Date de publication : 26/01/2026

Formation : Defend against cyberthreats with Microsoft's security operations platform (Microsoft SC-200)

Cours officiel SC-200, préparation à l'examen

Formation pratique - 4j - 28h00 - Réf. MCJ
Prix : 2890 € H.T.

4,4 / 5

Avec cette formation, vous apprendrez à détecter, analyser et répondre aux menaces grâce à Microsoft Sentinel, Microsoft Defender XDR et Microsoft Defender for Cloud. Vous verrez comment les utiliser pour renforcer la sécurité et enquêter sur les incidents et réduire les cybermenaces.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Comprendre et appliquer les principes de la sécurité dans Azure.
- Gérer les identités et les accès utilisateurs.
- Sécuriser les réseaux, données et applications.
- Surveiller et corriger les menaces et vulnérabilités.
- Mettre en œuvre des solutions de protection et de conformité.

Public concerné

Professionnels de la sécurité chargés de détecter, analyser et répondre aux menaces à l'aide des outils Microsoft de protection et de surveillance.

Prérequis

Des connaissances de base en sécurité Microsoft, Azure et Microsoft 365 sont recommandées avant de suivre cette formation.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français. Support de cours officiel au format numérique et en anglais. Bonne compréhension de l'anglais à l'écrit.

PARTICIPANTS

Professionnels de la sécurité chargés de détecter, analyser et répondre aux menaces à l'aide des outils Microsoft de protection et de surveillance.

PRÉREQUIS

Des connaissances de base en sécurité Microsoft, Azure et Microsoft 365 sont recommandées avant de suivre cette formation.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

Programme de la formation

1 Mitiger les menaces à l'aide de Microsoft Defender XDR

- Introduction à la protection contre les menaces avec Microsoft Defender XDR.
- Atténuer les incidents avec Microsoft Defender.
- Remédier aux menaces avec Microsoft Defender pour Office 365.
- Gérer la protection des identités avec Microsoft Entra ID (Identity Protection).
- Sécuriser votre environnement avec Microsoft Defender for Identity.
- Sécuriser les applications et services cloud avec Microsoft Defender for Cloud Apps.

2 Atténuer les menaces à l'aide de Microsoft Security Copilot

- Introduction à l'IA générative et aux agents.
- Décrire Microsoft Security Copilot.
- Décrire les fonctionnalités de base de Microsoft Security Copilot.
- Décrire les expériences intégrées de Microsoft Security Copilot.
- Explorer les cas d'utilisation de Microsoft Security Copilot.

3 Atténuer les menaces avec Microsoft Purview

- Enquêter et répondre aux alertes de prévention de perte de données (DLP) Microsoft Purview.
- Enquêter sur les alertes de risque interne et les activités associées.
- Effectuer des recherches et des enquêtes avec Microsoft Purview Audit.
- Rechercher du contenu avec Microsoft Purview eDiscovery.

4 Atténuer les menaces avec Microsoft Defender pour Endpoint

- Protéger contre les menaces avec Microsoft Defender for Endpoint.
- Déployer l'environnement Microsoft Defender for Endpoint.
- Implémenter les améliorations de sécurité Windows.
- Effectuer des investigations sur les appareils.
- Effectuer des actions sur un appareil.
- Effectuer des investigations sur les preuves et entités.
- Configurer et gérer l'automatisation.
- Configurer les alertes et les détections.
- Utiliser la gestion des menaces et des vulnérabilités.

5 Atténuer les menaces à l'aide de Microsoft Defender pour le Cloud

- Planifier des protections de charge de travail cloud à l'aide de Microsoft Defender pour le Cloud.
- Connecter des ressources Azure à Microsoft Defender pour le Cloud.
- Connecter des ressources non Azure à Microsoft Defender pour le Cloud.
- Gérer votre gestion de la posture de sécurité cloud.
- Expliquer les protections de charge de travail cloud dans Microsoft Defender pour le Cloud.
- Corriger les alertes de sécurité à l'aide de Microsoft Defender pour le Cloud.

Options

Certification : 200 € H.T.

Microsoft Certified: Security Operations Analyst Associate (SC-200)
Comment passer votre examen ?

L'option de certification se présente sous la forme d'un voucher et de « practice tests » qui vous permettront de vous entraîner et de passer l'examen à l'issue de la formation.

Ce programme est une création originale, conçu par les équipes pédagogiques d'ORSYS Formation. Toute reproduction, représentation, adaptation ou exploitation, totale ou partielle, sans autorisation préalable écrite d'ORSYS, est strictement interdite. ORSYS se réserve le droit d'engager toute action nécessaire à la protection de ses droits de propriété intellectuelle.

Dates et lieux

CLASSE À DISTANCE
2026 : 6 oct., 15 déc.

2027 : 30 mars, 30 mars, 25 mai, 25 mai, 7 sep., 7 sep., 16 nov., 16 nov.

PARIS LA DÉFENSE
2026 : 6 oct., 15 déc.

2027 : 30 mars, 25 mai, 7 sep., 16 nov.

LYON
2026 : 15 déc.

2027 : 30 mars, 7 sep.