



SC-200 Domain 1: The Security Operations Environment

SC-200 skills measured, domain 1 Manage a security operations environment (20-25 %), as of 2026 | Defender portal and unified SecOps, unified RBAC, device groups and automation levels, alert tuning, indicators, advanced features, Sentinel onboarding, data lake and retention, Security Copilot set-up

SC-200 Domain 1 Defender XDR Unified RBAC Sentinel

One portal, many signals

Unified security operations in the Defender portal

×1

Overview
One console, security.microsoft.com, where SOC analysts see incidents from Defender XDR products, Defender for Cloud and Microsoft Sentinel.

×10

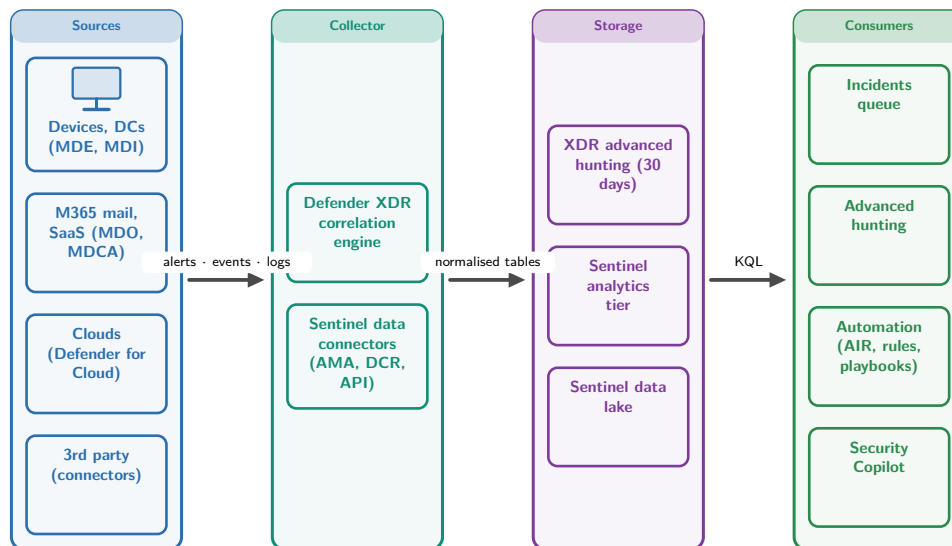
Close up
Sentinel is connected (onboarded) to the portal; its incidents, analytics rules, hunting and automation appear next to XDR features:

- one incident queue with correlation across Sentinel and XDR alerts
- advanced hunting queries both Sentinel workspace tables and XDR tables
- automatic attack disruption and Security Copilot work across both

×100

Under the microscope
Under the hood: Defender XDR keeps 30 days of advanced-hunting data; Sentinel keeps the analytics tier (90 days included, up to 2 years) and the data lake for long, cheap retention.

- onboarding needs Owner or User Access Administrator on the subscription plus Sentinel Contributor
- one primary workspace, others can be added
- Azure portal Sentinel experience is being retired (check the date)



Where each signal lands and where the analyst works

Access: unified RBAC and Entra roles

Category	Permissions inside	Give it to
Security operations	- security data basics (read alerts, incidents) - alerts management - response (isolate, AV scan) - live response basic / advanced - file collection - email quarantine and advanced actions	tier 1-2 analysts, responders
Security posture	- vulnerability management - exception and remediation handling - application handling - secure score	vulnerability and posture teams
Authorization and settings	- core security settings - detection tuning (custom detections, alert tuning) - system settings - role management	SOC engineers, platform admins

Defender XDR unified RBAC: a custom role = chosen permissions × data sources (MDE, MDO, MDI, MDCA, Defender for Cloud...)

Microsoft Entra role	In the Defender portal
Security Administrator	manage settings, policies, incidents across Defender products
Security Operator	manage alerts and incidents, run response actions; no policy changes
Security Reader / Global Reader	read-only investigation
Global Administrator	everything; avoid for daily SOC work (PIM)

EXAM TIP

Least-privilege SOC questions: 'tier 1 must manage incidents but not change policies' → **Security Operator** (or a unified RBAC role with security operations permissions only). 'Analyst must run advanced live-response scripts on servers only' → unified RBAC role with **live response advanced** scoped to the **server device group**. Remember to **activate** unified RBAC for each workload after creating roles.

☀ Defender for Endpoint tenant settings

Setting	Where / values	Why it matters
Device groups	rank-ordered rules (name, domain, OS, tag); first match wins; 'Un-grouped devices' last	scope analyst access and set automation per group
Automation level	Full; Semi (approval for any / core / non-temp folders); No auto-mated response	full = AIR remediates without waiting (recommended)
Advanced features	automated investigation, live response (+ for servers, + unsigned scripts), EDR in block mode, tamper protection, custom network indicators, web content filtering, device discovery	many exam answers are 'turn on the advanced feature first'
Indicators	file hash, IP, URL/domain, certificate; allow / audit / warn / block / block and remediate; up to 15,000 per tenant (as of 2026)	custom IP/URL indicators need network protection in block mode
Alert tuning	conditions on evidence (file, process, IP, device, user); action hide or resolve	removes known false positives without disabling the detection
Integrations	Intune (compliance by risk), Defender for Identity, Defender for Cloud Apps, Purview	share signals and block unsanctioned apps from the endpoint

Action	How
Settings -> Endpoints -> Device groups -> Add device group	name, automation level, membership rule (Tag Equals 'Servers-Prod'), user groups with access
Set-MpPreference -DisableRealtimeMonitoring \$true	is ignored (logged) when tamper protection is on: the expected exam answer to 'admin keeps disabling AV'
Settings -> Microsoft Defender XDR -> Alert tuning -> Add rule	hide or resolve alerts from a known benign tool
Settings -> Endpoints -> Indicators -> File hashes -> Add	block a SHA-256 across all or some device groups

📖 Sentinel and data retention for the SOC

- **Connect Sentinel to the Defender portal** Defender portal → System → Settings → Microsoft Sentinel → connect workspace; incidents then sync both ways and Sentinel rules appear under Analytics
- **Defender XDR connector in Sentinel** brings XDR incidents and alerts (free) and, optionally, raw advanced-hunting tables (billed) into the workspace
- **Analytics tier vs data lake** detections and fast hunting on the analytics tier; months or years of cheap history in the lake, queried with KQL jobs and notebooks

- **Search jobs and restore** search jobs scan long-term data asynchronously into a _SRCH table; restore re-hydrates a time range for interactive queries

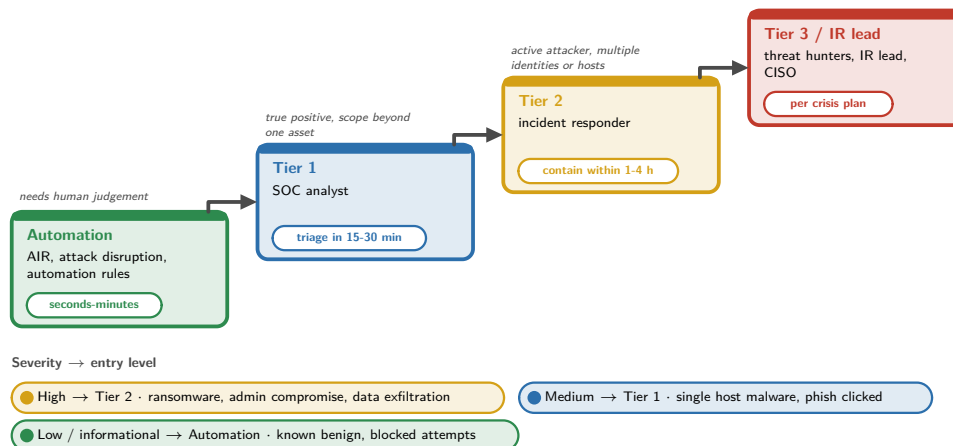
Quantity	Formula
Daily volume	$V = D \times s$
Retention gap	$G = t_{detect} - R_{XDR}$

where V = raw advanced-hunting data ingested per day (GB/day); D = number of onboarded devices (devices); s = average raw event volume per device per day (measure with the Usage table) (GB/device/day); G = days of evidence you would miss without extra retention (negative = covered) (days); t_{detect} = dwell time before the compromise is found (days); R_{XDR} = advanced-hunting retention in Defender XDR, 30 days (days)

Sizing raw XDR data streamed to Sentinel

📄 Worked example

$D = 2,000$ devices, $s = 0.03$ GB/day (30 MB) → $V = 2,000 \times 0.03 = \mathbf{60 \text{ GB/day}}$ if every DeviceEvents-type table is streamed: stream only the tables you hunt on (DeviceProcessEvents, DeviceNetworkEvents...) or send them to the data lake tier. A breach found after $t = 45$ days: $G = 45 - 30 = \mathbf{15 \text{ days}}$ of endpoint telemetry lost unless kept in Sentinel or the lake.



A typical SOC escalation model (targets are examples; set your own SLAs)

🔒 Security Copilot set-up

Capacity	provision security compute units (SCUs) per hour in Azure (or the Copilot portal), with optional overage; usage dashboard shows consumption per plugin and user
Experiences	standalone (securitycopilot.microsoft.com) and embedded: Defender incident summaries, guided response, script analysis, KQL from natural language, Entra, Intune, Purview
Access	Copilot owner / contributor roles in Copilot; data access still follows the user's own product permissions (on-behalf-of)
Plugins and prompt-books	Microsoft plugins on by default per product; custom plugins (KQL, API, GPT); promptbooks package repeatable investigations

🚩 Myths, recap and self-test

YOU MAY HEAR

"Security Reader can isolate a device"

BUSTED

✓ ACTUALLY

Response actions need security operations permissions

Security Operator or a unified RBAC role with response permissions.

YOU MAY HEAR

"Device groups are evaluated all at once"

BUSTED

✓ ACTUALLY

Rank order: a device joins the first matching group

Put narrow groups (servers, VIP) above broad ones.

YOU MAY HEAR

"Alert tuning deletes the detection"

BUSTED

✓ ACTUALLY

It hides or resolves matching alerts only

Detection still runs; review tuning rules regularly.

YOU MAY HEAR

"Advanced hunting keeps data for 180 days"

BUSTED

✓ ACTUALLY

Advanced hunting keeps 30 days; incidents are kept longer

Stream to Sentinel or the data lake for longer hunting.

Tick a box only when you could explain the point to someone else

☐ Unified RBAC: permissions × data sources, then activate per workload

☐ Device groups in rank order set access and automation level

☐ Tamper protection + EDR in block mode + full automation

☐ Onboard Sentinel to the Defender portal for one queue

☐ Plan retention: 30 days XDR, analytics tier, data lake

Q1 Which Entra role manages incidents but cannot change security policies?

A Security Operator.

Q2 Which automation level lets AIR remediate without approval?

A Full - remediate threats automatically.

Q3 A device matches two device-group rules. Which group wins?

A The higher-ranked group (lower rank number); first match.

Q4 An admin keeps disabling Defender AV with PowerShell. What stops it?

A Tamper protection.

Q5 Custom URL/IP indicators do not block. What is missing?

A Network protection in block mode (and custom network indicators advanced feature).

Q6 How long does Defender XDR advanced hunting keep data?

A 30 days.

Q7 Which feature hides recurring false-positive alerts from a known admin tool?

A Alert tuning (formerly suppression rules).

Q8 Where do you send raw XDR events to a third-party SIEM?

A Streaming API to Event Hubs (or a storage account).

Q9 What do you provision to use Security Copilot?

A Security compute units (SCUs).