignement sur les menaces
- Gestion des informations et des événements de sécurité (SIEM)
- Orchestration, automatisation et réponse aux incidents de sécurité (SOAR)
- Détection et réponse étendues (XDR)
- Planification de la réponse aux incidents
- Rôles et opérations des CSIRT
- Playbooks de surveillance de la sécurité

Méthodologies de recherche proactive de menaces (Threat Hunting)

Programme des travaux pratiques

- Explorer les technologies cryptographiques
- Explorer le système d'exploitation Windows
- Explorer le système d'exploitation Linux
- Explorer la sécurité des terminaux
- Étudier les méthodologies utilisées par les attaquants
- Explorer les attaques TCP/IP
- Étudier les menaces persistantes avancées (APT)
- Utiliser les outils NSM pour analyser les différentes catégories de données
- Analyser les activités DNS suspectes
- Étudier les attaques basées sur les navigateurs Web
- Corréler les journaux d'événements, les captures PCAP et les alertes relatives à une attaque
- Explorer les playbooks SOC

Rechercher les trafics réseau malveillants

Méthodes pédagogiques :

Méthodes pédagogiques : Un support de cours officiel sera remis aux stagiaires au format électronique. 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. Pour profiter pleinement du support électronique dès le 1er jour, nous invitons les participants à se munir d'un PC ou d'une tablette, qu'ils pourront connecter en WiFi dans nos locaux de Rueil, Lyon ou nos agences en régions. **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.Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés. Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.À l'issue de cette session, chaque stagiaire bénéficiaire sera contacté par un prestataire choisi par l'Opco Atlas afin d'évaluer « à chaud » la qualité de la formation suivie. **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 vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.

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