

SecOps Review

A Bechtle Packaged Solution

As your Azure usage grows, so do potential security risks and vulnerabilities, which can challenge your organisation's ability to maintain compliance and secure critical workloads. To help you strengthen your security posture, we offer a comprehensive SecOps assessment for your Microsoft Azure estate.

Our assessment evaluates your current security configuration, analyses threat vectors, and reviews compliance alignment. Once completed, our team will deliver a detailed report outlining actionable insights to address gaps, mitigate risks, and enhance protection. You'll also receive a physical copy of the assessment, ensuring you have everything needed to fortify your Azure environment against evolving threats.

What criteria is covered in a SecOps review?

- | | |
|---|--|
|  Azure Secure Score breakdown |  PIM and RBAC Identity review |
|  Secure Score recommendations |  RBAC Service Principles and Permissions Review |
|  User access and assigned roles review |  Network summary and VNet peering's |
|  Network Security Groups and rule Sets |  Security Centre Alerts |

WHY CHOOSE THIS PACKAGE?

- Strengthen your security posture
- Reduce risk and compliance costs
- Uncover hidden vulnerabilities
- Vendor-neutral recommendations

WHAT'S THE COST?

Starting from £1,160
excl. VAT

Please note that the total cost will be determined by the size and complexity of the environment

WHY BECHTLE?

- Europe's largest IT provider
- Experienced Microsoft consultant
- Certified Azure experts, experienced in optimising Azure Services
- One of Microsoft's largest European partners
- Azure Expert MSP Status

Gold

Microsoft Partner
Azure Expert MSP



Bechtle Limited
www.bechtle.com/gb | 01249 467900 | sales.uk@bechtle.com



version 1.2

SecOps Review

A Bechtle Packaged Solution



Azure Secure Score

Azure Secure Score recommendations offer actionable insights to enhance security by addressing identity management, data protection, network security, compliance, and threat detection. Key actions include enabling MFA, encrypting data, using NSGs, applying RBAC, and enabling Defender for Cloud. Implementing these steps mitigates risks, reduces vulnerabilities, and improves your security posture.



User access and assigned roles

In Azure, user access is managed through role-based access control (RBAC), which assigns permissions to users, groups, or service principals based on roles. Roles, such as Owner, Contributor, or Reader, define what actions can be performed on resources and are assigned at different scopes (subscription, resource group, or resource). Access is managed via the Azure portal, PowerShell, or CLI, and follows the principle of least privilege to ensure users have only the permissions they need. Regular reviews and Conditional Access policies enhance security and governance.



RBAC Service Principles and Permissions

RBAC Service Principals and Permissions are evaluated to ensure that service accounts (service principals) have only the necessary permissions to perform their tasks. Service principals are assigned specific roles through RBAC, and the review also checks that permissions are correctly scoped to limit access to the appropriate resources and that any unused or unnecessary service principals are removed, reducing potential attack vectors and improving overall security.



Network summary and VNet peering's

This Network Summary in Azure provides an overview of resources like VNets, subnets, NSGs, and gateways, helping manage connectivity and security. VNet Peering connects VNets for seamless communication using Azure's private backbone, offering low latency, high bandwidth, and cross-region connectivity while maintaining individual configurations. It's ideal for resource sharing, hub-and-spoke architectures, and linking environments securely.



Network Security Groups and rule Sets

Network Security Groups (NSGs) in Azure are critical for controlling network traffic to and from resources within virtual networks. They use rule sets to define security policies, specifying which inbound and outbound traffic is allowed or denied based on parameters like IP address, port, and protocol. Reviewing NSGs involves ensuring that rule sets are properly configured to minimise exposure to threats, maintain least privilege access, and align with security best practices. A thorough review would identify overly permissive rules, missing rules, or potential misconfigurations that could compromise the network's security.



Security Center Alerts

Security Center Alerts are assessed to ensure that Azure resources are being effectively monitored for potential security threats and vulnerabilities. The review examines the configuration and response to alerts generated by Microsoft Defender for Cloud, ensuring that critical issues such as suspicious activities, unpatched systems, and misconfigurations are promptly identified. It also verifies that alert severity is appropriately categorised and that recommended actions for mitigation are followed to enhance the organisation's overall security posture.

