# CISCO
## Technicien de soutien certifié Cisco Cybersécurité

RS :

Le candidat retenu possède les connaissances et les compétences de base nécessaires pour démontrer ses compétences en cybersécurité. Ce test sera un point d'entré dans le programme Cisco Certified. La prochaine certification dans ce parcours est le Cisco Certified CyberOps Associate.

Les candidats à cet examen commencent leurs parcours dans le domaine de la cybersécurité. Cet examen évalue leur compréhension des principaux paradigmes de sécurité, de la terminologie et de l'état d'esprit. Les candidats retenus auront une conscience aiguë de l'importance de la sécurité et des menaces pour un entreprise lorsque les procédures de sécurité ne sont pas respectées. Ils sont prêts à enseigner aux autres les questions de sécurité. Ils acquièrent les compétences d'enquête et de mise en œuvre nécessaires

pour réussir sur le terrain et ont l'aptitude et le désir d'en apprendre davantage. Ils connaissent l'ensemble des outils à un niveau fondamental et peut contribuer à l'atténuation des menaces et à l'intervention en cas d'incident.

**Prérequis :** Les candidats retenus sont des techniciens en cybersécurité qualifiés et prêts à travailler qui ont au moins 150 heures d'instruction et d'expérience pratique.

Ils acquièrent les compétences d'enquête et de mise en œuvre nécessaires pour réussir sur le terrain et ont l'aptitude et le désir d'en apprendre davantage. Ils connaissent l'ensemble des outils à un niveau fondamental et peut contribuer à l'atténuation des menaces et à l'intervention en cas d'incident. Les candidats retenus sont des techniciens en cybersécurité qualifiés et prêts à travailler qui ont au moins 150 heures d'instruction et d'expérience pratique.

# Objectifs Cybersécurité du CCST

**Principes essentiels de sécurité**

### 1.1 Définir les principes de sécurité essentiels

- Vulnérabilités, menaces, exploits et risques ; vecteurs d'attaque ; durcissement ; défense en profondeur ; la confidentialité, l'intégrité et la disponibilité ; types d'agresseurs ; les raisons des attaques ; code de déontologie

## Principes essentiels de sécurité

### 1.2 Expliquer les menaces et les vulnérabilités courantes

• Logiciels malveillants, ransomware, déni de service, botnets, attaques d'ingénierie sociale (tailgating, spear phishing, phishing, vishing, smishing, etc.), attaques physiques, homme au milieu, vulnérabilités IdO, menaces internes, menace avancée persistante (APT)

### 1.3 Expliquer les principes de gestion de l'accès

• Authentification, autorisation et comptabilité (AAA) ; RAYON ; authentification multifactorielle (AMF) ; politiques de mot de passe

### 1.4 Expliquer les méthodes et les applications de chiffrement

• Types de chiffrement, hachage, certificats, infrastructure à clé publique (ICP) ; algorithmes de chiffrement forts ou faibles ; l'état des données et le chiffrement approprié (données en transit, données au repos, données utilisées) ; protocoles utilisant le chiffrement

## Concepts de base de sécurité réseau

### 2.1 Décrire les vulnérabilités du protocole TCP/IP

• TCP, UDP, HTTP, ARP, ICMP, DHCP, DNS

### 2.2 Expliquer comment les adresses réseau affectent la sécurité du réseau

• Adresses IPv4 et IPv6, adresses MAC, segmentation de réseau, notation CIDR, NAT, réseaux publics vs privés)

### 2.3 Décrire l'infrastructure et les technologies du réseau

• Architecture de sécurité réseau, DMZ, virtualisation, cloud, honeypot, serveur proxy, IDS, IPS

### 2.4 Configurer un réseau SoHo sans fil sécurisé

• Filtrage des adresses MAC, normes et protocoles de cryptage, SSID

### 2.5 Mettre en œuvre des technologies d'accès sécurisé

• LCA, pare-feu, RPV, CNA

## Concepts de sécurité des terminaux

### 3.1 Décrire les concepts de sécurité du système d'exploitation

• Windows, macOS et Linux ; les caractéristiques de sécurité, y compris Windows Defender et les pares-feux basés sur l'hôte ; CLI et PowerShell ; les autorisations de fichiers et de répertoires ; augmentation des privilèges

### 3.2 Démontrer sa connaissance des outils de mesure appropriés qui recueillent des renseignements sur l'évaluation de la sécurité

• Netstat, nslookup, tcpdump

### 3.3 Vérifier que les systèmes terminaux respectent les politiques et les normes de sécurité

• Inventaire du matériel (gestion des actifs), inventaire des logiciels, déploiement des programmes, sauvegardes de données, conformité réglementaire (PCI DSS, HIPAA, GDPR), BYOD (gestion des appareils, cryptage des données, distribution des applications, gestion des configurations)

## Concepts de sécurité des terminaux

### 3.4 Mettre en œuvre les mises à jour logicielles et matérielles

• Mise à jour Windows, mises à jour des applications, pilotes de périphériques, micrologiciel, correctif

### 3.5 Interpréter les journaux du système

• Event Viewer, journaux d'audit, journaux système et application, syslog, identification des anomalies

### 3.6 Démontrer une connaissance de la suppression des logiciels malveillants

• Systèmes de numérisation, examen des journaux de numérisation, correction des logiciels malveillants

## Évaluation de la vulnérabilité et gestion des risques

### 4.1 Expliquer la gestion des vulnérabilités

• Détermination, gestion et atténuation des vulnérabilités ; reconnaissance active et passive ; testing (port scanning, automation)

### 4.2 Utiliser des techniques de renseignement sur les

• menaces pour cerner les vulnérabilités potentielles du réseau

Utilisations et limites des bases de données de vulnérabilité; les outils normalisés de l'industrie utilisés pour évaluer les vulnérabilités et formuler des recommandations, des politiques et des rapports; Vulnérabilités et expositions communes (CVE), rapports sur la cybersécurité, nouvelles sur la cybersécurité, services d'abonnement et renseignements collectifs; des renseignements ponctuels et automatisés sur les menaces; l'importance de mettre à jour la documentation et les autres formes de communication de façon proactive avant, pendant et après les incidents de cybersécurité; comment sécuriser, partager et mettre à jour la documentation

### 4.3 Expliquer la gestion des risques

• Vulnérabilité par rapport au risque, classement des risques, approches de gestion des risques, stratégies d'atténuation des risques, niveaux de risque (faible, moyen, élevé, extrêmement élevé), risques associés à des types particuliers de données et de classifications de données, évaluations de sécurité des systèmes de TI (sécurité de l'information, gestion du changement, opérations informatiques, assurance de l'information)

### 4.4 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 (PRD) et des plans de continuité des activités (PCA), sauvegarde, contrôles de reprise après sinistre (détection, prévention et correction)

## Traitement des incidents

### 5.1 Surveiller les événements de sécurité et savoir quand une intervention par palier est requise

• 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 à mesure qu'ils se produisent

Traitement des incidents

**5.2 Expliquer la criminalistique numérique et les processus d'attribution des attaques**

• Cyber Kill Chain, MITRE ATT&CK Matrix et Diamond Model ; Tactiques, techniques et procédures (TTP) ; sources de preuves (artéfacts) ; traitement des preuves (préservation des preuves numériques, chaîne de possession)

**5.3 Expliquer l'incidence des cadres de conformité sur le traitement des incidents**

• Cadres de conformité (RGPD, HIPAA, PCI-DSS, FERPA, FISMA), exigences de déclaration et de notification

**5.4 Décrire les éléments de l'intervention en cas d'incident de cybersécurité**

• Les éléments de politique, de plan et de procédure ; étapes du cycle de vie des interventions (Publication spéciale 800-61, sections 2.3, 3.1-3.4)

**4.3**

**4.4**

**5.1**