

Microsoft Certified: Security Operations Analyst Associate

Domínios, pesos oficiales y habilidades clave del temario de SC-200, para repasar antes del examen.

Nivel: Intermediate (Associate) Duración: 100 min Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Manage a security operations environment

40–45%

Configure automation for Microsoft Defender XDR and Microsoft Sentinel

- En Configuración > Microsoft Defender XDR > Notificaciones por correo hay tres tipos de reglas: Incidentes (por gravedad de alerta, origen y grupo de dispositivos), Acciones (manuales o automáticas, completadas o fallidas) y Threat analytics (informes nuevos o actualizados por tipo o etiqueta). Se necesita el permiso Manage security settings o ser Security Administrator o superior.
- Las reglas de ajuste de alertas pueden ocultar (solo alertas de Defender for Endpoint), resolver o convertir en comportamientos las alertas esperadas, las integradas no afectan a AIR ni a los correos. La correlación agrupa alertas en incidentes y los fusiona salvo estado cerrado, propietarios o clasificaciones distintos; las reglas analíticas se incluyen o excluyen con #INC_CORR# o #DONT_CORR#.
- Las características avanzadas de Defender for Endpoint se activan en Configuración > Endpoints > Características avanzadas. Incluyen EDR en modo de bloqueo (actúa aunque el antivirus esté en modo pasivo), resolución automática de alertas, permitir o bloquear archivos, indicadores de red personalizados, protección contra manipulaciones, ocultar dispositivos duplicados y limitar la correlación a grupos de dispositivos.
- En Configuración > Endpoints > Reglas se administran los Indicadores (archivos, IP, URL y dominios, certificados), con acciones como permitir, auditar, advertir o bloquear, y las cargas de automatización y exclusiones de carpetas de la investigación automatizada. En conflictos de IP y URL gana Permitir sobre Advertir y Bloquear; un indicador de certificado de bloqueo prevalece sobre uno de hash que permite.
- La recopilación de datos personalizada amplía la telemetría predeterminada con reglas filtradas por tabla, acción y condiciones, no la sustituye. Los eventos se envían a un área de trabajo de Microsoft Sentinel y se consultan en tablas DeviceCustom*. Los dispositivos se seleccionan con etiquetas dinámicas de Asset Rule Management, no con etiquetas manuales.

Configure the Microsoft Sentinel SIEM and platform

- Microsoft Sentinel usa roles de Azure RBAC: Reader (ver), Responder (más gestionar incidentes), Contributor (más crear recursos e instalar soluciones), Playbook Operator (ejecutar playbooks) y Automation Contributor (para que Sentinel ejecute playbooks desde reglas). Se asigna mejor en el grupo de recursos; el data lake usa roles de Entra como Security operator.
- En Sentinel cada tabla vive en el nivel Analytics (retención de análisis, para reglas, búsqueda y libros; más retención total esperada al data lake) o solo en el nivel Data lake, más barato pero sin análisis en tiempo real. Los datos XDR están 30 días en búsqueda avanzada y se pueden ampliar. Se gestiona en Microsoft Sentinel > Configuration > Tables.
- Los libros de Sentinel se basan en Azure Monitor Workbooks y son recursos de Azure con RBAC. Se crean desde una plantilla instalada con una solución del Content hub (Save y luego edición) o desde cero con Add workbook, con origen de datos Logs y recurso Log Analytics. Se recomienda usar analizadores ASIM en las consultas, y para la optimización de SOE genera recomendaciones a medida de valor de datos (tablas poco usadas: activar reglas, cambiar o borrar libros hace falta el rol Workbook Contributor).
- El agente filtra en el origen, escribe en SecurityEvent y exige Azure Arc en los equipos que no son máquinas de Azure. Con WEF, los equipos reenvían eventos a un servidor Windows Event Collector mediante suscripciones push o pull, con cifrado Kerberos en dominio y una lista de acceso por suscripción. WEF es pasivo: la directiva de auditoría debe aplicarse aparte. Para Sentinel, el WEC ejecuta Azure Monitor Agent y los eventos van a la tabla WindowsEvent, con un demonio rsyslog o syslog-ng. Una DCR define facilities y niveles; Syslog va a la tabla Syslog y CEF a CommonSecurityLog. Hay que evitar duplicados con la misma facility y los reenviadores que no son de Azure.

Ingest data into the Microsoft Sentinel SIEM and platform

- El conector depende del origen: Windows Security Events via AMA lleva eventos de seguridad a SecurityEvent, Windows Forwarded Events (con un WEC) a WindowsEvent, Syslog y CEF via AMA (reenviador Linux) a Syslog y CommonSecurityLog y los servicios de Azure usan configuración de diagnóstico. Las máquinas que no son de Azure necesitan Azure Arc.
- El conector Windows Security Events via AMA crea reglas de recopilación de datos (DCR) que eligen los equipos y el conjunto de eventos: All, Common, Minimal o Custom con consultas XPath 1.0 con el formato Registro!Consulta.
- El agente filtra en el origen, escribe en SecurityEvent y exige Azure Arc en los equipos que no son máquinas de Azure.
- Con WEF, los equipos reenvían eventos a un servidor Windows Event Collector mediante suscripciones push o pull, con cifrado Kerberos en dominio y una lista de acceso por suscripción. WEF es pasivo: la directiva de auditoría debe aplicarse aparte. Para Sentinel, el WEC ejecuta Azure Monitor Agent y los eventos van a la tabla WindowsEvent, con un demonio rsyslog o syslog-ng. Una DCR define facilities y niveles; Syslog va a la tabla Syslog y CEF a CommonSecurityLog.
- El registro de actividad se recoge por defecto, pero para analizarlo en Sentinel hay que enviarlo con una configuración de diagnóstico a la tabla AzureActivity; los registros de recursos tampoco se recogen sin ella. Para hacerlo a escala se asigna una iniciativa de Azure Policy (rol Propietario en el ámbito) con una tarea de corrección para los recursos existentes.

Configure detections

- Una regla de detección personalizada se basa en una consulta de búsqueda avanzada que debe devolver columnas como Timestamp, ReportId y DeviceId para etiquetar bien las alertas. Defines frecuencia, entidades afectadas y acciones automáticas (dispositivo, archivo, usuario o correo). La frecuencia continua (NRT) solo admite consultas de una tabla y sin uniones.
- En Hunting > Custom detection rules ves cada regla con su última ejecución, el estado de esa ejecución, la de próxima ejecución y si está activada. Desde la página de detalles puedes ejecutarla al instante, editarla, modificar su consulta, desactivarla o eliminarla, y revisar las alertas y acciones que generó. Para editar una regla necesitas permisos sobre los dispositivos de su ámbito.
- Las reglas programadas ejecutan una consulta KQL a intervalos con un periodo de retrospectiva que no debe ser menor que el intervalo. Las reglas NRT se ejecutan cada minuto y consultan por hora de ingesta. Las plantillas de inteligencia de amenazas, Fusion y ML Behavior Analytics crean una sola regla con poca configuración, y las reglas de Microsoft security dejan de estar disponibles al incorporar Sentinel al portal de Defender.
- La página MITRE ATT&CK de Microsoft Analytics muestra por defecto la cobertura de las reglas programadas y NRT activas, y permite simular la cobertura posible con las detecciones disponibles sin configurar. Las técnicas se asignan a reglas, incidentes y consultas de búsqueda, y desde cada técnica puedes saltar a las consultas de búsqueda asociadas.
- Las reglas de anomalía de Sentinel usan aprendizaje automático para fijar una línea base y registran lo inusual en la tabla Anomalies, sin generar alertas propias. Las reglas integradas no se pueden editar: se duplican, se ajusta la copia en modo Flighting y, si funciona bien, se pasa a Production, momento en que la original pasa a Flighting.

2. Respond to security incidents

35–40%

Respond to alerts and incidents in Microsoft Defender XDR

- AIR de Defender for Office 365 Plan 2 investiga alertas como los envíos de usuarios y deja en cola acciones de corrección, como eliminar temporalmente correos o clústeres, para que SecOps las apruebe. En Threat Explorer puedes lanzar una investigación manual. La interrupción automática de ataques contiene usuarios y dispositivos a nivel de incidente y el equipo puede deshacer sus acciones.
- Con Data sharing activado en Insider Risk Management, las alertas de insider risk llegan a las colas de alertas e incidentes de Defender, agrupadas por usuario y correlacionadas con DLP o Entra ID. Verlas exige un rol de Defender y pertenecer a un grupo de roles de Insider Risk Management. En Purview se confirma la alerta y se crea un caso, o se descarta; la búsqueda avanzada usa AlertInfo, DataSecurityEvents y DataSecurityBehaviors.
- Las alertas de Defender for Cloud las generan los planes de protección de cargas de trabajo, se priorizan por gravedad y se correlacionan en incidentes. En Take action se encuentran los pasos de mitigación, las recomendaciones, la logic app y la regla de supresión; Workflow automation lanza logic apps automáticamente. En contenedores, el portal de Defender permite aislar, restringir o terminar pods.
- En Defender for Cloud Apps cada alerta de anomalía se clasifica como verdadero positivo, positivo benigno o falso positivo, y la guía indica la corrección recomendada, como suspender al usuario, restablecer la contraseña o confirmarlo como comprometido. Para aplicaciones OAuth de riesgo se filtra por nivel de permisos y uso en la comunidad, y se revoca o prohíbe la aplicación.
- Entra ID Protection distingue riesgo de usuario y riesgo de inicio de sesión. La primera opción es la autocorrección con directivas de acceso condicional (MFA o cambio seguro de contraseña); si no es posible, el administrador restablece la contraseña, bloquea al usuario o revoca sesiones. Tras investigar se marca el riesgo como comprometido, seguro o descartado; descartar no cambia la contraseña.

Respond to alerts and incidents in Microsoft Defender for Endpoint

- La escala de tiempo de un dispositivo muestra en orden cronológico los eventos y las alertas observados en él. Puedes filtrar por fechas, marcar eventos, ver el árbol de procesos y las técnicas MITRE ATT&CK, y lanzar Hunt for related events para consultar eventos cercanos en el mismo punto de conexión. Los eventos de firewall requieren habilitar la auditoría de Windows.
- Desde la página del dispositivo puedes aislarlo conservando su conexión con Defender for Endpoint, restringir la ejecución de aplicaciones, ejecutar un análisis antivirus o recopilar un paquete de investigación en formato zip. La respuesta en vivo ofrece una consola remota con comandos básicos y avanzados, y los scripts deben cargarse antes en la biblioteca para ejecutarse con run.
- Defender for Endpoint ofrece páginas de entidad para archivos, direcciones IP, URL y dominios, y cuentas de usuario, que muestran alertas relacionadas y los dispositivos de la organización implicados. Desde un archivo puedes lanzar un análisis profundo, detenerlo y ponerlo en cuarentena o crear un indicador de bloqueo. La búsqueda de IP y URL solo devuelve entidades observadas en dispositivos de la organización.
- La interrupción automática de ataques correlaciona señales de varios productos y, con alta confianza, contiene dispositivos, IP y usuarios para frenar el movimiento lateral. El incidente muestra la etiqueta Attack Disruption y el estado de los activos. Tras investigar, liberas los activos desde el incidente o el Centro de acciones, y puedes seguir los resultados en búsqueda avanzada.

Investigate Microsoft 365 activities to identify threats

- Microsoft Purview Audit registra en un registro unificado las operaciones de usuarios y administradores. Para buscar necesitas el rol Audit Logs o View-Only Audit Logs, y puedes filtrar por actividades, usuarios o archivos y exportar a CSV. MailItemsAccessed ayuda a acotar el alcance de un buzón comprometido, y las directivas de retención amplían la conservación de los registros.
- La búsqueda de contenido de eDiscovery en Microsoft Purview consulta buzones de Exchange Online, sitios de SharePoint, OneDrive, Teams, grupos de Microsoft 365 y Viva Engage en una sola búsqueda, con palabras clave, KeyQL y condiciones. Las vistas Statistics y Sample ayudan a afinar la consulta antes de exportar, y eliminar mensajes exige el rol Search And Purge, distinto del de búsqueda.
- Los registros de actividad de Microsoft Graph son un rastro de auditoría de todas las solicitudes HTTP que recibe Graph en el inquilino. Se activan con una configuración de diagnóstico hacia Log Analytics, almacenamiento o Event Hubs, se consultan en la tabla MicrosoftGraphActivityLogs y se correlacionan con los inicios de sesión mediante SignInActivityId y UniqueTokenIdentifier.

3. Perform threat hunting

20-25%

Detect threats by using Microsoft Defender XDR

- Elegir la tabla correcta del esquema de búsqueda avanzada depende del tipo de actividad: DeviceProcessEvents para procesos, DeviceNetworkEvents para conexiones, EmailEvents para correo, UrlClickEvents para clics en enlaces, IdentityQueryEvents para consultas a Active Directory y CloudAppEvents para aplicaciones en la nube. Cada tabla depende del servicio de Defender que la alimenta.
- La búsqueda avanzada usa Kusto Query Language: una tabla seguida de operadores con barra vertical como where, summarize, join, project y top. Para consultas eficaces y duraderas, filtra pronto por tiempo, prefiere has a contains, identifica procesos por nombre de archivo y usa kind=inner cuando necesites todas las filas del lado izquierdo de un join.
- En la página de búsqueda avanzada puedes crear consultas con el modo guiado (generador visual) o con el modo avanzado (KQL). Guarda las consultas en My queries o Shared queries, usa gráficos con summarize y render, y conviértelas en reglas de detección personalizadas devolviendo Timestamp, ReportId y un identificador de entidad como DeviceId.
- Threat analytics reúne informes de inteligencia de Microsoft con datos de tu entorno: incidentes relacionados, activos afectados, alertas a lo largo del tiempo, exposición de los puntos de conexión y acciones recomendadas. Los informes se clasifican en Activity, Actor, Technique, Tool, Vulnerability y otros, e incluyen consultas de búsqueda que puedes ejecutar o convertir en detecciones.
- El hunting graph de la búsqueda avanzada de Defender representa entidades como nodos y aristas, y ofrece escenarios predefinidos (consultas ya preparadas) con filtros para trazar rutas de ataque. En un incidente, View blast radius muestra las rutas posibles desde un nodo hasta destinos críticos, acotadas a tu ámbito RBAC. Su utilidad crece cuantos más datos y activos críticos estén definidos.

Detect threats by using the Microsoft Sentinel platform

- Las consultas de hunting de Sentinel, integradas, de soluciones del Content hub o personalizadas, se ejecutan desde la pestaña Queries de Hunting y se asignan a tácticas y técnicas MITRE ATT&CK. Para monitorizarlas se usan los resultados y las columnas Results delta, los marcadores y las hunts; si una consulta aporta mucho valor, se convierte en regla de análisis. Los livestreams se sustituyen por trabajos KQL, reglas o playbooks.
- Los trabajos KQL ejecutan una consulta única o programada sobre datos del data lake y tablas federadas, y pueden promover los resultados a una tabla del nivel de análisis (sufijo _KQL_CL) o escribirlos en el data lake. Se crean desde el editor de consultas o la página Jobs; no admiten adx(), arg(), externaldata() ni ingestion_time(), y conviene compensar la latencia de ingesta.
- Las reglas de resumen agregan en segundo plano grandes volúmenes de datos de cualquier nivel de registros y guardan el resultado en una tabla personalizada (sufijo _CL) con el plan Analytics, lista para consultar rápido o para alimentar reglas de análisis. La consulta no debe llevar filtro de tiempo, el intervalo y el retraso del bin controlan cuándo se ejecuta cada agregación y LASummaryLogs permite vigilar los fallos.
- Los cuadernos de Jupyter, ejecutados en VS Code con la extensión de Sentinel sobre pools de Spark, leen tablas del data lake con MicrosoftSentinelProvider y permiten usar Python, datos externos y aprendizaje automático al cazar amenazas. El servidor MCP de Sentinel ofrece colecciones de herramientas (Data exploration, Triage, creación de agentes) accesibles desde clientes compatibles con una cuenta que tenga, como mínimo, el rol Security Reader.