1.

A fase de aquisição de conhecimento corresponde ao momento inicial de um ataque, no qual o atacante recolhe informações sobre a infraestrutura-alvo. Esta recolha pode ser passiva ou ativa e visa preparar fases posteriores, como a infiltração e a propagação. Entre os meios utilizados destacam-se a análise de DNS, varrimentos de rede (scanning), fingerprinting de sistemas, engenharia social, exploração de meta dados públicos, e análise de redes sociais ou motores de busca. Ferramentas automatizadas, como scanners de portas ou serviços de WHOIS, também são frequentemente usadas.

2.a

Para implementar controlo de fluxos e proteção contra ataques DDoS, é necessário isolar logicamente os domínios funcionais em zonas distintas com firewalls entre elas. A DMZ deve ser separada da rede interna e ligada aos routers de acesso à Internet através de firewalls (F3 e F4). O Datacenter C, que aloja serviços críticos, deve ser uma zona protegida acessível apenas à VLAN 5, com filtragem restrita. O Datacenter B deverá também constituir uma zona autónoma para os serviços internos e de backup, sendo separado da rede interna por uma firewall adicional. O tráfego entre os edifícios A e B deve ser filtrado de acordo com os serviços autorizados (ex: TCP 445 para Samba). A introdução de firewalls stateful e segmentação com microzonas melhora o controlo de tráfego e facilita a mitigação de DDoS, por exemplo com inspeção profunda e limitação de sessões por IP. Recomenda-se ainda a integração com um orquestrador de segurança para balanceamento e resposta automatizada.

2.b

Para o requisito (v), o backup no Datacenter B deve comunicar com os servidores Web HTTPS na DMZ e no Datacenter C e enviar dados para o exterior. As zonas envolvidas são: DMZ, Datacenter B, Datacenter C e Exterior.
As regras devem ser configuradas nas firewalls entre:

- Datacenter B e DMZ (Firewall F3): permitir tráfego TCP origem Datacenter B destino DMZ na porta TCP 5555.
- Datacenter B e Datacenter C (Firewall F4): permitir tráfego TCP origem Datacenter B destino Datacenter C na porta TCP 5555.
- Datacenter B e Exterior (Firewall F3 ou F4): permitir tráfego TCP origem Datacenter B destino Internet na porta TCP 5555.

Estas regras devem ser stateful, limitadas ao IP do servidor de backup como origem e aos IPs de destino esperados, com logging ativo para auditoria.

3.

A comunicação segura entre o Datacenter B e as máquinas virtuais na cloud da

Microsoft deve ser feita através de túneis IPsec dinâmicos, utilizando a solução DMVPN (Dynamic Multipoint VPN). Esta abordagem suporta redes remotas dinâmicas, permitindo criação e destruição de túneis com baixa sobrecarga de gestão. O protocolo IPsec assegura a confidencialidade, integridade e autenticação do tráfego. A negociação de túneis pode ser feita com IKEv2 e autenticação por certificados digitais integrados na infraestrutura PKI da empresa.
As firewalls no Datacenter B devem permitir tráfego UDP nas portas 500 e 4500 para suportar IKE/IPsec e encapsulamento NAT-T, além de ESP (IP protocolo 50). Deve também existir inspeção de pacotes nos túneis para deteção de tráfego anómalo. Por fim, a utilização de interfaces VTI facilita a gestão do tráfego criptografado como interfaces normais.

4.a

Para detetar terminais comprometidos com Worms/Trojans a comunicar com o exterior via Google Drive (HTTPS), o SIEM deve integrar logs de firewalls, proxies e capturas de fluxo (NetFlow/IPFIX). Regras:

- Alerta quando um terminal envia múltiplos ficheiros grandes (>100MB) para drive.google.com em janelas temporais curtas.
- Alerta quando há conexões HTTPS persistentes e fora de horas com *.googleusercontent.com por terminais que normalmente não usam serviços cloud.

4.b

Para deteção de DDoS:

- Alerta quando múltiplos IPs externos iniciam conexões simultâneas para a mesma porta (TCP 443) em servidores da DMZ com alta taxa de pacotes por segundo.
- Alerta quando o número de sessões SYN recebidas excede o limiar normal por IP de origem ou quando há indícios de SYN flood (muitas sessões incompletas).

4.c

Para identificar comunicações C&C sobre DNS:

- Alerta quando um terminal faz múltiplas requisições DNS curtas e não-categorizadas para domínios desconhecidos ou recém-registados.
- Alerta quando há tráfego DNS com payloads incomuns (indicando DNS tunneling) com baixa taxa de dados, mas elevada frequência.

4.d

Para propagação lateral de Worms/Trojans:

- Alerta para múltiplas tentativas de conexão TCP em portas típicas de partilha (ex: 445, 135, 139) entre máquinas internas em curto intervalo.
- Alerta para execução remota de comandos (via PowerShell, WMI, etc.) entre terminais de diferentes VLANs sem autorização prévia ou agendada.