

Programme

Cisco Certified Support Technician : Cybersecurity

CERTIFIER

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

La certification Cisco Certified Support Technician : Cybersecurity prouve la maîtrise des principes fondamentaux pour :

- la gestion des principes essentiels de sécurité ;
- la gestion des concepts de base de la sécurité des réseaux ;
- la gestion des concepts de sécurité des points de terminaison ;
- l'évaluation de la vulnérabilité et la gestion des risques ;
- le traitement des incidents.

Les candidats retenus ont une conscience aiguë de l'importance de la sécurité et des menaces qui pèsent sur une entreprise lorsque les procédures de sécurité ne sont pas respectées. Ils développent les compétences d'investigation et de mise en œuvre nécessaires pour réussir dans ce domaine et ont l'aptitude et le désir d'en apprendre davantage. Ils connaissent l'ensemble des outils à un niveau fondamental et peuvent contribuer à l'atténuation des menaces et à la réponse aux incidents.

Durée : 50 minutes d'examen

Langues : français, anglais

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

1. GÉRER LES PRINCIPES ESSENTIELS DE SÉCURITÉ

- **Définir les principes essentiels de sécurité**

- Vulnérabilités, menaces, exploits et risques
- Vecteurs d'attaque
- Renforcement
- Défense en profondeur
- Confidentialité, intégrité et disponibilité (CIA)
- Types d'attaquants
- Raisons des attaques
- Code d'éthique

- **Expliquer les menaces et les vulnérabilités courantes**

- Malwares
- Ransomwares
- Dénis de service
- Botnets
- Attaques d'ingénierie sociale (*tailgating, spear phishing, phishing, vishing, smishing, etc.*)

- Attaques physiques

- *Man in the middle*

- Vulnérabilités IoT

- Menaces d'initiés

- *Advanced Persistent Threat* (APT)

- **Expliquer les principes de la gestion des accès**

- Authentification

- Autorisation et comptabilité (AAA)

- RADIUS

- Authentification multifactorielle (MFA)

- Politiques en matière de mots de passe

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

1. GÉRER LES PRINCIPES ESSENTIELS DE SÉCURITÉ

- **Expliquer les méthodes et les applications de cryptage**
 - Types de cryptage
 - Hachage
 - Certificats
 - Infrastructure à clé publique (PKI)
 - Algorithmes de cryptage forts ou faibles
 - États des données et cryptage approprié (données en transit, données au repos, données en cours d'utilisation)
 - Protocoles utilisant le cryptage

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

2. GÉRER LES CONCEPTS DE BASE DE LA SÉCURITÉ DES RÉSEAUX

• Décrire les vulnérabilités du protocole TCP/IP

- TCP
- UDP
- HTTP
- ARP
- ICMP
- DHC
- DNS

• Expliquer l'impact des adresses réseau sur la sécurité du réseau

- Adresses IPv4 et IPv6
- Adresses MAC
- Segmentation du réseau
- Notation CIDR
- NAT
- Réseaux publics et privés

• Décrire l'infrastructure et les technologies de réseau

- Architecture de sécurité réseau
- DMZ
- Virtualisation
- Cloud
- Honeypot
- Serveur proxy
- IDS
- IPS

• Mettre en place un réseau sans fil sécurisé SoHo

- Filtrage d'adresse MAC
- Normes et protocoles de cryptage
- SSID

• Mettre en œuvre des technologies d'accès sécurisé

- ACL
- Pare-feu
- VPN
- NAC

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

3. COMPRENDRE LES CONCEPTS DE SÉCURITÉ DES POINTS DE TERMINAISON

- **Décrire les concepts de sécurité des systèmes d'exploitation**
 - Windows, macOS et Linux
 - Fonctions de sécurité, y compris Windows Defender et les pare-feux basés sur l'hôte
 - CLI et PowerShell
 - Autorisations de fichier et de répertoire
 - Élévation de privilèges
- **Démontrer une bonne connaissance des outils de recueil des informations sur l'évaluation de la sécurité**
 - *Netstat*
 - *Nslookup*
 - *Tcpdump*
- **Vérifier la conformité des systèmes de points de terminaison aux politiques et aux normes de sécurité**
 - Inventaire matériel (gestion des actifs)
 - Inventaire logiciel
 - Déploiement de programmes
 - Sauvegardes de données
 - Conformité réglementaire (PCI DSS, HIPAA, GDPR)
 - BYOD (gestion des appareils, chiffrement des données, distribution d'apps, gestion de la configuration)
- **Mettre en œuvre les mises à jour des logiciels et du matériel informatique**
 - Mise à jour de Windows
 - Mises à jour d'applications, pilotes de périphériques, micrologiciels
 - Correctifs

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

3. COMPRENDRE LES CONCEPTS DE SÉCURITÉ DES POINTS DE TERMINAISON

- **Interpréter les journaux du système**
 - *Event Viewer*
 - Journaux d'audit
 - Journaux de système et d'application
 - *Syslog*
 - Identification des anomalies
- **Démontrer une bonne connaissance de la suppression des logiciels malveillants**
 - Analyse des systèmes
 - Examen des journaux d'audit
 - Remédier aux logiciels malveillants

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

4. ÉVALUER LA VULNÉRABILITÉ ET GÉRER LES RISQUES

- **Expliquer la gestion de la vulnérabilité**

- Identification, gestion et atténuation des vulnérabilités
- Reconnaissance active et passive
- Tests (scan de port, automatisation)

- **Utiliser des techniques de renseignement sur les menaces pour identifier les vulnérabilités potentielles du réseau**

- Utilisation et limites des bases de données sur les vulnérabilités
- Outils standard utilisés pour évaluer les vulnérabilités et formuler des recommandations, des politiques et des rapports
- Vulnérabilités et expositions communes (CVEs), rapports sur la cybersécurité, actualités sur la cybersécurité, services d'abonnement et renseignements collectifs

- Renseignement ad hoc et automatisé sur les menaces
- Importance de la mise à jour de la documentation et d'autres formes de communication de manière proactive avant, pendant et après les incidents de cybersécurité
- Comment sécuriser, partager et mettre à jour la documentation

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

4. ÉVALUER LA VULNÉRABILITÉ ET GÉRER LES RISQUES

- **Expliquer la gestion des risques**

- Vulnérabilité et risque
- Classement des risques
- Approches de la gestion des risques
- Stratégies d'atténuation des risques
- Niveaux de risque (faible, moyen, élevé, extrêmement élevé)
- Risques associés à des types spécifiques de données et à des classifications de données
- Évaluations de la sécurité des systèmes informatiques (sécurité de l'information, gestion du changement, opérations informatiques, assurance de l'information)

- **Expliquer l'importance de la reprise après sinistre et de la planification de la continuité des activités**

- Catastrophes naturelles et d'origine humaine
- Caractéristiques des plans de reprise après sinistre (DRP) et des plans de continuité des activités (BCP)
- Sauvegarde, contrôles de reprise après sinistre (d'inspection, préventifs et correctifs)

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

5. TRAITER LES INCIDENTS

- **Surveiller les événements liés à la sécurité et savoir quand une escalade est nécessaire**
 - Rôle du SIEM et du SOAR
 - Surveillance des données du réseau pour identifier les incidents de sécurité (captures de paquets, diverses entrées de fichiers journaux, etc.)
 - Identification des événements suspects au fur et à mesure qu'ils se produisent
- **Expliquer les processus de criminalistique numérique et l'attribution des attaques**
 - Chaîne de destruction
 - Matrice MITRE ATT&CK et Diamond Model
 - Tactiques, techniques et procédures (TTP)
 - Sources de preuves (artefacts)
 - Traitement des preuves (préservation des preuves numériques, chaîne de conservation)
- **Expliquer l'impact des cadres de conformité sur le traitement des incidents**
 - Cadres de conformité (GDPR, HIPAA, PCI-DSS, FERPA, FISMA)
 - Exigences en matière de rapports et de notifications
- **Décrire les éléments de la réponse aux incidents de cybersécurité**
 - Éléments de politique, de plan et de procédure
 - Étapes du cycle de vie de la réponse aux incidents (NIST Special Publication 800-61 sections 2.3, 3.1-3.4)

APPRENDRE

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

E-learning

La certification Cisco Certified Support Technician (CCST) : Cybersecurity est idéale pour qui débute en cybersécurité et souhaite devenir spécialiste du domaine. Les objectifs couvrent les sujets essentiels pour un spécialiste en cybersécurité : principes fondamentaux, sécurité des réseaux, sécurité des terminaux, évaluation des vulnérabilités, gestion des risques et traitement des incidents. La maîtrise de ces fondamentaux constitue une base solide pour réussir l'examen et devenir professionnel de la cybersécurité. Animé par Michael Solomon, expert sécurité de LearnKey, le cours couvre les cinq domaines de l'examen. Un certificat de réussite est délivré à partir de 80 % de bonnes réponses à toutes les évaluations de fin de domaine ; un badge à partir de 90 %. Le cours couvre :

- la gestion des principes essentiels de sécurité ;
- la gestion des concepts de base de la sécurité des réseaux ;
- la gestion des concepts de sécurité des points de terminaison ;
- l'évaluation de la vulnérabilité et la gestion des risques ;
- le traitement des incidents.

Un certificat d'achèvement peut être obtenu en obtenant un score de 80 % ou plus à tous les tests de post-évaluation de l'e-learning. Un badge peut être obtenu en obtenant un score de 90 % ou plus à tous les tests de post-évaluation.

Ce cours est valable pendant un an en ligne sauf indication contraire, et est limité à l'utilisation par une seule personne. Les licences deviendront inactives si elles sont utilisées par plusieurs personnes.

Durée : 7h17 d'e-learning

Langue : anglais





TESTER

CISCO CERTIFIED SUPPORT TECHNICIAN : CYBERSECURITY CERTIFICATION

S'entraîner

Les tests pratiques Cisco Certified Support Technician Cybersecurity sont alignés sur les objectifs de certification Cisco Certified Support Technician : Cybersecurity.

Les tests pratiques sont des évaluations basées sur la performance qui permettent aux candidats de se familiariser avec l'environnement de test et de gagner en confiance avant le jour de l'examen. Ils préparent les candidats à l'examen Cisco Certified Support Technician : Cybersecurity.

Inclus :

- 1 examen blanc

Langues : français, anglais