APPSEC engineer

Azure Defense Checklist

Name	Approach
SQL Injection Defense	☐ Use Azure SQL Database or Azure SQL Managed Instance, which have built-in protection against SQL injection attacks. ☐ Employ input validation and parameterized queries in your application to prevent SQL injection.
DDoS Protection	☐ Use Azure DDoS Protection Standard to mitigate distributed denial-of-service attacks. ☐ Configure application gateways or Web Application Firewalls (WAF) to filter out malicious traffic.
Brute Force Attack Defense	☐ Implement Azure AD Identity Protection to detect and block suspicious sign-ins. ☐ Enforce strong password policies and enable multi-factor authentication (MFA) for Azure AD accounts.
Cross-Site Scripting (XSS) Defense	☐ Use Azure Application Gateway with WAF to filter out malicious scripts. ☐ Sanitize user input and employ content security policies in your web applications.
Data Breach Defense	☐ Implement Azure Information Protection to classify and encrypt sensitive data. ☐ Use Azure Key Vault to securely manage encryption keys. ☐ Regularly monitor data access and use Azure Security Center for threat detection.
Account Compromise Defense	☐ Enable Conditional Access policies to control access based on conditions and user risk. ☐ Implement strong authentication mechanisms, such as biometrics and smart cards.
Phishing Defense	☐ Train users to recognize phishing emails and use Exchange Online Protection for email filtering. ☐ Implement Azure AD Conditional Access policies to limit access from unfamiliar locations.
Malware Defense	☐ Use Azure Security Center to detect and respond to malware threats. ☐ Install and configure endpoint protection on virtual machines using Azure Security Center recommendations.
Data Exfiltration Defense	☐ Implement data loss prevention (DLP) policies in Azure Information Protection to prevent sensitive data from leaving your organization. ☐ Employ access controls and encryption to protect data at rest and in transit.
API Security Defense	☐ Secure your APIs using Azure API Management with authentication and authorization policies. ☐ Implement OAuth or JWT authentication for API access.
Insecure Container Defense	☐ Secure Docker containers and Kubernetes deployments in Azure Kubernetes Service (AKS) using best practices for container security. ☐ Implement network policies and role-based access control (RBAC) for AKS.
Unprotected Data Storage Defense	☐ Use Azure Storage Service Encryption to encrypt data at rest in Azure Blob Storage and Azure File Storage. ☐ Set appropriate access controls and firewall rules for Azure storage resources.
Account Lockout Defense	☐ Configure account lockout policies to prevent brute force attacks. ☐ Monitor and alert on repeated failed login attempts.
Third-Party Software Defense	☐ Regularly update and patch third-party software running on virtual machines and Azure services. ☐ Use Azure Security Center to identify vulnerabilities and apply remediations.
Incident Response and Forensics	☐ Develop an incident response plan and create playbooks for responding to security incidents. ☐ Implement auditing and logging for thorough forensic analysis.
Defense in Depth	☐ Azure uses a defense-in-depth approach to security, which means that multiple layers of protection are implemented to make it difficult for attackers to succeed. This includes security measures at the physical, network, application, and data layers. ☐ Azure AD is a cloud-based identity and access management (IAM) service that helps you manage and secure user identities and access to your Azure resources. Azure AD includes features such as multi-factor authentication (MFA), conditional access, and risk-based sign-in monitoring to help protect against unauthorized access. ☐ Azure Security Center is a unified security management platform that provides visibility and insights into the security posture of your Azure resources. It also provides recommendations and tools to help you improve your security posture and mitigate security risks. ☐ Azure Sentinel is a cloud-native security information and event management (SIEM) solution that helps you detect and respond to threats across your Azure, hybrid, and on-premises environments. Azure Sentinel uses artificial intelligence (AI) to analyze large volumes of data to identify suspicious activity and potential threats.
Session Hijacking Attacks	☐ Azure AD provides a number of session management features, such as session expiry and session timeouts, to help prevent attackers from hijacking user sessions. ☐ SSO allows users to sign in to multiple applications with a single set of credentials. This can help to reduce the risk of session hijacking, as users are less likely to enter their credentials on untrusted websites. ☐ Conditional Access can be used to control access to your Azure resources based on factors such as the user's identity, device, and location. This can help to prevent attackers from accessing your resources even if they have hijacked a user's session.