1.a)

A fase de exfiltração de dados corresponde ao momento em que os atacantes, após comprometerem a rede e agregarem a informação desejada, transferem os dados recolhidos para um sistema sob o seu controlo. Esta fase pode ocorrer de forma direta ou disfarçada, sendo muitas vezes executada com técnicas furtivas para evitar a deteção por mecanismos de segurança. Entre os métodos mais comuns estão a esteganografia, onde os dados são ocultados em ficheiros aparentemente inofensivos como imagens ou documentos, e a utilização de serviços legítimos como Google Drive ou Dropbox, que dificultam a distinção entre tráfego autorizado e malicioso, mascarando a saída de dados sob canais normais de comunicação HTTPS.

1.b)

Indicadores de compromisso para esta fase incluem anomalias no volume ou padrão de tráfego outbound, e conexões frequentes ou persistentes com serviços cloud fora do horário normal ou por terminais que não usam normalmente esses serviços. A monitorização pode ser feita através de sistemas SIEM que integrem dados de logs de firewalls, exportações NetFlow/IPFIX e sistemas de deteção de anomalias baseados em inteligência artificial. Ferramentas com o Suricata ou Zeek, em conjunto com agregadores de logs centralizados, permitem detetar e correlacionar comportamento suspeitos associados à exfiltração furtiva.

2.a)

A arquitetura da rede deve ser segmentada em zonas funcionais distintas com firewalls a isolar os domínios críticos. A DMZ aloja os servidores Web e de email e deve estar protegida por firewalls com inspeção profunda e limitação de sessões para mitigação de ataques volumétricos. O Datacenter B constitui a zona de serviços internos, acessível apenas pelas VLANs 3 e 6, e o acesso deve ser estritamente controlado com políticas de camada 3 e autenticação por 802.1X nas portas de acesso. O Datacenter C, com função de replicação, deve estar isolado da rede interna e apenas acessível pelos IPs dos servidores da DMZ. A WAN deve ser protegida por IPsec e os acesos monitorizados. A implementação de um sistema de deteção/prevenção de intrusões (IDS/IPS) na fronteira da DMZ e integração com SIEM são essenciais. Um orquestrador pode gerir o balanceamento e failover das firewalls para garantir disponibilidade e desempenho.

2.b)

As regras de firewall devem permitir TCP 443 da Internet para os servidores Web da DMZ, bem como TCP 587 e 993 para os servidores de email, tanto para tráfego externo como interno. Deve ser permitido o tráfego TCP 22 apenas das VLANs 3 e 6 para os servidores do Datacenter B. O tráfego TCP 5000 dos servidores da DMZ para

o Datacenter C deve ser autorizado. Todo o restante tráfego não explicitamente autorizado, deve ser bloqueado por omissão. As firewalls que separam a DMZ da rede interna, o DatacenterB das VLANs, e o Datacenter C da WAN devem aplicar estas regras com logging ativo para deteção de desvios e tentativas de intrusão.

3.

Para garantir confidencialidade e integridade no tráfego IPv4 entre o Datacenter B e a cloud da AWS, recomenda-se a utilização de túneis IPsec com modo túnel, estabelecendo conexões seguras gateway-to-gateway. Dado o carácter dinâmico da infraestrutura remota, a solução mais indicada é a implementação de DMVPN (Dynamic Multipoint VPN), que permite a criação e destruição automática de túneis conforme a necessidade, sem configuração manual ponto a ponto. A autenticação e negociação de SAs deve ser feita com IKEv2 e certificados digitais integrados numa infraestrutura de chave pública (PKI). As firewalls devem permitir tráfego ESP (protocolo 50), UDP nas portas 500 e 4500, e permitir o tráfego encapsulado entre os IPs autorizados. A criação de interfaces VTI permite tratar os túneis como interfaces regulares, facilitando o controlo e monitorização do tráfego por regras de firewall convencionais.

4.a)

O SIEM deve estar integrado com os logs dos servidores Web na DMZ e capaz de analisar padrões de acesso. As regras devem gerar alertas quando existirem múltiplas tentativas de acesso a diretórios administrativos como /admin, /config ou /login com respostas 403 ou 401, ou quando um mesmo IP tentar aceder a áreas restritas num curto intervalo de tempo, sugerindo força brutal ou enumeração.

4.b)

Para deteção de atividades de scanning interno, o SIEM deve cruzar logs de rede, NetFlow e IDs. As regras devem gerar alertas quando: um terminal realiza varrimento de múltiplos IPs internos numa mesma porta (horizontal scan), quando há tentativas de conexão a um grande número de portas num mesmo destino (vertical scan), e quando há tentativas sucessivas de SYN sem follow-up (indicador de varrimento stealth). Também deve ser considerado o volume e frequência dos pacotes enviados, especialmente em protocolos como TCP, UDP e ICMP.

4.c)

A deteção de comunicação com C&C sobre HTTPS pode ser feita com base em análise comportamental. O SIEM deve gerar alertas quando há conexões HTTPS persistentes e regulares com domínios recentemente registados ou com baixa reputação, especialmente se realizadas fora do horário normal. O cruzamento de logs de DNS com logs de firewall permite correlacionar acessos a domínios suspeitos com tráfego cifrado, identificando possíveis canais de controlo ativos.

4.d)

A tentativa de ataque man-in-the-middle por dispositivos inseridos em portas de acesso pode ser detetada através de anomalias no comportamento das portas. O SIEM deve alertar quando há mudança do endereço MAC associado a uma porta, sinais de MAC flooding, ou alterações na topologia Layer 2. A integração com 802.1X permite bloquear o acesso não autenticado. Técnicas como port security e monitorização de DHCP snooping e ARP inspection também são essenciais para detetar e mitigar estes ataques.