SC-200 // EXAM REFERENCE GUIDE

Blueprint map, service boundaries, high-signal controls, response workflow, and exam tactics.

ASSESSMENT	PASS	DOMAINS
100 min	700+	3

01 // BLUEPRINT // EFFECTIVE 2026-07-28

Manage the environment	40-45%
Respond to incidents	35-40%
Perform threat hunting	20-25%

Biggest lever: configuration + ingestion + detection. Microsoft can test commonly used preview features. Verify the study guide for your exam date.

UNIFIED OPERATIONS // KNOW THE FLOW

SOURCE : CONNECT : DETECT : INCIDENT : RESPOND

Signals -> connector / AMA + DCR -> Sentinel tables / XDR schema -> analytics or custom detection -> correlated alert(s) -> incident -> automation rule -> playbook or analyst action.

SERVICE BOUNDARIES // PICK THE OWNER

DEFENDER XDR	Unified incidents, evidence, attack story, Action center, disruption.
MDE	Endpoint prevention, exposure, EDR, AIR, device actions, hunting.
SENTINEL	SIEM + SOAR: ingest, retain, detect, hunt, visualize, automate.
DEFENDER CLOUD	Multicloud workload posture and workload threat protection.
ENTRA ID	Risky users/sign-ins, identity protection, authentication signals.
PURVIEW	Audit, content search/eDiscovery, information and insider signals.

MDE VARIANTS // DO NOT CONFUSE THE PLAN

P1	NGAV + ASR + manual response + portal/Intune management.
P2	P1 + EDR + AIR + vulnerability management + threat analytics/deep analysis.
BUSINESS	Endpoint security for organizations up to 300 users; server coverage is separate.
SERVERS	Defender for Cloud P1/P2 workload plans; both integrate MDE P2. P2 adds agentless scanning and more.

02 // MANAGE THE ENVIRONMENT // 40-45%

AUTOMATION // DEFENDER XDR + SENTINEL

- Tune notifications, suppression, correlation, and alert rules before adding volume.
- Configure MDE advanced features, device groups, RBAC, automation levels, custom collection, ASR, and attack disruption.
- Automation rule = trigger/conditions/order + incident actions. Playbook = Azure Logic Apps workflow for enrichment or response.
- AIR investigates and proposes/takes remediation; review all pending/completed work in the unified Action center.

SENTINEL PLATFORM

- Assign least privilege. Reader views; Responder manages incidents; Contributor manages content/configuration.
- Know Analytics, Data lake, and XDR retention tiers; match cost, latency, and query pattern.
- Workbooks visualize; SOC optimization recommends coverage and operational improvements.

INGESTION // SOURCE -> TABLE

- Windows Security Events via AMA: DCR chooses event set/XPath and destination. WEF can aggregate events before collection.
- Syslog via AMA -> Syslog. CEF via AMA -> CommonSecurityLog. A Linux machine can act as a forwarder.
- Azure activity: Azure Policy and diagnostic settings. Also know service-to-service connectors, threat indicators, and custom tables.
- Validate connector health, data latency, expected volume, table schema, and retention before building a rule.

DETECTIONS // ENGINEERING CHECKLIST

- Defender custom detection: start from Advanced Hunting, use the correct schema, define frequency/scope, and attach response actions.
- Sentinel analytics: scheduled, NRT, threat-intelligence, and ML. Configure query, scheduling, threshold, entity mapping, tactics, and incident grouping.
- Coverage is not count: map detections to MITRE ATT&CK, tune false positives, test safely, and track gaps/anomalies.

RBAC + PLAYBOOK EXAM TRAPS

- Responder can access an incident but needs Playbook Operator to run a playbook manually.
- Sentinel Automation Contributor lets the Sentinel service run playbooks; Logic App roles create/edit the workflow.
- Contributor attaches playbooks to analytics/automation rules; Owner or User Access Administrator grants access.

03 // RESPOND TO INCIDENTS // 35-40%

VALIDATE | SCOPE | CONTAIN | REMEDIATE | CLOSE

INCIDENT TRIAGE // BUILD THE ATTACK STORY

- Confirm severity, status, owner, classification, affected assets, alerts, evidence, and chronology. Correlation turns multiple alerts into one attack story.
- Pivot across device, user, mailbox, app, IP, URL, file/hash, and cloud resource. Use Go hunt / Advanced Hunting to expand scope.
- Review automated investigation, attack disruption, and remediation state before duplicating or reversing an action.
- Document decisions with comments, tags, tasks, bookmarks, and closure classification/determination.

ENDPOINT RESPONSE // CHOOSE REVERSIBLE ACTIONS

- Device timeline/evidence first; then isolate device, run AV scan, collect investigation package, restrict code execution, contain, or start live response as authorized.
- Action center is the audit/review point for manual, AIR, and automatic attack-disruption remediation.
- For complex attacks, trace lateral movement and cross-domain stages before declaring containment complete.

OTHER INVESTIGATION SURFACES

- Defender for Office 365, Cloud Apps, Identity, Cloud workload protections, Entra ID, and Purview can each own evidence and remediation.
- Use agentic AI, including embedded Microsoft Security Copilot, to assist investigation while validating its evidence and actions.
- Microsoft 365 activity: Purview Audit, eDiscovery Content search, and Microsoft Graph activity logs.
- Sentinel case management: incident queue, entities, tasks, bookmarks, automation, and playbooks.

04 // THREAT HUNTING // 20-25%

- Hypothesis -> choose schema/table -> bound UTC time -> filter behavior -> summarize/pivot -> validate -> preserve evidence -> operationalize.
- Defender: Advanced Hunting queries, threat analytics, hunting graphs/blast radius, and custom detections.
- Sentinel: hunting queries, bookmarks/sessions, Sentinel Graph, KQL jobs in Data lake, Summary rule tables, and notebooks including the Sentinel MCP Server.
- A good hunt states what would falsify the hypothesis and separates weak signals from confirmed compromise.

EXAM TACTICS // READ FOR THE CONTROL POINT

Underline the requested product, scope, trigger, permission, and desired state. Distinguish alert vs incident, automation rule vs playbook, prevention vs EDR, and query syntax vs table schema. Prefer the least-privileged, first-valid action.