

Guia de preparação CompTIA CySA+

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.

4 capítulos por domínio	**28** questões comentadas	**83%** 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 CompTIA CySA+: 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 83%).

Mapa do exame

Cada prova do curso tem 85 questões e 165 minutos, no formato do exame. Referência de aprovação: 83%.

Domínio (capítulo)	Peso	Neste guia
1. Gestão de Vulnerabilidades	26%	18 conceitos · 14 pegadinhas
2. Operações de Segurança	34%	18 conceitos · 14 pegadinhas
3. Relatórios e Comunicação	16%	16 conceitos · 13 pegadinhas
4. Resposta e Gestão de Incidentes	24%	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 12 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 · Gestão de Vulnerabilidades

Num teste autorizado do portal de uma distribuidora, o Burp Suite mostra a requisição "GET /download.php?arquivo=../../../../etc/passwd" e a resposta HTTP 200 contendo "root:x:0:0:root:/root:/bin/bash". Qual é a interpretação correta?

A. O parâmetro permite incluir arquivos de um servidor remoto controlado pelo atacante, caracterizando RFI
B. O parâmetro permite executar consultas SQL no banco, e o retorno mostra a tabela de usuários do banco
C. O parâmetro permite injetar scripts no navegador, e o retorno mostra o script refletido na resposta
D. O parâmetro permite ler arquivos locais do servidor fora da pasta prevista, caracterizando path traversal

D2 · Gestão de Vulnerabilidades

A varredura interna de uma universidade aponta SMBv1 habilitado no servidor 10.50.2.10, mas a varredura externa contra o IP público que faz NAT para esse servidor não mostra a porta 445. Qual é a interpretação correta?

A. O NAT desabilitou o protocolo SMBv1 no servidor, e a varredura interna não percebeu essa mudança no host
B. O perímetro bloqueia a 445 vinda da internet, mas a falha continua alcançável por quem está na rede interna
C. O servidor corrigiu o SMBv1 entre as duas varreduras, e a varredura interna mostrou um resultado antigo do cache
D. O achado interno é falso, porque a varredura externa é a referência mais confiável do ambiente

D3 · Gestão de Vulnerabilidades

Um painel interno de uma transportadora recebe o nome de um relatório em um parâmetro e o repassa a um comando do sistema operacional para gerar o PDF. O teste confirmou injeção de comandos com o uso de ponto e vírgula. Além de evitar chamar o shell, qual prática de codificação segura trata melhor a entrada?

A. Remover do parâmetro o caractere ponto e vírgula encontrado, mantendo os demais caracteres
B. Validar o parâmetro no servidor com uma lista de permissões dos nomes de relatório aceitos
C. Validar o parâmetro no navegador com JavaScript, bloqueando caracteres especiais no formulário
D. Codificar a saída do relatório em HTML para que o conteúdo não seja interpretado pelo navegador

D4 · Operações de Segurança

Um SOC usa várias ferramentas que não se comunicam de forma nativa e quer estender a plataforma de orquestração para acionar ações em um produto de EDR específico ao receber um alerta. Qual mecanismo de integração adiciona essa capacidade sem trocar a plataforma inteira?

A. Um aumento do tempo de retenção dos alertas no armazenamento central da equipe
B. Um plug-in que conecta a plataforma de orquestração ao produto de EDR específico
C. Uma reinstalação completa da plataforma de orquestração em um servidor novo e maior
D. Uma planilha compartilhada com a lista das ações que devem ser executadas à mão

D5 · Operações de Segurança

A equipe de caça a ameaças de uma empresa de SaaS quer uma regra YARA que marque um arquivo quando ele contiver as duas strings declaradas, PingSleep e 203.0.113.9, ao mesmo tempo. Qual condição expressa esse requisito?

A. condition: 1 of them
B. condition: any of them
C. condition: none of them
D. condition: all of them

D6 · Operações de Segurança

Em uma filial de uma rede de lojas, estações passaram a receber endereços 192.168.50.x com gateway e DNS 192.168.50.1, entregues pelo servidor DHCP 192.168.50.1. O DHCP oficial é 10.40.0.5 e distribui a faixa 10.40.x. Logo depois, usuários relatam alertas de certificado ao acessar sites. Qual é a interpretação e o controle mais adequados?

A. Servidor DHCP rogue entregando gateway e DNS falsos; ativar DHCP snooping nos switches
B. Conflito de IP entre estações; habilitar a detecção de conflito no servidor oficial
C. Falha do relay DHCP no roteador; reiniciar o serviço de encaminhamento da filial
D. Esgotamento do escopo DHCP oficial; ampliar a faixa 10.40.x no servidor da filial

D7 · Relatórios e Comunicação

O gráfico de tendência de uma empresa de call center mostra que as mesmas vulnerabilidades do navegador reaparecem nas estações algumas semanas depois de corrigidas, logo após a recriação das máquinas a partir da imagem padrão. Qual conclusão o relatório deve registrar?

A. Ataque em andamento, em que um invasor reinstala versões vulneráveis do navegador
B. Imagem padrão desatualizada, que reintroduz as falhas e precisa entrar no plano de correção
C. Comportamento normal, que pode ser desconsiderado porque as falhas já foram corrigidas
D. Falha do scanner, que mantém em cache os resultados das varreduras antigas das estações

D8 · Relatórios e Comunicação

Um analista de uma companhia aérea precisa compartilhar o relatório técnico de vulnerabilidades, que lista hosts expostos, versões e falhas exploráveis, com as equipes responsáveis. Qual cuidado de distribuição é adequado?

A. Restringir o acesso por necessidade de conhecer, classificar o documento e usar canal protegido
B. Publicar o relatório na intranet aberta para dar transparência ao programa de segurança
C. Compartilhar o relatório com fornecedores e parceiros para acelerar as correções
D. Enviar o relatório para a lista de e-mail geral da empresa, já que os dados são classificados como de uso interno

D9 · Relatórios e Comunicação

O time de inteligência de ameaças de um banco produz um relatório interno sobre um grupo que ataca instituições financeiras da América Latina. O relatório será lido pelo SOC e pela diretoria. Como adaptar o conteúdo?

A. Restringir o relatório ao SOC, já que a diretoria não participa da defesa operacional
B. Dar ao SOC IOCs e TTPs para detecção e à diretoria o risco para o negócio e as decisões
C. Entregar o mesmo texto técnico aos dois públicos para manter a consistência da informação
D. Entregar à diretoria a lista de IOCs, que é a parte mais objetiva do relatório recebido

D10 · Resposta e Gestão de Incidentes

Em um incidente em uma empresa de SaaS, o analista discute se deve tirar do ar o servidor de API comprometido ou mantê-lo funcionando com o tráfego desviado para monitoramento. Os critérios avaliados são a preservação de evidências, a disponibilidade do serviço para clientes, o tempo e os recursos para implementar e a duração prevista da solução. Em qual fase do processo essa decisão é tomada?

A. Recuperação
B. Análise
C. Contenção
D. Erradicação

D11 · Resposta e Gestão de Incidentes

Na fila do SOC de uma rede de laboratórios de análises clínicas há três alertas. A1: varredura de portas interna de 10.0.9.5 contra a sub-rede 10.0.20.0/24 à 01:00; a origem está cadastrada como scanner de vulnerabilidades, e a mudança CHG-2290 agenda a varredura para 01:00-03:00. A2: rundll32.exe executando comsvcs.dll com o parâmetro MiniDump no servidor LIS-01. A3: logon da conta de serviço svc-lis numa estação da recepção às 03:40. Qual alerta pode ser fechado como falso positivo após a triagem?

A. A1, pela origem e pela janela iguais às do scanner autorizado na mudança aprovada
B. A2 e A3, por serem eventos de servidores internos sem tráfego para a internet
C. A2, porque rundll32.exe é binário assinado e nativo do sistema Windows do servidor
D. A3, porque contas de serviço costumam autenticar fora do horário comercial da rede

D12 · Resposta e Gestão de Incidentes

Em um incidente de ransomware em uma rede de supermercados, a equipe de TI, o CSIRT, o jurídico e a comunicação recebem ordens conflitantes de três gerentes diferentes, e as decisões de contenção estão paradas. Segundo as boas práticas de definição de papéis, qual medida resolve a situação?

A. Encarregar o jurídico de conduzir as ações técnicas de contenção do caso
B. Designar um líder do incidente como ponto único de coordenação e decisão
C. Transferir a coordenação ao fornecedor do antivírus contratado pela empresa
D. Deixar cada área decidir as próprias ações e consolidar tudo no final

01

CAPÍTULO 1 · 26% DA PROVA

Gestão de Vulnerabilidades

Este domínio vale 26% e mistura três frentes: planejar a varredura certa para cada ativo, interpretar a saída das ferramentas (Nmap, ZAP, Burp, Nikto, Nessus, OpenVAS, Nuclei, Trivy, Checkov, Prowler, ScoutSuite, Metasploit, Atomic Red Team, Caldera) e priorizar com CVSS, EPSS, KEV e contexto do ativo. A prova adora vetor CVSS para ler métrica por métrica, classificação de falso positivo e falso negativo e escolha entre aceitar, transferir, evitar e mitigar. Também caem tipos e funções de controle, exceções com dono do risco, SLOs, SAST, DAST, SCA, SAMM e SBOM. Onde mais erro: ler o percentil do EPSS como probabilidade, esquecer que o CVSS 4.0 não tem Scope, tratar FAIL de configuração como invasão e confiar em chamado fechado como prova de correção.

Neste capítulo

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

Tópicos-chave

Planejamento da varredura

Requisito regulatório dá o piso de frequência, escopo e evidência; a política interna só pode ser mais rigorosa. Desempenho: em link fraco, limite hosts e verificações simultâneas ou use scanner local; varredura pesada vai para janela de manutenção, não para o pico. Segmentação: scanner dentro do segmento ou regra restrita liberando só o IP do scanner. Combine com o SOC (IP e janela registrados, exceção controlada no IPS) e trate o relatório como confidencial.

Inventário e descoberta

Não dá para proteger o que não se conhece: o inventário com dono e criticidade vem antes do scanner. Inventário vivo combina descoberta ativa periódica com monitoramento passivo do tráfego. Rede desconhecida pede varredura de mapeamento; host misterioso pede fingerprinting (pilha TCP/IP e banners) antes de escolher a política; host sem dono deve ganhar dono e entrar no inventário, não ser explorado nem tirado do escopo.

Com agente e sem agente

Agente avalia o host por dentro e envia o resultado quando há conexão: ideal para notebooks que vivem fora da rede e para instâncias efêmeras (agente na imagem base). Sem agente varre pela rede, com credencial de leitura onde possível: ideal para roteadores, switches, impressoras e telefones IP que não aceitam software de terceiros.

Varredura credenciada

Com login, o scanner lê no host versões de arquivos e pacotes e enxerga bibliotecas desatualizadas que a visão de rede não vê. Use conta de serviço dedicada, de privilégio mínimo, com senha em cofre e uso monitorado. Se o login falhou, o resultado virou não credenciado: poucos achados refletem falta de acesso, não ausência de falhas.

Baselines: CIS, ISO 27000 e PCI DSS

CIS Benchmarks dão a configuração item a item por sistema e versão: Nível 1 é a base prática de produção e Nível 2 é o reforçado para ambientes mais sensíveis. A série ISO 27000 define o sistema de gestão e controles, sem configuração por produto. O PCI DSS exige varredura interna e externa trimestral, a externa feita por ASV; o escopo é o ambiente do titular do cartão e os sistemas conectados que podem afetar sua segurança.

Nmap

open aceita conexão, closed responde com RST, filtered não permite concluir porque um filtro descartou as sondagens; em UDP, sem resposta é open|filtered e ICMP port unreachable é closed. -sV detecta versão, -O sistema, -sC ou --script scripts NSE, -A = -O + -sV + -sC + traceroute, -sn só descobre hosts, -Pn pula a descoberta, -sT faz connect sem root, -sU varre UDP. ssl-enum-ciphers: least strength é a nota da pior cifra aceita.

Descoberta e OSINT

Angry IP Scanner mostra quem está vivo, nome e portas abertas, sem testar vulnerabilidades. Masscan envia SYN assíncrono em alta taxa para grandes faixas; depois o Nmap aprofunda. Maltego monta grafos de vínculos a partir de OSINT e pode revelar ativo esquecido. Recon-ng é framework de OSINT em linha de comando, com módulos e workspaces.

Ferramentas web

ZAP: o baseline faz spider e análise passiva sem ataques; a varredura ativa testa os parâmetros; leia tipo, risco, parâmetro e evidence do alerta. Burp Suite mostra requisição e resposta. Nikto aponta configuração do servidor web (banner com versão, TRACE, phpinfo, diretórios, cabeçalhos ausentes), não invasão. Nuclei usa templates YAML de requisição e correspondência, bom para exposição nova.

Falhas web na saída das ferramentas

../ com /etc/passwd na resposta é path traversal (arquivo local exposto); se o arquivo é incluído e interpretado, LFI; URL externa incluída na página é RFI. XSS refletido volta na própria resposta; armazenado fica guardado e é entregue depois. Trocar o ID e ver dado alheio é IDOR. Ponto e vírgula executando comando é injeção de comandos.

Codificação segura

SQL injection se corrige com consulta parametrizada (instruções preparadas e parâmetros vinculados); escape artesanal é frágil e WAF é paliativo. Entrada se valida no servidor com lista de permissões; lista de bloqueio e validação só no navegador são contornáveis. XSS: valide a entrada e codifique a saída conforme o contexto.

Nuvem, contêineres e IaC

Prowler avalia conta de nuvem requisito a requisito, com PASS ou FAIL de configuração. ScoutSuite audita várias nuvens pelas APIs e gera relatório HTML por serviço. Trivy analisa imagens, sistemas de arquivos e IaC, acha segredos e gera SBOM (--format cyclonedx ou spdx); Fixed Version preenchida significa que a correção existe. Checkov analisa IaC antes do deploy, apontando por exemplo SSH aberto para 0.0.0.0/0 ou contêiner com escalada de privilégio.

Metasploit e BAS

Validar não é explorar: módulos auxiliary e o método check confirmam a condição vulnerável sem entregar payload; exploit invade; post pressupõe acesso já obtido. Atomic Red Team é uma biblioteca de testes pequenos, cada um mapeado a uma técnica do ATT&CK; Caldera automatiza emulação de adversários com agentes e perfis. Teste atômico que roda sem gerar alerta é lacuna de detecção.

CVSS 3.1

Explorabilidade: AV (N rede, A adjacente, L local, P físico), AC, PR (N, L, H) e UI (N nenhuma, R exige a vítima). Scope: S:U fica no componente; S:C indica impacto além da autoridade do componente vulnerável, como fuga de VM, e eleva a nota. Impactos C, I e A em N, L ou H. AV:L com PR:H significa que o atacante já precisa estar dentro e com poder.

CVSS 4.0

Não existe mais Scope: os impactos se separam em sistema vulnerável (VC, VI, VA) e sistemas subsequentes (SC, SI, SA). AT:P indica que o ataque depende de condições presentes no alvo. A nomenclatura diz quais grupos entraram: CVSS-B, BT, BE e BTE; a métrica E (maturidade de exploração) é do grupo Threat e, não informada, equivale a Attacked. Métricas suplementares não alteram a nota. Para priorizar, prefira a BTE.

EPSS e KEV

O EPSS, publicado pela FIRST para as CVEs com o mesmo valor para todos, estima a probabilidade de atividade de exploração nos próximos 30 dias; o percentil é só a posição relativa (EPSS 0,12 com percentil 0,92 = 12%). O catálogo KEV da CISA registra exploração observada, exige orientação clara de remediação para a entrada, não atribui nota e tem campo de uso em ransomware. Evidência (KEV) vence estimativa (EPSS).

Classificação dos resultados e validação

Falso positivo: alertou sobre algo que não existe (banner antigo com correção por backport; prove com o changelog). Falso negativo: falha real que a ferramenta não viu. Verdadeiro negativo: silêncio correto. O QoD do OpenVAS é confiança na detecção, não gravidade. Remediação só se valida com nova varredura ou novo teste; se ainda acusa, procure outra cópia do componente.

Controles: tipo e função

Tipo diz como o controle é feito: administrativo (política, norma), técnico (tecnologia, como firewall, GPO, regra no proxy) e físico (tranca, câmera). Função diz quando ele age: preventivo bloqueia antes (portão no pipeline), detectivo sinaliza depois, responsivo reage ao evento em curso para conter (isolamento automático) e corretivo desfaz o estrago e volta ao baseline.

Risco, exceções e SAST/DAST/SCA/SAMM/SBOM

Inerente é antes dos controles, residual é o que sobra depois, apetite é quanto risco a liderança aceita. Aceitar (decisão formal, dono, revisão), transferir (seguro, cláusula), evitar (encerrar a atividade), mitigar (controle que reduz probabilidade ou impacto). Exceção exige dono do risco, compensatório, data de expiração e plano de saída; prazos internos por severidade são SLOs. SAST analisa o código parado e aponta a linha; DAST testa a aplicação rodando; SCA acha biblioteca de terceiro vulnerável; SAMM mede maturidade do programa; SBOM (SPDX ou CycloneDX) diz onde está cada componente.

Macetes para memorizar

💡 CVSS x EPSS x contexto

CVSS = quão grave; EPSS = quão provável; contexto = quanto importa para você.

💡 LFI x RFI

Remoto entrou na página: RFI. Local vazou: LFI.

💡 Varredura passiva

Passivo é seguro, mas cego para quem não fala.

💡 Função do controle

Bloqueia antes: preventivo. Só alerta: detectivo. Reage ao ataque em curso: responsivo. Desfaz: corretivo.

💡 Estratégias de risco

Desligou a fonte: evitou. Pôs controle e o serviço segue: mitigou. Seguro ou contrato: transferiu. Decisão formal sem mudança: aceitou.

💡 Nmap -A

-A = -O + -sV + -sC + traceroute.

💡 Inerente x residual

Inerente = sem controles; residual = com controles; apetite = quanto a direção topa correr.

💡 SBOM

SBOM fala SPDX ou CycloneDX.

Tabela de memorização: não confunda

Quando é...	...e quando é

Varredura passiva Ambiente frágil como OT/ICS, ou descobrir ativos novos sem impacto; só enxerga quem gera tráfego no ponto observado.	**Varredura ativa** Encontrar também os hosts silenciosos e avaliar serviços; sonda os alvos e pode afetar equipamentos frágeis.
Com agente Notebooks que quase nunca estão na rede interna e instâncias efêmeras (agente na imagem base).	**Sem agente** Roteadores, switches, impressoras e telefones IP que não aceitam software instalado.
CVSS Severidade técnica da falha: quão grave.	**EPSS** Probabilidade de exploração nos próximos 30 dias: quão provável. Os dois se completam com o contexto do ativo.
KEV Há evidência de exploração real; prevalece na priorização.	**EPSS** Estimativa estatística para antecipar o que ainda não entrou no KEV; esperar o KEV é esperar a exploração acontecer.
SAST Há acesso ao código e se quer a linha responsável, integrado ao pipeline.	**DAST** Aplicação em execução sem acesso ao código, como na homologação.
LFI O parâmetro lê ou inclui arquivo local do servidor (../../etc/passwd).	**RFI** O parâmetro inclui recurso de um servidor remoto indicado pelo usuário.
Atomic Red Team Teste pequeno e portátil de uma técnica do ATT&CK para checar a detecção.	**Caldera** Campanha automatizada que encadeia técnicas com agentes, perfis de adversário e interface web.

Números que caem

Item	Valor
Peso do domínio na prova	**26% (cerca de 22 das 85 questões)**
Janela do EPSS	**Probabilidade de atividade de exploração nos próximos 30 dias**
Varreduras do PCI DSS	**Interna e externa trimestrais; a externa feita por ASV**
Portas típicas nas saídas	**445 SMB; 3389 RDP (ms-wbt-server); 9100 impressão em rede**
SPDX	**Padrão de SBOM da Linux Foundation reconhecido como ISO/IEC 5962**
0.0.0.0/0	**Qualquer endereço IPv4, inclusive a internet**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Classificar como verdadeiro positivo porque a versão do banner é anterior à corrigida no upstream.
Como não cair: Distribuições corporativas aplicam backport sem mudar a versão. Se o changelog do pacote cita a CVE, é falso positivo documentado com evidência.

⚠ **Alerta de prova:** Ler EPSS 0,12 com percentil 0,92 como 92% de chance de exploração, ou achar que o EPSS é calculado para os ativos da empresa ou para um ano.
Como não cair: A probabilidade é 0,12 (12%) em 30 dias; o percentil é posição relativa. O EPSS é o mesmo para todas as organizações e cobre as CVEs publicadas, não só as do KEV.

⚠ **Alerta de prova:** Tratar o KEV como sinal de que não há correção ou como nota de severidade que substitui o CVSS.
Como não cair: O KEV registra exploração observada e exige orientação de remediação para incluir a CVE; não atribui nota.

⚠ **Alerta de prova:** Ler filtered no Nmap como porta fechada ou host desligado.
Como não cair: closed é RST; filtered é dúvida causada por firewall. Se outras portas responderam, o host está ativo.

⚠ **Alerta de prova:** Invalidar o achado interno porque a varredura externa não mostra a porta.
Como não cair: A externa mede a exposição na internet; a interna mede o risco para quem já está dentro. Fechado por fora não quer dizer seguro por dentro.

⚠ **Alerta de prova:** Concluir que não há SQL injection porque o baseline do ZAP não alertou.
Como não cair: O baseline faz spider e análise passiva, sem ataques nos parâmetros; injeção só é testada na varredura ativa.

⚠ **Alerta de prova:** Ler FAIL do Prowler, FAILED de baseline CIS ou achado do Checkov como prova de invasão ou como CVE.
Como não cair: São configurações fora do padrão. Bucket público é exposição, não registro de acesso indevido; item de benchmark em geral não tem CVE.

⚠ **Alerta de prova:** Considerar a falha corrigida porque o chamado foi fechado, o sistema de patches reportou a instalação ou o commit foi aprovado.
Como não cair: Só nova varredura (de preferência autenticada) ou novo teste confirma que o achado não aparece mais.

⚠ **Alerta de prova:** Corrigir SQL injection escapando aspas com função própria, criando regra de WAF para UNION e SELECT ou cifrando a coluna.
Como não cair: A correção definitiva é consulta parametrizada. WAF pode ser compensatório temporário (patch virtual), mas não corrige o código.

⚠ **Alerta de prova:** Priorizar a CVE com maior nota base porque acima de 9,0 seria crítica em qualquer contexto.
Como não cair: A nota base é a mesma em qualquer ambiente; exploração ativa, exposição à internet, valor do ativo e EPSS mudam a ordem. No CVSS 4.0, use a BTE.

⚠ **Alerta de prova:** Dizer que o CVSS 4.0 mantém a métrica de escopo ou que a maturidade de exploração é do grupo base.
Como não cair: O 4.0 separa impactos em vulnerável (V) e subsequentes (S), sem Scope; a métrica E é do grupo Threat (BT).

⚠ **Alerta de prova:** Tirar o ativo da varredura, mudar a porta ou varrer mais vezes como forma de tratar um risco.
Como não cair: Tirar do escopo cria ponto cego, porta trocada é obscuridade e varrer mais só confirma a falha. Trate com mitigação, exceção formal ou correção.

⚠ **Alerta de prova:** Chamar de corretivo um controle que é uma norma ou política.
Como não cair: Norma é tipo administrativo; corretivo é função. Tipo diz como; função diz quando age.

⚠ **Alerta de prova:** Confundir apetite de risco com risco residual ou inerente.
Como não cair: Inerente e residual são resultados de análise (sem e com controles); apetite é a declaração da liderança sobre quanto risco aceita.

Como cai na prova

📝 **Como cai:** Saída de ferramenta (Nmap, ZAP, Nikto, Trivy, Prowler, Checkov, Metasploit) e a pergunta 'qual é a interpretação correta?'
Como resolver: Identifique a ferramenta e o campo que importa (estado da porta, evidence, Fixed Version, PASS/FAIL). Descarte alternativas que exageram (ataque ocorreu, invasão confirmada) ou trocam o tipo de falha.

📝 **Como cai:** Vetor CVSS completo e a pergunta sobre explorabilidade ou impacto
Como resolver: Leia métrica por métrica (AV, AC, PR, UI, S ou AT, C/I/A ou VC/SC). As erradas descrevem exatamente outra letra: AV:N, PR:N, UI:R, S:U.

📝 **Como cai:** Duas ou três CVEs para priorizar com CVSS, EPSS, KEV, exposição e valor do ativo
Como resolver: Ordem de peso: exploração ativa ou KEV, exposição à internet, valor e criticidade do ativo, EPSS; a nota base sozinha não decide. Ambiente isolado reduz a urgência, mas não zera.

📝 **Como cai:** Classificar o resultado em verdadeiro ou falso, positivo ou negativo
Como resolver: Pergunte duas coisas: a ferramenta alertou? A falha existe de fato? Alertou e não existe = FP; não alertou e existe = FN.

📝 **Como cai:** Planejamento com restrição (link fraco, VLAN segmentada, OT frágil, pico de negócio, regulador)
Como resolver: Escolha a alternativa que mantém a cobertura e reduz o impacto. Desconfie das que tiram ativos do escopo, removem o firewall ou cancelam a varredura.

📝 **Como cai:** Qual tipo, função de controle ou estratégia de risco foi adotada
Como resolver: Separe tipo (como: administrativo, técnico, físico) de função (quando: preventivo, detectivo, responsivo, corretivo) e veja se o serviço continua (mitigar) ou foi desligado (evitar).

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Notebooks que quase nunca se conectam à VPN, ou instâncias que nascem e morrem entre varreduras	**Varredura com agente (agente na imagem base)**
CLPs e IHMs que já travaram com ping sweep	**Monitoramento passivo por SPAN e, se sondar, verificações seguras**
Biblioteca de terceiro com CVE no repositório	**SCA; e a SBOM diz onde o componente está**
Código-fonte disponível e necessidade de apontar a linha	**SAST no pipeline**
Faixa enorme (/16) e pouco tempo para achar portas abertas	**Masscan primeiro, Nmap depois**
Várias nuvens auditadas pelas APIs com relatório HTML por serviço	**ScoutSuite**
Exposição nova descrita em template YAML de requisição e correspondência	**Nuclei**
Trocar o ID na URL e ver o registro de outro usuário	**IDOR (falha de controle de acesso)**
Validar a falha sem entregar payload no Metasploit	**Módulo auxiliary ou método check**
Prazos internos de correção por severidade acompanhados por comitê	**SLOs da política de vulnerabilidades**

Seguro cibernético ou cláusula contratual repassando o impacto	**Transferir o risco**
Falha explorada e sem patch disponível	**Mitigar já com controle compensatório que ataca o vetor e corrigir quando o patch sair**
CVE no KEV em ativo exposto à internet	**Topo da fila, mesmo com CVSS menor, sem esperar a janela**
Ferramenta restaura sozinha a configuração alterada	**Controle corretivo**

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

- EPSS é probabilidade em 30 dias; percentil é só posição relativa.
- KEV é evidência de exploração e passa na frente da estimativa do EPSS.
- CVSS 4.0 não tem Scope e a nota para priorizar é a BTE.
- Corrigido é o que a nova varredura não encontra mais.
- Exceção precisa de dono do risco, compensatório, validade e revisão.

Essenciais para a prova (checklist)

☐ Sei escolher entre varredura interna ou externa, com ou sem agente, credenciada ou não, passiva ou ativa.

☐ Sei interpretar os estados open, closed, filtered e open|filtered e as principais flags do Nmap.

☐ Sei dizer o que fazem Angry IP Scanner, Masscan, Maltego, Recon-ng, Nikto, Nuclei, ScoutSuite, Prowler, Trivy e Checkov.

☐ Sei ler um vetor CVSS 3.1 e explicar as mudanças do CVSS 4.0 (VC/SC, AT, BTE, sem Scope).

☐ Sei interpretar EPSS e percentil e usar o KEV na priorização.

☐ Sei classificar um resultado como FP, FN, VP ou VN e justificar.

☐ Sei a correção certa para SQL injection, XSS e injeção de comandos.

☐ Sei classificar um controle por tipo e por função.

☐ Sei distinguir aceitar, transferir, evitar e mitigar e o que uma exceção formal precisa ter.

☐ Sei quando usar SAST, DAST, SCA, SAMM e SBOM.

Questões de revisão do capítulo

R1.1 · Gestão de Vulnerabilidades

O gerente de infraestrutura de uma rede de farmácias propõe trocar o CVSS pelo EPSS como único critério de prioridade, argumentando que o EPSS já diz o que é perigoso. Qual argumento técnico o analista deve apresentar?

A. O EPSS é calculado por cada organização a partir dos próprios ativos, o que torna o resultado incomparável entre empresas
B. O EPSS estima a probabilidade de exploração e o CVSS a severidade técnica; os dois se completam com o contexto do ativo
C. O EPSS só pontua vulnerabilidades já incluídas no catálogo KEV, deixando de fora as falhas que ainda não foram exploradas
D. O EPSS mede o impacto da exploração no negócio, por isso precisa do CVSS para estimar a probabilidade de um ataque real

R1.2 · Gestão de Vulnerabilidades

Em uma empresa de mineração, a ferramenta de gestão de vulnerabilidades mostra o vetor CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H para uma falha em um agente de backup instalado nos servidores. O que esse vetor indica sobre a explorabilidade?

A. O atacante já precisa de acesso local ao servidor e de privilégios elevados para explorar a falha
B. O atacante precisa convencer um usuário a executar uma ação, o que reduz a chance de exploração
C. O atacante pode explorar a falha pela rede sem autenticação, desde que o agente esteja em execução
D. O atacante precisa de acesso físico ao servidor, como conectar um dispositivo USB ao equipamento

R1.3 · Gestão de Vulnerabilidades

O relatório da última varredura de uma rede de hospitais traz cada servidor vulnerável, as versões dos serviços e as credenciais que falharam no login. Um gerente quer publicá-lo na pasta pública da intranet. Qual cuidado de planejamento deve ser aplicado?

A. Publicar o relatório na intranet para que os colaboradores acompanhem a evolução do risco
B. Enviar o relatório completo por e-mail aos fornecedores de cada sistema citado na varredura do mês
C. Guardar o relatório só na estação do analista para evitar que ele circule pela organização
D. Classificar o relatório como confidencial e restringir o acesso aos responsáveis pela correção

R1.4 · Gestão de Vulnerabilidades

A varredura ativa do ZAP no portal de uma editora gerou o alerta "Remote File Inclusion" de risco alto: ao colocar uma URL externa no parâmetro pagina, a resposta trouxe o conteúdo daquele site externo dentro da página. Qual é a interpretação correta?

A. A aplicação aceita requisições forjadas de outros sites, caracterizando CSRF na página
B. A aplicação lê arquivos locais do servidor por travessia de diretório, caracterizando LFI
C. A aplicação inclui recursos remotos indicados pelo usuário, caracterizando RFI
D. A aplicação reflete o parâmetro na página sem codificar, caracterizando XSS refletido

Respostas comentadas

R1.1. B) O EPSS estima a probabilidade de exploração e o CVSS a severidade técnica; os dois se completam com o contexto do ativo

Por quê: CVSS e EPSS são métodos de pontuação complementares; a priorização madura combina severidade, probabilidade de exploração e contexto do ativo. (objetivo 2.3)

✗ A) Incorreta. O EPSS é publicado pela FIRST para as CVEs, com o mesmo valor para todas as organizações.
✗ C) Incorreta. O EPSS pontua as CVEs publicadas, não só as que estão no KEV.
✗ D) Incorreta. Os papéis estão invertidos: o EPSS estima probabilidade, e o CVSS descreve severidade técnica.

> **Dica de prova:** CVSS = quão grave; EPSS = quão provável; contexto = quanto importa para você.

R1.2. A) O atacante já precisa de acesso local ao servidor e de privilégios elevados para explorar a falha

Por quê: As métricas de explorabilidade do CVSS (AV, AC, PR, UI) mostram o que o atacante precisa ter; acesso local com privilégio alto torna a exploração mais difícil. (objetivo 2.3)

✗ B) Incorreta. O vetor traz UI:N: não há necessidade de interação do usuário.
✗ C) Incorreta. Exploração pela rede seria AV:N e sem autenticação seria PR:N.
✗ D) Incorreta. Acesso físico seria AV:P; AV:L indica acesso local, como sessão no sistema.

> **Dica de prova:** AV:L + PR:H = o atacante já precisa estar dentro e com poder.

R1.3. D) Classificar o relatório como confidencial e restringir o acesso aos responsáveis pela correção

Por quê: Os níveis de sensibilidade também valem para os produtos da varredura: relatórios e credenciais exigem classificação e acesso restrito (objetivo 2.1).

✗ A) Incorreta. Publicar amplamente expõe o caminho mais fácil para um atacante interno.
✗ B) Incorreta. Enviar o relatório inteiro a terceiros vaza dados de outros sistemas sem necessidade.
✗ C) Incorreta. Guardar numa estação isolada impede o uso pelos responsáveis e não é controle adequado.

> **Dica de prova:** Relatório de varredura é mapa do tesouro: trate como confidencial.

R1.4. C) A aplicação inclui recursos remotos indicados pelo usuário, caracterizando RFI

Por quê: RFI ocorre quando a aplicação inclui arquivos remotos indicados pelo usuário; o ZAP testa isso na varredura ativa (objetivo 2.2).

✗ A) Incorreta. CSRF trata de ações forjadas em nome do usuário, não de inclusão de arquivo.

✗ B) Incorreta. LFI envolve arquivos locais do servidor; aqui o recurso veio de fora.

✗ D) Incorreta. O alerta mostra a inclusão do conteúdo externo, não o reflexo do texto enviado.

> **Dica de prova:** Remoto entrou na página: RFI. Local vazou: LFI.

02

CAPÍTULO 2 · 34% DA PROVA

Operações de Segurança

Este é o domínio de maior peso (34%) e o mais prático da prova: é preciso olhar um trecho de log, a saída de uma ferramenta ou uma linha de comando e dizer o que está acontecendo. Cai muito indicador de atividade maliciosa (LOLBins, beaconing, tunelamento DNS, BEC, impossible travel, fadiga de MFA, cryptomining na nuvem), qual ferramenta resolve cada tarefa (CyberChef, Wireshark, tcpdump, Suricata, Snort, Zeek, YARA, MISP, OpenCTI, AbuseIPDB, WHOIS) e conceitos de arquitetura como ZTNA, SASE, PAM, gestão de segredos e OT/ICS. Também entram threat intelligence, threat hunting, SOAR, playbooks e os riscos e usos da IA no SOC. Onde mais erro: achar que o binário legítimo é o malware (o problema é o uso), trocar o ID de evento ou o campo de um filtro e deixar passar o detalhe que separa o normal do anômalo (processo pai, caminho, horário, volume, destino).

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

Tópicos-chave

LOLBins (living off the land)

Binários legítimos e assinados do sistema, como certutil, bitsadmin, rundll32, regsvr32 e wmic, abusados para baixar, decodificar ou executar código sem ferramenta externa. A prova cobra que o binário é confiável e o uso não: certutil baixando .exe ou decodificando Base64, bitsadmin baixando de servidor externo, rundll32 com comsvcs.dll MiniDump no PID do lsass (despejo de credenciais) e regsvr32 /i:URL scrobj.dll filho do Word (scriptlet remoto). Para binários Unix permitidos no sudo que viram shell de root, consulte o GTFOBins.

Árvore de processos do Windows

O lsass.exe tem uma só instância, é filho do wininit.exe e roda de System32; o services.exe também é filho do wininit.exe e é pai das instâncias de svchost.exe. svchost.exe fora de System32 ou com pai explorer.exe é masquerading (nome certo, lugar e pai errados). winword.exe gerando cmd.exe ou powershell.exe indica macro maliciosa; w3wp.exe (IIS) gerando cmd.exe indica web shell.

IDs de evento do Windows mais cobrados

4688 criação de processo (traz o processo criador; ative a linha de comando), 4104 bloco de script do PowerShell, 4624 logon bem-sucedido (tipo 10 = RDP, 3 = rede, 4 = batch), 4625 falha de logon, 4672 privilégios especiais no logon, 4720 conta criada, 4732 inclusão em grupo, 4740 conta bloqueada, 4698 tarefa agendada, 7045 serviço instalado e 1102 log de segurança limpo. Para força bruta, agrupe os 4625 por conta e conte.

Beaconing de C2

Conexões regulares, de baixo volume e tamanho constante, sempre ao mesmo destino, visíveis no conn.log do Zeek ou no proxy. HTTPS na porta 443 não legitima o tráfego. Exfiltração em massa gera grande volume de bytes e varredura gera muitos destinos; beaconing é o relógio certinho com bytes iguais.

Tunelamento DNS e DGA

Tunelamento: um host gera milhares de subdomínios longos, aleatórios ou codificados, em rajada, muitas vezes com consultas TXT, para exfiltrar dados ou falar com o C2. DGA: rajada de NXDOMAIN para nomes sem sentido de um só host, o malware procurando o servidor de C2. Não confunda com amplificação DNS, em que uma vítima externa recebe respostas grandes que não pediu.

Indicadores de identidade

Impossible travel: a distância entre dois logins (vinda do GeoIP) não é possível no tempo decorrido; trate como conta comprometida e revogue sessões, mas antes confira se o IP é da saída do proxy em nuvem da própria empresa. Fadiga de MFA: push negado várias vezes e aprovado em seguida, muitas vezes seguido do registro de novo método. Conta de serviço em logon RDP interativo (4624 tipo 10) é desvio do padrão.

BEC (business email compromise)

Fraude sem malware e muitas vezes sem anexo ou link: pedido de dinheiro (transferência, cartão-presente) com urgência e sigilo, a partir de domínio quase igual ao real ou de conta tomada. Conta tomada costuma ganhar regra de caixa que oculta e encaminha mensagens (nome '.', mover para RSS Subscriptions, marcar como lida). SPF e DKIM com pass só mostram que o domínio falso autorizou o próprio envio.

SPF, DKIM e DMARC

SPF verifica se o IP de envio está autorizado no DNS do domínio. DKIM assina a mensagem e prova origem e integridade das partes assinadas; não cifra nem confirma leitura. DMARC define o que fazer quando nem SPF nem DKIM passam alinhados ao domínio: p=none só monitora e reporta, p=quarantine manda para quarentena ou spam, p=reject recusa.

CyberChef

From Base64 decodifica Base64; From Hex transforma pares hexadecimais em texto; Gunzip descomprime (bytes iniciais 1f 8b); XOR Brute Force testa chaves de um byte (pista: um byte repetido onde deveriam estar zeros). PowerShell -EncodedCommand é Base64 de UTF-16LE: From Base64 seguido de Decode text em UTF-16LE. %2e é ponto e %2f é barra na codificação de URL.

Wireshark e tcpdump

No Wireshark, Follow TCP Stream reconstrói a conversa nos dois sentidos, Export Objects salva arquivos transferidos (por exemplo via HTTP), http.response.code filtra o status HTTP e dns.flags.response == 1 mostra só respostas DNS (o nome consultado é dns.qry.name; use contains para casar parte de um nome). No tcpdump: -i interface, -w grava em arquivo, -r lê arquivo, -nn não resolve nomes nem portas; filtros BPF como host, port e dst port.

Suricata, Snort e Zeek

No EVE JSON do Suricata, event_type classifica o registro (alert, dns, http, flow); o ID da regra é o signature_id dentro de alert. tls.sni casa o SNI de uma sessão TLS, e flow:established,to_server casa sessão já aberta do cliente para o servidor. No Snort, limiar de frequência dentro da regra é detection_filter com track, count e seconds. O Zeek gera logs como conn.log e dns.log, base do threat hunting de rede.

YARA, strings, VirusTotal e sandbox

Em YARA, condition all of them exige todas as strings; any of them ou 1 of them basta uma. strings é análise estática; para ver o comportamento em execução (rede, arquivos) use sandbox como Cuckoo ou Joe Sandbox. No VirusTotal, poucas detecções não provam que a amostra é inofensiva, sobretudo se é recente: olhe comportamento e data da primeira submissão.

IoCs e Pyramid of Pain

Hash e IP são indicadores atômicos, fáceis de trocar pelo adversário (base da pirâmide); TTPs são comportamentais e ficam no topo, porque mudá-los obriga o adversário a reformular o modo de operar. Por isso a atribuição pesa TTP, não IP, que é reutilizado ou falsificado. Ciclo do IoC: coleta, análise e aplicação (enviar o indicador às ferramentas para bloquear).

Fontes, plataformas e confiança da inteligência

Confiança se mede por atualidade (o indicador estava certo, mas está velho), relevância (atinge o meu setor e as minhas tecnologias) e precisão (confirmado em várias fontes independentes); OSINT é pública e fonte fechada exige assinatura ou acordo. MISP usa warninglists contra falso positivo, galaxies para atores e técnicas e sightings para observações; OpenCTI organiza tudo em grafo; OTX agrupa indicadores em pulsos; AbuseIPDB dá reputação de IP, WHOIS traz registrador e datas, GeoIP estima a localização. STIX representa a inteligência, TAXII a transporta, o AIS da CISA troca indicadores máquina a máquina e ISACs compartilham indicadores do setor sem assumir a resposta dos membros.

STRIDE e threat hunting

STRIDE: Spoofing (fingir identidade), Tampering (alterar dado, integridade), Repudiation (negar ação), Information disclosure (ler dado sem autorização, confidencialidade), Denial of service (disponibilidade), Elevation of privilege (autorização). Heat map de TTPs: cor forte é técnica mais observada, prioridade de detecção; o ATT&CK Navigator gera as camadas. Threat mapping das detecções na matriz mostra onde faltam regras. Deception: honeypot atrai e observa; honeytoken ou canary dispara alerta quando tocado.

Arquitetura, identidade e proteção de dados

ZTNA libera cada aplicação por sessão após checar identidade e postura; SASE une SD-WAN com SWG, CASB, FWaaS e ZTNA pela nuvem; PAM com cofre, just-in-time e gravação de sessão trata privilégio permanente; ABAC decide por atributos e contexto. OAuth 2.0 autoriza, OIDC acrescenta o ID token (JWT) para autenticar, SAML usa asserção XML assinada; FIDO2 e passkeys resistem a proxy de phishing; na nuvem, IMDSv2 contra roubo de credenciais via SSRF. Mascaramento mostra parte do dado, tokenização guarda um substituto do PAN, criptografia envelope protege a chave de dados com uma KEK no KMS ou HSM e DLP inspeciona conteúdo e rótulos para impedir a saída. Base64 é codificação, não proteção: segredos vão para cofre com rotação e auditoria, e Secrets do Kubernetes pedem criptografia em repouso no etcd e RBAC restrito.

OT, ICS e SCADA

SCADA supervisiona ativos espalhados por grandes distâncias (estação mestre, IHM e RTUs via telemetria); DCS controla processos concentrados numa planta. Protocolos industriais sem autenticação pedem segmentação com zonas, conduítes e DMZ industrial entre TI e OT. Se os dados só podem sair da OT, use gateway unidirecional (diodo de dados). CLPs e IHMs em geral não suportam agentes: em OT frágil, comece pelo monitoramento passivo.

Eficiência, automação e IA no SOC

Playbook é o fluxo de decisão de um tipo de incidente (padroniza a equipe); runbook são os passos técnicos repetíveis de uma tarefa. SOAR enriquece e age sozinho; dashboard só apresenta. Webhook é uma ferramenta chamando a API de outra em tempo real; plug-in estende a orquestração a um produto específico; IaC é configuração versionada em código e aplicada por automação. Riscos de IA: alucinação, exposição de dados, envenenamento de modelo e injeção de prompt; governança via política de uso de IA; a IA resume, compara, correlaciona e rascunha, mas a decisão de agir fica com o analista.

Macetes para memorizar

💡 LOLBins

Binário confiável, uso suspeito: julgue o comando, não o nome do executável.

💡 Pyramid of Pain

Hash muda num clique; TTP muda o jeito de operar. Quanto mais alto, mais dói no atacante.

💡 DMARC

none olha, quarantine esconde, reject devolve.

💡 OAuth x OIDC

OAuth Autoriza, OIDC Identifica.

💡 STIX x TAXII

STIX é a carta, TAXII é o carteiro.

💡 tcpdump

-w write grava, -r read lê, -i interface, -nn nada de nomes.

💡 Cabeçalho Received

Leia como camadas de bolo: a de baixo foi a primeira a ser colocada, é a origem.

💡 Confiança da inteligência

Atual (quando), relevante (para quem), preciso (confirmado por quantos).

Tabela de memorização: não confunda

Quando é...	...e quando é
VPN Conecta o usuário à rede inteira; depois do login o alcance é amplo e permite varredura e movimento lateral.	**ZTNA** Conecta o usuário à aplicação, liberada por sessão após checar identidade e postura do aparelho; é a resposta quando o cenário quer acesso mínimo para terceiros.

Playbook Fluxo de decisão para um tipo de incidente, que reduz a variação entre analistas (por exemplo, phishing).	**Runbook** Passos técnicos repetíveis de uma tarefa operacional (por exemplo, reiniciar o coletor de logs).
SPF Pergunta se o IP que enviou consta no registro SPF publicado no DNS do domínio.	**DKIM** Pergunta se a assinatura do domínio confere e se as partes assinadas não foram alteradas em trânsito.
Mascaramento Exibir parcialmente o dado, como os últimos dígitos do cartão na tela do atendente.	**Tokenização** Guardar sem guardar: a aplicação armazena um token no lugar do PAN.
OAuth 2.0 Autorização delegada de acesso a recursos.	**OIDC** Autenticação do usuário, com o ID token em JWT sobre o OAuth 2.0 (asserção XML assinada é SAML).
Honeypot Sistema isca montado para atrair o intruso e registrar o comportamento dele.	**Honeytoken (canary)** Arquivo, credencial ou documento isca que dispara alerta ao ser acessado.
Análise estática (strings) Inspecionar o binário em repouso, sem executar.	**Análise dinâmica (sandbox)** Executar a amostra em ambiente controlado (Cuckoo, Joe Sandbox) e registrar rede, arquivos e processos.

Números que caem

Item	Valor
Peso do domínio na prova	**34% (cerca de 29 das 85 questões)**
Retenção de logs no PCI DSS	**Histórico de pelo menos 12 meses, com os 3 meses mais recentes disponíveis de imediato para análise**
IMDSv2	**Token de sessão obtido por PUT e hop limit da resposta igual a 1**
Logon Type no evento 4624	**10 = RDP (remoto interativo); 3 = rede; 4 = batch (tarefa agendada)**
Regex de 13 a 16 dígitos	**\b\d{13,16}\b (quantificador com chaves e vírgula)**
Linux	**UID 0 é root, qualquer que seja o nome; threads do kernel descendem do kthreadd (PID 2)**
Instâncias do lsass.exe	**Uma só, filha do wininit.exe, em System32**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Concluir que certutil, bitsadmin ou rundll32 são vírus, ou que o certutil está apenas instalando certificado ou atualizando lista de revogação.
Como não cair: São componentes legítimos do Windows; o que denuncia é o uso: download de IP externo, .exe gravado em pasta pública, decodificação de Base64. Instalar certificado usaria parâmetros como -addstore.

⚠ **Alerta de prova:** Aceitar o tráfego como legítimo porque usa HTTPS na porta 443 ou ocorre de madrugada com TLS.
Como não cair: Porta e criptografia não legitimam destino. Periodicidade fixa com tamanho constante é beaconing; grande volume para nuvem não contratada é exfiltração.

⚠ **Alerta de prova:** Ler milhares de subdomínios aleatórios ou rajadas de NXDOMAIN como amplificação DNS, cache expirado ou CDN.
Como não cair: Na amplificação a vítima externa recebe respostas; aqui é um host interno gerando as consultas. Subdomínios codificados com TXT = tunelamento; NXDOMAIN aleatórios = DGA.

⚠ **Alerta de prova:** Chamar de password spraying um cenário de fadiga de MFA ou de impossible travel.
Como não cair: Spraying testa poucas senhas em muitas contas e gera falhas. Se a senha da mesma conta estava certa e houve aprovação ou sucesso, é credencial comprometida.

⚠ **Alerta de prova:** Considerar o e-mail legítimo porque SPF e DKIM passaram, porque está no idioma da vítima ou porque não tem anexo.
Como não cair: O pass só prova que o domínio parecido autorizou o próprio envio. BEC costuma vir sem anexo nem link justamente para escapar dos filtros; olhe o domínio letra por letra e o pedido de dinheiro com sigilo.

⚠ **Alerta de prova:** Buscar a origem do e-mail no Received do topo ou no campo From.
Como não cair: Leia os Received de baixo para cima: o mais ao fundo foi adicionado pelo primeiro servidor da cadeia. O From é facilmente forjado.

⚠ **Alerta de prova:** Acreditar que um processo com nome entre colchetes no ps é thread do kernel.
Como não cair: Colchetes são só exibição e podem ser imitados. Thread do kernel descende do kthreadd (PPID 2), não tem executável em /proc/PID/exe e não roda como www-data.

⚠ **Alerta de prova:** Concluir que a amostra é inofensiva por ter poucas detecções no VirusTotal.
Como não cair: Amostra recente ainda não tem assinatura em muitos motores; decida pelo comportamento (domínios contatados) e pela data da primeira submissão.

⚠ **Alerta de prova:** Tratar Base64 como proteção de segredo ou hash, por exemplo nos Secrets do Kubernetes ou numa credencial no repositório.
Como não cair: Base64 é codificação reversível por qualquer um. Segredo vai para cofre com rotação e auditoria; no Kubernetes, criptografia em repouso no etcd e RBAC restrito.

⚠ **Alerta de prova:** Escolher criptografia de disco ou backup para impedir que um usuário logado leve dados de cartão para fora.
Como não cair: Criptografia de disco protege o equipamento perdido e backup protege disponibilidade. Impedir a saída do dado é papel do DLP de endpoint e de rede.

⚠ **Alerta de prova:** Marcar como problema de precisão um feed com indicadores corretos, porém antigos.
Como não cair: Dado certo e velho falha na atualidade (timeliness). Precisão é confirmação em várias fontes; relevância é aderência ao setor e às tecnologias.

⚠ **Alerta de prova:** Achar que SMS, TOTP ou push resolvem phishing com proxy reverso, ou que exigir MFA no próximo login invalida um token roubado.
Como não cair: Código digitado e push aprovado são repassados em tempo real pelo proxy. FIDO2 e passkeys vinculam a autenticação à origem; com token roubado, revogue as sessões.

⚠ **Alerta de prova:** Resolver alerta ruidoso baixando a gravidade de todos, mandando para a caixa de cada analista ou aumentando a retenção.
Como não cair: O ruído se resolve com tuning da regra que gera o padrão ruidoso, preservando o que é relevante.

⚠ **Alerta de prova:** Na regra YARA, usar any of them ou 1 of them quando o requisito exige as duas strings juntas.
Como não cair: all of them exige todas; any of them e 1 of them disparam com uma só; none of them é o oposto.

Como cai na prova

📝 **Como cai:** Trecho de log, saída de netstat, ps ou comando e a pergunta 'o que isso indica?'
Como resolver: Identifique o binário ou campo-chave, o processo pai, o destino e o horário. Descarte as explicações benignas que não batem com um detalhe concreto (IP externo, pasta pública, conta de serviço fora do padrão, sem chamado aprovado).

📝 **Como cai:** Qual ferramenta ou operação usar (CyberChef, Wireshark, MISP, AbuseIPDB, WHOIS, sandbox, UEBA)
Como resolver: Traduza a tarefa em verbo: decodificar, reconstruir sessão, extrair arquivo, reputação, titularidade, localização, comportamento em execução, desvio de comportamento. Cada verbo tem uma ferramenta; as erradas fazem outra coisa útil.

📝 **Como cai:** Qual sintaxe está correta (filtro tcpdump ou Wireshark, regra Suricata ou Snort, regex, YARA)
Como resolver: Confira token por token: flags trocadas (-w e -r), campos inexistentes (dns.query.name), protocolo errado (udp para HTTPS), classe no lugar de quantificador ([13,16] em vez de {13,16}).

📝 **Como cai:** Cenário de arquitetura pedindo o controle que resolve (acesso de terceiros, privilégio, segredo, metadados da nuvem, OT)
Como resolver: Ataque o vetor descrito: acesso amplo pede ZTNA; privilégio permanente pede PAM com JIT; segredo no código pede cofre; SSRF em metadados pede IMDSv2; OT exposta pede segmentação ou diodo.

📝 **Como cai:** IA no SOC em Escolha DUAS (riscos e uso seguro)
Como resolver: Marque revisão humana, mascaramento de dados sensíveis, privilégio mínimo nas integrações e auditoria. Descarte o que tira o analista da decisão, desliga a auditoria ou envia segredos ao modelo.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Subdomínios longos e codificados em rajada, com consultas TXT, de um só host	**Tunelamento DNS para exfiltração ou C2**
Rajada de NXDOMAIN com nomes sem sentido de uma estação	**Malware usando DGA para achar o C2**
Conexões a intervalos fixos, bytes iguais, sempre ao mesmo destino	**Beaconing de implante de C2**
Push negado várias vezes e aprovado na tentativa seguinte	**Fadiga de MFA com senha já comprometida**
Dois continentes em minutos para a mesma conta, com outro navegador	**Impossible travel: revogar sessões, investigar; antes, conferir se o IP é da saída em nuvem da empresa**
vssadmin delete shadows e evento 1102 de madrugada	**Antiforense e bloqueio da recuperação antes do ransomware**

GPU em região nunca usada e alerta de orçamento, ou system:anonymous criando pod com CPU a 100%	**Cryptomining com credencial comprometida ou API server exposto**
Principal '*' no bucket e milhares de GetObject anônimos de IP externo	**Bucket exposto publicamente sendo drenado**
Login de root sem MFA seguido de StopLogging e DeleteDetector	**Uso anômalo da root tentando cegar o monitoramento**
MAC desconhecido (OUI de Raspberry Pi) varrendo ARP na VLAN de servidores	**Dispositivo rogue; 802.1X com NAC nas portas**
Mesmo SSID, BSSID fora do inventário e autenticação mais fraca	**Evil twin**
Estações recebendo gateway e DNS estranhos de um servidor DHCP desconhecido	**DHCP rogue; DHCP snooping nos switches**
Uma porta (445) testada em milhares de IPs em minutos	**Varredura horizontal preparando movimento lateral**
IEX, DownloadString e -enc, ou authorized_keys, cron.d e chave Run alterados	**Download cradle (execução em memória) e persistência, respectivamente**

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

- O binário legítimo não é o problema; o uso é (LOLBins).
- Beaconing é regularidade e baixo volume; exfiltração é volume; varredura é muitos destinos.
- SPF autoriza IP, DKIM assina e prova integridade, DMARC decide (none, quarantine, reject).
- Na Pyramid of Pain, TTP no topo; IP e hash são atômicos e fáceis de trocar.
- IA ajuda a resumir e correlacionar, mas o analista revisa e decide, com tudo auditado.

Essenciais para a prova (checklist)

- ☐ Sei reconhecer certutil, bitsadmin, rundll32, regsvr32 e wmic usados como LOLBins.
- ☐ Sei o pai e o caminho esperados de lsass.exe, services.exe e svchost.exe.
- ☐ Sei para que servem os eventos 4688, 4624 (tipos 3, 4 e 10), 4625, 4720, 4732, 7045, 4104 e 1102.
- ☐ Sei diferenciar beaconing, tunelamento DNS, DGA e exfiltração em massa pelo padrão de tráfego.
- ☐ Sei montar filtros básicos de tcpdump e Wireshark e ler campos do EVE JSON do Suricata.
- ☐ Sei qual operação do CyberChef usar para Base64, hex, gzip, XOR e -EncodedCommand.
- ☐ Sei classificar um problema de inteligência em atualidade, relevância ou precisão.
- ☐ Sei explicar ZTNA, SASE, PAM com JIT, ABAC, OIDC, SAML e FIDO2 pelo problema que resolvem.
- ☐ Sei a diferença entre playbook, runbook, SOAR, webhook, plug-in e dashboard.

☐ Sei citar os riscos de IA (alucinação, exposição de dados, envenenamento, injeção de prompt) e os controles de cada um.

Questões de revisão do capítulo

R2.1 · Operações de Segurança

Um analista de um banco recupera de um host comprometido um bloco de configuração ofuscado; no hexadecimal, o mesmo byte 5a se repete onde o formato original teria sequências de zeros, indício clássico de XOR com chave de um byte. Qual operação do CyberChef ajuda a recuperar o texto claro sem conhecer a chave?

A. A operação XOR Brute Force, que testa chaves de um byte e mostra as saídas candidatas
B. A operação Gunzip, que descomprime fluxos de dados gravados no formato de compressão gzip
C. A operação From Base64, que decodifica dados que foram representados no formato Base64
D. A operação To Hex, que converte os bytes para a sua representação em hexadecimal

R2.2 · Operações de Segurança

Um analista de uma distribuidora de energia quer criar no SIEM uma busca por criações de processo em que o pai é o WINWORD.EXE e o filho é o powershell.exe ou o wscript.exe, padrão comum de macro maliciosa. Qual evento do log de segurança do Windows traz o processo criado e o processo que o criou?

A. O evento 4624, logon bem-sucedido, com o tipo de logon e a conta autenticada
B. O evento 5140, acesso a compartilhamento de rede, com o nome do compartilhamento
C. O evento 4688, criação de processo, com o novo processo e o processo criador
D. O evento 4634, logoff de conta, com o encerramento da sessão de logon da conta

R2.3 · Operações de Segurança

Uma rede de clínicas com 40 filiais e 300 funcionários remotos envia todo o tráfego de internet para o firewall do data center da matriz, o que gera latência e não protege bem o acesso a aplicações SaaS. A diretoria quer um modelo único de rede e segurança entregue pela nuvem. Qual arquitetura atende a esse objetivo?

A. NAC, validando a postura dos dispositivos antes da conexão às portas das filiais
B. MPLS, substituindo a internet das filiais por enlaces privados até a matriz da rede
C. SASE, unindo SD-WAN e serviços como SWG, CASB, FWaaS e ZTNA entregues pela nuvem
D. SIEM, centralizando os logs das filiais para correlacionar os eventos de navegação

R2.4 · Operações de Segurança

Após confirmar que uma estação de uma fábrica foi comprometida, o analista precisa cortá-la da rede rapidamente, preservando-a para análise, direto do console da ferramenta de endpoint. Qual capacidade de um EDR atende a essa necessidade?

A. A varredura de portas externas do host comprometido feita a partir de um sistema na internet
B. O isolamento de rede do host pela própria plataforma, mantendo o acesso para a investigação
C. A geração de um relatório de vulnerabilidades do sistema operacional instalado naquele host
D. A consulta de reputação do domínio do servidor de atualizações que o host costuma contatar

Respostas comentadas

R2.1. A) A operação XOR Brute Force, que testa chaves de um byte e mostra as saídas candidatas

Por quê: Em XOR de um byte, os zeros do original viram a própria chave; o CyberChef tem a operação XOR Brute Force para testar as chaves e revelar o conteúdo ofuscado (objetivo 1.3).

✗ B) Incorreta. A operação Gunzip descomprime dados em gzip e não reverte uma cifra XOR aplicada ao conteúdo.
✗ C) Incorreta. A operação From Base64 serve a dados em Base64, e o conteúdo descrito foi ofuscado por XOR.
✗ D) Incorreta. A operação To Hex muda a representação dos bytes para hexadecimal, sem decifrar o conteúdo ofuscado.

> **Dica de prova:** Byte repetido no lugar dos zeros sugere XOR de um byte: XOR Brute Force no CyberChef.

R2.2. C) O evento 4688, criação de processo, com o novo processo e o processo criador

Por quê: O evento 4688 do Windows registra a criação de processo com o processo criador, essencial para detectar cadeias como o Word gerando um interpretador de scripts (objetivo 1.3).

✗ A) Incorreta. O evento 4624 trata de logon e registra o tipo de sessão e a conta, e não a árvore de processos.
✗ B) Incorreta. O evento 5140 registra acesso a um compartilhamento de rede, fora do contexto de criação de processos.
✗ D) Incorreta. O evento 4634 marca o logoff da sessão, sem informação sobre criação de processos.

> **Dica de prova:** Processo pai e filho no log de segurança do Windows: evento 4688.

R2.3. C) SASE, unindo SD-WAN e serviços como SWG, CASB, FWaaS e ZTNA entregues pela nuvem

Por quê: SASE converge rede (SD-WAN) e segurança entregue pela nuvem (SWG, CASB, FWaaS, ZTNA) perto do usuário, eliminando o backhaul para o data center e aplicando a mesma política em filiais e no trabalho remoto. (objetivo 1.1)

✗ A) Incorreta. O NAC controla quem conecta à rede local; não protege a navegação de remotos nem o acesso a SaaS.
✗ B) Incorreta. MPLS até a matriz reforça o backhaul que causa a latência e não traz segurança entregue pela nuvem.
✗ D) Incorreta. O SIEM correlaciona eventos, mas não entrega conectividade nem aplica política de acesso no caminho do tráfego.

> **Dica de prova:** Rede e segurança como serviço na nuvem, perto do usuário: SASE.

R2.4. B) O isolamento de rede do host pela própria plataforma, mantendo o acesso para a investigação

Por quê: EDR e XDR oferecem ações de resposta, como o isolamento de rede do endpoint pelo console, limitando o atacante sem perder o acesso investigativo (objetivo 1.3).

✗ A) Incorreta. A varredura de portas externas é uma atividade de reconhecimento, e não a contenção do host comprometido.

✗ C) Incorreta. Um relatório de vulnerabilidades mapeia fraquezas do sistema, mas não contém o host comprometido.

✗ D) Incorreta. Consultar a reputação de um domínio não isola a máquina da rede nem interrompe a ação do atacante.

Dica de prova: Cortar um host da rede pelo console e seguir investigando = isolamento do EDR.

03

CAPÍTULO 3 · 16% DA PROVA

Relatórios e Comunicação

Este é o menor domínio (16%), mas é onde se ganham pontos fáceis ou se perdem por descuido. Cai muito conta de métrica (MTTD, MTTC, média, variação percentual, taxa de cliques, taxa de falsos positivos, cumprimento de SLA), escolha do conteúdo certo para cada público (relatório técnico, sumário executivo, scorecard) e classificação de inibidores de remediação. Também entram declaração e escalonamento de incidentes, comunicação com jurídico, relações públicas, regulador, polícia e clientes, relatório pós-incidente, passagem de turno e relatório interno de threat intelligence. Onde mais erro: usar a mediana no lugar da média, dividir pelo denominador errado e esconder o problema em vez de escalonar.

Neste capítulo

16 tópicos-chave · 13 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Relatório técnico de vulnerabilidades

Responde onde, o quê, prova e como corrigir: host, porta, CVE, evidência da detecção, severidade e correção recomendada. Agrupe os achados pela ação de correção (uma atualização que fecha vários CVEs) e envie a cada responsável os achados dos seus ativos; para desenvolvedores, itens no backlog da equipe dona do código.

Sumário executivo

Impacto financeiro e operacional, situação atual, riscos restantes e decisões pedidas à diretoria, com recomendações priorizadas e custo estimado. Sem jargão, sem cabeçalho de e-mail, sem log: se o diretor precisa de glossário, o sumário falhou. Termina em decisão.

Risk scorecard e top risks

Scorecard dá uma nota por área ou unidade para a liderança comparar e decidir; complementa, não substitui, o relatório técnico. Nota vermelha se explica pelo fator que pesa (itens críticos vencidos, exposição externa) e pelo plano para tirá-la. Top risks combinam probabilidade de exploração com impacto nos ativos e processos críticos, não contagem de achados.

Achados de conformidade

Controle não atendido ou parcialmente atendido é lacuna de conformidade, mesmo sem CVE (por exemplo, ausência de varredura em parte do parque). Benchmark adotado como padrão interno vira requisito e desvio vira achado. FAIL de ASV vira achado: corrigir e revarrer até a varredura aprovada; no PCI DSS, alto risco interno também se corrige e se revarre.

Inibidores de remediação

Contratual: o contrato impede de corrigir sozinho (aciona o fornecedor ou MSP, negocia janela emergencial). Governança organizacional: processo lento (use a mudança emergencial com justificativa ao CAB). Interrupção de processo de negócio: parada no momento errado (janela com a área ou reinício escalonado). Degradação de funcionalidade: o patch quebra algo. Legado: fora de suporte e sem atualização. Proprietário: código fechado, o fabricante corrige. Disponibilidade de patch: sem correção, item aberto com mitigação documentada.

Plano de ação e dependências

Tarefa sem dono e sem prazo não é plano: cada item precisa de responsável, prazo, dependências e critério de conclusão verificado por nova varredura. POA&M registra fraqueza, recursos necessários, marcos com datas, responsável e status. Correção em cadeia (nova imagem base, reconstrução, implantação) exige mapear a sequência e o dono de cada elo.

Métricas de vulnerabilidade

Tendência e top risks para a liderança. Aging: tudo o que passou do SLA está vencido, não só a última faixa. Backlog cresce quando entra mais do que sai. Cumprimento de SLA = corrigidas no prazo dividido pelo total do período. Cobertura de varredura: menos achados com menos ativos varridos não é melhora.

Métricas do SOC

Volume de alertas mostra carga e necessidade de ajuste; taxas de falsos e verdadeiros positivos medem a qualidade da detecção. MTTD vai do início da atividade maliciosa até a detecção; tempo de resposta vai da detecção à primeira ação; tempo de remediação vai da detecção até corrigir a causa; MTTC vai da abertura ao fechamento formal do caso.

Cálculo correto de métricas

Média é soma dividida pela quantidade; não use a mediana (valor central), o máximo ou a moda. Variação percentual é a diferença dividida pelo valor anterior. Defina numerador e denominador antes de calcular e atenção à casa decimal (0,14 = 14%).

Métricas de phishing

Taxa de cliques = cliques divididos pelos e-mails entregues (não pelos enviados, e sem somar quem também enviou dados). Cliques caindo e reportes subindo mostram que a conscientização funciona; zero clique não é meta realista.

Declaração e escalonamento

Nem todo evento é incidente: use os critérios do plano. Sem autoridade para declarar, escalone com evidência e avaliação inicial de impacto. Critério atendido: declare e escalone, o detalhe técnico vem depois. Fato novo e mais grave: reclassifique e escalone; estourou o tempo do plano: escalone, não maquie.

Comunicação com stakeholders

Lista de stakeholders com papéis, contatos e substitutos, mantida antes da crise. Jurídico orienta notificações, contratos e redação externa; relações públicas fala com a imprensa; regulador recebe via jurídico e compliance, com fatos validados pela equipe técnica; polícia é decisão da liderança com o jurídico, por um ponto focal. Clientes: o que houve, o que os afeta, o que devem fazer e contato; cliente corporativo pelo gestor de conta, no prazo do contrato.

Canais e conscientização

Atualizações em horários fixos por um canal definido, com ponto focal, evitam cem ligações. Atacante no e-mail: coordene fora de banda. Golpe em curso: avise quem atende (service desk) pelo canal operacional, com o padrão e como verificar a identidade. Alerta de phishing aos usuários vem do canal oficial, com exemplo e botão de reporte.

Relatório pós-incidente e lições aprendidas

After action report: o que houve, o que funcionou, o que falhou, causa raiz e o que muda. Inclui cronologia detalhada e causa raiz; logs brutos são referenciados, senhas nunca entram, culpados não são apontados. Lições aprendidas: logo após o encerramento, com quem estava lá, foco em processo, e cada lição vira ação com dono e prazo.

Passagem de turno e de incidente

Handover registra status do caso, ações feitas, pendências, evidências coletadas e contatos acionados, escrito no caso e confirmado de viva voz; quem assume continua sem precisar perguntar. Troca de comandante: briefing formal de status, decisões e pendências e anúncio do novo comandante a todos.

Relatório interno de threat intelligence

Inteligência útil fala do seu ambiente: filtra ameaças pelo setor, região e tecnologias e termina em lacuna de cobertura e ação, por exemplo mapeando as TTPs do grupo contra as detecções atuais. Mesma ameaça, dois relatórios: tático (IoCs e TTPs) para o SOC e estratégico (risco e decisões) para a diretoria. TLP: CLEAR sem limite, GREEN comunidade, AMBER organização e clientes que precisam saber, AMBER+STRICT só a organização que recebe, RED só os destinatários.

Macetes para memorizar

Público do relatório

Conselho quer tendência e risco; equipe técnica quer host, CVE e correção.

Métricas de tempo

D de detectar (início até detecção), R de responder (detecção até agir), C de close (abertura até fechar).

Variação percentual

Sempre divida pelo passado: diferença sobre o valor anterior.

Sumário executivo

Impacto, situação, risco e decisão: se precisa de glossário, falhou.

Comunicação externa

Antes de falar para fora, fale com o jurídico; imprensa é com PR.

Plano de ação

Dono, prazo, dependência e prova: sem os quatro não é plano.

Tabela de memorização: não confunda

Quando é...	...e quando é
Relatório técnico Equipes de correção: host, porta, CVE, evidência, severidade e correção.	**Sumário executivo** Diretoria: impacto, situação, riscos e decisões, sem jargão.
MTTD Do início da atividade maliciosa até a detecção.	**MTTC** Da abertura do caso até o encerramento formal.
Média Métrica pedida como tempo médio: soma dividida pela quantidade de casos.	**Mediana** Valor central da lista ordenada; aparece como alternativa errada e esconde casos extremos.
Inibidor contratual Uma cláusula ou contrato com fornecedor ou MSP impede a correção direta.	**Degradação de funcionalidade** O patch existe e foi testado, mas quebra uma função do negócio.
Sistema legado Fora de suporte e sem como atualizar: plano próprio e exceção documentada.	**Sistema proprietário** Código fechado: quem corrige é o fabricante; você acompanha com prazo e mitiga.
TLP:AMBER Pode circular na organização e com clientes que precisam saber para se proteger.	**TLP:AMBER+STRICT** Fica restrito à organização que recebe.

Números que caem

Item	Valor
Peso do domínio na prova	**16% (cerca de 14 das 85 questões)**

Variação percentual	**(valor novo menos valor anterior) dividido pelo valor anterior**
Cumprimento de SLA	**Corrigidas no prazo dividido pelo total do período**
Taxa de cliques em phishing	**Cliques divididos pelos e-mails entregues**
Níveis de TLP	**CLEAR, GREEN, AMBER, AMBER+STRICT e RED**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Responder a média com a mediana, o maior valor ou o valor mais frequente.
Como não cair: Some todos os valores e divida pela quantidade de casos; confira se não contou um caso a mais ou a menos.

⚠ **Alerta de prova:** Calcular a variação percentual dividindo pelo valor final ou dando a diferença absoluta.
Como não cair: Variação = (novo menos anterior) dividido pelo anterior. De 120 para 90 é queda de 25%, não 30 nem 33,3%.

⚠ **Alerta de prova:** Calcular a taxa de cliques sobre os e-mails enviados ou somando cliques com envios de dados.
Como não cair: Use cliques divididos pelos e-mails entregues; quem clicou e enviou dados não conta duas vezes.

⚠ **Alerta de prova:** Na taxa de falsos positivos, excluir os inconclusivos da base ou responder a taxa de verdadeiros positivos.
Como não cair: Siga a definição adotada (normalmente sobre o total triado) e confira se o número pedido é FP ou TP.

⚠ **Alerta de prova:** Usar as corrigidas no prazo como denominador do cumprimento de SLA, ou contar as corrigidas fora do prazo.
Como não cair: SLA cumprido = no prazo dividido pelo total do período; corrigir depois do prazo não cumpre o SLA.

⚠ **Alerta de prova:** No aging, considerar vencidas só as da faixa acima de 90 dias.
Como não cair: Toda faixa acima do SLA está vencida; a faixa dentro do SLA é a única em dia.

⚠ **Alerta de prova:** Comemorar menos achados quando menos ativos foram varridos.
Como não cair: Olhe a cobertura de varredura: menos achados com menos ativos não é melhora.

⚠ **Alerta de prova:** Fechar o item porque a mitigação foi aplicada ou tirá-lo dos indicadores porque o patch não existe.
Como não cair: Mitigação reduz risco, mas não é correção: o item fica aberto, com patch indisponível, mitigação e acompanhamento do fabricante registrados.

⚠ **Alerta de prova:** Rebaixar a severidade, reabrir o chamado ou reiniciar o caso para fugir do gatilho de escalonamento.
Como não cair: Isso distorce o registro e esconde o atraso; escalone pelo caminho do plano com situação e bloqueios.

⚠ **Alerta de prova:** Deixar o analista responder à imprensa, notificar o regulador ou o fornecedor notificar em nome da empresa.
Como não cair: Imprensa vai para relações públicas; regulador recebe via jurídico e compliance; a obrigação é da organização regulada, o analista fornece fatos.

⚠ **Alerta de prova:** Fazer lições aprendidas meses depois, sem a equipe técnica, apontando erros de colegas.
Como não cair: Logo após o encerramento, com os envolvidos, sem culpados e com ações que têm dono e prazo.

⚠ **Alerta de prova:** Classificar como inibidor contratual ou de governança um patch que quebra as impressoras ou o ERP no fechamento.
Como não cair: Patch que quebra função é degradação de funcionalidade; parada no momento crítico é interrupção de processo de negócio. Contratual exige contrato no cenário.

⚠ **Alerta de prova:** Escolher TLP:RED para um relatório que as equipes internas precisam usar.
Como não cair: RED fica só com os destinatários individuais e impede a ação; AMBER+STRICT restringe à organização que recebe.

Como cai na prova

📝 **Como cai:** Tabela de tempos ou contagens e a pergunta pela média, taxa ou variação
Como resolver: Identifique a métrica e sua definição (intervalo de início e fim, numerador e denominador), calcule e confira contra as alternativas-armadilha: mediana, máximo, soma sem dividir, base trocada.

📝 **Como cai:** Qual conteúdo incluir no relatório para um público (diretoria, comitê, equipe de correção, cliente)
Como resolver: Diretoria e comitê: impacto, tendência, top risks e decisão. Equipe técnica: host, CVE, evidência e correção. Cliente: o que houve, o que o afeta, o que fazer e contato.

📝 **Como cai:** Cenário em que a correção não pode ser aplicada e a pergunta sobre o tipo de inibidor ou a ação
Como resolver: Ache o bloqueio real (contrato, comitê, parada do negócio, função quebrada, fora de suporte, código fechado, sem patch), registre o inibidor e escolha a ação que mantém o risco visível e com prazo.

📝 **Como cai:** Quem deve ser acionado ou comunicado (jurídico, PR, regulador, polícia, RH, gestor de conta)
Como resolver: Siga o plano: cada público tem dono e canal. Descarte o analista falando para fora, avisos em massa e contatos informais.

📝 **Como cai:** Gatilho de declaração ou escalonamento atingido durante a análise
Como resolver: Declare ou escalone no prazo com o que já tem; o detalhe técnico continua em paralelo. Nunca rebaixe a severidade para evitar o gatilho.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Contrato com fornecedor ou MSP define quem e quando pode corrigir	**Inibidor contratual: registrar e negociar janela emergencial**
Patch testado quebra uma função usada pelo negócio	**Degradação de funcionalidade**
Sistema fora de suporte sem atualização possível	**Inibidor de sistema legado com plano próprio e exceção**
Sistema 24x7 ou ERP no fechamento contábil	**Interrupção de processo de negócio: janela combinada ou reinício escalonado**
Comitê de mudanças lento e exploração ativa	**Mudança emergencial prevista no processo, com justificativa ao CAB**
Uma atualização resolve dezenas de achados	**Agrupar o relatório pela ação de correção**
CVE entrou no KEV e o ativo é exposto	**Escalonamento previsto, prazo reduzido e aviso ao dono do ativo**
Jornalista ligou para o SOC	**Encaminhar para relações públicas, sem comentar**

Atacante com acesso ao e-mail corporativo	**Canal fora de banda previsto no plano**
Do início do ataque até o alerta	**MTTD**
Da abertura ao encerramento formal do caso	**MTTC**
Menos alertas e os mesmos incidentes reais	**O tuning funcionou: menos ruído e taxa de verdadeiros positivos maior**
Entram mais achados por mês do que são corrigidos	**Backlog crescendo; capacidade de correção abaixo da detecção**
Diretoria e SOC querendo o mesmo relatório de ameaça	**Dois relatórios: estratégico para a diretoria, tático para o SOC**

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

- Média não é mediana: some tudo e divida pela quantidade.
- Defina numerador e denominador antes de qualquer taxa.
- Corrigido é o que a nova varredura não encontra mais; mitigado continua aberto.
- Comunicação externa passa pelo jurídico, imprensa vai para PR e regulador vai via jurídico e compliance.
- Escalone pelo plano em vez de esconder atraso ou rebaixar severidade.

Essenciais para a prova (checklist)

☐ Sei o que vai no relatório técnico, no sumário executivo e no scorecard.

☐ Sei calcular média, variação percentual, taxa de cliques, taxa de FP e TP e cumprimento de SLA.

☐ Sei os intervalos de MTTD, tempo de resposta, tempo de remediação e MTTC.

☐ Sei classificar os inibidores de remediação: contratual, governança, processo de negócio, degradação, legado, proprietário e patch indisponível.

☐ Sei montar um plano de ação com dono, prazo, dependências e critério de verificação.

☐ Sei quem comunica com imprensa, regulador, polícia, clientes e funcionários.

☐ Sei o que entra e o que não entra num relatório pós-incidente.

☐ Sei fazer uma passagem de turno e de comando completa.

☐ Sei adaptar um relatório de threat intelligence ao ambiente e escolher o TLP certo.

Questões de revisão do capítulo

R3.1 · Relatórios e Comunicação

Uma vulnerabilidade de execução remota de código num firewall de borda de uma transportadora foi divulgada hoje, com exploração ativa, e o fabricante ainda não publicou correção, só uma mitigação temporária. Como o item deve aparecer no relatório de remediação?

A. Marcar o item como corrigido depois de aplicar a mitigação temporária recomendada
B. Registrar o patch indisponível, a mitigação aplicada e o acompanhamento do fabricante
C. Encerrar o item, já que a remediação depende do fabricante e não da transportadora
D. Retirar o item do relatório até que o fabricante publique a versão corrigida do sistema

R3.2 · Relatórios e Comunicação

Uma universidade usa os CIS Controls v8 como referência. Uma avaliação mostra que as varreduras autenticadas cobrem os servidores, mas estações de trabalho e ativos expostos à internet não são varridos. Como apresentar esse resultado?

A. Reportar como vulnerabilidade de software, com CVE e pontuação para cada estação
B. Reportar como incidente de segurança, acionando o plano de resposta a incidentes da universidade
C. Reportar como conformidade plena, já que os servidores são os ativos mais críticos
D. Reportar como lacuna de conformidade no controle de gestão contínua de vulnerabilidades

R3.3 · Relatórios e Comunicação

Num hospital, o scanner encontra vulnerabilidades críticas no sistema operacional de um tomógrafo. O fabricante já publicou a correção, mas o contrato proíbe que o hospital instale atualizações sem homologação dele, sob pena de perder a garantia e o suporte. Como esse impedimento deve aparecer no relatório?

A. Um falso positivo, porque equipamentos médicos não são cobertos pelo scanner corporativo
B. Uma falha de governança interna, a ser resolvida pelo comitê de mudanças do hospital
C. Um inibidor contratual, com o fornecedor acionado para homologar e liberar a correção
D. Um caso de patch indisponível, já que o tomógrafo ainda aguarda uma correção do fabricante

R3.4 · Relatórios e Comunicação

Num SOC 24x7 de uma operadora de saúde, o turno da noite assume um caso de contenção em andamento, mas a passagem foi uma mensagem curta no chat: 'caso do RH em contenção, ver depois'. Duas horas depois, um host isolado é reconectado por engano. Qual prática teria evitado o problema?

A. Redução do número de casos abertos por turno, transferindo os casos para o dia seguinte
B. Extensão do turno da noite até o encerramento completo do caso que estava em contenção
C. Mensagens mais curtas no chat, para que o turno seguinte consiga ler tudo com rapidez
D. Passagem estruturada, registrada no caso e confirmada em conversa com quem assume o turno

Respostas comentadas

R3.1. B) Registrar o patch indisponível, a mitigação aplicada e o acompanhamento do fabricante

Por quê: Disponibilidade de patch é inibidor de remediação: quando não há correção, o relatório mantém o item aberto, registra mitigações e acompanha o fornecedor. (objetivo 4.1)

✗ A) Incorreta. Mitigação reduz risco, mas não é correção; o item fica aberto até o patch.

✗ C) Incorreta. O risco é da transportadora, mesmo que a correção dependa do fabricante.

✗ D) Incorreta. Tirar o item esconde uma exposição ativa da liderança.

> **Dica de prova:** Sem patch, o item fica aberto com mitigação documentada.

R3.2. D) Reportar como lacuna de conformidade no controle de gestão contínua de vulnerabilidades

Por quê: Achados de conformidade com frameworks como CIS Controls apontam o controle não atendido e a lacuna observada, e entram no relatório com plano e prazo. (objetivo 4.1)

✗ A) Incorreta. Ausência de varredura é falha de processo, sem CVE associado.

✗ B) Incorreta. Lacuna de processo não é incidente; não houve evento adverso confirmado.

✗ C) Incorreta. Cobrir só os servidores deixa parte do controle sem atendimento.

> **Dica de prova:** Controle parcialmente atendido é lacuna de conformidade.

R3.3. C) Um inibidor contratual, com o fornecedor acionado para homologar e liberar a correção

Por quê: Acordos contratuais (garantia, SLA, homologação do fornecedor) são inibidores de remediação: a correção depende do fornecedor, e o relatório registra o bloqueio, o contato e o prazo. (objetivo 4.1)

✗ A) Incorreta. O achado é real; o tipo de equipamento não torna a vulnerabilidade inexistente.

✗ B) Incorreta. O comitê interno não pode afastar uma obrigação contratual com o fabricante.

✗ D) Incorreta. A correção já existe; o bloqueio é o contrato, não a falta de patch.

> **Dica de prova:** Contrato impede de corrigir sozinho: inibidor contratual, aciona o fornecedor.

R3.4. D) Passagem estruturada, registrada no caso e confirmada em conversa com quem assume o turno

Por quê: A passagem de turno ou de incidente deve ser estruturada, registrada no sistema de casos e confirmada com quem assume, incluindo restrições ativas como hosts isolados. (objetivo 4.2)

✗ A) Incorreta. Empurrar casos para outro turno atrasa a resposta sem melhorar a passagem.

✗ B) Incorreta. Estender turnos causa fadiga e não resolve a falta de registro.

✗ C) Incorreta. O problema foi falta de informação; mensagens ainda mais curtas pioram.

> **Dica de prova:** Handover: escrito no caso e confirmado de viva voz.

04

CAPÍTULO 4 · 24% DA PROVA

Resposta e Gestão de Incidentes

Este domínio vale 24% e gira em torno do ciclo de resposta: preparação, detecção, análise, contenção, erradicação, recuperação e pós-incidente. A prova pede para dizer em que fase está uma ação, ordenar passos, escolher a melhor contenção sob restrição do negócio e mapear eventos na Cyber Kill Chain, no Diamond Model e no MITRE ATT&CK. Também cai coleta de evidências (volatilidade, hash, cadeia de custódia, legal hold), linha do tempo com fusos, severidade, priorização, escalonamento e causa raiz. Onde mais erro: confundir detecção com análise e erradicação com recuperação, escolher desligar quando o certo é isolar, restaurar o backup mais recente e ordenar eventos por horário bruto sem converter para UTC.

Neste capítulo

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

Tópicos-chave

Ciclo de resposta a incidentes

Preparação, detecção, análise, contenção, erradicação, recuperação e pós-incidente, que alimenta de volta a preparação. Se surge host comprometido novo, volta-se à análise para refazer o escopo antes de seguir. Erradicar sem conter avisa o atacante; restaurar sem erradicar devolve um ambiente comprometido.

Preparação

Tudo o que acontece antes de o alarme tocar: adquirir e testar ferramentas forenses, manter a lista de contatos, instalar sensores, escrever playbooks e treinar. Melhorias decididas no pós-incidente são implantadas como preparação.

Detecção x análise

Detecção é o sinal chegando: alerta do SIEM ou EDR, usuário que liga relatando, aviso externo. Análise é investigar, validar (verdadeiro ou falso positivo) e dimensionar o escopo: quantos hosts, com busca ativa de IoCs. Falso positivo se prova com contexto, como uma mudança aprovada.

Contenção

Limitar o dano preservando evidências: isolar pela função do EDR mantendo a máquina ligada, mover para VLAN de quarentena pelo NAC, suspender a conta e bloquear a origem, suspender a VM pelo hipervisor. Na nuvem: security group de isolamento, captura de memória e snapshot antes de encerrar; no Kubernetes: retirar os rótulos do pod do seletor e aplicar NetworkPolicy. Ativo crítico que não pode parar: cortar o C2 e vigiar.

Erradicação

Remover tudo o que o atacante deixou e fechar a porta de entrada: web shell, contas criadas, persistências, falha explorada, credenciais expostas. Achou três persistências, procure a quarta. Golden ticket se erradica trocando a senha da krbtgt duas vezes, com replicação entre as trocas; segredo vazado se revoga e reemite.

Recuperação

Voltar a operar com segurança: reconstruir de fonte confiável, restaurar do backup anterior à persistência, seguir a ordem de dependência (identidade, dados, aplicação) e manter monitoramento reforçado com os IoCs e TTPs do caso. Sair do isolamento exige critérios cumpridos (vetor fechado, verificação limpa) e aprovação formal do líder do incidente.

Pós-incidente

Reunião de revisão depois do encerramento, com lições aprendidas, linha do tempo e causa raiz. A causa raiz é o processo ou controle que, corrigido, impede a repetição, não a pessoa nem o sintoma. Ação corretiva boa tem o quê, quem, até quando e como verificar, e se fecha com teste.

Cyber Kill Chain

Sete fases: reconnaissance (pesquisar alvos), weaponization (montar o artefato, ainda não enviado), delivery (enviar), exploitation (código sendo executado na vítima), installation (persistência), command and control (beacon) e actions on objectives (criptografar, exfiltrar). Quebre a corrente no elo mais à esquerda possível: sandbox no gateway de e-mail age na delivery.

Diamond Model

Quatro vértices: adversário (quem), capacidade (ferramenta ou malware), infraestrutura (domínios, IPs, servidores de C2) e vítima (contas e ativos atacados). Timestamp, resultado, direção e fase são meta-características. Serve para agrupar intrusões por elementos em comum e para pivotear: um IP leva a domínios, que levam ao adversário.

MITRE ATT&CK

Tática é o porquê (por exemplo, Credential Access, TA0006), técnica é o como, subtécnica é o como em detalhe e procedimento é o jeito específico daquele grupo. Exemplos cobrados: T1053.005 Scheduled Task, T1547.001 Registry Run Keys. Há matrizes Enterprise, Mobile (Android e iOS) e ICS (CLP, IHM, SCADA). Cobertura de detecção se mede em técnicas e se valida com teste do Atomic Red Team.

Coleta de evidências

Do mais volátil ao menos volátil: rede e memória antes do disco. Ameaça sem arquivo exige capturar a RAM antes de desligar, com hash do arquivo gerado. No disco: fotografar e documentar, conectar bloqueador de escrita, calcular hash da origem, gerar imagem e conferir o hash. Antes de reimagem: memória, disco, hash e custódia.

Integridade, cadeia de custódia e legal hold

Hash não tem meio-termo: igual ou diferente; se não bate, documente, descarte a cópia e refaça do original. Toda troca de mãos registra quem entregou, quem recebeu, quando e assinaturas, e o hash é conferido na saída e na chegada. Legal hold vence a política de retenção no escopo do caso e só termina com liberação do jurídico.

Linha do tempo

Normalize tudo para UTC antes de ordenar e corrija o desvio de relógio (relógio adiantado: subtraia). Perto da meia-noite o fuso muda também o dia. Ordem impossível, como persistência antes da entrada, denuncia fuso não convertido. Primeira tentativa não é primeiro acesso: o acesso é o 4624 depois dos 4625.

Categorias de impacto

Impacto funcional: nenhum, baixo, médio (serviço crítico perdido para parte dos usuários) e alto (nenhum usuário recebe o serviço crítico). Impacto informacional: privacidade, informação proprietária e integridade (dado alterado ou apagado). Recuperabilidade: regular (recursos atuais), suplementada (previsível com recursos adicionais), estendida (imprevisível) e não recuperável (dados publicados).

Triagem, priorização e escalonamento

Incidentes simultâneos se ordenam pela matriz do plano, não pela ordem de chegada. Sobe na fila o que envolve ativo crítico, conta privilegiada, dado regulado e atividade em curso; o que foi bloqueado ou ficou em quarentena fica no nível 1. Gatilho do plano atingido: escalone no prazo, com o que já tem, pelo canal previsto (inclusive de madrugada).

Correlação e enriquecimento

Correlação liga eventos de fontes diferentes por usuário e janela de tempo (crachá dentro e VPN de fora). Enriquecimento anexa contexto ao evento: ativo vindo da CMDB, usuário vindo do diretório e do RH, GeoIP, reputação de IP via API. Agregação reduz duplicidade, mas pode apagar diferenças de criticidade.

Papéis e comunicação na resposta

Uma crise, um líder: o líder do incidente é o ponto único de coordenação, e a autoridade vem do plano de resposta aprovado pela alta direção. Na dúvida legal, jurídico; suspeito funcionário, RH com o jurídico; ameaça interna se escala em sigilo, sem confrontar. Atacante no e-mail ou no tenant: use o canal fora de banda previsto no plano.

Treinamento e plano x playbook

Tabletop é exercício de mesa baseado em discussão, para testar decisões; simulação executa técnicas reais em ambiente controlado. O plano de resposta diz quem decide e por quê; o playbook diz o que fazer passo a passo num cenário (por exemplo, ransomware).

Macetes para memorizar

Fases da resposta

Prepara, detecta, analisa, contém, erradica, recupera e aprende; o aprendizado volta para a preparação.

Cyber Kill Chain

Reco, arma, entrega, explora, instala, comanda e age: 7 passos, quebre o mais à esquerda.

Diamond Model

Quem, com quê, por onde e contra quem; o resto é meta.

ATT&CK

Tática é o porquê; técnica é o como; procedimento é o como daquele grupo.

Erradicar x recuperar

Remover é erradicar; restaurar é recuperar.

Contenção com evidência

Ransomware ativo: isole, não desligue. VM: suspenda. Nuvem: isole, memória, snapshot, só depois encerre.

Volatilidade

Primeiro o que some: rede e memória; depois o que fica: disco e arquivo.

Tabela de memorização: não confunda

Quando é...	...e quando é
Detecção O alerta chegou ou alguém avisou (usuário, parceiro externo).	**Análise** O alerta está sendo investigado, validado e dimensionado (quantos hosts, qual vetor).
Contenção Limitar o dano agora: isolar, bloquear C2, suspender conta, mantendo evidências.	**Erradicação** Arrancar a causa: remover persistência, contas e artefatos e corrigir o vetor.

Erradicação Remover o que o atacante criou.	**Recuperação** Restaurar e reconstruir de fonte confiável e voltar a operar com monitoramento reforçado.
Precursor Sinal de que um incidente pode ocorrer (varreduras, anúncio de ataque) sem exploração.	**Indicador** Sinal de que o incidente ocorreu ou está ocorrendo.
Tabletop Sala de reunião e perguntas, sem mexer no ambiente, para testar quem decide.	**Simulação** Mão no teclado: execução real de técnicas em ambiente controlado.
Remediação Mira o caso: remover o artefato, fechar o vetor, trocar credenciais e verificar.	**Ação corretiva** Mira a causa raiz de processo, para não repetir (por exemplo, conciliar inventário com varredura externa).
Cyber Kill Chain Ordenar as fases de uma intrusão e escolher onde quebrar a corrente.	**Diamond Model** Relacionar adversário, capacidade, infraestrutura e vítima e agrupar intrusões diferentes.

Números que caem

Item	Valor
Peso do domínio na prova	**24% (cerca de 20 das 85 questões)**
Fases da Cyber Kill Chain	**7**
Vértices do Diamond Model	**4 (adversário, capacidade, infraestrutura, vítima)**
Recuperabilidade (NIST SP 800-61r2)	**4 categorias: regular, suplementada, estendida, não recuperável**
Impacto funcional (NIST SP 800-61r2)	**Nenhum, baixo, médio, alto**
Senha da krbtgt após golden ticket	**Trocar 2 vezes, aguardando a replicação entre as trocas**
IDs do ATT&CK cobrados	**T1053.005 Scheduled Task; T1547.001 Registry Run Keys; T1003.001 LSASS Memory; TA0006 Credential Access**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Desligar a máquina com ransomware ativo ou o host com beacon para parar o ataque.
Como não cair: Desligar destrói a memória volátil. Isole pela rede (EDR ou NAC) mantendo ligado; VM se suspende pelo hipervisor, que grava a memória em arquivo.

⚠ **Alerta de prova:** Reiniciar o servidor para eliminar processo injetado ou ameaça sem arquivo.
Como não cair: Reiniciar apaga a RAM, onde está o artefato, e não remove a persistência que o recarrega. Capture a memória primeiro.

⚠ **Alerta de prova:** Restaurar o backup mais recente para voltar mais rápido.
Como não cair: O mais recente provavelmente já contém a persistência. Use o último anterior à persistência ou verifique as cópias novas contra os IoCs.

⚠ **Alerta de prova:** Restaurar arquivos antes de conter a estação que está cifrando.
Como não cair: Os arquivos recuperados seriam cifrados de novo. Em criptografia via SMB, isole quem cifra, não quem é cifrado.

⚠ **Alerta de prova:** Trocar a senha ou exigir MFA de novo e considerar a conta resolvida, ou excluir a conta comprometida.
Como não cair: Senha nova não mata token velho: bloqueie o login, revogue sessões e tokens, revise regras de caixa e métodos de MFA. Excluir a conta apaga artefatos da investigação.

⚠ **Alerta de prova:** Apagar o commit com o segredo e seguir em frente.
Como não cair: Clones e forks mantêm o histórico. Revogue e reemita o segredo, limpe o histórico e rode varredura de segredos.

⚠ **Alerta de prova:** Considerar o host limpo porque ficou sem alertas, porque o chamado foi fechado ou porque ninguém reclamou.
Como não cair: Verificação é ativa: caçar os mesmos IoCs e persistências no parque e repetir a varredura.

⚠ **Alerta de prova:** Ordenar eventos pelos horários brutos de fontes com fusos diferentes ou somar o desvio de um relógio adiantado.
Como não cair: Converta tudo para UTC e subtraia o adiantamento antes de ordenar.

⚠ **Alerta de prova:** Aceitar um hash que difere em poucos caracteres ou culpar o algoritmo.
Como não cair: SHA-256 é determinístico: qualquer diferença indica alteração. Registre, não use a cópia e gere outra do original; nunca sobrescreva o hash de referência.

⚠ **Alerta de prova:** Apontar como causa raiz o operador, o script exposto ou a porta aberta.
Como não cair: Isso é pessoa, causa intermediária ou sintoma. Causa raiz é a falta de processo ou controle (gestão de segredos, verificação no pipeline, rotina de teste de restauração).

⚠ **Alerta de prova:** Fechar falso positivo pedindo exceção para a pasta inteira do agente.
Como não cair: Exceção boa é estreita: hash e assinatura do binário legítimo.

⚠ **Alerta de prova:** Confrontar o funcionário suspeito ou avisar o gestor dele por e-mail.
Como não cair: Ameaça interna se escala em sigilo ao líder de resposta pelo canal do plano, com RH e jurídico; confrontar pode levar à destruição de evidências.

⚠ **Alerta de prova:** Responder a golden ticket trocando a senha dos administradores ou reiniciando os controladores de domínio.
Como não cair: Os tickets forjados são assinados pela chave da krbtgt: troque a senha da krbtgt duas vezes, aguardando a replicação.

⚠ **Alerta de prova:** Classificar como contenção ou recuperação a reunião de revisão que define melhorias.
Como não cair: A reunião de revisão do incidente encerrado é pós-incidente; as melhorias que saem dela é que vão para a preparação.

Como cai na prova

📝 **Como cai:** Uma ação descrita e a pergunta 'em que fase do processo ela se encaixa?'
Como resolver: Pergunte em ordem: há incidente? O sinal acabou de chegar (detecção)? Está sendo investigado (análise)? Está limitando dano (contenção)? Removendo (erradicação)? Restaurando (recuperação)? Já encerrou (pós-incidente)?

📝 **Como cai:** Lista numerada de passos para colocar na ordem certa (resposta ou coleta forense)
Como resolver: Classifique cada passo pela fase antes de ordenar. Na forense: documentar, bloqueador de escrita, hash, imagem, conferir hash; na resposta: detectar, analisar, conter, erradicar, recuperar, revisar.

📝 **Como cai:** Melhor primeira ação ou contenção com restrição de negócio (linha de produção, pagamentos, ativo crítico)
Como resolver: Escolha a que contém sem destruir evidência e respeita a restrição: isolamento lógico, quarentena NAC, bloqueio do C2 com monitoramento. Descarte desligar, formatar, excluir e restaurar antes de conter.

📝 **Como cai:** Eventos de fontes com fusos e relógios diferentes e a pergunta sobre o primeiro acesso ou a ordem
Como resolver: Converta para UTC, corrija o desvio de relógio, confira se a data muda, ordene e verifique se a sequência faz sentido (entrada antes de persistência).

📝 **Como cai:** Evento para mapear na Kill Chain, no Diamond Model ou no ATT&CK
Como resolver: Identifique o que o evento mostra de fato (envio, execução, persistência, comunicação, impacto; ferramenta, servidor, alvo; objetivo ou método) e não a fase anterior ou seguinte.

📝 **Como cai:** Vários incidentes ao mesmo tempo para priorizar ou escalar
Como resolver: Aplique a matriz do plano: atividade em curso, conta privilegiada, dado regulado e ativo crítico vão para o topo; eventos já contidos ficam no nível 1.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Artefato montado, mas ainda não enviado	**Weaponization**
Chave Run ou tarefa agendada gravada após o anexo	**Installation**
Host interno chamando para fora em intervalos fixos	**Command and Control**
w3wp.exe executando whoami logo após um POST malicioso, ainda sem arquivo gravado nem persistência	**Exploitation (com web shell gravado e persistência, já é Installation)**
Arquivos cifrados ou dados levados	**Actions on objectives**
Navegação no site, mapeamento de pessoas e DNS, transferência de zona negada	**Reconnaissance**
Usuário ligou ou parceiro externo avisou	**Fase de detecção**
Ferramenta usada x domínio que ela contata	**Vértice de capacidade x vértice de infraestrutura**
Detalhe de qual ferramenta, parâmetros e destino um grupo específico usou	**Procedimento (não técnica nem subtécnica)**
Celular corporativo ou CLP, IHM e SCADA	**Matriz ATT&CK Mobile ou ATT&CK for ICS**
Dados já publicados na internet	**Recuperabilidade: não recuperável, com ou sem backup**
Prazo previsível, mas dependendo de reforço externo	**Recuperabilidade suplementada**
Crachá registrado no prédio e VPN vinda de fora no mesmo horário	**Correlação de log físico com log lógico**
Serviço crítico parado para uma unidade e funcionando nas outras	**Impacto funcional médio**

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

- Isolar, não desligar: a memória é evidência.
- Backup bom é o anterior à persistência, não o mais recente.
- Linha do tempo só depois de normalizar para UTC.
- Senha nova não invalida token roubado: revogue as sessões.
- Causa raiz é processo ou controle, nunca a pessoa.

Essenciais para a prova (checklist)

- ☐ Sei classificar qualquer ação em uma das sete fases do processo de resposta.
- ☐ Sei dar exemplos de contenção que preservam evidências em host, VM, nuvem e Kubernetes.
- ☐ Sei ordenar as 7 fases da Cyber Kill Chain e localizar um evento nelas.
- ☐ Sei identificar os quatro vértices do Diamond Model e as meta-características.
- ☐ Sei diferenciar tática, técnica, subtécnica e procedimento no ATT&CK e escolher a matriz certa.
- ☐ Sei a ordem de volatilidade e os passos da aquisição forense de disco.
- ☐ Sei o que registrar na cadeia de custódia e quando o legal hold termina.
- ☐ Sei montar uma linha do tempo convertendo fusos e corrigindo desvio de relógio.
- ☐ Sei classificar impacto funcional, informacional e recuperabilidade.
- ☐ Sei escrever uma ação corretiva com o quê, quem, prazo e verificação.

Questões de revisão do capítulo

R4.1 · Resposta e Gestão de Incidentes

O SIEM de uma construtora gera o alerta de impossible travel para a usuária carla.n: login às 10:02 UTC a partir de Porto Alegre e às 10:19 UTC a partir de Fortaleza. Na triagem, o analista verifica que o IP do segundo login, 203.0.113.18, pertence ao ponto de saída do serviço SASE contratado pela empresa, que encaminha o tráfego dos usuários remotos, e que o dispositivo, o navegador e o fator de MFA são os mesmos dos acessos habituais dela. Como o alerta deve ser tratado?

A. Encerrar sem registro, já que alertas de geolocalização não têm valor para o SOC
B. Classificar como verdadeiro positivo e bloquear a conta até a usuária se apresentar ao SOC
C. Classificar como falso positivo e pedir o ajuste da regra com os IPs de saída do SASE
D. Escalar ao nível 3 como comprometimento de conta e abrir incidente de severidade 1

R4.2 · Resposta e Gestão de Incidentes

Às 02h10 o SIEM de um banco dispara 'Possible brute force: 38 x EventID 4625 followed by 4624 (LogonType 4) for user ops.batch from 10.20.4.77'. O analista de plantão consulta o inventário, vê que 10.20.4.77 é o servidor de agendamento cujo job usa ops.batch com senha recém-trocada, confirma com o dono do sistema e conclui que não houve atividade maliciosa. Em qual fase do processo de resposta o analista estava trabalhando?

A. Detecção
B. Contenção
C. Análise
D. Erradicação

R4.3 · Resposta e Gestão de Incidentes

Um hospital já tem um plano de resposta a incidentes que define missão, autoridade, papéis e comunicação. A coordenadora do SOC quer agora um documento com os passos e os pontos de decisão específicos para quando o EDR detectar criptografia em massa: quem isolar, como verificar os backups e quando acionar a diretoria. Qual documento deve ser criado?

A. Um plano de continuidade de negócios
B. Um acordo de nível de serviço do SOC
C. Uma política de segurança da informação
D. Um playbook de resposta a ransomware

R4.4 · Resposta e Gestão de Incidentes

Após uma campanha de phishing numa seguradora, três caixas do Microsoft 365 tinham regras de encaminhamento externo para recibos@empresa-exemplo.net. O analista removeu as regras, redefiniu as senhas e revogou as sessões. Qual etapa de verificação confirma melhor que a remediação está completa?

A. Buscar no tenant inteiro regras de encaminhamento e consentimentos OAuth semelhantes
B. Aguardar uma semana sem reclamações dos usuários afetados e encerrar o caso
C. Conferir se o alerta do filtro antiphishing foi fechado no console de segurança do Microsoft 365
D. Pedir aos três usuários que confirmem por e-mail que receberam as novas senhas

Respostas comentadas

R4.1. C) Classificar como falso positivo e pedir o ajuste da regra com os IPs de saída do SASE

Por quê: Triagem é confirmar ou descartar o alerta com contexto (origem do IP, dispositivo, MFA, mudanças conhecidas); falso positivo comprovado é fechado com justificativa e gera ajuste da regra. (objetivo 3.3)

✗ A) Incorreta. Todo fechamento precisa de registro da justificativa, e a regra tem valor quando ajustada ao ambiente.

✗ B) Incorreta. Os dados da triagem explicam o deslocamento aparente; bloquear a conta traria impacto ao negócio sem indício de ameaça.

✗ D) Incorreta. Escalar sem indício de comprometimento consome o nível 3 e infla os incidentes.

> **Dica de prova:** Falso positivo confirmado: feche com justificativa e ajuste a regra.

R4.2. C) Análise

Por quê: A detecção gera o sinal (alerta, relato, aviso externo); a análise valida esse sinal, separa falso de verdadeiro positivo e determina o escopo antes de qualquer contenção. (objetivo 3.2)

✗ A) Incorreta. A detecção foi o disparo do alerta pelo SIEM; o que o analista fez depois foi analisar e validar.

✗ B) Incorreta. Nenhuma ação para limitar dano foi tomada, e nem seria necessária num falso positivo.

✗ D) Incorreta. Não houve remoção de artefatos maliciosos, pois o evento era legítimo.

> **Dica de prova:** Alerta chegou: detecção. Alerta investigado e validado: análise.

R4.3. D) Um playbook de resposta a ransomware

Por quê: O plano de resposta a incidentes é estratégico (missão, autoridade, papéis); playbooks são táticos e específicos por tipo de incidente, como ransomware, phishing ou conta comprometida, com passos e pontos de decisão. (objetivo 3.3)

✗ A) Incorreta. O plano de continuidade mantém processos críticos em interrupções, não guia a resposta técnica ao ransomware.

✗ B) Incorreta. Um SLA fixa prazos e níveis de serviço, mas não descreve como responder ao incidente.

✗ C) Incorreta. A política define diretrizes gerais e responsabilidades, sem passos para um cenário específico.

> **Dica de prova:** Plano diz quem e por quê; playbook diz o que fazer passo a passo.

R4.4. A) Buscar no tenant inteiro regras de encaminhamento e consentimentos OAuth semelhantes

Por quê: Verificar a remediação é procurar ativamente o mesmo artefato e mecanismos alternativos de persistência em todo o ambiente afetado, não só nos casos conhecidos. (objetivo 3.3)

✗ B) Incorreta. Esperar reclamações é verificação passiva; regras de encaminhamento operam em silêncio.

✗ C) Incorreta. O status do alerta não verifica a ausência do atacante.

✗ D) Incorreta. Confirma a troca de senha, mas não procura outras regras ou acessos.

> **Dica de prova:** Verificação: procure o mesmo artefato além dos casos conhecidos.

DIA DA PROVA

Estratégia de prova

O CySA+ CS0-004 coloca você na cadeira de um analista de SOC nível 2 ou de vulnerabilidades: quase toda questão é um cenário com log, saída de ferramenta, vetor CVSS, comando ou sequência de passos, e a pergunta é o que isso indica ou qual é a melhor ação agora. A prova mistura múltipla escolha com questões baseadas em desempenho (PBQ), como análise de logs, simulações e arrastar e soltar. As alternativas erradas costumam ser coisas reais e úteis, mas da fase errada, para o público errado ou que destroem evidência, tiram ativos do escopo ou contornam o plano. Vence quem lê o detalhe concreto do enunciado (horário, processo pai, destino, flag, denominador) e escolhe a resposta que resolve o problema descrito com o menor dano e dentro do processo.

Como responder

✓ Administre o tempo: são até 85 questões em 165 minutos, perto de 2 minutos por questão; se uma PBQ ou um cenário longo travar, marque e volte depois.

✓ Leia primeiro a pergunta final e depois o cenário, procurando o detalhe que decide (processo pai, caminho, porta, horário em UTC, conta, volume, destino).

✓ Em questão de saída de ferramenta, identifique a ferramenta e o campo antes de ler as alternativas, e descarte as que exageram (ataque confirmado, invasão) ou trocam o tipo de falha.

✓ Em questão de processo, classifique a ação na fase (detecção, análise, contenção, erradicação, recuperação, pós-incidente) antes de escolher; quando houver ordem, aplique a ordem do ciclo e a de volatilidade.

✓ Prefira alternativas que preservam evidência e respeitam a restrição do negócio (isolar em vez de desligar, suspender a VM, bloquear o C2 e vigiar o ativo crítico).

✓ Nas contas de métricas, escreva a definição (início e fim do intervalo, numerador e denominador) antes de calcular; as erradas trazem mediana, máximo e base trocada.

✓ Em Escolha DUAS, avalie cada alternativa de forma independente como verdadeira ou falsa e confirme que marcou exatamente duas.

✓ A prova é aplicada em inglês: domine os termos técnicos em inglês (playbook, threat hunting, LOLBins, beaconing, impossible travel, legal hold, after action report).

Erros que derrubam candidatos

✗ Tratar o binário legítimo como malware ou, ao contrário, absolver o comando só porque o executável é assinado pela Microsoft.

✗ Escolher desligar, reiniciar, formatar ou excluir para conter e perder a memória e as evidências.

✗ Ler o percentil do EPSS como probabilidade, priorizar só pela nota base do CVSS e esquecer que o CVSS 4.0 não tem Scope.

✗ Aceitar chamado fechado, silêncio do host ou e-mail do responsável como prova de correção, em vez de nova varredura e caça ativa.

✗ Ordenar a linha do tempo com horários brutos de fusos diferentes.

✗ Usar a mediana no lugar da média ou o denominador errado nas taxas.

✗ Escolher a alternativa que contorna o plano: tirar o ativo do escopo, rebaixar a severidade, falar com a imprensa ou confrontar o suspeito.

Na semana da prova

- ☐ Refazer os simulados focando nos erros e reescrever, para cada um, qual detalhe do enunciado decidia a resposta.
- ☐ Revisar as tabelas rápidas: IDs de evento do Windows, flags do Nmap e do tcpdump, operações do CyberChef, métricas do CVSS 3.1 e 4.0, fases da Kill Chain e vértices do Diamond Model.
- ☐ Treinar à mão as contas de métricas (média, variação percentual, taxa de cliques, FP e TP, SLA) até sair sem hesitar.
- ☐ Reler as pegadinhas de cada capítulo e os itens de 'lembrar', principalmente isolar x desligar, KEV x EPSS e erradicação x recuperação.
- ☐ Revisar os termos técnicos em inglês, já que a prova é aplicada em inglês, e chegar descansado para administrar os 165 minutos.

REVISÃO FINAL

Folha de cola

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

1. Gestão de Vulnerabilidades

‣ Notebooks que quase nunca se conectam à VPN, ou instâncias que nascem e morrem entre varreduras → **Varredura com agente (agente na imagem base)**

‣ CLPs e IHMs que já travaram com ping sweep → **Monitoramento passivo por SPAN e, se sondar, verificações seguras**

‣ Biblioteca de terceiro com CVE no repositório → **SCA; e a SBOM diz onde o componente está**

‣ Código-fonte disponível e necessidade de apontar a linha → **SAST no pipeline**

‣ Faixa enorme (/16) e pouco tempo para achar portas abertas → **Masscan primeiro, Nmap depois**

⚠ Distribuições corporativas aplicam backport sem mudar a versão. Se o changelog do pacote cita a CVE, é falso positivo documentado com evidência.

⚠ A probabilidade é 0,12 (12%) em 30 dias; o percentil é posição relativa. O EPSS é o mesmo para todas as organizações e cobre as CVEs publicadas, não só as do KEV.

⚠ O KEV registra exploração observada e exige orientação de remediação para incluir a CVE; não atribui nota.

2. Operações de Segurança

‣ Subdomínios longos e codificados em rajada, com consultas TXT, de um só host → **Tunelamento DNS para exfiltração ou C2**

‣ Rajada de NXDOMAIN com nomes sem sentido de uma estação → **Malware usando DGA para achar o C2**

‣ Conexões a intervalos fixos, bytes iguais, sempre ao mesmo destino → **Beaconing de implante de C2**

‣ Push negado várias vezes e aprovado na tentativa seguinte → **Fadiga de MFA com senha já comprometida**

‣ Dois continentes em minutos para a mesma conta, com outro navegador → **Impossible travel: revogar sessões, investigar; antes, conferir se o IP é da saída em nuvem da empresa**

⚠ São componentes legítimos do Windows; o que denuncia é o uso: download de IP externo, .exe gravado em pasta pública, decodificação de Base64. Instalar certificado usaria parâmetros como -addstore.

⚠ Porta e criptografia não legitimam destino. Periodicidade fixa com tamanho constante é beaconing; grande volume para nuvem não contratada é exfiltração.

⚠ Na amplificação a vítima externa recebe respostas; aqui é um host interno gerando as consultas. Subdomínios codificados com TXT = tunelamento; NXDOMAIN aleatórios = DGA.

3. Relatórios e Comunicação

‣ Contrato com fornecedor ou MSP define quem e quando pode corrigir → **Inibidor contratual: registrar e negociar janela emergencial**

‣ Patch testado quebra uma função usada pelo negócio → **Degradação de funcionalidade**

‣ Sistema fora de suporte sem atualização possível → **Inibidor de sistema legado com plano próprio e exceção**

‣ Sistema 24x7 ou ERP no fechamento contábil → **Interrupção de processo de negócio: janela combinada ou reinício escalonado**

‣ Comitê de mudanças lento e exploração ativa → **Mudança emergencial prevista no processo, com justificativa ao CAB**

⚠ Some todos os valores e divida pela quantidade de casos; confira se não contou um caso a mais ou a menos.

⚠ Variação = (novo menos anterior) dividido pelo anterior. De 120 para 90 é queda de 25%, não 30 nem 33,3%.

⚠ Use cliques divididos pelos e-mails entregues; quem clicou e enviou dados não conta duas vezes.

4. Resposta e Gestão de Incidentes

‣ Artefato montado, mas ainda não enviado → **Weaponization**

‣ Chave Run ou tarefa agendada gravada após o anexo → **Installation**

‣ Host interno chamando para fora em intervalos fixos → **Command and Control**

‣ w3wp.exe executando whoami logo após um POST malicioso, ainda sem arquivo gravado nem persistência → **Exploitation (com web shell gravado e persistência, já é Installation)**

‣ Arquivos cifrados ou dados levados → **Actions on objectives**

⚠ Desligar destrói a memória volátil. Isole pela rede (EDR ou NAC) mantendo ligado; VM se suspende pelo hipervisor, que grava a memória em arquivo.

⚠ Reiniciar apaga a RAM, onde está o artefato, e não remove a persistência que o recarrega. Capture a memória primeiro.

⚠ O mais recente provavelmente já contém a persistência. Use o último anterior à persistência ou verifique as cópias novas contra os IoCs.

GABARITO

Respostas do diagnóstico

D1. D) O parâmetro permite ler arquivos locais do servidor fora da pasta prevista, caracterizando path traversal → revise o capítulo 1

Por quê: Travessia de diretório (path traversal) aparece na saída de ferramentas web quando um parâmetro aceita sequências ../ e devolve arquivos do servidor fora da pasta prevista; se o arquivo for incluído e interpretado pela aplicação, fala-se em LFI (objetivo 2.2).

✗ A) Incorreta. Em RFI o parâmetro carrega um recurso remoto; aqui o caminho é local.
✗ B) Incorreta. O conteúdo é do arquivo de contas do Linux, não de uma tabela de banco.
✗ C) Incorreta. Não há script na resposta; há o conteúdo de um arquivo do servidor.

> **Dica de prova:** ../ com /etc/passwd na resposta: arquivo local exposto.

D2. B) O perímetro bloqueia a 445 vinda da internet, mas a falha continua alcançável por quem está na rede interna → revise o capítulo 1

Por quê: Varreduras internas e externas se complementam: a externa mede a exposição na internet; a interna, o risco para atacantes já dentro da rede (objetivo 2.1).

✗ A) Incorreta. NAT traduz endereços; não altera protocolos habilitados no servidor.
✗ C) Incorreta. Nada indica correção; a diferença se explica pela posição de cada scanner.
✗ D) Incorreta. A visão externa não vê o que está atrás do perímetro; ela não invalida a interna.

> **Dica de prova:** Fechado por fora não quer dizer seguro por dentro.

D3. B) Validar o parâmetro no servidor com uma lista de permissões dos nomes de relatório aceitos → revise o capítulo 1

Por quê: Validação de entrada no servidor por lista de permissões é boa prática de codificação segura; listas de bloqueio e validação só no cliente são contornáveis. (objetivo 2.3)

✗ A) Incorreta. Lista de bloqueio é incompleta: há outros separadores e operadores de shell, como pipe e e-comercial.
✗ C) Incorreta. A validação no navegador é contornada com facilidade enviando a requisição direto ao servidor.
✗ D) Incorreta. A codificação de saída protege a exibição no navegador, não a execução de comandos no servidor.

> **Dica de prova:** Valide no servidor com lista do que é permitido, não do que é proibido.

D4. B) Um plug-in que conecta a plataforma de orquestração ao produto de EDR específico → revise o capítulo 2

Por quê: Plug-ins, APIs e webhooks integram tecnologias e estendem as plataformas de orquestração sem substituí-las, elevando a eficiência (objetivo 1.5).

✗ A) Incorreta. Aumentar a retenção dos alertas não conecta a plataforma de orquestração ao EDR.
✗ C) Incorreta. Reinstalar a plataforma é desproporcional e não acrescenta a integração com o EDR que o cenário procura.
✗ D) Incorreta. Uma planilha preenchida à mão não integra as ferramentas nem automatiza ações no EDR.

> **Dica de prova:** Estender a orquestração para falar com um produto específico = plug-in.

D5. D) condition: all of them → revise o capítulo 2

Por quê: Em YARA, all of them exige a presença de todas as strings declaradas; any of them e 1 of them se satisfazem com uma só (objetivo 1.3).

✗ A) Incorreta. A condição 1 of them exige pelo menos uma string, o mesmo efeito de any of them, insuficiente para o requisito.

✗ B) Incorreta. A condição any of them dispara se qualquer uma das strings aparecer, sem exigir as duas juntas como o requisito pede.

✗ C) Incorreta. A condição none of them só casa quando nenhuma das strings aparece, o oposto do comportamento pretendido.

> **Dica de prova:** YARA: all of them exige todas as strings; any of them basta uma.

D6. A) Servidor DHCP rogue entregando gateway e DNS falsos; ativar DHCP snooping nos switches → revise o capítulo 2

Por quê: Um DHCP não autorizado na rede é dispositivo rogue que pode se colocar como gateway e DNS das vítimas (adversary-in-the-middle); o DHCP snooping só aceita ofertas vindas de portas confiáveis. (objetivo 1.2)

✗ B) Incorreta. Conflito de IP afeta endereços isolados, não muda faixa, gateway e DNS de várias estações.

✗ C) Incorreta. Falha de relay também deixaria estações sem endereço; não surgiria um servidor 192.168.50.1 respondendo.

✗ D) Incorreta. Escopo esgotado deixaria estações sem endereço, não entregaria outra faixa com gateway diferente.

> **Dica de prova:** Gateway estranho entregue por DHCP desconhecido: DHCP rogue; a defesa é DHCP snooping.

D7. B) Imagem padrão desatualizada, que reintroduz as falhas e precisa entrar no plano de correção → revise o capítulo 3

Por quê: A análise de tendências revela vulnerabilidades recorrentes e sua causa, como imagens padrão desatualizadas, que o plano de ação precisa tratar na origem. (objetivo 4.1)

✗ A) Incorreta. Não há indício de atacante; a coincidência com a recriação explica o padrão.

✗ C) Incorreta. As máquinas recriadas estão vulneráveis de novo; o risco é real.

✗ D) Incorreta. A recorrência acompanha a recriação das máquinas, não um problema de cache.

> **Dica de prova:** Vulnerabilidade que volta sempre: corrija a origem, não a máquina.

D8. A) Restringir o acesso por necessidade de conhecer, classificar o documento e usar canal protegido → revise o capítulo 3

Por quê: Relatórios de varredura são sensíveis e devem ser distribuídos por necessidade de conhecer, com classificação e canal adequado. (objetivo 4.1)

✗ B) Incorreta. Intranet aberta expõe o mapa de vulnerabilidades a quem não precisa e a contas comprometidas.

✗ C) Incorreta. Compartilhamento externo só com necessidade definida e controles; não em massa.

✗ D) Incorreta. Lista geral amplia demais o acesso a informação sensível.

> **Dica de prova:** Relatório de vulnerabilidade é mapa do tesouro: trate como confidencial.

D9. B) Dar ao SOC IOCs e TTPs para detecção e à diretoria o risco para o negócio e as decisões → revise o capítulo 3

Por quê: Relatórios internos de threat intelligence são adaptados à organização e ao público: indicadores e TTPs para operações, risco e recomendações para a liderança. (objetivo 4.2)

✗ A) Incorreta. Ameaças ao setor afetam decisões de investimento e risco da diretoria.
✗ C) Incorreta. Um único texto técnico não serve à diretoria, que precisa de risco e decisão.
✗ D) Incorreta. IOCs não informam a diretoria sobre risco nem orientam decisões.

> **Dica de prova:** Mesma ameaça, dois relatórios: tático para o SOC, estratégico para a diretoria.

D10. C) Contenção → revise o capítulo 4

Por quê: Cada tipo de incidente pede uma estratégia de contenção, escolhida por critérios como dano potencial, preservação de evidências, disponibilidade do serviço, recursos necessários e duração da solução. (objetivo 3.2)

✗ A) Incorreta. A recuperação devolve o serviço ao normal depois que a ameaça foi removida.
✗ B) Incorreta. A análise já confirmou o comprometimento; agora se decide como limitar o dano.
✗ D) Incorreta. A erradicação vem depois e trata da remoção da causa, não de como limitar o dano.

> **Dica de prova:** Desligar ou manter sob observação é escolha de contenção.

D11. A) A1, pela origem e pela janela iguais às do scanner autorizado na mudança aprovada → revise o capítulo 4

Por quê: Triagem confirma o falso positivo com evidência de contexto (ativo autorizado, janela de mudança); LOLBins e contas de serviço fora do padrão não são descartados só por serem nativos ou internos. (objetivo 3.3)

✗ B) Incorreta. Atividade interna sem tráfego externo pode ser movimento lateral ou roubo de credenciais.
✗ C) Incorreta. rundll32 com comsvcs.dll MiniDump é técnica conhecida de despejo do LSASS; binário assinado não significa uso legítimo.
✗ D) Incorreta. Conta de serviço autenticando numa estação de recepção é desvio do padrão e pede investigação.

> **Dica de prova:** Falso positivo se prova com contexto, como a mudança aprovada.

D12. B) Designar um líder do incidente como ponto único de coordenação e decisão → revise o capítulo 4

Por quê: Definir papéis antes do incidente inclui nomear o líder do incidente, que coordena CSIRT, TI, jurídico, RH e comunicação e mantém uma cadeia de decisão clara. (objetivo 3.3)

✗ A) Incorreta. O jurídico orienta sobre riscos legais; ações técnicas cabem ao CSIRT e ao TI.
✗ C) Incorreta. Um fornecedor pode apoiar, mas a coordenação e as decisões cabem à organização.
✗ D) Incorreta. Decisões isoladas por área causam ações contraditórias e lacunas na contenção.

> **Dica de prova:** Uma crise, um líder.

Agora, treine no formato real

Faça as 6 provas completas do curso CompTIA CySA+: 510 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 CompTIA. As questões são inéditas e não reproduzem a prova real.