

Guia de preparação SC-200

Tudo o que a prova cobra, organizado por domínio: conceitos-chave, comparações que confundem, pegadinhas reais, gatilhos do enunciado, questões comentadas e um plano para chegar pronto ao exame.

3 capítulos por domínio	**21** questões comentadas	**70%** nota de corte
6 provas completas no curso		

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso SC-200: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

Quando	O que fazer
Semana 1	Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame.
Semana 2	Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3.
Semana 3	Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação.
Semana 4	Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 70%).

Mapa do exame

Cada prova do curso tem 50 questões e 100 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Gerenciar um ambiente de operações de segurança	40-45%	18 conceitos · 14 pegadinhas
2. Realizar caça a ameaças	20-25%	18 conceitos · 14 pegadinhas
3. Responder a incidentes de segurança	35-40%	18 conceitos · 14 pegadinhas

Como ler os capítulos: os **tópicos-chave** são o que mais cai; a **tabela de memorização** separa o que a prova costuma confundir; os **alertas de prova** mostram as armadilhas das alternativas erradas; os **gatilhos** ligam palavras do enunciado à resposta; e o **checklist** diz se você está pronto para o domínio.

Estude um pouco todo dia, de graça

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

DIAGNÓSTICO

Você já sabe isso?

Responda às 9 questões sem consultar nada. As respostas, com a explicação e o capítulo para revisar, estão no fim do guia. Comece o estudo pelos capítulos em que errou.

D1 · Gerenciar um ambiente de operações de segurança

Um engenheiro da Fábrica de Tintas Arco vai criar com o Azure CLI uma tabela personalizada no workspace do Sentinel para eventos das catracas e informou o nome PortaoAcesso, sem sufixo, como faria no portal. O que ele precisa saber?

A. Tabelas personalizadas não podem ser criadas pelo Azure CLI, só pelo portal do Defender
B. O sufixo correto de tabelas personalizadas é _SRCH, adicionado pelo próprio Log Analytics
C. Fora do portal, inclua o sufixo _CL no nome, que deve casar com o stream do DCR
D. O nome da tabela é livre, pois o DCR acrescenta o sufixo _CL durante a ingestão

D2 · Gerenciar um ambiente de operações de segurança

Na Agropecuária Boi Gordo, uma regra de coleta de dados personalizada do Defender for Endpoint que captura todos os eventos de processo parou de enviar dados de alguns servidores no meio do dia e voltou a coletar no dia seguinte. O que provavelmente ocorreu e qual é a recomendação?

A. A tag dinâmica dos servidores expirou; recriar a marcação como tag manual pelo portal
B. O workspace do Sentinel atingiu uma cota; mudar a tabela de destino para a camada Data lake
C. A regra atingiu o limite de eventos por dispositivo em 24 horas; criar regras mais focadas
D. O sensor reiniciou após uma atualização; ativar o EDR in block mode nesses servidores

D3 · Gerenciar um ambiente de operações de segurança

Um centro de compartilhamento de informações do setor elétrico oferece indicadores de ameaça em um servidor TAXII 2.1. O analista da Energética Serra Alta vai configurar o conector Threat Intelligence - TAXII no Sentinel. Quais informações do provedor ele precisa obter?

A. O nome da tabela _CL e o endpoint de coleta de dados (DCE) do provedor
B. O ID do aplicativo do Microsoft Entra e o segredo do cliente do provedor
C. A chave primária e o ID do workspace do Log Analytics do provedor
D. A URL da API root e o ID da coleção (collection ID) do servidor TAXII

D4 · Realizar caça a ameaças

O analista da Cooperativa Sabor do Sul quer listar no Advanced hunting as mensagens que o zero-hour auto purge (ZAP) moveu depois da entrega por causa de phishing, além das remediações manuais feitas pela equipe. Qual tabela usar?

A. A tabela EmailPostDeliveryEvents
B. A tabela UrlClickEvents
C. A tabela IdentityDirectoryEvents
D. A tabela EmailAttachmentInfo

D5 · Realizar caça a ameaças

Investigando um incidente, o analista da Universidade Campo Largo quer saber se existe algum caminho que leve do notebook comprometido de um estagiário até a conta de um administrador de banco de dados. Qual cenário predefinido do hunting graph usar?

A. O cenário Paths between two entities
B. O cenário Critical identities with storage access
C. O cenário Entity relationship map
D. O cenário Choke points to SQL data stores

D6 · Realizar caça a ameaças

O caçador da Metalúrgica Aço Vivo quer, no hunting graph do Advanced hunting, ver as possíveis rotas que um invasor poderia percorrer pela rede até o servidor de banco de dados classificado como ativo crítico. Qual cenário predefinido usar?

A. O cenário External users with cloud resource access
B. O cenário Attack paths to critical asset
C. O cenário Entity relationship map
D. O cenário Potential data exfiltration by device

D7 · Responder a incidentes de segurança

A Rede de Lojas Brisa tem Microsoft Defender for Office 365 Plano 1. A analista quer investigar uma campanha de phishing e ver também as atividades pós-entrega das mensagens, além das visões Campaigns e URL clicks. O que ela vai encontrar e o que é preciso?

A. As duas ferramentas exigem o Plano 2, e o Plano 1 oferece apenas o relatório de status do fluxo de e-mail
B. Threat Explorer está incluído no Plano 1, desde que o log de auditoria do Microsoft 365 esteja ligado
C. Real-time detections mostra só detecções na entrega; as visões extras exigem o Threat Explorer, do Plano 2
D. Real-time detections já traz as visões Campaigns e URL clicks e a atividade pós-entrega no Plano 1 também

D8 · Responder a incidentes de segurança

A Seguradora Futuro Digital começou a usar clientes de IA que consultam dados do locatário pelo Microsoft MCP Server for Enterprise e quer monitorar essas requisições nos logs de atividade do Microsoft Graph, que já envia ao Log Analytics. Como identificar essas requisições?

A. Pela coluna RequestUri, que inclui /enterprise nas requisições ao MCP Server
B. Pela coluna Wids, que identifica o agente de IA responsável pela chamada
C. Pela coluna ClientAuthMethod, que recebe o valor 3 nas requisições feitas por IA
D. Pela tabela SigninLogs, que registra cada chamada feita pelos clientes de IA

D9 · Responder a incidentes de segurança

No grafo de um incidente da Distribuidora Vale Seco, o analista seleciona a entidade de um IP externo e quer ver todos os alertas de segurança que envolvem esse IP, inclusive de outros incidentes, sem montar a consulta manualmente. Qual opção do Go hunt usar?

A. A opção All User anomalies
B. A opção All Activity
C. A opção Link to incident
D. A opção Related Alerts

01

CAPÍTULO 1 · 40-45% DA PROVA

Gerenciar um ambiente de operações de segurança

Este é o domínio de maior peso, e eu preciso dominar a configuração do SOC: notificações e alert tuning no Defender XDR, recursos avançados, indicadores, regras ASR, grupos de dispositivos e níveis de automação do Defender for Endpoint, além de todo o lado Sentinel: conectores, retenção, regras de análise, regras de automação, playbooks, funções e otimização do SOC. A prova cobra o nome exato da configuração e onde ela fica (Advanced features, Email notifications, Alert tuning, Automated response, Asset rule management). Muitas alternativas parecem certas, mas são do produto errado ou da aba errada. Onde mais erro é em limites numéricos (150 alertas, 30 alertas NRT, 75.000 eventos, 14 dias, 12 horas), na ordem das regras de automação e na função mínima do Sentinel. Também cai muito o que muda quando o Sentinel vai para o portal do Defender.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Notificações por e-mail no Defender XDR

Em Settings > Microsoft Defender XDR > Email notifications há abas: Incidents (severidade, grupos de dispositivos, fontes e a opção de uma notificação por incidente), Threat analytics (relatórios por tipo ou tag; nome só com letras e números em inglês) e Actions (ações de resposta manuais ou automáticas, com status Completed ou Failed; ainda não cobre detecções personalizadas com ações). As notificações de Settings > Endpoints avisam alerta a alerta, respeitam RBAC e o escopo de todos os grupos é reservado ao Global Administrator; se o grupo excluído era o único de uma regra, a regra é excluída junto.

Alert tuning

Oculta ou resolve alertas de comportamento esperado. Hide alert vale só para o Defender for Endpoint (alerta oculto em AlertInfo/AlertEvidence); Resolve alert cria alerta e incidente já resolvidos; Set as behavior transforma o sinal em comportamento em BehaviorInfo/BehaviorEntities, sem alerta nem incidente, e não vale para Defender for Cloud e Defender for Office 365. Regras internas de tuning não se aplicam a detecções personalizadas nem a Custom TI. Regras de supressão do Defender for Endpoint ficam em Settings > Endpoints > Rules > Alert suppression, onde a edição libera alertas já suprimidos.

Recursos avançados do Defender for Endpoint

Enable live response, Enable live response for servers e Allow unsigned script execution in live response; EDR in block mode (bloqueia e remedeia com antivírus de terceiros e Defender em passivo); Automatically resolve alerts (não sobrescreve status manual); Allow or block file (exige Defender Antivirus ativo e proteção na nuvem); Custom network indicators; Restrict correlation to within scoped device groups (não recomendado salvo SOCs regionais); Share endpoint alerts with Microsoft Compliance Center (alertas ao Insider Risk Management).

Indicadores do Defender for Endpoint

Arquivos: Allow, Audit, Warn, Block execution e Block and remediate; IPs e URLs/domínios: Allow, Audit, Warn e Block execution; certificados: Allow e Block and remediate; limite de 15.000 por locatário. Indicador de domínio cobre subdomínios; caminho HTTPS só é verificado no Microsoft Edge; não há curingas nem faixas. Fora dos navegadores Microsoft, o bloqueio de rede exige proteção de rede em modo de bloqueio. Para bloquear um aplicativo inteiro, o preferido é WDAC ou AppLocker.

Regras de redução da superfície de ataque (ASR)

Exigem Defender Antivirus ativo como principal, proteção em tempo real e na nuvem; não funcionam em modo passivo (nem com EDR in block mode) e só existem no Windows. São distribuídas por ferramentas de gerenciamento, com a política de segurança de endpoint do Intune como recomendada. Em Audit, as detecções aparecem no evento 1122, em DeviceEvents e no relatório de regras ASR. Falsos positivos se resolvem com exclusões de arquivo ou pasta, não desligando a regra.

Proteção padrão e modo Warn das ASR

Regras de proteção padrão (drivers assinados vulneráveis, roubo de credenciais do LSASS e persistência via WMI) podem ir direto para Block; as demais passam por Audit. No Warn o usuário pode desbloquear por 24 horas; a partir da plataforma 4.18.26060 o Unblock exige aprovação de administrador. As regras do LSASS e de injeção de código por aplicativos do Office não suportam Warn.

Coleta de dados personalizada

Fica em Settings > Endpoints > Rules > Custom Data Collection, exige Defender for Endpoint Plano 2 e workspace do Sentinel conectado. O direcionamento é por todos os dispositivos ou por tags dinâmicas (Asset rule management); tags manuais não servem. Limite de 75.000 eventos por dispositivo por regra em 24 horas, por isso prefira regras focadas e piloto. Os eventos vão para tabelas DeviceCustom, com custo de ingestão.

Grupos de dispositivos e níveis de automação

Dispositivo que casa com várias regras entra só no grupo de rank mais alto. Ungrouped devices não pode ser excluído nem mudar de rank, mas aceita nível de remediação e grupos do Entra com acesso. Grupos do Entra precisam ter função RBAC do Defender for Endpoint antes de aparecerem em User access. O nível Full é o recomendado; Semi ainda permite a interrupção automática sem aprovação; No automated response exclui o grupo da contenção automática. Ativar o RBAC do Defender for Endpoint é irreversível e leitores perdem o acesso até receberem função.

Investigação e resposta automatizadas (AIR)

Desde 01/09/2026 a AIR do Defender for Endpoint deixou de ser experiência separada e não aceita disparo manual; a alternativa é varredura antivírus completa. A AIR do Defender for Office 365 continua: começa por alertas próprios (e-mail suspeito, ZAP, envios de usuários, cliques em URL) ou por Take action, exige log de auditoria ligado e não dispara se essas políticas forem desativadas ou trocadas por alertas personalizados.

Interrupção automática: configuração e exclusões

Exclusões ficam em Automated response: identidades (contas de serviço, emergência), IPs e, para dispositivos, o nível de automação do grupo; a Microsoft não recomenda excluir. Pré-requisitos por produto: Defender for Office 365 exige caixas no Exchange Online e auditoria de caixa (como MailItemsAccessed); Defender for Identity exige sensor no DC, auditoria e conta de ação com permissão (LocalSystem por padrão).

Action center

Reúne ações pendentes (Pending, aguardando aprovação) e concluídas (History, log de auditoria) sobre dispositivos, e-mail e identidades. A coluna Action source diferencia Manual device action, ações automáticas, Advanced hunting action, Explorer e Manual live response action. Em History é possível desfazer ações como Isolate device e Restrict code execution.

Regras de automação do Sentinel

Gatilhos: incidente criado, incidente atualizado e alerta criado (alertas de regras Scheduled e NRT). Regras do mesmo gatilho rodam em sequência pelo número de ordem e cada uma avalia o estado deixado pela anterior; as de criação rodam antes das de atualização. Executam ações sem playbook (status com motivo, tag, responsável, tarefas), aceitam data de expiração e, no gatilho de atualização, a condição Updated by evita laços. Só chamam playbooks do mesmo tipo de gatilho.

Playbooks

São fluxos do Azure Logic Apps, Consumption ou Standard; Standard roda em locatário único e aceita private endpoint e rede virtual. A autenticação recomendada do conector do Sentinel é identidade gerenciada. Playbook acinzentado na ação Run playbook indica que a conta de serviço do Sentinel precisa de Microsoft Sentinel Automation Contributor no grupo de recursos do playbook, concedida por quem é Owner ali.

Funções do Sentinel

Cumulativas: Reader vê dados, incidentes e workbooks; Responder gerencia incidentes; Contributor cria conteúdo e gerencia o Content hub. Playbook Operator executa playbooks manualmente; Logic App Contributor cria e edita; Workbook Contributor cria workbooks. Convidados precisam de Directory Reader no Entra para atribuir incidentes. Equipes fora do SOC usam RBAC de contexto de recurso. No data lake, valem funções do Entra: leitura com Security Reader ou Global Reader; jobs com Security Operator ou superior.

Retenção e camadas de dados

Dados de caça do Defender XDR ficam 30 dias no padrão XDR; estendendo a retenção de análise até 90 dias paga-se a ingestão e o armazenamento é gratuito. Na camada Analytics há retenção de análise (até dois anos) e total (espelho no Data lake, até 12 anos). Mudança na retenção de análise vale na hora; reduzir a total tem espera de 30 dias. O Data lake é barato e lento, sem caça e sem regras em tempo real; mover a tabela para lá faz parar Advanced hunting, regras de análise e detecções personalizadas sobre ela. Alterar camada e retenção exige Data (manage).

Conectores e coleta via AMA

Serviços Microsoft usam conectores serviço a serviço (Microsoft Defender XDR). Windows Security Events via AMA grava em SecurityEvent, com conjuntos All events (Security e AppLocker), Common (trilha completa com volume menor), Minimal (sem 4634) e Custom (XPath 1.0, validado com Get-WinEvent -FilterXPath); servidores fora do Azure precisam de Azure Arc, e um DCR serve a várias assinaturas do mesmo locatário. WEF grava em WindowsEvent com o AMA só no coletor, e a recomendação é instalar parsers ASIM. Syslog e CEF via AMA usam encaminhador Linux, script de instalação e tabelas Syslog e CommonSecurityLog.

Ingestão personalizada e inteligência de ameaças

Tabelas personalizadas usam sufixo _CL e exigem TimeGenerated (o portal cria a transformação se faltar). A Logs Ingestion API exige registro de aplicativo com Monitoring Metrics Publisher no DCR e DCE quando há private link; a HTTP Data Collector API perdeu suporte em 14/09/2026. Inteligência: TAXII pede API root e collection ID; a upload API pede app do Entra e Microsoft Sentinel Contributor e substitui o conector TIP; o conector premium exige o SKU MDTI API Access; regras de ingestão valem só para conectores e Delete não afeta versões já ingeridas.

Regras de análise e detecções personalizadas

Regras agendadas: intervalo e lookback de 5 minutos a 14 dias, intervalo menor ou igual ao lookback, atraso de cinco minutos, limite de alerta avaliado por execução e supressão Stop running query after alert is generated. NRT: a cada minuto, até 50 regras, 30 alertas por execução e fontes com atraso menor que 12 horas. Detecções personalizadas: até 150 alertas por execução, lookback fixo para dados do Defender XDR (1 hora = 4 horas, 3 horas = 12 horas, diária = 30 dias) e a consulta deve retornar Timestamp e, em tabelas do Defender for Endpoint, DeviceId e ReportId (arg_max em consultas com summarize).

Macetes para memorizar

💡 Ações de alert tuning

HIDE = só endpoint; RESOLVE = nasce resolvido; BEHAVIOR = vira comportamento (nem Cloud nem Office).

💡 Limites de alertas

150 agendada, 150 detecção personalizada, 30 NRT; NRT: 1 minuto, 50 regras, 12 horas de atraso máximo.

💡 Lookback de detecção personalizada (Defender XDR)

Multiplique por 4: 1 hora olha 4 horas, 3 horas olha 12 horas; diária olha 30 dias.

💡 Escada de funções do Sentinel

Reader olha, Responder responde, Contributor constrói; Playbook Operator só aperta o play.

💡 Tags de correlação

INC = INClui; DONT = Don't (exclui).

💡 Retenção do Sentinel

XDR 30 dias, Analytics até 2 anos, lake até 12 anos; mexeu na total, 30 dias de arrependimento.

💡 Conjuntos do Windows Security Events

Minimal mínimo demais (sem logoff 4634); Common é o equilíbrio com trilha completa.

💡 Indicadores e ações

Block and remediate só para arquivo e certificado; certificado não tem Audit.

Tabela de memorização: não confunda

Quando é...	...e quando é
Hide alert Alerta do Defender for Endpoint que deve sumir da fila, mantido como alerta oculto em AlertInfo/AlertEvidence.	**Set as behavior** Tirar da fila e não gerar incidente, mantendo o sinal consultável como comportamento em BehaviorInfo/BehaviorEntities (não vale para Defender for Cloud e Defender for Office 365).
Regra de automação Agir sobre incidentes ou alertas do Sentinel: fechar com motivo, tag, comentário, data de expiração, chamar playbook.	**Alert tuning** Ocultar ou resolver alertas de comportamento esperado no Defender XDR, sem tags, comentários ou expiração.
Regra agendada Intervalo de 5 minutos a 14 dias, até 150 alertas por execução com Event grouping por evento.	**Regra NRT** Roda a cada minuto, até 30 alertas por execução, até 50 regras e só para fontes com atraso menor que 12 horas.
Camada Analytics Dados usados por regras, Advanced hunting, workbooks e detecções; retenção de análise até dois anos.	**Camada Data lake** Retenção longa (até 12 anos) e barata, consultas lentas por KQL jobs, notebooks e search jobs.
Microsoft Sentinel Responder Gerenciar incidentes (atribuir, mudar status) sem criar regras nem instalar soluções.	**Microsoft Sentinel Contributor** Criar e editar regras e conteúdo e gerenciar o Content hub.

Playbook Operator Usuário que executa playbooks manualmente sem criar ou editar.	**Automation Contributor** Conta de serviço do Sentinel, no grupo de recursos do playbook, para regras de automação chamarem playbooks.
Windows Security Events via AMA AMA em cada máquina e eventos na tabela SecurityEvent.	**Windows Forwarded Events** Estações já encaminham por WEF; AMA só no coletor e eventos na tabela WindowsEvent.

Números que caem

Item	Valor
Alertas por execução: regra agendada com um alerta por evento	**150 (o 150º resume o conjunto)**
Regras NRT	**A cada minuto, atraso de dois minutos, até 50 regras, até 30 alertas por execução, fontes com atraso menor que 12 horas**
Regras agendadas: intervalo e lookback	**5 minutos a 14 dias; atraso de cinco minutos**
Detecções personalizadas	**Até 150 alertas por execução; primeira execução verifica 30 dias**
Título dinâmico e detalhes personalizados	**Até três colunas por campo; até 20 pares e 4 KB**
Coleta de dados personalizada	**75.000 eventos por dispositivo por regra em 24 horas**
Indicadores do Defender for Endpoint	**15.000 por locatário**
Retenção de dados de caça do Defender XDR	**30 dias no padrão; armazenamento gratuito até 90 dias pagando a ingestão**
Retenção de análise / total	**Até dois anos / até 12 anos; redução da total com 30 dias de espera**
Otimização do SOC: Threat-based coverage	**High acima de 75%, Medium 30% a 74%, Low 0% a 29%; recálculo a cada 24 horas; Data ingested de 90 dias**
Status de conector gerenciado por Azure Policy	**Verde só com ingestão nos últimos 14 dias**
Regras de ingestão de inteligência de ameaças	**Até 15 minutos para agir**
XPath no DCR	**Até 20 expressões por caixa e até 100 caixas por regra; só XPath 1.0**
Auto refresh de workbooks	**De 5 minutos a 1 dia**
Unblock do modo Warn de ASR	**24 horas; exige aprovação de administrador a partir da plataforma 4.18.26060**
HTTP Data Collector API	**Sem suporte desde 14/09/2026**

AIR do Defender for Endpoint como experiência separada	**Deixou de existir em 01/09/2026, sem disparo manual (a AIR do Defender for Office 365 continua)**
RBAC unificado obrigatório	**Clientes novos desde 16/02/2025**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Usar Hide alert para um alerta do Defender for Office 365.
Como não cair: Hide alert só vale para o Defender for Endpoint; para Office 365 use Resolve alert.

⚠ **Alerta de prova:** Achar que uma regra interna de tuning cobre também o alerta de uma detecção personalizada.
Como não cair: Regras internas não se aplicam a detecções personalizadas nem a Custom TI; crie regra própria ou ajuste a consulta.

⚠ **Alerta de prova:** Configurar notificação de incidentes em Settings > Endpoints > Email notifications.
Como não cair: Essa é alerta a alerta do Defender for Endpoint; incidentes ficam na aba Incidents de Email notifications do Defender XDR.

⚠ **Alerta de prova:** Esperar 400 alertas de uma regra agendada com Trigger an alert for each event.
Como não cair: O limite é 150 por execução, com o 150º resumindo o conjunto; 30 (29 + 1) é das NRT.

⚠ **Alerta de prova:** Somar resultados de execuções seguidas para atingir o limite de alerta.
Como não cair: O threshold é avaliado em cada execução separadamente.

⚠ **Alerta de prova:** Definir intervalo maior que o lookback para economizar.
Como não cair: O intervalo precisa ser menor ou igual ao lookback, senão ficam lacunas.

⚠ **Alerta de prova:** Contra atraso de ingestão, só ampliar o lookback.
Como não cair: Isso duplica alertas; amplie TimeGenerated pelo atraso e limite ingestion_time() ao lookback original.

⚠ **Alerta de prova:** Achar que a regra 2 avalia a severidade original do incidente.
Como não cair: Regras de automação rodam em sequência e cada uma avalia o estado deixado pela anterior.

⚠ **Alerta de prova:** Colocar #DONT_CORR# nas outras regras para incluir só uma na correlação.
Como não cair: Com o padrão desligado, use #INC_CORR# na regra que deve entrar; #DONT_CORR# exclui quando o padrão está ligado.

⚠ **Alerta de prova:** Achar que alertas de um workspace secundário correlacionam com o Defender se tiverem #INC_CORR#.
Como não cair: Só o workspace primário correlaciona com o Defender XDR; secundários ficam em incidentes próprios.

⚠ **Alerta de prova:** Criar indicador de arquivo com Defender Antivirus em modo passivo e EDR in block mode.
Como não cair: Indicadores de arquivo exigem Defender Antivirus ativo, proteção na nuvem e Allow or block file ligado.

⚠ **Alerta de prova:** Escolher Warning como nível mínimo no portal para pular o nível Error do Syslog.
Como não cair: Nível mínimo coleta ele e todos os mais graves; filtros específicos exigem DCR criado por API.

⚠ **Alerta de prova:** Supor que reduzir a retenção total apaga os dados na hora.
Como não cair: Há 30 dias de espera antes da remoção; só a retenção de análise muda imediatamente.

⚠ **Alerta de prova:** Atribuir Microsoft Sentinel Contributor ao app da Logs Ingestion API.
Como não cair: Logs Ingestion API pede Monitoring Metrics Publisher no DCR; Sentinel Contributor é da upload API de inteligência.

Como cai na prova

📝 **Como cai:** Requisito de negócio com várias restrições (sem desativar regras, sem lembrar de desfazer, com tag e comentário).
Como resolver: Liste cada restrição e elimine opções que falham em uma: alert tuning não tem tag nem expiração, desativar regra é proibido, playbook dá mais esforço. Sobra regra de automação com data de expiração.

📝 **Como cai:** Função de menor privilégio para uma tarefa do Sentinel ou do Defender.
Como resolver: Identifique o verbo (ver, gerenciar incidente, executar playbook, criar workbook, instalar solução) e escolha a função exata; Contributor e Owner atendem, mas são excesso de privilégio.

📝 **Como cai:** Cálculo com limites: quantos alertas, que lookback, o que acontece com dados entre 90 e 180 dias.
Como resolver: Aplique o número documentado sem interpretação criativa: 150 com resumo no último, threshold por execução, retenção de análise imediata x total com 30 dias.

📝 **Como cai:** Qual conector e qual tabela para uma fonte (firewall CEF, WEF, servidores físicos, log de atividade do Azure).
Como resolver: Mapeie fonte, conector e tabela: CEF via AMA = CommonSecurityLog; Syslog = Syslog; WEF = WindowsEvent; Security Events via AMA = SecurityEvent; físico precisa de Azure Arc; Azure Activity = AzureActivity via diagnóstico.

📝 **Como cai:** O que muda com o Sentinel no portal do Defender.
Como resolver: Fila unificada, criação e correlação de incidentes pelo Defender XDR, regras Microsoft security e Fusion fora, agendadas e NRT continuam, workspace primário correlaciona, secundários não.

📝 **Como cai:** Por que uma configuração de endpoint não funciona (ASR, indicador, live response).
Como resolver: Confira pré-requisitos: Defender Antivirus ativo (não passivo), proteção na nuvem, recurso avançado ligado, plataforma Windows e permissão RBAC.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Uma notificação por incidente, sem e-mail a cada alerta	**Aba Incidents de Email notifications com a opção de uma notificação por incidente**
Aviso quando ação automática falhar	**Aba Actions de Email notifications, status Failed**
Antivírus de terceiros, mas quer bloquear artefatos detectados pelo EDR	**EDR in block mode**
Indicador de domínio não bloqueia no Chrome	**Custom network indicators + proteção de rede em modo de bloqueio**
Coleta personalizada parou no meio do dia e voltou no dia seguinte	**Limite de 75.000 eventos por dispositivo por regra em 24 horas**
SOCs regionais não conseguem agir em incidentes com dispositivos de várias regiões	**Restrict correlation to within scoped device groups**
Teste de intrusão com período definido, fechar incidentes sozinho	**Regra de automação com condição, tag, fechamento e data de expiração**
Regras de automação disparando umas às outras	**Condição Updated by diferente de Automation rule**

Playbook acinzentado em Run playbook	**Microsoft Sentinel Automation Contributor para a conta de serviço no grupo de recursos do playbook**
Playbook precisa acessar API atrás de private endpoint	**Logic Apps Standard**
Regra gera alerta a cada execução durante horas sobre o mesmo evento	**Stop running query after alert is generated (supressão da regra)**
Regras Microsoft security e Fusion desabilitadas após ir para o portal do Defender	**Defender XDR passa a criar e correlacionar incidentes**
Consultas independentes do fabricante de firewall ou VPN	**Parsers ASIM**
Nenhum alerta das regras de anomalia	**Tabela Anomalies: regras de anomalia não geram alertas próprios**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Regras de automação: mesmo gatilho em sequência pela ordem, estado atual; gatilho de alerta só chama playbook de alerta.
- Com o Sentinel no portal do Defender, quem cria e correlaciona incidentes é o Defender XDR; regras Microsoft security e Fusion deixam de ser usadas.
- Regras ASR exigem Defender Antivirus ativo, tempo real e nuvem, e só valem para Windows.
- Mover uma tabela da camada Analytics para o Data lake faz parar Advanced hunting, regras de análise e detecções personalizadas sobre ela.
- Dispositivo entra só no grupo de maior rank; o nível No automated response tira o grupo da contenção automática.

Essenciais para a prova (checklist)

☐ Sei qual aba de Email notifications usar para incidentes, relatórios de Threat analytics e ações de resposta.

☐ Sei as três ações de alert tuning e a quais produtos cada uma se aplica.

☐ Sei os recursos avançados do Defender for Endpoint e o que cada um habilita.

☐ Sei as combinações de tipo de indicador e ação e os requisitos de indicadores de arquivo e de rede.

☐ Sei os requisitos, o ciclo Audit/Block/Warn e as regras de proteção padrão das ASR.

☐ Sei configurar grupos de dispositivos, rank, nível de automação e exclusões da interrupção automática.

☐ Sei a ordem de execução, os gatilhos e a expiração das regras de automação do Sentinel.

☐ Sei escolher a função mínima do Sentinel e as permissões de playbooks.

☐ Sei os limites de regras agendadas, NRT e detecções personalizadas e como tratar atraso de ingestão.

☐ Sei o conector e a tabela de cada fonte (CEF, Syslog, WEF, Security Events, Azure Activity, Logs Ingestion API).

Questões de revisão do capítulo

R1.1 · Gerenciar um ambiente de operações de segurança

A equipe de inteligência da Cooperativa Financeira União recebe indicadores de um feed TAXII com muitos itens antigos e de baixa confiança. Ela quer descartar, antes da gravação no workspace, os indicadores sem atualização há seis meses e com confiança baixa. Qual recurso usar e o que esperar dele?

A. Regras de automação com gatilho de alerta, que removem os indicadores antes da ingestão
B. Regras de ingestão com a ação Delete, que também apagam versões já ingeridas dos indicadores
C. Regras de supressão do Defender for Endpoint aplicadas aos indicadores do feed TAXII
D. Regras de ingestão com a ação Delete, válidas para conectores, com até 15 minutos para agir

R1.2 · Gerenciar um ambiente de operações de segurança

Em outubro de 2026, um analista da Gráfica Estrela Guia procura no portal do Defender a opção de disparar manualmente uma investigação automatizada (AIR) do Defender for Endpoint para um dispositivo suspeito, como fazia antes. O que a documentação atual orienta?

A. Encerrar o incidente e recriá-lo manualmente para que o Defender inicie uma nova investigação
B. Abrir uma solicitação de coleta de amostra no Action center, que inicia a investigação automatizada
C. Ativar o nível de automação Full no grupo do dispositivo, o que libera o botão de investigação manual
D. Executar uma varredura antivírus completa, já que a AIR de endpoint deixou de ser experiência separada

R1.3 · Gerenciar um ambiente de operações de segurança

Na Corretora Valor Real, o analista Diego tem a função Security Operator no Microsoft Entra ID, e o RBAC do Defender for Endpoint está ativado. Ele não consegue criar uma regra de detecção personalizada que consulta a tabela DeviceProcessEvents. O que falta a ele?

A. A função Security Reader no Microsoft Entra ID, somada à função atual
B. A permissão Manage Security Settings no RBAC do Defender for Endpoint
C. A função Microsoft Sentinel Playbook Operator no workspace do Sentinel
D. O recurso avançado Enable live response for servers ligado no locatário

R1.4 · Gerenciar um ambiente de operações de segurança

Na Transportadora Rio Claro, um alerta de baixa severidade do Microsoft Defender for Office 365 é gerado sempre que a equipe de mensageria envia lotes de teste já autorizados. O analista vai criar uma regra de alert tuning com condições que identificam só esses envios e quer que os alertas correspondentes não fiquem abertos na fila. Qual ação deve escolher na regra?

A. Classificar como falso positivo cada alerta, sem regra de tuning
B. Hide alert, que suprime o alerta e impede a criação do incidente
C. Set as behavior, que transforma o sinal em comportamento para a caça avançada
D. Resolve alert, que gera o alerta e o incidente já com o status resolvido

Respostas comentadas

R1.1. D) Regras de ingestão com a ação Delete, válidas para conectores, com até 15 minutos para agir

Por quê: Regras de ingestão de inteligência de ameaças valem só para conectores (não para a upload API nem para objetos criados manualmente), são aplicadas em ordem até uma ação Delete e permitem, por exemplo, descartar objetos antigos de baixa confiança ou estender a validade de IOCs confiáveis.

✗ A) Incorreta. Regras de automação agem sobre incidentes e alertas, não sobre a ingestão de inteligência de ameaças.
✗ B) Incorreta. A ação Delete não afeta versões anteriores já ingeridas do objeto.
✗ C) Incorreta. Regras de supressão do Defender for Endpoint tratam de alertas de endpoint, não de indicadores do Sentinel.

> **Dica de prova:** Filtrar indicadores de um feed antes de gravar: regras de ingestão (só para conectores).

R1.2. D) Executar uma varredura antivírus completa, já que a AIR de endpoint deixou de ser experiência separada

Por quê: Mudança de 01/09/2026: a investigação e resposta automatizadas do Defender for Endpoint deixaram de ser uma experiência separada e de aceitar disparo manual, porque suas capacidades rodam automaticamente na pilha do antivírus. A AIR do Defender for Office 365 continua disponível.

✗ A) Incorreta. Recriar o incidente não dispara AIR de endpoint e ainda faria a equipe perder o histórico da investigação.
✗ B) Incorreta. A coleta de amostra (Request sample) obtém o arquivo para análise; não inicia investigação automatizada.
✗ C) Incorreta. O nível de automação não traz de volta o disparo manual da AIR de endpoint, que foi descontinuado como experiência separada.

> **Dica de prova:** Investigação sob demanda em endpoint, após setembro de 2026: varredura antivírus completa.

R1.3. B) A permissão Manage Security Settings no RBAC do Defender for Endpoint

Por quê: Gerenciar detecções personalizadas exige permissões sobre os dados consultados: Security settings (manage), Security Administrator ou Security Operator (com Manage Security Settings se o RBAC do Defender for Endpoint estiver ativo). Para dados do Sentinel, Microsoft Sentinel Contributor. Tabelas como IdentityLogonEvents exigem permissões nos dois produtos que as alimentam.

✗ A) Incorreta. Security Reader dá apenas leitura e não acrescenta permissão de gerenciamento.

✗ C) Incorreta. Playbook Operator executa playbooks do Sentinel; não concede gerenciamento de detecções sobre dados do Defender.

✗ D) Incorreta. Live response não tem relação com a criação de detecções personalizadas.

> **Dica de prova:** Security Operator + RBAC do Defender for Endpoint ativo: falta Manage Security Settings.

R1.4. D) Resolve alert, que gera o alerta e o incidente já com o status resolvido

Por quê: Alert tuning (antes chamado de alert suppression) oculta ou resolve alertas quando as condições de um comportamento esperado são atendidas. Hide alert vale só para o Defender for Endpoint; Resolve alert cria o alerta já resolvido; Set as behavior não vale para Defender for Cloud e Defender for Office 365.

✗ A) Incorreta. Classificar alerta por alerta é trabalho manual repetitivo; a classificação ajuda a melhorar a qualidade da detecção, mas não impede que novos alertas cheguem abertos à fila.

✗ B) Incorreta. A ação Hide alert só se aplica a alertas do Defender for Endpoint; não atende a um alerta do Defender for Office 365.

✗ C) Incorreta. Set as behavior não é suportada para alertas do Defender for Cloud nem do Defender for Office 365.

> **Dica de prova:** Alerta esperado fora do Defender for Endpoint: Resolve alert; Hide alert é exclusivo de endpoint.

02

CAPÍTULO 2 · 20-25% DA PROVA

Realizar caça a ameaças

Aqui eu preciso escolher a tabela certa do Advanced hunting, escrever KQL eficiente e conhecer as ferramentas de caça do Sentinel: página Hunting, hunts, KQL jobs, summary rules, notebooks, grafos e o servidor MCP. A prova mostra consultas e pede a correta, então tenho de enxergar detalhes como has x contains, join innerunique, dcount x count, arg_max e janelas de tempo. Muitas questões são só de tabela: e-mail, identidade, dispositivo, nuvem e vulnerabilidade, e o distrator é sempre uma tabela vizinha. O Threat analytics cai pelas abas, tipos de relatório e permissões. Onde mais erro é nos limites (30 dias, 100.000 linhas, 10 minutos, 500.000 linhas no lake) e nos nomes dos cenários do hunting graph.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Cotas do Advanced hunting

Consulta 30 dias de dados nativos do Defender XDR (dados do Sentinel conforme a retenção de análise), até 100.000 linhas, 64 MB de resultado e 10 minutos de execução, limite não configurável pelo usuário; a CPU é medida em ciclos de 15 minutos. Filtros de tempo são avaliados em UTC e o portal só converte a exibição. Há modo guiado (construtor de consultas) e modo avançado (KQL).

Tabelas de e-mail

Todas exigem Defender for Office 365: EmailEvents (entrega, remetente, destinatário, assunto), EmailAttachmentInfo (anexos), EmailUrlInfo (URLs), EmailPostDeliveryEvents (ações pós-entrega, como ZAP e remediação manual) e UrlClickEvents (cliques do Safe Links, com IsClickedThrough). Campanhas de phishing se caçam unindo EmailEvents e UrlClickEvents pelo NetworkMessageId.

Tabelas de identidade

IdentityDirectoryEvents (eventos no DC, como adições a grupos sensíveis), IdentityLogonEvents (autenticações no AD e em serviços online), IdentityQueryEvents (consultas LDAP e DNS a objetos do AD, típicas de reconhecimento) e IdentityInfo vêm principalmente do Defender for Identity. Entradas na nuvem com risco e status de acesso condicional ficam em EntraIdSignInEvents; entidades de serviço e identidades gerenciadas em EntraIdSpnSignInEvents.

Tabelas de dispositivo

DeviceProcessEvents (criação de processos), DeviceNetworkEvents (conexões), DeviceRegistryEvents (persistência em chaves Run), DeviceImageLoadEvents (carregamento de DLL, sideloading), DeviceFileEvents (arquivos), DeviceLogonEvents (logons), DeviceEvents (eventos diversos, como detecções de antivírus e ASR) e DeviceFileCertificateInfo (certificados). As colunas InitiatingProcess* mostram quem originou a ação.

Tabelas de alertas, nuvem e vulnerabilidades

AlertInfo traz título, categoria e severidade; AlertEvidence traz as entidades e seus papéis, unidas por AlertId. CloudAppEvents cobre atividades em apps de nuvem (Microsoft 365 e conectados ao Defender for Cloud Apps), com IsAnonymousProxy e UncommonForUser. CloudAuditEvents é o plano de controle (ARM, Kubernetes) e CloudProcessEvents os processos em cargas de nuvem. DeviceTvmSoftwareVulnerabilities lista CVEs por dispositivo.

Operadores de string do KQL

has procura o termo inteiro pelo índice e é mais rápido; contains acha trechos dentro de palavras e varre os valores. Ambos ignoram maiúsculas (versões sensíveis: has_cs, contains_cs). has_any aceita qualquer termo da lista, has_all exige todos, in~ compara sem diferenciar maiúsculas. Termos de três caracteres ou menos não são indexados.

Parsing e dados dinâmicos

A boa prática é preferir parse e parse_json a extract() e matches regex. mv-expand gera uma linha por elemento de array ou property bag (comum em AdditionalFields). project-rename só renomeia colunas e project-away remove colunas.

Agregação e séries temporais

dcount conta valores distintos (ex.: IPs contatados) e count conta linhas. arg_max retorna a linha do valor máximo, preservando Timestamp e ReportId do evento mais recente; usar max separado mistura linhas. Para anomalias, crie a série com make-series (from, to, step) e aplique series_decompose_anomalies(), que separa tendência e sazonalidade.

Join no Advanced hunting

O padrão innerunique deduplica a tabela da esquerda pela chave; use kind=inner quando todas as linhas da esquerda importam. Deixe a tabela menor à esquerda, filtre o tempo nos dois lados e una por janelas de tempo, como where (LogonTime - EmailReceivedTime) between (0min .. 30min). Há dicas como hint.shufflekey e hint.strategy = broadcast.

Boas práticas de busca

Filtre cedo, projete só as colunas necessárias e procure em colunas específicas. Em vez de search em todo o esquema, use search in (tabelas); evite union * e find sem tabelas. Teste o tamanho com count antes de consultas grandes. PIDs são reciclados no Windows: identifique o processo por dispositivo, PID e horário de criação (ou ProcessUniqueId).

Take actions e consultas salvas

Nos resultados é possível agir em dispositivos (isolar, coletar pacote, varrer, restringir apps), identidades, arquivos e e-mails, conforme Response (manage). A quarentena de arquivo precisa de DeviceId e de uma coluna de hash SHA1 ou SHA256 (inclusive InitiatingProcess). A aba Queries tem Shared queries, My queries e Community queries; bookmarks não existem no Advanced hunting.

Threat analytics

Tipos de relatório: Activity, Actor, Core threat, Technique, Tool, Vulnerability e OSINT (prévia). Abas: Overview, Analyst report, Related incidents, Impacted assets (dispositivos, usuários e caixas com alertas), Endpoints exposure, Recommended actions (só o que o Secure Score acompanha) e Indicators (prévia, só locatários verificados). O painel destaca Latest, High-impact (mais alertas) e Highest exposure (gravidade das vulnerabilidades e dispositivos exploráveis). Defender for Endpoint Plano 1 não dá acesso.

Hunting graph e blast radius

O hunting graph renderiza cenários como grafos de nós e arestas mapeados a técnicas MITRE ATT&CK: Attack paths to critical asset, Paths between two entities, Entity relationship map, Choke points to SQL data stores, Access to key vaults, Access to Azure DevOps repositories, Paths to domain admins, entre outros. No incidente, o blast radius substitui a análise de attack path, usa o grafo do Sentinel data lake, depende de ativos críticos definidos e exige Exposure management (read).

Sentinel graph e grafos personalizados

O Sentinel graph modela ativos, identidades, atividades e inteligência como nós e arestas. Grafos personalizados são criados em notebook no VS Code, publicados por graph job e consultados com GQL (ex.: MATCH (x)-[y]->(z) RETURN * LIMIT 100) na página Graphs. Jobs sob demanda retêm o grafo por 30 dias; agendados reconstroem na frequência definida. Com Sentinel scope, só Security Reader, Security Operator, Security Admin ou Global Admin acessam os grafos.

Página Hunting e hunts do Sentinel

Consultas agrupadas por táticas MITRE; Results delta compara as últimas 24 horas com as 24 a 48 horas anteriores; favoritas rodam sempre que a página é aberta. Hunts (prévia) organizam uma caçada por hipótese, com status. Uma consulta que achou um padrão vira alerta pela criação de regra de análise. Bookmarks só podem ser criados no portal do Azure, e livestreams não estão mais disponíveis (use KQL jobs, regras de análise ou playbooks).

KQL jobs e consultas no data lake

Jobs únicos ou agendados (por minuto, hora, dia, semana ou mês) promovem resultados filtrados do lake para tabelas; tabelas novas na Analytics recebem o sufixo _KQL_CL e são criadas pela identidade gerenciada do data lake, que precisa de Log Analytics Contributor. O nome do job é único no locatário, com até 256 caracteres, sem # e -; início agendado ao menos 30 minutos após a criação e latência de até 15 minutos. A página KQL queries aceita workspace('nome').Tabela, faz union por padrão entre workspaces e limita a 500.000 linhas ou 64 MB e 8 minutos, com períodos de até 12 anos.

Summary rules

Agregam grandes volumes, inclusive de camadas de baixo custo, em tabelas personalizadas _CL com plano Analytics, atualizadas na frequência da regra; não geram alertas. Ficam em Microsoft Sentinel > Configuration > Summary rules e exigem Microsoft Sentinel Contributor; modelos vêm do Content hub. Exclusão é irreversível e o histórico de execuções depende do diagnóstico SummaryLogs. Exemplo típico: guardar por IP a primeira e a última vez visto.

Notebooks, MCP e Copilot na caça

Notebooks do data lake rodam Python e Spark no VS Code com a extensão Microsoft Sentinel, lendo tabelas com MicrosoftSentinelProvider; tabelas federadas aparecem em System tables > Federated tables. O servidor MCP do Sentinel é hospedado, tem as coleções Data exploration, Triage e Security Copilot agent creation, exige no mínimo Security Reader e é adicionado no VS Code por MCP: Add Server (HTTP). O assistente de consultas do Copilot gera KQL com See the logic behind the query.

Macetes para memorizar

💡 has x contains

HAS = palavra inteira pelo índice (rápido); CONTAINS = pedaço da palavra (lento). Na dúvida de desempenho, has.

💡 Limites de consulta

Advanced hunting 30-100k-10: 30 dias, 100.000 linhas, 10 minutos. Lake 500k-8: 500.000 linhas, 8 minutos, até 12 anos.

💡 Tabelas Identity*

Directory = mudou algo no DC; Logon = autenticou; Query = perguntou ao AD; Info = quem é a conta.

💡 Tabelas de e-mail

Events chegou, AttachmentInfo anexo, UrlInfo link, PostDelivery depois da entrega, UrlClick clicou.

💡 Hunting graph

Map = vizinhança da entidade; Paths between = A até B; Attack paths = até a joia da coroa; Choke points = gargalo mais cruzado.

💡 Sufixos de tabela

_CL tabela personalizada e summary rule; _KQL_CL tabela nova de KQL job; _SRCH resultado de search job.

Join

innerunique UNIfica a esquerda; inner mantém tudo.

Tabela de memorização: não confunda

Quando é...	...e quando é
has Procurar um termo inteiro usando o índice, com melhor desempenho.	**contains** Só quando realmente precisa achar um trecho dentro de uma palavra.
join padrão (innerunique) Basta uma linha da esquerda por chave.	**join kind=inner** Todas as linhas da esquerda importam (ex.: os 40 e-mails com o mesmo anexo).
KQL job Promover do lake para Analytics só as linhas e colunas necessárias, uma vez ou agendado (tabela _KQL_CL).	**Summary rule** Agregar continuamente grandes volumes em tabela _CL para relatórios e buscas rápidas.
Entity relationship map Ver todas as conexões diretas de uma entidade, de entrada e de saída.	**Paths between two entities** Saber se existe caminho entre uma origem e um destino específicos.
Attack paths to critical asset Rotas possíveis até um ativo crítico escolhido.	**Choke points to SQL data stores** Nós que mais aparecem nos caminhos até armazenamentos SQL, para priorizar controles.
Impacted assets Dispositivos, usuários e caixas com alertas ligados à ameaça.	**Endpoints exposure** Nível de exposição e implantação de atualizações de segurança contra a ameaça.
IdentityQueryEvents Consultas a objetos do AD (enumeração por LDAP, reconhecimento).	**IdentityDirectoryEvents** Eventos no controlador de domínio, como adição de contas a grupos sensíveis.

Números que caem

Item	Valor
Advanced hunting: dados nativos	**30 dias**
Advanced hunting: resultado e tempo	**Até 100.000 linhas, 64 MB e 10 minutos por consulta; CPU em ciclos de 15 minutos**
Consultas KQL no data lake	**500.000 linhas ou 64 MB, expiram após 8 minutos; período de até 12 anos; histórico de 30 dias**

Nome de KQL job	**Único no locatário, até 256 caracteres, sem # e -**
Agendamento de KQL job	**Início pelo menos 30 minutos após a criação; latência de até 15 minutos para dados novos no lake**
Grafo de graph job sob demanda	**Retido por 30 dias**
Results delta da página Hunting	**Últimas 24 horas x 24 a 48 horas anteriores**
Consulta GQL sugerida	**LIMIT 100 padrão**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que has_any exige todos os termos.
Como não cair: has_any aceita qualquer um; todos é has_all; começar com é startswith ou hasprefix.

⚠ **Alerta de prova:** Contar IPs com count() e agrupar só por PID.
Como não cair: Use dcount(RemoteIP) e agrupe por dispositivo, PID e horário de criação do processo, porque PIDs são reciclados.

⚠ **Alerta de prova:** Usar LocalPort 445 para caçar varredura SMB de saída.
Como não cair: LocalPort 445 indica conexões recebidas; varredura de saída usa RemotePort 445.

⚠ **Alerta de prova:** Aplicar max() separado para Timestamp e ReportId.
Como não cair: max separado mistura linhas; use arg_max para manter o evento mais recente inteiro.

⚠ **Alerta de prova:** Inverter as tabelas ou remover o filtro de tempo para corrigir join que mostra uma linha por chave.
Como não cair: A deduplicação vem do innerunique padrão; troque para kind=inner e mantenha filtros nos dois lados.

⚠ **Alerta de prova:** Escrever a consulta pensando no horário local do portal.
Como não cair: Consultas usam UTC; o portal só converte a exibição dos resultados.

⚠ **Alerta de prova:** Achar que dá para aumentar o tempo limite da consulta para 60 minutos.
Como não cair: O limite é de 10 minutos e não é configurável; limite as tabelas com search in.

⚠ **Alerta de prova:** Supor que favoritar uma consulta de caça gera alertas ou e-mails.
Como não cair: Favorita só roda ao abrir a página Hunting; alerta vem de regra de análise criada a partir da consulta.

⚠ **Alerta de prova:** Tentar criar bookmark no Advanced hunting ou usar livestream.
Como não cair: Bookmarks só no portal do Azure; livestreams não existem mais.

⚠ **Alerta de prova:** Dar nome de job com # ou - ou terminar em _KQL_CL.
Como não cair: Nome único no locatário, até 256 caracteres, sem # e -; o sufixo _KQL_CL é da tabela nova, não do job.

⚠ **Alerta de prova:** Atribuir função ao engenheiro quando o KQL job falha ao criar a tabela.
Como não cair: Quem cria a tabela é a identidade gerenciada do data lake, que precisa de Log Analytics Contributor.

⚠ **Alerta de prova:** Achar que a aba Indicators do Threat analytics depende do conector TAXII.
Como não cair: Ela exige locatário verificado e lista todos os IOCs da ameaça, inclusive expirados.

⚠ **Alerta de prova:** Achar que a aba Recommended actions traz todas as recomendações do relatório.
Como não cair: Ela lista só as mitigações acompanhadas pelo Secure Score; o Analyst report traz as demais.

⚠ **Alerta de prova:** Escrever consulta de grafo com sintaxe KQL ou SQL.
Como não cair: Grafos personalizados do Sentinel usam GQL: MATCH (x)-[y]->(z) RETURN * LIMIT 100.

Como cai na prova

📝 **Como cai:** Quatro consultas KQL parecidas, uma só segue a documentação.
Como resolver: Confira tabela, coluna de filtro (RemotePort x LocalPort), função de agregação (dcount x count, arg_max x max x arg_min) e chaves do summarize. Elimine a que agrupa por Timestamp e ReportId (perde a contagem) e a que usa take no lugar de filtro.

📝 **Como cai:** Qual tabela do Advanced hunting usar para um comportamento.
Como resolver: Traduza o comportamento em evento: processo criado, conexão, registro, DLL, e-mail entregue, pós-entrega, clique, consulta ao AD, mudança no DC, entrada na nuvem. Descarte a tabela vizinha do mesmo prefixo.

📝 **Como cai:** Consulta lenta ou com resultado errado e qual ajuste fazer.
Como resolver: Pense nas boas práticas: has em vez de contains, search in em vez de search geral, parse em vez de regex, kind=inner em join que deduplica, filtro de tempo nos dois lados.

📝 **Como cai:** Qual ferramenta do Sentinel para uma necessidade de caça (hipótese, persistir resultados, agregar volume, explorar com IA, grafo).
Como resolver: Hipótese = hunts; promover dados do lake = KQL job; agregar volume = summary rule; Python e Spark = notebook no VS Code; IA em linguagem natural = servidor MCP; relações = grafo com GQL.

📝 **Como cai:** Qual aba ou seção do Threat analytics responde a pergunta do gerente.
Como resolver: Ativos com alertas = Impacted assets; vulnerabilidades e patches = Endpoints exposure; mitigações = Recommended actions; IOCs = Indicators; texto dos especialistas = Analyst report.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Mensagens movidas pelo ZAP ou remediadas depois da entrega	**EmailPostDeliveryEvents**
Quem clicou no link mesmo após o aviso do Safe Links	**UrlClickEvents com IsClickedThrough**
Enumeração de usuários e grupos do AD por LDAP	**IdentityQueryEvents**
Entradas interativas e não interativas com risco e acesso condicional	**EntraIdSignInEvents**
Persistência na chave de registro Run	**DeviceRegistryEvents**
DLL carregada de pasta temporária (sideloading)	**DeviceImageLoadEvents**
Dispositivos com software afetado por uma CVE	**DeviceTvmSoftwareVulnerabilities**
Downloads em massa no SharePoint e regras de caixa de entrada com IP e país	**CloudAppEvents**
Entidades e papéis de cada alerta	**AlertInfo unida a AlertEvidence por AlertId**
Dias anômalos em série temporal	**make-series + series_decompose_anomalies()**
Coluna dinâmica com lista e quer uma linha por item	**mv-expand**
Logs só no Data lake e precisa de consulta rápida sobre parte deles	**KQL job promovendo para tabela _KQL_CL**

Em que dias um IP apareceu, além da retenção, em terabytes de logs	**Summary rule diária com primeira e última vez visto**
Incidentes da detecção aparecendo em Related incidents do relatório	**Vincular o campo Threat analytics report ao criar a regra**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- has é mais rápido que contains; termos de três caracteres ou menos não são indexados.
- O join padrão innerunique deduplica a esquerda; para manter todas as linhas use kind=inner.
- Consultas usam UTC; o tempo limite de 10 minutos não é configurável.
- Para detecção personalizada, a consulta deve devolver Timestamp e, em tabelas do Defender for Endpoint, DeviceId e ReportId, com arg_max quando houver summarize.
- Bookmarks só no portal do Azure; livestreams não existem mais; favoritos só rodam ao abrir a página Hunting.

Essenciais para a prova (checklist)

☐ Sei a tabela certa para e-mail, identidade, dispositivo, nuvem, alertas e vulnerabilidades.

☐ Sei a diferença entre has, contains, has_any, has_all e in~.

☐ Sei quando usar dcount, arg_max, mv-expand, parse e make-series com series_decompose_anomalies.

☐ Sei corrigir um join que deduplica e unir registros por janela de tempo.

☐ Sei os limites do Advanced hunting e das consultas no data lake.

☐ Sei as abas, os tipos de relatório e as permissões do Threat analytics.

☐ Sei escolher o cenário predefinido do hunting graph para cada pergunta.

☐ Sei criar KQL jobs e summary rules, com nomes, sufixos e permissões.

☐ Sei o fluxo de grafos personalizados (notebook, graph job, GQL) e os pré-requisitos do servidor MCP do Sentinel.

Questões de revisão do capítulo

R2.1 · Realizar caça a ameaças

Um caçador da Rede de Varejo Bom Lar costumava usar livestreams do Microsoft Sentinel para acompanhar continuamente uma consulta durante incidentes e receber avisos. Ao procurar o recurso hoje, não o encontra. O que a documentação indica?

A. Livestreams não estão mais disponíveis; usar KQL jobs, regras de análise ou playbooks
B. Livestreams passaram a se chamar summary rules, com as mesmas notificações por e-mail
C. Livestreams só aparecem depois de ligar o UEBA e a detecção de anomalias no workspace
D. Livestreams foram movidos para o Advanced hunting, na aba de consultas compartilhadas

R2.2 · Realizar caça a ameaças

Uma analista recém-chegada ao SOC da Cooperativa Grão Fino ainda não domina KQL, mas precisa montar consultas no Advanced hunting do portal do Defender sem escrever o código do zero. Qual recurso nativo do Advanced hunting atende?

A. O modo avançado, que converte texto livre em consultas KQL
B. Os bookmarks do Advanced hunting, com consultas prontas
C. O modo guiado (guided mode), com construtor de consultas
D. O livestream do Sentinel, que monta consultas sozinho

R2.3 · Realizar caça a ameaças

Um caçador da Rede de Lojas Mundo Tech quer usar o agente do GitHub Copilot no Visual Studio Code para explorar, em linguagem natural, tabelas do Sentinel data lake por meio do servidor MCP do Sentinel. Como adicionar a coleção de ferramentas de exploração de dados?

A. Criando uma regra de detecção personalizada que chame o servidor MCP a cada execução da regra
B. Configurando o servidor MCP como fonte de dados de um workbook do Sentinel no portal do Azure
C. Com MCP: Add Server, tipo HTTP, com a URL da coleção e autenticando com Security Reader
D. Instalando o conector MCP no Content hub do Sentinel e atribuindo a função Sentinel Responder

R2.4 · Realizar caça a ameaças

Um analista da Cooperativa Rio Verde, com o fuso de Brasília configurado no portal, escreve uma consulta no Advanced hunting filtrando eventos entre 9h e 10h, achando que é o horário local, e não encontra o que esperava. O que a documentação informa?

A. As consultas usam UTC, e o portal converte apenas a exibição dos resultados para o fuso
B. As consultas usam o fuso do portal, e os resultados são exibidos sempre em UTC
C. As consultas usam o fuso do dispositivo que gerou cada um dos eventos registrados
D. As consultas usam UTC só para tabelas do Sentinel e o fuso local para as do Defender

Respostas comentadas

R2.1. A) Livestreams não estão mais disponíveis; usar KQL jobs, regras de análise ou playbooks

Por quê: Durante um comprometimento, a documentação sugere usar KQL jobs para monitorar o comportamento do atacante e persistir resultados no data lake, analisando com Security Copilot, notebooks, Advanced hunting e consultas KQL, e notificar equipes por outros canais.

✗ B) Incorreta. Summary rules agregam dados; não substituem livestreams com notificações.

✗ C) Incorreta. UEBA e anomalias não reativam livestreams.

✗ D) Incorreta. O recurso não foi movido para o Advanced hunting.

> **Dica de prova:** Livestream do Sentinel: aposentado; use KQL jobs, regras de análise ou playbooks.

R2.2. C) O modo guiado (guided mode), com construtor de consultas

Por quê: O Advanced hunting consulta até 30 dias de dados brutos do Defender XDR (e dados do Sentinel conforme a retenção) e tem dois modos: guiado, com construtor de consultas, e avançado, com KQL. As mesmas consultas podem virar regras de detecção personalizadas.

✗ A) Incorreta. O modo avançado é para quem escreve KQL do zero; gerar KQL a partir de linguagem natural é recurso do Security Copilot.

✗ B) Incorreta. Bookmarks não estão disponíveis no Advanced hunting.

✗ D) Incorreta. Os livestreams do Sentinel não estão mais disponíveis.

> **Dica de prova:** Sem saber KQL no Advanced hunting: modo guiado.

R2.3. C) Com MCP: Add Server, tipo HTTP, com a URL da coleção e autenticando com Security Reader

Por quê: O servidor MCP do Sentinel é hospedado, não exige infraestrutura e usa o Microsoft Entra para identidade. As coleções (data exploration, criação de agentes do Security Copilot e triage) funcionam em clientes como VS Code, Security Copilot, Copilot Studio e Microsoft Foundry.

✗ A) Incorreta. Regras de detecção não são a forma de conectar clientes de IA ao servidor MCP.

✗ B) Incorreta. Workbooks não usam o servidor MCP como fonte de dados.

✗ D) Incorreta. As coleções do MCP do Sentinel são hospedadas e adicionadas no cliente, não instaladas pelo Content hub.

> **Dica de prova:** MCP do Sentinel no VS Code: MCP: Add Server (HTTP) + Security Reader.

R2.4. A) As consultas usam UTC, e o portal converte apenas a exibição dos resultados para o fuso

Por quê: Filtros como ago() e intervalos explícitos são avaliados em UTC. Para analisar um horário local, converta o intervalo para UTC (Brasília costuma estar três horas atrás) ou desloque o Timestamp na consulta.

✗ B) Incorreta. É o inverso: a consulta usa UTC e a exibição usa o fuso configurado.

✗ C) Incorreta. Os dados não são consultados pelo fuso de cada dispositivo.

✗ D) Incorreta. O uso de UTC vale para todos os dados do Advanced hunting.

> **Dica de prova:** Advanced hunting: escreva consultas em UTC.

03

CAPÍTULO 3 · 35-40% DA PROVA

Responder a incidentes de segurança

Aqui eu preciso saber trabalhar um incidente de ponta a ponta no portal do Defender: ler a história do ataque, conter dispositivos e identidades, remediar e-mail, investigar no Purview e documentar tudo em casos. A prova traz cenários de SOC e pede a ferramenta exata (grafo do incidente, Go hunt, Action center, live response, Threat Explorer, eDiscovery, Audit) e, muitas vezes, a permissão ou o plano de licença que libera a ação. Os distratores sempre trocam ferramentas vizinhas: Action center x linha do tempo, Threat analytics x grafo do incidente, Plano 1 x Plano 2, Search And Purge x Audit Logs. A interrupção automática de ataques e as capacidades do Security Copilot e dos agentes caem com frequência e em detalhes. Onde mais erro é em prazos e limites (60 a 90 minutos da auditoria, 180 dias, 1.000 dispositivos, 48 horas do ZAP, 60 dias do modo de teste) e em qual função concede cada ação.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Interrupção automática de ataques (attack disruption)

Contém ativos comprometidos durante um ataque ativo (ransomware, BEC, AiTM). O incidente ganha a tag Attack Disruption (que também aparece nos e-mails de notificação de incidentes), uma faixa amarela, o status dos ativos no grafo e um cartão de resumo com View activities e View related assets. Pela API, o título do incidente termina com (attack disruption). Toda ação pode ser desfeita pela própria equipe, no incidente ou no Action center, depois de investigar.

Ações de contenção da interrupção

Defender for Endpoint: Contain device, Contain IP (para IPs de dispositivos não descobertos ou não integrados), Isolate device e Contain user. Defender for Identity: Disable user. Entra ID: Revoke user session e Suspend user. Contain user aplica política nos dispositivos integrados para bloquear a comunicação a partir da identidade, reduzindo movimento lateral sem desabilitar a conta no AD. O isolamento automático (prévia) vale só para estações de trabalho gerenciadas pelo Defender for Endpoint e é desfeito após um prazo definido, podendo ser liberado antes.

Acompanhar a interrupção (Activities e Advanced hunting)

Na aba Activities do incidente, filtre Performed by = AttackDisruption e leia a coluna Policy status: Active (em vigor), Inactive (aplicada antes, mas não mais), Not applicable (ex.: ações de liberação) e No status. No Advanced hunting: DisruptionAndResponseEvents dá todas as ações da organização (filtre IncidentId para um incidente), DeviceEvents com ActionType ContainedDevice/ContainedUser mostra o que foi bloqueado e IdentityDirectoryEvents ajuda a achar contas desabilitadas pelos DCs.

Blindagem preditiva

Age antes de o ataque progredir, ao contrário da interrupção, que reage ao ataque ativo. Ações como Safeboot hardening (bloqueia adulteração por reinício em modo de segurança), GPO hardening (bloqueia abuso de Group Policy) e contenção proativa de usuários de alto risco aparecem na aba Activities. São automáticas, não manuais, e não são regras ASR nem acesso condicional.

Grafo da história do ataque e Go hunt

O grafo mostra como o ataque se espalhou, com reprodução no tempo, e permite agir nas entidades sem sair do incidente. Go hunt oferece See all available queries, All Activity (todas as atividades), Related Alerts (todos os alertas da entidade, inclusive de outros incidentes) e All User anomalies (só para usuários, exige UEBA do Sentinel). Resultados podem ser vinculados com Link to incident. A visão All associated incidents amplia o contexto sem mesclar nada.

Correlação e mescla de incidentes

O motor considera entidades, artefatos, janelas de tempo e sequências de ataques em vários estágios, inclusive entre produtos diferentes. Na mescla não nasce incidente novo: o conteúdo vai para o destino, a origem é fechada com a tag Redirected e as atividades ficam com a identidade Microsoft Defender XDR - alert correlation; o histórico da origem continua acessível no Sentinel do portal do Azure. Não há mescla com incidente fechado, responsáveis diferentes, classificações diferentes ou limite de entidades excedido; mesclar é preferível a mover alertas.

Gerenciamento de casos no Defender

Incident cases (prévia, experiência recomendada; a legada segue disponível) nascem de incidentes correlacionados; casos genéricos registram trabalho de SecOps fora de incidentes, com tarefas, anexos, objetos vinculados, campos personalizados, prazos e e-mail, e são criados com Alerts (manage). Tarefas de incident case exigem Response (manage) e têm notas de fechamento. A auditoria vai para a tabela SecurityCaseEvent no Log Analytics. Casos existem só no portal do Defender.

Políticas de SLA de casos

Definem início, término e pausa do timer, com durações por severidade, origem ou responsável. Estados: Active, At Risk, Breached, Paused, Completed (Met) e Completed (Breached). Se o caso passa a casar com outro timer, Carry on mantém o tempo decorrido e Reset recomeça. E-mails sobre mudanças de SLA saem de regra de automação com gatilho Case updated.

Ações de resposta em dispositivos e planos

Plano 1: Run antivirus scan, Isolate device, Stop and quarantine a file e indicador de arquivo. Plano 2: live response, pacote de investigação, Restrict app execution e demais. Restrict app execution deixa rodar só arquivos assinados pela Microsoft, sem cortar a rede (Windows 10 1709+, Windows 11, Server 2019+ com Defender Antivirus). A varredura remota funciona com o Defender em modo passivo, aceita rápida ou completa e limita a CPU a 50% sem ScanAvgCPULoadFactor.

Isolamento de dispositivo

Desconecta da rede mantendo a conexão com o serviço do Defender for Endpoint. O isolamento seletivo mantém Outlook e Teams (e exclusões de processos e destinos); VPN de túnel completo pode cortar o acesso ao Defender. Libera-se com Release from isolation. Contain device é diferente: aplica política nos outros dispositivos para bloquear a comunicação com o contido.

Live response e pacote de investigação

Comandos básicos: cd, dir, fileinfo, getfile, processes, registry, scheduledtasks. Avançados: analyze, run, library, putfile, remediate, undo. getfile traz arquivo do dispositivo, putfile leva da biblioteca ao dispositivo, run executa script da biblioteca, undo restaura entidade remediada e connections mostra as conexões ativas. O pacote de investigação do Windows traz Autoruns, programas instalados, conexões (cache DNS e ARP), Prefetch, processos, tarefas agendadas, log de segurança, serviços, sessões SMB, usuários e grupos; não traz RAM nem caixa de correio.

Ações em arquivos

Stop and quarantine file encerra processos, põe em quarentena e remove dados persistentes em dispositivos onde o arquivo foi visto nos últimos 30 dias, com limite de 1.000 dispositivos e tempo limite de três dias; para escala ou bloqueio permanente, use indicador. Deep analysis executa o arquivo em sandbox na nuvem e gera relatório. Download file entrega zip com senha e exige a permissão de coleta de arquivos. Observed in organization mostra até seis meses para dispositivos e 30 dias para apps de nuvem.

Linha do tempo do dispositivo

Mostra 30 dias por padrão; cada exportação cobre no máximo sete dias. Flags com o filtro Flagged events montam a cronologia limpa; linhas em negrito com ícone azul são técnicas MITRE ATT&CK; Hunt for related events abre o Advanced hunting com eventos próximos. Evento de modo crítico do MsSense.exe indica falta de recursos (lacuna de eventos). Eventos de firewall como 5025, 5031 e 5157 exigem a auditoria Filtering Platform Connection.

Threat Explorer e remediação de e-mail

Plano 1 tem Real-time detections (detecções na entrega); Plano 2 tem Threat Explorer, com atividade pós-entrega, Campaigns, URL clicks e remediação. A remediação é por aprovação direta (função Search and Purge) ou em duas etapas (Add to remediation, aprovada em Action center > Pending), e fica em History. Soft delete permite recuperação pelo usuário; Delete sender's copy só vale para remetente interno. A remediação gera o alerta Administrative action submitted by an Administrator. Ver e baixar mensagens exige a função Preview.

Zero-hour auto purge (ZAP) e AIR de e-mail

O ZAP age sobre mensagens entregues nas últimas 48 horas em caixas na nuvem: malware e high confidence phishing vão para quarentena (lidas ou não), phishing e spam seguem a política antispam, e os usuários não são avisados. Confira no Mailflow status e no Explorer filtrando Additional action. Na AIR do Defender for Office 365, a maioria das ações aguarda aprovação, mas clusters de similaridade maliciosos (URL e arquivo) são remediados com aprovação automática.

Purview Audit

Audit (Standard) retém 180 dias (era 90 antes de outubro de 2023); com E5 ou equivalente, Entra ID, Exchange, OneDrive e SharePoint ficam um ano, e políticas vão até um ano ou dez anos com complemento. Registros de entidades não humanas têm um ano fixo. Registros dos serviços principais surgem em 60 a 90 minutos. Pesquisar exige Audit Logs ou View-Only Audit Logs; extração programática usa a Office 365 Management Activity API. MailItemsAccessed: Sync registra a pasta (Outlook desktop), Bind registra a mensagem com InternetMessageId.

Pesquisa e expurgo do eDiscovery

Fluxo para incidentes como vazamento de dados: pesquisar exige eDiscovery Manager ou Compliance Search; expurgar com New-ComplianceSearchAction -Purge exige Search And Purge (ou Organization Management do Purview). Remove até 10 itens por caixa por vez, até 50.000 caixas por pesquisa, só em Exchange Online e pastas públicas (sites dão erro, Teams não sai, caixas em retenção de litígio não são suportadas). Em casos premium, use o Graph com até 100 itens por local. Com Defender for Office 365 Plano 2, prefira a remediação pelo Explorer.

Entra ID Protection e Defender for Identity

Risco de usuário: remediado por troca segura de senha (Remediated); risco de entrada: por MFA; o sistema pode dispensar (Dismissed, assessed sign-in safe). Menor privilégio: Security Operator dispensa risco, User Administrator redefine senha, Security Administrator edita políticas de risco. No Defender for Identity, High é o limiar padrão; Medium e Low alertam sem aprendizado; Recommended test mode dura até 60 dias; Revert to default é irreversível. Ações no AD (Disable, Enable, Force password change) são executadas pelo sensor do DC; na interrupção, a conta de ação é LocalSystem por padrão.

Macetes para memorizar

Live response

GET traz, PUT põe, RUN roda, UNDO desfaz.

Planos do Defender for Endpoint

Plano 1 = VISI: Varredura, Isolar, Stop and quarantine, Indicador. Tudo que é forense (live response, pacote) é Plano 2.

Prazos de Audit

60-90 minutos para aparecer, 180 dias sem E5, 1 ano com E5, 10 anos com complemento, 1 ano fixo para não humanos.

Permissões do Purview

Ler auditoria = Audit Logs; achar conteúdo = Compliance Search/eDiscovery Manager; apagar = Search And Purge; ver mensagem = Preview.

Estados de risco do ID Protection

Usuário resolveu = Remediated; sistema resolveu = Dismissed; admin decidiu = Confirmed compromised ou Confirmed safe.

Copilot por entidade

Quem é o usuário = identity summary; como está a máquina = device summary; o que faz o arquivo = file analysis; o que faz o script = script analysis; o que fazer agora = guided responses.

SLA de casos

Carry on carrega o tempo gasto; Reset reseta o relógio.

Tabela de memorização: não confunda

Quando é...	...e quando é
Real-time detections (Defender for Office 365 Plano 1) Basta ver detecções na entrega, com as visões Malware, Phish e Content malware.	**Threat Explorer (Plano 2)** Precisa de atividade pós-entrega, Campaigns, URL clicks, consultas salvas e ações de remediação.
Stop and quarantine file Conter rápido um arquivo visto nos últimos 30 dias em até 1.000 dispositivos.	**Indicador de arquivo (Block)** Bloquear em escala ou de forma permanente, inclusive em dispositivos desligados e em execuções futuras.
Isolate device Cortar a rede do dispositivo, mantendo contato com o Defender (seletivo libera Outlook e Teams).	**Restrict app execution** Impedir novas execuções sem desconectar da rede: só roda o que é assinado pela Microsoft.
getfile Trazer um arquivo suspeito do dispositivo para análise (comando básico).	**putfile** Levar um arquivo da biblioteca para o dispositivo (comando avançado); para executar script da biblioteca use run.

Remediação de e-mail no Threat Explorer Phishing entregue com Defender for Office 365 Plano 2, com aprovação e rastreio no Action center.	**Pesquisa e expurgo do eDiscovery** Vazamento de dados sem Plano 2, com limite de 10 itens por caixa (100 por local em caso premium via Graph).
Audit Logs / View-Only Audit Logs Pesquisar o log de auditoria unificado do Purview.	**Search And Purge / Compliance Search** Compliance Search cria a pesquisa de conteúdo; Search And Purge expurga mensagens.
Risco de entrada (MFA) A entrada arriscada é remediada quando o usuário completa MFA.	**Risco de usuário (troca segura de senha)** O usuário de risco exige troca segura de senha; em híbridos, a troca local só vale com PHS e Allow on-premises password change to reset user risk.

Números que caem

Item	Valor
Stop and quarantine file: limite de dispositivos	**1.000 dispositivos, tempo limite de três dias, arquivos vistos nos últimos 30 dias**
Recommended test mode do Defender for Identity	**Até 60 dias, com data de término obrigatória**
Registros de auditoria dos serviços principais	**Surgem em 60 a 90 minutos**
Retenção do Audit (Standard)	**180 dias (90 antes de outubro de 2023)**
Retenção com E5 (Entra ID, Exchange, OneDrive, SharePoint)	**Um ano por padrão; políticas até um ano ou dez anos com complemento**
Trabalhos de pesquisa de auditoria	**Disponíveis por 30 dias, até 10 simultâneos por usuário**
Expurgo do eDiscovery	**10 itens por caixa por vez, até 50.000 caixas por pesquisa; 100 itens por local em caso premium via Graph**
ZAP	**Mensagens entregues nas últimas 48 horas**
Sincronização Defender x Insider Risk Management	**Até 30 minutos**
Alertas do Defender for Cloud	**Visíveis por 90 dias, mesmo com o recurso excluído**
Observed in organization (página do arquivo)	**Até seis meses para dispositivos e 30 dias para apps de nuvem**
Linha do tempo do dispositivo	**30 dias por padrão; exportação de até sete dias por vez**
Aprendizado da detecção de país pouco frequente (Defender for Cloud Apps)	**Sete dias**
Varredura antivírus remota sem ScanAvgCPULoadFactor	**CPU limitada a 50%**

Sentinel no portal do Azure	**Sem suporte depois de 31/03/2027**
File policies do Defender for Cloud Apps	**Aposentadas em 06/01/2027 (migrar para DLP ou rotulagem automática do Purview)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que o Plano 1 do Defender for Endpoint inclui live response ou pacote de investigação.
Como não cair: Plano 1 tem Run antivirus scan, Isolate device, Stop and quarantine a file e indicador de arquivo; live response, pacote de investigação e Restrict app execution exigem Plano 2.

⚠ **Alerta de prova:** Usar Stop and quarantine para um arquivo presente em milhares de dispositivos.
Como não cair: A ação tem limite de 1.000 dispositivos e três dias de tempo limite; para escala e permanência, crie indicador.

⚠ **Alerta de prova:** Acreditar que mudar o grafo para All associated incidents mescla ou move alertas.
Como não cair: A visão só amplia o contexto; a tag Redirected só aparece em mescla real.

⚠ **Alerta de prova:** Concluir que o incidente de origem de uma mescla foi excluído.
Como não cair: Ele é fechado com a tag Redirected e continua acessível no Sentinel do portal do Azure.

⚠ **Alerta de prova:** Escolher putfile para baixar um arquivo do dispositivo ou undo para copiar para a biblioteca.
Como não cair: getfile baixa; putfile envia; undo restaura entidade remediada; connections mostra conexões.

⚠ **Alerta de prova:** Achar que o ZAP só move mensagens não lidas e avisa o usuário, ou que só age nas primeiras horas.
Como não cair: Para malware, quarentena de lidas e não lidas, sem aviso, cobrindo as últimas 48 horas.

⚠ **Alerta de prova:** Concluir que o log de auditoria está desligado porque o evento de 20 minutos atrás não apareceu.
Como não cair: Nos serviços principais os registros levam de 60 a 90 minutos para surgir.

⚠ **Alerta de prova:** Esperar encontrar acessos de oito meses atrás de um usuário E3 no Audit.
Como não cair: Sem E5 ou complemento, a retenção é de 180 dias; um ano padrão é só com E5 (ou equivalente) para Entra ID, Exchange, OneDrive e SharePoint.

⚠ **Alerta de prova:** Atribuir Search and Purge a quem precisa visualizar ou baixar a mensagem no Threat Explorer.
Como não cair: Ver e baixar exige Preview (padrão em Data Investigator e eDiscovery Manager); Search and Purge move e exclui.

⚠ **Alerta de prova:** Escrever a consulta do eDiscovery com and/not em minúsculas, *termo* ou from: com espaço.
Como não cair: Operadores em maiúsculas, só curinga de prefixo e propriedade:valor sem espaço; espaço entre termos vale como OR.

⚠ **Alerta de prova:** Recomendar Revoke session para conta do AD local ou Mark as compromised para conta do AD.
Como não cair: No AD local: Disable, Enable e Force password change pelo sensor do DC; Revoke session e Mark as compromised são ações para contas do Entra ID.

⚠ **Alerta de prova:** Achar que Revert to default no Defender for Identity é só um desfazer do último ajuste.
Como não cair: É irreversível e volta todas as detecções para High; o Recommended test mode exige data de término de até 60 dias.

⚠ **Alerta de prova:** Supor que resolver no Defender for Cloud um alerta do Defender for Endpoint de uma VM muda o status no portal do Defender.
Como não cair: Alertas do Defender for Endpoint sobre recursos de nuvem não sincronizam status; os do próprio Defender for Cloud sincronizam.

⚠ **Alerta de prova:** Pensar que alertas de DLP sumiram da fila porque foram descontinuados ou porque dependem do Sentinel.
Como não cair: A regra interna de alert tuning de DLP os transforma em comportamentos (BehaviorInfo/BehaviorEntities); desabilite-a em Settings > Microsoft Defender XDR.

Como cai na prova

📝 **Como cai:** Cenário longo de incidente com várias exigências (cronologia, agir na entidade, caçar, ver incidentes relacionados sem mexer no agrupamento).
Como resolver: Marque cada exigência e elimine alternativas que falham em uma só: fila de alertas e mescla mudam agrupamento, Action center só lista remediações, Threat analytics fala de ameaças acompanhadas. Sobra o grafo da história do ataque com Go hunt e All associated incidents.

📝 **Como cai:** Qual ação de resposta usar, com restrição escondida (sem desconectar, milhares de dispositivos, manter Teams, reversível).
Como resolver: Ache a restrição e mapeie: sem desconectar = Restrict app execution; escala = indicador; manter Outlook/Teams = isolamento seletivo; identidade no AD sem desabilitar = Contain user.

📝 **Como cai:** Qual permissão ou função mínima para uma tarefa (pesquisar auditoria, expurgar, ver mensagem, dispensar risco, criar caso).
Como resolver: Separe ler de agir. Descarte funções amplas demais (Global Administrator, Security Administrator) e funções de outro produto; escolha a que corresponde exatamente ao verbo do enunciado.

📝 **Como cai:** Prazo ou limite: o registro não apareceu, o alerta sumiu, a conta foi liberada sozinha.
Como resolver: Lembre o número documentado (60 a 90 minutos, 180 dias, 48 horas, 30 minutos de sincronização, 90 dias de alerta no Defender for Cloud) e desconfie de alternativas com prazos inventados como 5 minutos ou 24 horas.

📝 **Como cai:** Qual agente ou capacidade do Security Copilot atende ao pedido.
Como resolver: Identifique a entrada e a saída: e-mail reportado = Phishing Triage Agent; relatório de inteligência = Briefing Agent; alerta de falso negativo = Dynamic Threat Detection Agent; KQL em linguagem natural = assistente de consultas.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Título do incidente pela API com texto adicional no final	**Sufixo (attack disruption)**
Quais ações da interrupção ainda estão em vigor	**Aba Activities, Performed by AttackDisruption + coluna Policy status**
Relatório de todas as ações de interrupção na organização	**DisruptionAndResponseEvents no Advanced hunting**
Safeboot hardening, GPO hardening	**Blindagem preditiva**
Todos os alertas de um IP a partir do grafo, inclusive de outros incidentes	**Go hunt > Related Alerts**
Opção All User anomalies não aparece no Go hunt	**Habilitar UEBA do Sentinel**
Executar arquivo desconhecido com segurança e obter relatório	**Deep analysis (sandbox na nuvem)**

Linha de comando PowerShell ofuscada no incidente, com Security Copilot	**Analyze (script analysis do Copilot)**
Analista júnior não sabe por onde começar a responder	**Guided responses do Copilot**
Alerta com Detection source Security Copilot sem nenhum agente configurado	**Dynamic Threat Detection Agent**
Briefing de inteligência em minutos, banner no Threat analytics	**Threat Intelligence Briefing Agent**
Aviso por e-mail quando o caso entra em At Risk ou Breached	**Regra de automação com gatilho Case updated e condição de status de SLA**
Requisições de clientes de IA ao MCP Server for Enterprise nos logs do Graph	**Coluna RequestUri com /enterprise em MicrosoftGraphActivityLogs**
Alertas de risco médio do ID Protection sumiram da fila do Defender	**Alert service settings: trocar para High + Medium**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Ações da interrupção automática são desfeitas pela própria equipe, no incidente ou no Action center; fechar o incidente ou tirar a tag não libera nada.
- Com Defender for Office 365 Plano 2, phishing entregue se remove pelo Threat Explorer; o expurgo do eDiscovery é para vazamento de dados e só atua em caixas do Exchange Online.
- All associated incidents não mescla; mescla real fecha a origem com a tag Redirected.
- Security Operator é a função de menor privilégio para dispensar risco de usuário; User Administrator redefine senha.
- Casos genéricos: Alerts (manage); tarefas de incident case: Response (manage); auditoria de casos: SecurityCaseEvent.

Essenciais para a prova (checklist)

☐ Sei identificar um incidente interrompido na interface (tag, faixa amarela, cartão) e pela API (sufixo no título).

☐ Sei quais tabelas do Advanced hunting mostram ações de interrupção (DisruptionAndResponseEvents) e bloqueios por contenção (DeviceEvents ContainedDevice/ContainedUser).

☐ Sei separar ações de resposta do Plano 1 e do Plano 2 do Defender for Endpoint.

☐ Sei os comandos básicos e avançados do live response e o conteúdo do pacote de investigação.

☐ Sei as quatro opções do Go hunt e o requisito de All User anomalies.

☐ Sei quando o Defender não mescla incidentes e o que acontece com a origem de uma mescla.

- ☐ Sei montar remediação de e-mail em duas etapas e quais funções (Search and Purge, Preview) cada etapa exige.
- ☐ Sei os prazos de retenção e de disponibilidade do Purview Audit e as funções para pesquisar.
- ☐ Sei a sintaxe KeyQL do eDiscovery e os limites do expurgo.
- ☐ Sei qual capacidade do Security Copilot ou qual agente usar para cada pedido.

Questões de revisão do capítulo

R3.1 · Responder a incidentes de segurança

Na Indústria Gráfica Papel Fino, um analista registrou num caso genérico do Defender a revisão das contas de serviço com senha antiga. Ele quer anexar a planilha de contas, vincular os objetos relacionados e avisar por e-mail a equipe de infraestrutura sobre a atualização do caso. Isso é possível?

A. Só o e-mail; anexos ficam restritos a casos com SLA configurado
B. Não: anexos e e-mails existem apenas em incident cases ligados a alertas
C. Só os anexos; notificações por e-mail exigem um playbook do Sentinel
D. Sim: casos genéricos aceitam anexos, objetos vinculados e e-mail

R3.2 · Responder a incidentes de segurança

Às 10h, um usuário da Fábrica de Doces Mel excluiu em massa arquivos de uma biblioteca do SharePoint. Às 10h20 o analista pesquisou o log de auditoria do Purview e não encontrou os registros. O que a documentação informa?

A. Registros do SharePoint só aparecem no dia seguinte, depois do processamento noturno
B. Os registros só ficam pesquisáveis depois que o usuário encerra a sessão no SharePoint
C. Nos serviços principais, os registros costumam surgir 60 a 90 minutos após o evento
D. Os registros aparecem em até 5 minutos; se não apareceram, a auditoria está desligada

R3.3 · Responder a incidentes de segurança

O gerente de inteligência de ameaças da Siderúrgica Ferro Azul quer relatórios de inteligência personalizados, gerados em minutos a partir da atividade recente de atores de ameaça e das vulnerabilidades internas e externas da empresa, sem horas de coleta manual. A empresa tem Security Copilot, Defender for Endpoint e Defender External Attack Surface Management. Qual agente usar e onde ele aparece no portal?

A. Dynamic Threat Detection Agent, na fila de alertas com Detection source Security Copilot
B. Phishing Triage Agent, na página de Submissions das mensagens reportadas por usuários
C. Threat Hunting Assistant, no editor de consultas do Advanced hunting do portal
D. Threat Intelligence Briefing Agent, num banner no topo da página de Threat analytics

R3.4 · Responder a incidentes de segurança

O analista da Indústria Moveleira Cedro quer entender o comportamento de um executável desconhecido, que nenhum mecanismo classificou, executando-o com segurança fora do ambiente da empresa e obtendo um relatório detalhado. Qual ação da página do arquivo usar?

A. Deep analysis, que executa o arquivo num sandbox seguro na nuvem e gera um relatório
B. Stop and quarantine, que analisa o comportamento do arquivo enquanto ele fica em quarentena
C. Download file, que executa o arquivo num zip protegido por senha no computador do analista
D. Manage indicator com Audit, que registra cada execução e gera o relatório de comportamento

Respostas comentadas

R3.1. D) Sim: casos genéricos aceitam anexos, objetos vinculados e e-mail

Por quê: Casos genéricos registram trabalho de SecOps fora de incidentes com responsável, prioridade, status, tarefas, comentários, histórico, anexos, objetos vinculados, campos personalizados, prazos e notificações por e-mail.

✗ A) Incorreta. Anexos não dependem de política de SLA.
✗ B) Incorreta. Esses recursos também existem em casos genéricos; a documentação não os restringe a incident cases.
✗ C) Incorreta. A notificação por e-mail é recurso do próprio caso genérico.

> **Dica de prova:** Caso genérico: anexos, objetos vinculados e e-mail de notificação.

R3.2. C) Nos serviços principais, os registros costumam surgir 60 a 90 minutos após o evento

Por quê: A pesquisa de auditoria do Purview usa trabalhos de busca que continuam com o navegador fechado. Para outros serviços, a disponibilidade pode demorar mais, e falhas fora do serviço de auditoria podem atrasar registros; por isso não há compromisso de tempo.

✗ A) Incorreta. A documentação não descreve processamento noturno para o SharePoint.
✗ B) Incorreta. A disponibilidade não depende do encerramento da sessão do usuário.
✗ D) Incorreta. Não há esse prazo de 5 minutos, e a ausência aos 20 minutos é esperada.

> **Dica de prova:** Registro de auditoria recente não apareceu: aguarde de 60 a 90 minutos nos serviços principais.

R3.3. D) Threat Intelligence Briefing Agent, num banner no topo da página de Threat analytics

Por quê: O agente de briefing usa plugins do Microsoft Threat Intelligence (e, opcionalmente, do Defender EASM) e funciona melhor com Defender for Endpoint e EASM ligados. Deve ser conectado a uma conta ou, de preferência, a uma identidade de agente com as permissões exigidas.

✗ A) Incorreta. O Dynamic Threat Detection Agent gera alertas sobre ameaças não detectadas, não relatórios.
✗ B) Incorreta. O Phishing Triage Agent classifica e-mails reportados por usuários.
✗ C) Incorreta. O Threat Hunting Assistant ajuda a caçar ameaças com consultas, não a produzir briefings.

> **Dica de prova:** Briefing de inteligência em minutos: Threat Intelligence Briefing Agent, no Threat analytics.

R3.4. A) Deep analysis, que executa o arquivo num sandbox seguro na nuvem e gera um relatório

Por quê: A página do arquivo oferece Stop and quarantine file, Manage indicator, Download file, Collect file, Ask Defender Experts, Go hunt e Deep analysis. Relatórios de análises anteriores também ficam acessíveis pela ação Deep analysis.

✗ B) Incorreta. Stop and quarantine interrompe processos e põe o arquivo em quarentena; não analisa o comportamento.

✗ C) Incorreta. Download file baixa o arquivo num zip protegido por senha; não o executa nem gera relatório.

✗ D) Incorreta. Um indicador com Audit gera alertas quando o arquivo roda, mas não produz análise de comportamento.

> **Dica de prova:** Ver o comportamento de um arquivo com segurança: Deep analysis (sandbox na nuvem).

DIA DA PROVA

Estratégia de prova

A prova SC-200 tem cerca de 50 itens em 100 minutos, de múltipla escolha e múltipla resposta, com pontuação de 1 a 1000 e mínimo de 700. Quase tudo vem como cenário de SOC: uma empresa, um problema, várias restrições e a pergunta pela configuração, ferramenta, tabela ou função exata. As alternativas erradas costumam ser recursos reais do produto, mas da aba errada, do produto vizinho ou com um número trocado. O peso maior está em gerenciar o ambiente (40-45%), seguido de responder a incidentes (35-40%) e caçar ameaças (20-25%). A prova também cobra mudanças recentes, como o Sentinel no portal do Defender, a AIR do Defender for Endpoint deixando de ser experiência separada e os agentes do Security Copilot.

Como responder

✓ Leia a última frase do enunciado primeiro para saber se pedem ferramenta, função mínima, tabela ou comportamento esperado, e só depois leia o cenário.

✓ Sublinhe as restrições (sem desconectar, sem desativar regras, menor privilégio, sem esperar incidente, menor custo); a alternativa certa é a única que atende todas.

✓ Em itens de múltipla resposta (Escolha DUAS ou TRÊS), avalie cada opção como verdadeiro ou falso de forma independente, sem tentar completar um par.

✓ Quando duas opções parecem certas, prefira a mais específica e de menor privilégio; Global Administrator, Owner e Contributor quase sempre são excesso.

✓ Em consultas KQL, compare as alternativas linha a linha: tabela, coluna de filtro, função de agregação e chaves do summarize ou do join.

✓ Desconfie de números redondos inventados (5 minutos, 24 horas, ilimitado, 60 minutos de consulta) e confie nos limites documentados.

✓ Com o tempo de 100 minutos para cerca de 50 itens, marque os cenários longos para revisão e volte a eles no fim, sem deixar nenhum em branco.

✓ Identifique o produto pelo vocabulário: grupos de dispositivos e indicadores são Defender for Endpoint; regras de automação, playbooks e DCR são Sentinel; Search and Purge e Audit são Purview ou Office 365.

Erros que derrubam candidatos

✗ Escolher uma ferramenta do produto vizinho, como Action center para cronologia ou Threat analytics para o incidente do próprio ambiente.

✗ Confundir limites: 150 alertas da regra agendada com os 30 da NRT, 30 dias do Advanced hunting com 90 do Defender for Cloud.

✗ Dar a função ampla quando o enunciado pede menor privilégio.

✗ Ignorar o pré-requisito do Defender Antivirus ativo em indicadores de arquivo e regras ASR.

✗ Esquecer que, no portal do Defender, o Defender XDR cria e correlaciona os incidentes do Sentinel.

✗ Tratar Hide alert, Resolve alert e Set as behavior como equivalentes para qualquer produto.

✗ Achar que um alerta ou ação some para sempre quando, na verdade, é desfeito no Action center ou liberado no incidente.

Na semana da prova

- ☐ Refaça as provas práticas por domínio e anote, para cada erro, qual alternativa vizinha enganou você e por quê.
- ☐ Revise as tabelas de números de cada capítulo até saber de cor os limites de regras, retenção, auditoria e Advanced hunting.
- ☐ Monte uma folha de tabelas do Advanced hunting (e-mail, identidade, dispositivo, nuvem) e recite o que cada uma registra.
- ☐ Revise a escada de funções do Sentinel e as permissões do RBAC unificado (Security data basics, Response, Alerts, Data manage).
- ☐ Na véspera, releia só as seções lembrar e pegadinhas dos três capítulos e durma bem.

REVISÃO FINAL

Folha de cola

Leia na véspera e na manhã da prova: os gatilhos e as pegadinhas mais importantes de cada domínio.

1. Gerenciar um ambiente de operações de segurança

‣ Uma notificação por incidente, sem e-mail a cada alerta → **Aba Incidents de Email notifications com a opção de uma notificação por incidente**

‣ Aviso quando ação automática falhar → **Aba Actions de Email notifications, status Failed**

‣ Antivírus de terceiros, mas quer bloquear artefatos detectados pelo EDR → **EDR in block mode**

‣ Indicador de domínio não bloqueia no Chrome → **Custom network indicators + proteção de rede em modo de bloqueio**

‣ Coleta personalizada parou no meio do dia e voltou no dia seguinte → **Limite de 75.000 eventos por dispositivo por regra em 24 horas**

⚠ Hide alert só vale para o Defender for Endpoint; para Office 365 use Resolve alert.

⚠ Regras internas não se aplicam a detecções personalizadas nem a Custom TI; crie regra própria ou ajuste a consulta.

⚠ Essa é alerta a alerta do Defender for Endpoint; incidentes ficam na aba Incidents de Email notifications do Defender XDR.

2. Realizar caça a ameaças

‣ Mensagens movidas pelo ZAP ou remediadas depois da entrega → **EmailPostDeliveryEvents**

‣ Quem clicou no link mesmo após o aviso do Safe Links → **UrlClickEvents com IsClickedThrough**

‣ Enumeração de usuários e grupos do AD por LDAP → **IdentityQueryEvents**

‣ Entradas interativas e não interativas com risco e acesso condicional → **EntraIdSignInEvents**

‣ Persistência na chave de registro Run → **DeviceRegistryEvents**

⚠ has_any aceita qualquer um; todos é has_all; começar com é startswith ou hasprefix.

⚠ Use dcount(RemoteIP) e agrupe por dispositivo, PID e horário de criação do processo, porque PIDs são reciclados.

⚠ LocalPort 445 indica conexões recebidas; varredura de saída usa RemotePort 445.

3. Responder a incidentes de segurança

‣ Título do incidente pela API com texto adicional no final → **Sufixo (attack disruption)**

‣ Quais ações da interrupção ainda estão em vigor → **Aba Activities, Performed by AttackDisruption + coluna Policy status**

‣ Relatório de todas as ações de interrupção na organização → **DisruptionAndResponseEvents no Advanced hunting**

‣ Safeboot hardening, GPO hardening → **Blindagem preditiva**

‣ Todos os alertas de um IP a partir do grafo, inclusive de outros incidentes → **Go hunt > Related Alerts**

⚠ Plano 1 tem Run antivirus scan, Isolate device, Stop and quarantine a file e indicador de arquivo; live response, pacote de investigação e Restrict app execution exigem Plano 2.

⚠ A ação tem limite de 1.000 dispositivos e três dias de tempo limite; para escala e permanência, crie indicador.

⚠ A visão só amplia o contexto; a tag Redirected só aparece em mescla real.

GABARITO

Respostas do diagnóstico

D1. C) Fora do portal, inclua o sufixo _CL no nome, que deve casar com o stream do DCR → revise o capítulo 1

Por quê: Tabelas personalizadas recebem o sufixo _CL e exigem a coluna TimeGenerated. No portal, o sufixo é adicionado sozinho; nos demais métodos, inclua-o no nome e mantenha a correspondência com o stream do DCR.

✗ A) Incorreta. Tabelas personalizadas podem ser criadas pelo portal, Azure CLI, PowerShell, REST, Bicep e ARM.
✗ B) Incorreta. _SRCH identifica tabelas de resultados de search jobs; tabelas personalizadas usam _CL.
✗ D) Incorreta. O DCR não renomeia a tabela; o nome no fluxo de dados deve coincidir com o nome com _CL no workspace.

> **Dica de prova:** Tabela personalizada fora do portal: escreva o _CL você mesmo.

D2. C) A regra atingiu o limite de eventos por dispositivo em 24 horas; criar regras mais focadas → revise o capítulo 1

Por quê: A coleta personalizada tem limite de 75.000 eventos por dispositivo por regra em 24 horas. Regras amplas, como coletar todos os eventos de uma tabela, atingem o limite rápido; a documentação recomenda piloto com poucos dispositivos e regras específicas.

✗ A) Incorreta. A coleta personalizada só aceita tags dinâmicas; tags manuais não servem para direcionar a regra.
✗ B) Incorreta. O comportamento descrito corresponde ao limite documentado da regra por dispositivo, e mudar a camada da tabela não altera esse limite.
✗ D) Incorreta. O EDR em modo de bloqueio não tem relação com o volume de eventos da coleta personalizada.

> **Dica de prova:** Coleta personalizada parou e voltou no dia seguinte: limite de 75.000 eventos por dispositivo por regra.

D3. D) A URL da API root e o ID da coleção (collection ID) do servidor TAXII → revise o capítulo 1

Por quê: O Sentinel tem um cliente TAXII embutido. Para importar STIX de um servidor TAXII 2.x, obtenha a API root e o collection ID (às vezes a partir do endpoint de descoberta), instale a solução Threat Intelligence no Content hub e configure o conector Threat Intelligence - TAXII.

✗ A) Incorreta. Os indicadores vão para as tabelas de inteligência de ameaças do Sentinel, sem tabela personalizada nem DCE.
✗ B) Incorreta. ID de aplicativo e segredo são usados pela upload API, não pelo conector TAXII.
✗ C) Incorreta. O conector TAXII não usa chaves de workspace; ele atua como cliente TAXII do provedor.

> **Dica de prova:** Conector TAXII: API root + collection ID.

D4. A) A tabela EmailPostDeliveryEvents → revise o capítulo 2

Por quê: Tabelas de e-mail do Advanced hunting: EmailEvents (entrega), EmailAttachmentInfo (anexos), EmailUrlInfo (URLs), EmailPostDeliveryEvents (ações pós-entrega, como ZAP e remediação manual) e UrlClickEvents (cliques). Todas exigem o Defender for Office 365.

✗ B) Incorreta. UrlClickEvents registra cliques em links protegidos pelo Safe Links.

✗ C) Incorreta. IdentityDirectoryEvents traz eventos de controladores de domínio do Active Directory local.

✗ D) Incorreta. EmailAttachmentInfo traz informações dos arquivos anexados aos e-mails.

> **Dica de prova:** Ações depois da entrega (ZAP, remediação manual): EmailPostDeliveryEvents.

D5. A) O cenário Paths between two entities → revise o capítulo 2

Por quê: O hunting graph permite traçar caminhos e pontos de estrangulamento e agir a partir dos resultados, revelando relações que consultas tabulares podem não mostrar. Cada cenário tem entradas próprias e técnicas MITRE ATT&CK associadas.

✗ B) Incorreta. Esse cenário lista identidades críticas com acesso a armazenamento de dados sensíveis.

✗ C) Incorreta. Entity relationship map mostra as conexões diretas de uma entidade, não o caminho até outra.

✗ D) Incorreta. Esse cenário identifica nós que mais aparecem em caminhos até armazenamentos SQL, sem partir de uma origem específica.

> **Dica de prova:** Existe caminho de A até B: cenário Paths between two entities.

D6. B) O cenário Attack paths to critical asset → revise o capítulo 2

Por quê: O hunting graph renderiza cenários de ameaça como grafos interativos de nós e arestas. Os cenários predefinidos são consultas prontas (como caminhos de ataque, caminhos entre duas entidades, acesso a key vaults e pontos de estrangulamento) mapeadas a técnicas do MITRE ATT&CK.

✗ A) Incorreta. Esse cenário lista contas convidadas com permissões privilegiadas em recursos de nuvem.

✗ C) Incorreta. Entity relationship map mostra as conexões diretas de uma entidade, não rotas até um alvo.

✗ D) Incorreta. Esse cenário parte de um dispositivo e mostra as contas de armazenamento que ele pode acessar.

> **Dica de prova:** Rotas até um ativo crítico no hunting graph: Attack paths to critical asset.

D7. C) Real-time detections mostra só detecções na entrega; as visões extras exigem o Threat Explorer, do Plano 2 → revise o capítulo 3

Por quê: Threat Explorer e Real-time detections ficam em Email & collaboration no portal do Defender. O Plano 1 tem Real-time detections; o Plano 2 tem o Threat Explorer, com os mesmos dados e capacidades e mais visões, filtros, consultas salvas e ações de remediação.

✗ A) Incorreta. O Plano 1 inclui Real-time detections, com as visões Malware, Phish e Content malware.

✗ B) Incorreta. O Threat Explorer é recurso do Defender for Office 365 Plano 2, independentemente do log de auditoria.

✗ D) Incorreta. As visões Campaigns e URL clicks são exclusivas do Threat Explorer.

> **Dica de prova:** Pós-entrega, Campaigns e URL clicks: Threat Explorer (Defender for Office 365 Plano 2).

D8. A) Pela coluna RequestUri, que inclui /enterprise nas requisições ao MCP Server → revise o capítulo 3

Por quê: Os logs de atividade do Graph registram requisições de apps de linha de negócio, clientes de API, SDKs, aplicativos da Microsoft e clientes de IA que consultam o Microsoft MCP Server for Enterprise, permitindo monitorar interações de IA com as APIs do Graph.

✗ B) Incorreta. Wids indica as funções de todo o locatário atribuídas ao usuário.

✗ C) Incorreta. ClientAuthMethod indica como o cliente se autenticou (0 público, 1 segredo, 2 certificado), não o tipo de aplicativo.

✗ D) Incorreta. SigninLogs registra entradas, não cada requisição feita à API do Graph.

> **Dica de prova:** Requisições do MCP Server for Enterprise nos logs do Graph: RequestUri com /enterprise.

D9. D) A opção Related Alerts → revise o capítulo 3

Por quê: Go hunt usa o Advanced hunting para verificar as tabelas relevantes por eventos ou alertas da entidade: See all available queries, All Activity, Related Alerts e All User anomalies. Os resultados podem ser vinculados ao incidente.

✗ A) Incorreta. All User anomalies vale só para entidades de usuário com UEBA habilitado.

✗ B) Incorreta. All Activity retorna todas as atividades da entidade, não apenas alertas.

✗ C) Incorreta. Link to incident vincula resultados a um incidente; não é uma consulta do Go hunt.

> **Dica de prova:** Todos os alertas de uma entidade a partir do grafo: Go hunt > Related Alerts.

Agora, treine no formato real

Faça as 6 provas completas do curso SC-200: 300 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

Ver as 6 provas completas e o cupom do mês →

Até o dia da prova, uma revisão por dia no seu feed

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

Material independente de preparação, sem afiliação ou endosso de Microsoft. As questões são inéditas e não reproduzem a prova real.