OpenCertif
Centre de formation et de certification professionnelle

SYLLABUS OFFICIEL

Examen SC-200

Analyste opérations de sécurité Microsoft

Certification : Microsoft Certified — Security Operations Analyst Associate

Niveau : Associate | Public : Analystes SOC / Threat Hunters / Incident responders

1. Présentation de la certification

L'examen **SC-200 : Microsoft Security Operations Analyst** valide les compétences des analystes en opérations de sécurité qui réduisent le risque organisationnel en effectuant du triage, en répondant aux incidents, en chassant les menaces et en concevant des détections. La nouvelle version d'avril 2026 du référentiel introduit une structure en trois domaines (au lieu de quatre) orientée workflow SOC moderne, incluant AI agents, Copilots, Sentinel Graph et capacités Data lake.

La réussite de cet examen unique conduit à l'obtention de la certification **Microsoft Certified : Security Operations Analyst Associate**, particulièrement valorisée pour les rôles d'analyste SOC, de threat hunter, de répondeur à incidents et de SecOps engineer dans des environnements Microsoft.

Informations clés

Code de l'examen	SC-200
Intitulé officiel	Microsoft Security Operations Analyst
Certification obtenue	Microsoft Certified : Security Operations Analyst Associate
Niveau	Associate
Statut	Actif (nouvelle structure en 3 domaines depuis le 16 avril 2026)
Nouveautés 2026	Sentinel Graph, AI agents, Copilots, KQL jobs, Summary rule tables, Sentinel MCP Server, Data lake tiers, attack disruption automatique
Durée de l'examen	Environ 100 minutes (selon planification)
Nombre de questions	40 à 60 questions (QCM, études de cas, glisser-déposer, scénarios pratiques, KQL)
Score de réussite	700 / 1000
Langues disponibles	Anglais, français, allemand, japonais, espagnol, chinois (simplifié), coréen, portugais (Brésil)
Validité	1 an, renouvellement gratuit en ligne via Microsoft Learn

Modalité	En centre agréé (OpenCertif — Pearson VUE) ou à distance (OnVUE)

2. Profil du candidat

En tant que candidat à cet examen, vous êtes un analyste en opérations de sécurité qui réduit le risque organisationnel en effectuant du triage, en répondant aux incidents, en chassant les menaces et en concevant des détections. En tant qu'analyste, vous supervisez, identifiez, enquêtez et répondez aux menaces dans des environnements multi-cloud et on-premises via :

- Microsoft Defender XDR.
- Microsoft Sentinel.
- Microsoft Entra ID.
- Microsoft Purview.
- Microsoft Defender for Cloud workload protections.
- KQL (Kusto Query Language) et Sentinel Graph pour le threat hunting.
- Automatisation des réponses aux menaces.

Vous collaborez avec la direction métier et sécurité pour définir les standards de sécurité de l'organisation. Vous travaillez avec d'autres rôles de l'entreprise digitale pour mettre en œuvre ces standards, améliorer la posture de sécurité et sensibiliser. Vous devez être familier avec :

- Les solutions Microsoft Security, Compliance et Identity.
- Microsoft 365 et les services Azure cloud.
- Les AI agents et Copilots.
- Les systèmes d'exploitation Windows, Linux et mobiles.

3. Prérequis et public cible OpenCertif

Aucun prérequis formel n'est exigé, mais OpenCertif recommande aux candidats de disposer d'une expérience préalable dans les domaines suivants :

- Notions de cybersécurité et de SOC (idéalement certification SC-900).
- Familiarité avec Microsoft Sentinel et Microsoft Defender XDR.
- Connaissance de base de KQL (Kusto Query Language).
- Compréhension du framework MITRE ATT&CK.;
- Expérience pratique d'un environnement Microsoft 365 / Azure.

Public cible OpenCertif

- Analystes SOC (Security Operations Center).
- Threat hunters et threat intelligence analysts.
- Répondeurs à incidents (incident responders).
- Ingénieurs SecOps utilisant Microsoft Sentinel et Defender XDR.
- Profils en transition vers la cybersécurité opérationnelle.
- Administrateurs système évoluant vers la sécurité opérationnelle.

4. Domaines de compétences mesurées

L'examen est structuré autour de 3 grands domaines de compétences. Le tableau ci-dessous indique le poids relatif de chaque domaine dans l'évaluation finale (version du 16 avril 2026).

Domaine	Intitulé	Pondération
1	Gérer un environnement d'opérations de sécurité	40 — 45 %
2	Répondre aux incidents de sécurité	35 — 40 %
3	Effectuer du threat hunting	20 — 25 %

Remarque : la majorité des questions concernent des fonctionnalités en disponibilité générale (GA). Certaines questions peuvent porter sur des fonctionnalités en préversion couramment utilisées.

5. Détail des compétences mesurées

Cette section détaille de manière exhaustive l'ensemble des compétences couvertes par l'examen SC-200, conformément au guide d'étude officiel Microsoft (version du 16 avril 2026).

1 Gérer un environnement d'opérations de sécurité — 40 — 45 %

1.1 Configurer l'automatisation pour Microsoft Defender XDR et Microsoft Sentinel

- Configurer les notifications par e-mail dans Microsoft Defender XDR : incidents, actions, threat analytics.
- Configurer les notifications d'alerte dans Microsoft Defender XDR : tuning, suppression, corrélation.
- Configurer les fonctionnalités avancées de Microsoft Defender for Endpoint.
- Configurer les paramètres de règles dans Microsoft Defender for Endpoint.
- Configurer la collecte de données personnalisées dans Microsoft Defender for Endpoint.
- Configurer les stratégies de sécurité pour Microsoft Defender for Endpoint, y compris les règles de réduction de la surface d'attaque (ASR).
- Gérer les capacités d'enquête et réponse automatisées dans Microsoft Defender XDR.
- Configurer la disruption automatique des attaques dans Microsoft Defender XDR.
- Configurer et gérer les groupes d'appareils, permissions et niveaux d'automatisation dans Microsoft Defender for Endpoint.
- Créer et configurer des règles d'automatisation dans Microsoft Sentinel.
- Créer et configurer des playbooks Microsoft Sentinel.

1.2 Configurer le SIEM Microsoft Sentinel et la plateforme

- Spécifier les rôles Microsoft Sentinel.
- Gérer la rétention des données pour les tables XDR et Microsoft Sentinel : tiers Analytics, Data lake et XDR.
- Créer et configurer des workbooks Microsoft Sentinel.
- Optimiser la plateforme Microsoft Sentinel, y compris les recommandations d'optimisation SOC.

1.3 Ingérer des données dans le SIEM Microsoft Sentinel

- Sélectionner les connecteurs de données selon les besoins des sources, y compris les journaux Windows et événements de sécurité.
- Configurer la collecte des événements de sécurité Windows via Windows Security Events via AMA, y compris les règles de collecte de données.
- Planifier et configurer la collecte des événements de sécurité Windows via Windows Event Forwarding (WEF).
- Planifier et configurer les connecteurs Syslog via AMA et Common Event Format (CEF) via AMA.
- Configurer la collecte des activités Azure via Azure Policy et les paramètres de diagnostic des ressources.
- Ingérer des indicateurs de menace dans Microsoft Sentinel.
- Créer des tables de logs personnalisées dans le workspace pour stocker les données ingérées.

1.4 Configurer les détections

- Créer des règles de détection personnalisées via Advanced Hunting dans Microsoft Defender XDR.
- Gérer les règles de détection personnalisées dans Microsoft Defender XDR.
- Configurer et gérer les règles d'analytique dans Microsoft Sentinel SIEM : planifiées, temps quasi-réel (NRT), threat intelligence, machine learning.
- Analyser la couverture des vecteurs d'attaque via la matrice MITRE ATT&CK.;
- Configurer les anomalies dans Microsoft Sentinel.

2 Répondre aux incidents de sécurité — 35 — 40 %

2.1 Répondre aux alertes et incidents dans Microsoft Defender XDR

- Enquêter et remédier aux menaces via Microsoft Defender for Office 365, y compris la disruption automatique.
- Enquêter et remédier aux menaces ou entités compromises identifiées par Microsoft Purview.
- Enquêter et remédier aux alertes et incidents identifiés par Microsoft Defender for Cloud workload protections.
- Enquêter et remédier aux risques de sécurité identifiés par Microsoft Defender for Cloud Apps.
- Enquêter et remédier aux identités compromises identifiées par Microsoft Entra ID.
- Enquêter et remédier aux alertes de sécurité de Microsoft Defender for Identity.
- Enquêter et remédier aux alertes et incidents identifiés par Microsoft Sentinel.
- Enquêter sur les incidents via l'IA agentique, y compris Copilot for Security intégré.
- Enquêter sur les attaques complexes : multi-stage, multi-domain et lateral movement.
- Gérer les incidents de sécurité via case management.

2.2 Répondre aux alertes et incidents dans Microsoft Defender for Endpoint

- Enquêter sur les timelines d'appareils.
- Effectuer des actions sur les appareils : live response, collecte de packages d'investigation.
- Effectuer des investigations d'entités et de preuves.
- Enquêter et remédier aux incidents identifiés par la disruption automatique des attaques.

2.3 Enquêter sur les activités Microsoft 365 pour identifier les menaces

- Enquêter sur les menaces via Audit de Microsoft Purview.
- Enquêter sur les menaces via Content Search dans Microsoft Purview.
- Enquêter sur les menaces via les journaux d'activité Microsoft Graph.

3 Effectuer du threat hunting — 20 — 25 %

3.1 Détecter les menaces via Microsoft Defender XDR

- Identifier la table appropriée à utiliser dans une requête KQL.
- Identifier les menaces via Kusto Query Language (KQL).
- Créer des requêtes Advanced Hunting.
- Interpréter les threat analytics dans Microsoft Defender XDR.
- Créer des graphes de chasse (hunting graphs), y compris blast radius.
- Analyser les relations entre entités via Sentinel Graph.

3.2 Détecter les menaces via la plateforme Microsoft Sentinel

- Créer et superviser des requêtes de chasse.
- Créer et gérer des KQL jobs dans le Data lake.
- Créer et gérer des Summary rule tables pour les requêtes.
- Chasser les menaces via les Notebooks, y compris la connexion au Sentinel MCP Server.

6. Modalités pédagogiques OpenCertif

OpenCertif accompagne les candidats au SC-200 à travers un parcours blended-learning complet, combinant ressources e-learning interactives, sessions tutorées et ateliers techniques pratiques sur les technologies Microsoft Sentinel, Microsoft Defender XDR, KQL, Sentinel Graph et Microsoft Defender for Cloud.

Format de la formation

Durée recommandée	50 à 65 heures de formation (selon profil et niveau d'entrée)
Modalité	100 % distanciel asynchrone, ou blended (distanciel + classes virtuelles)
Support pédagogique	Modules interactifs Articulate Rise 360, scénarios immersifs VTS, ateliers techniques
Plateforme LMS	lmsopencertif.fr (Moodle) — accès 24/7 pendant 12 mois
Encadrement	Tutorat asynchrone par expert certifié + classes virtuelles bimensuelles
Évaluations	Quiz formatifs par module, ateliers pratiques, examen blanc final, simulation OnVUE
Certification finale	Passage de l'examen SC-200 en centre OpenCertif (Pearson VUE) ou OnVUE

Parcours d'apprentissage proposé

- **Module 1 :** Architecture du SOC moderne et rôle de l'analyste.
- **Module 2 :** Microsoft Defender XDR — vue d'ensemble et configuration.
- **Module 3 :** Microsoft Sentinel SIEM — rôles, retention, workbooks.
- **Module 4 :** Connecteurs de données et ingérence (AMA, WEF, Syslog, CEF).
- **Module 5 :** Automatisation — règles, playbooks, attack disruption.
- **Module 6 :** Règles d'analytique — NRT, threat intelligence, ML.
- **Module 7 :** KQL niveau 1 — syntaxe et requêtes de base.
- **Module 8 :** KQL niveau 2 — jointures, parsing, time windows.
- **Module 9 :** Réponse aux incidents — Defender for Office 365, Endpoint, Identity.
- **Module 10 :** Réponse aux incidents — Defender for Cloud, Cloud Apps, Sentinel.
- **Module 11 :** Investigation — device timelines, live response, case management.
- **Module 12 :** Microsoft Purview — Audit, Content Search, Microsoft Graph logs.
- **Module 13 :** Threat hunting — Advanced Hunting, hunting graphs, Sentinel Graph.
- **Module 14 :** Threat hunting avancé — Notebooks, KQL jobs, Data lake, MCP Server.

- **Module 15 :** Copilot for Security et IA agentique pour l’analyste SOC.
- **Module 16 :** MITRE ATT&CK; et analyse de couverture.
- **Module 17 :** Examen blanc et préparation finale.

7. Ressources d’étude officielles

En complément du parcours OpenCertif, les ressources Microsoft Learn suivantes sont fortement recommandées :

- Documentation sécurité Microsoft (learn.microsoft.com/security).
- Documentation Microsoft 365 Defender.
- Documentation Microsoft Defender for Cloud.
- Documentation Microsoft Sentinel (azure/sentinel).
- Documentation Microsoft Defender XDR.
- Documentation Microsoft Defender for Endpoint, Office 365, Identity, Cloud Apps.
- Documentation KQL (Kusto Query Language).
- Documentation Sentinel Graph et MITRE ATT&CK; mapping.
- Documentation Copilot for Security.
- Parcours d’apprentissage Microsoft Learn dédiés au SC-200.
- Évaluation pratique gratuite proposée par Microsoft.
- Espace de simulation d’examen (aka.ms/examdemo).
- Security, compliance, and identity community hub.
- Chaînes vidéo : Exam Readiness Zone.

8. Modalités de passage de l’examen

Inscription	Via OpenCertif ou directement sur learn.microsoft.com
Centre d’examen	OpenCertif — Centre agréé Pearson VUE
Examen à distance	Mode OnVUE (surveillance en ligne, conditions strictes)
Pièce d’identité	2 pièces d’identité obligatoires le jour de l’examen
Aménagements	Demande possible (temps additionnel, assistance) sur Microsoft Learn
Résultat	Score communiqué immédiatement à la fin de l’examen
Renouvellement	Annuel, via évaluation gratuite en ligne sur Microsoft Learn
Politique de reprise	Délai d’attente de 24 heures pour la 1re reprise, puis 14 jours entre les tentatives suivantes (maximum 5 tentatives sur 12 mois)

9. Contact et inscription

Pour toute information complémentaire, demande de devis ou inscription à la formation préparatoire au SC-200, l'équipe OpenCertif reste à votre disposition.

OpenCertif
Centre de formation et de certification

app.opencertif.fr
lmsopencertif.fr

Centre agréé Certiport / Pearson VUE
Certifié Qualiopi — Actions de formation

10. Mentions légales et version

Ce syllabus est établi par OpenCertif sur la base du guide d'étude officiel Microsoft SC-200, dans sa version applicable (version du 16 avril 2026). Les compétences mesurées, les pondérations et les objectifs présentés reflètent fidèlement la structure de l'examen telle que publiée par Microsoft.

Version du syllabus : 2026.05 — Édition mai 2026
Source officielle : learn.microsoft.com/credentials/certifications/resources/study-guides/sc-200