1.

A fase de **aquisição de conhecimento** corresponde à segunda etapa típica de um ataque, logo após a infiltração. Nesta fase, o atacante já obteve um ponto de acesso à rede e inicia a **recolha de informação sobre os sistemas internos** com o objetivo de melhor planear as fases subsequentes de propagação, agregação e exfiltração. Os meios utilizados podem incluir a **observação do tráfego de rede**, a **enumeração de serviços e hosts ativos**, o uso de ferramentas de **scanning** (como Nmap ou scripts personalizados), e a análise de **logs ou configurações locais**. Também podem ser usados meios mais furtivos, como a exploração de **credenciais previamente recolhidas**, movimento lateral em sistemas com vulnerabilidades conhecidas ou mesmo aproveitamento de serviços legítimos para reconhecimento (por exemplo, DNS ou SMB).

2.a)

Para implementar controlo de fluxos eficaz e proteção contra DDoS, é necessário segmentar a arquitetura da rede em **zonas de segurança distintas**, conforme as funções e os requisitos de cada serviço. Deve ser criada uma **zona DMZ isolada** com acesso limitado apenas à Internet e aos servidores HTTPS públicos. O **Datacenter B**, por conter a intranet, deverá estar numa **zona interna segura**, acessível apenas a terminais da rede corporativa. Já o **Datacenter C** deve ter uma **zona restrita** adicional para os serviços críticos acessíveis apenas pela **VLAN 5**. A comunicação entre edifícios A e B deve passar por uma zona de **controle interdepartamental**, permitindo apenas o tráfego Samba (TCP 445). Por fim, o servidor de backup no Datacenter C deve comunicar com os servidores HTTPS da DMZ e Datacenter C, enviando os dados para o exterior através de uma **zona de exportação controlada**, sujeita a filtragem de protocolos e monitorização contra exfiltração abusiva. A presença de **firewalls nas fronteiras destas zonas** permite aplicar regras específicas e mitigação de ataques DDoS por mecanismos de rate limiting, análise de padrões de tráfego e listas de reputação.

2.b)

Para o requisito (v), deve-se garantir que o **servidor de backup** (Datacenter C) apenas possa comunicar com os **servidores Web HTTPS** na **DMZ** e no **Datacenter C**, e que pode enviar dados apenas para um **único servidor externo autorizado**. Assim, nas firewalls que separam:

- **Datacenter C ↔ DMZ** (Firewall interna): permitir tráfego **TCP 5555** unidirecional do servidor de backup para os servidores HTTPS.
- **Datacenter C (backup) ↔ Internet** (Firewall de borda): permitir tráfego **TCP 5555** apenas do IP do servidor de backup para o IP do servidor externo de backup.

Deve-se garantir que não há **resposta inversa iniciada externamente**, bloqueando tráfego TCP 5555 proveniente da Internet para dentro. Além disso, deve-se implementar **logs e alertas de anomalia** para esta comunicação, dado o seu papel sensível e risco de exfiltração.

3.

A solução mais adequada para garantir **comunicação segura entre o Datacenter B e múltiplas instâncias na Cloud da Amazon** é o uso de uma **VPN site-to-site dinâmica baseada em IPsec**, integrando funcionalidades de DMVPN (Dynamic Multipoint VPN). Esta abordagem permite a criação e destruição dinâmica de túneis entre o Datacenter B e os servidores virtuais da Amazon, usando **endereços de loopback e o protocolo NHRP** para manter conectividade mesmo com alterações constantes na infraestrutura remota. A confidencialidade é assegurada pelo uso do **modo túnel do IPsec com cabeçalhos ESP**, combinado com **autenticação forte baseada em certificados digitais** emitidos por uma CA corporativa. As firewalls que protegem o Datacenter B devem ser ajustadas para **permitir tráfego UDP nas portas 500 e 4500**, necessárias ao IKE/IPsec, e tráfego ESP (protocolo 50). Deve-se também aplicar regras que limitem o tráfego de saída dos túneis IPsec apenas para os IPs ou sub-redes válidas da Cloud, com monitorização e controlo rigoroso da carga.

4.a)

Para identificar clientes externos envolvidos em ataques DDoS, o sistema SIEM pode recolher dados via **NetFlow/IPFIX**, analisando **padrões de tráfego volumoso** e súbito. A primeira regra pode detetar IPs com mais de **X conexões estabelecidas por segundo** para os servidores HTTPS públicos da DMZ. A segunda pode identificar IPs que iniciam conexões para os servidores HTTPS com **taxa elevada de tentativas falhadas de handshake TLS** ou conexões muito curtas (indicando flood de conexão incompleta). Ambos os eventos devem gerar alertas imediatos para o SOC.

4.b)

Para identificar terminais comprometidos que usam OneDrive para comunicações ilícitas, o SIEM pode correlacionar logs de **DNS, HTTPS (via proxy/firewall) e NetFlow**. Uma regra pode detetar máquinas internas que estabelecem comunicações HTTPS frequentes e volumosas com domínios *.onedrive.live.com fora do horário normal de trabalho. Outra pode sinalizar dispositivos que estabelecem conexões com OneDrive, mas que não possuem login ou associação prévia de conta corporativa (baseando-se em logs de autenticação ou sistemas de inventário). Estes padrões são indicativos de possíveis exfiltrações usando serviços legítimos.

4.c)

A propagação de Worms/Trojans entre terminais internos pode ser identificada através de análise de tráfego lateral na rede e correlação de logs de endpoints. Uma regra pode disparar alertas sempre que um terminal tenta conectar-se por **SMB (TCP 445), RDP (TCP 3389)** ou **WinRM (TCP 5985/5986)** a mais de "n" terminais num curto intervalo de tempo. Outra pode sinalizar a **cópia de executáveis ou scripts** suspeitos entre partilhas de rede acessadas por múltiplos utilizadores, sobretudo se acompanhada de falhas de autenticação ou acessos fora do normal. A utilização de logs EDR ou de agentes locais nos terminais complementa esta deteção com visibilidade sobre processos maliciosos em execução.