

Mettre en oeuvre et gérer les solutions de sécurité Cisco

Durée: 5 Jours Réf de cours: SCOR Version: 3.0

Résumé:

Mettre en œuvre et exploiter les technologies de sécurité de base Cisco.

La formation « Implementing and Operating Cisco Security Core Technologies (SCOR) » vous permet d'acquérir les compétences et les connaissances techniques nécessaires à la mise en œuvre des solutions de sécurité Cisco de base. Cette formation vous permettra d'assurer une protection avancée contre les cyberattaques et vous préparera à occuper des postes de haut niveau dans le domaine de la sécurité. Cette formation vous permet également d'obtenir 30 crédits de formation continue (CE) valables pour le renouvellement de votre certification.

Mis à jour : 23/09/2026

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Expliquer comment opèrent les différents acteurs malveillants en décrivant leurs motivations, leurs vecteurs d'attaque courants, les schémas typiques de violation et d'utilisation abusive des identifiants, ainsi que le rôle du cycle de vie du renseignement sur les cybermenaces pour aider les organisations à comprendre et à suivre ces menaces en constante évolution
- Décrire comment les faiblesses structurelles des logiciels et des applications web sont identifiées, classées et hiérarchisées à l'aide de concepts tels que les classes de vulnérabilité, l'OWASP, le CVE et le CVSS, et expliquer comment les systèmes d'IA/LLM élargissent ce paysage avec de nouveaux schémas de vulnérabilité
- Expliquer pourquoi les personnes et l'identité restent un vecteur d'attaque majeur en décrivant les cycles de vie de l'ingénierie sociale et du vol d'identifiants, et en présentant les principales couches conceptuelles de défense que les organisations mettent en œuvre pour réduire, sans toutefois les éliminer complètement, les risques liés à l'identité
- Décrire les principaux éléments constitutifs de la cryptographie : le hachage, le chiffrement symétrique et asymétrique, l'échange de clés, les signatures numériques, l'infrastructure à clé publique (PKI) et les protocoles de transport chiffrés, et expliquer les garanties de sécurité spécifiques et les hypothèses de confiance que chacun d'entre eux introduit dans la conception d'une entreprise
- Expliquer comment le modèle « Zero Trust », la défense en profondeur et le cadre Cisco SAFE Blueprint combinent leurs forces pour transformer les informations relatives aux menaces, aux vulnérabilités, aux identités et à la cryptographie en une architecture de sécurité cohérente qui anticipe les défaillances, limite l'ampleur des impacts et guide le déploiement technologique dans l'ensemble de l'environnement
- Expliquer pourquoi le réseau d'accès de couche 2 constitue une frontière de sécurité fondamentale, en décrivant comment la segmentation, la topologie, l'adressage, la découverte des voisins et les contrôles des ports périphériques interagissent
- Décrire les architectures SASE et SSE ainsi que les fonctionnalités Cisco Secure Access qui offrent une protection unifiée, fournie via le cloud, des applications privées et d'Internet dans les environnements distants et les succursales
- Configurer la connectivité fournie via le cloud, l'authentification basée sur l'identité et des politiques d'accès granulaires afin de fournir un accès sécurisé aux applications privées pour les utilisateurs distants et des succursales
- Configurer la connectivité, l'identité et les contrôles de sécurité afin de fournir un accès sécurisé à Internet et aux applications SaaS pour les utilisateurs distants et des succursales
- Expliquer comment l'identité, le contexte des appareils et le contrôle d'accès basé sur des politiques fonctionnent conjointement dans les solutions d'accès réseau sécurisé, et décrire comment Cisco ISE prend en charge l'accès différencié via AAA, l'accès invité, le profilage et le BYOD
- Configurer le contrôle d'accès aux réseaux filaires et sans fil avec Cisco ISE en mettant en œuvre les protocoles 802.1X et MAB, en appliquant les politiques d'authentification et d'autorisation de Cisco ISE, en sélectionnant les approches EAP et supplicant appropriées, et en utilisant RADIUS et CoA pour appliquer le changement d'état d'accès
- Expliquer comment Cisco Duo prend en charge les principes «zero-trust» grâce à une vérification rigoureuse des utilisateurs, à la confiance accordée aux appareils, à des politiques d'accès adaptatives et à la visibilité des risques liés à l'identité avec Cisco Identity Intelligence
- Expliquer comment Cisco Secure Email Threat Defense est intégré et configuré dans les environnements de messagerie basés sur Microsoft 365 afin d'assurer la visibilité des messages, l'analyse des menaces et la correction des failles liées au phishing, à la compromission des e-mails professionnels et à la prise de contrôle de compte
- Expliquer comment les organisations établissent, valident et garantissent la fiabilité des terminaux grâce à la gestion des équipements, à la surveillance des ressources, à l'évaluation de la

pour empêcher les attaques locales de compromettre la sécurité des couches supérieures

- Sécuriser les équipements de l'infrastructure réseau en réduisant leur surface d'attaque, en protégeant les plans de gestion et de contrôle en tant que canaux d'autorité privilégiés, et en choisissant des architectures de plan de gestion qui créent des frontières de confiance claires et défendables
- Concevoir et exploiter le système AAA pour l'administration de l'infrastructure en choisissant les protocoles appropriés, en définissant le comportement AAA et le comportement de repli, et en dépannant systématiquement les défaillances AAA afin de rétablir un accès administratif sécurisé.
- Effectuer la configuration de base de Cisco Secure Firewall Threat Defense.
- Configurer une politique de contrôle d'accès comprenant une politique anti-intrusion, une politique relative aux fichiers et une politique anti-malware afin de répondre aux exigences de sécurité données.
- Configurer des solutions VPN site à site sécurisées pour établir une connectivité entre des sites distants avec Cisco Secure Firewall Threat Defense.
- Configurer des solutions VPN d'accès à distance sur Cisco Secure Firewall Threat Defense afin de fournir une connectivité sécurisée au réseau d'entreprise pour les utilisateurs distants
- Évaluer les stratégies de sécurité dans le cloud à l'aide des modèles de responsabilité partagée NIST 800-145, des cadres de sécurité et des solutions CASB pour les environnements multicloud
- Décrire les stratégies de sécurité des charges de travail dans le cloud englobant les principes de microsegmentation, les plateformes Cisco Secure Workload et Multicloud Defense, ainsi que les approches de sécurité basées sur eBPF

conformité et de l'état de sécurité, ainsi qu'au contrôle des applications, afin de réduire les risques liés à la sécurité des terminaux

- Comprendre comment les solutions modernes de sécurité des terminaux, telles que Cisco Secure Endpoint avec Cisco Secure Malware Analytics, combinent prévention, détection continue, analyse des logiciels malveillants et enquêtes basées sur les événements, en s'appuyant sur les concepts de plateforme de protection des terminaux (EPP) et de détection et réponse sur les terminaux (EDR)
- Décrire comment Splunk Enterprise et Splunk Cloud fonctionnent en tant que plateformes d'analyse de données pour les opérations de sécurité, comment les composants de la plateforme Splunk et ses modèles de déploiement prennent en charge le traitement et l'analyse évolutifs des données
- Construire des requêtes à l'aide du langage Splunk Processing Language pour rechercher et analyser les données ingérées
- Expliquer comment les produits de sécurité Cisco s'intègrent à Splunk et décrire comment Splunk Enterprise étend la plateforme avec des capacités SIEM
- Décrire comment Splunk SOAR prend en charge les opérations du SOC grâce à l'orchestration, à l'automatisation des playbooks et à la réponse axée sur les cas, et comment il fonctionne avec Splunk Enterprise Security et Cisco XDR pour automatiser les workflows d'investigation et de réponse
- Expliquer comment le XDR unifie la détection des menaces, l'investigation et la réponse à travers plusieurs domaines de sécurité, et décrire comment Cisco XDR offre une visibilité inter-domaines, une corrélation, une hiérarchisation, une investigation ainsi qu'une réponse coordonnée et automatisée à travers des contrôles de sécurité intégrés

Pré-requis:

Il n'y a pas de prérequis formel 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
- Utilisation du système d'exploitation Windows
- Connaissance pratique des réseaux et des concepts Cisco IOS
- Compréhension des principes fondamentaux de la sécurité des réseaux
- CCNA - Mettre en oeuvre et administrer des solutions réseaux Cisco

Test et certification

Cette formation vous prépare à l'examen « Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) v2.0 », d'une durée de 120 minutes, qui évalue vos connaissances en matière de mise en œuvre et d'exploitation des technologies de sécurité de base, notamment :

- Sécurité des réseaux
- Sécurité du cloud
- Sécurité des réseaux périphériques (Secure Service Edge)
- Protection et détection des terminaux
- Accès au réseau
- Visibilité
- Application des stratégies

Après avoir réussi cet examen, vous obtiendrez la certification « **Cisco Certified Specialist - Security Core** » et remplirez les conditions requises pour passer l'examen de base menant aux certifications « Cisco Certified Network Professional (CCNP) Security » et « Cisco Certified Internetwork Expert (CCIE) Security ».

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

Pas de recommandation spécifique.

- SAUI - Implementing Automation for Cisco Security Solutions
- SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention
- SFWIPA - Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention
- SISE - Mettre en oeuvre et configurer la solution Cisco Identity Services Engine
- SVPN - Implementing Secure Solutions with Virtual Private Networks
- SESA - Sécuriser les emails avec Cisco Email Security Appliance
- SWSA - Sécuriser le Web avec Cisco Web Security Appliance

Contenu:

Contenu du cours

- Analyse et veille sur les cybermenaces modernes
- Vulnérabilités, exploits et risques liés à l'IA
- Ingénierie sociale, usurpation d'identité et mesures de contrôle contre le phishing
- Principes fondamentaux de la cryptographie
- Sécurité Layer 2
- Principes de conception : Zero Trust et SAFE
- Renforcement de la sécurité des équipements et gestion sécurisée
- Dépannage AAA pour l'accès administrateur aux équipements
- Déploiement de Cisco Secure Firewall Threat Defense
- Politiques de sécurité de Cisco Secure Firewall
- Solutions VPN site à site
- Solutions VPN d'accès à distance
- Modèles et référentiels de sécurité dans le cloud
- Sécurité des workloads dans le cloud et eBPF
- DevSecOps et automatisation de la sécurité
- Identité « Zero Trust » avec Cisco Duo
- Architectures SASE et SSE
- Mise en œuvre de l'accès privé sécurisé
- Mise en œuvre de l'accès Internet sécurisé
- Principes fondamentaux de la gestion des identités et des accès
- Configuration de 802.1X, MAB et CoA avec Cisco ISE
- Cisco Secure Email Threat Defense (ETD)
- Fiabilité des terminaux, conformité et gestion des équipements
- Modern EDR et Malware Analytics
- Splunk et Security Analytics
- Automatisation du SOC et SOAR
- Détection et réponse étendues (XDR)

Exercices pratiques

- Renforcement de la sécurité des équipements Cisco IOS XE
- Authentification du protocole de routage OSPFv3
- Administration des périphériques réseau via TACACS+
- Configuration initiale du pare-feu Cisco Secure
- Gestion des politiques du pare-feu Cisco Secure
- VPN site à site du pare-feu Cisco Secure
- VPN d'accès à distance du pare-feu Cisco Secure
- Mise en œuvre d'un accès privé sécurisé
- Mise en œuvre d'un accès Internet sécurisé
- MAB Cisco ISE et 802.1X filaire
- Cisco Secure Email Threat Defense
- Cisco Secure Endpoint
- Intégration du pare-feu Cisco Secure avec Splunk
- Cisco XDR

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