Comprehensive Security Assessment Report

Checkov Results (Infrastructure as Code)

Summary: - ✅ Passed: 9 - ❌ Failed: 6 - ⏩ Skipped: 0

Failed Infrastructure Checks

CKV_AZURE_10
🔹 *File*: `/terraform/main.tf`
🔹 *Resource*: azurerm_network_security_group.honeynetx-nsg
🔹 *Guidance*: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/azure-policies/azure-networking-policies/bc-azr-networking-3

CKV_AZURE_178
🔹 *File*: `/terraform/main.tf`
🔹 *Resource*: azurerm_linux_virtual_machine.main
🔹 *Guidance*: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/azure-policies/azure-general-policies/azr-general-178

CKV_AZURE_50
🔹 *File*: `/terraform/main.tf`
🔹 *Resource*: azurerm_linux_virtual_machine.main
🔹 *Guidance*: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/azure-policies/azure-general-policies/bc-azr-general-14

CKV_AZURE_1
🔹 *File*: `/terraform/main.tf`
🔹 *Resource*: azurerm_linux_virtual_machine.main
🔹 *Guidance*: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/azure-policies/azure-networking-policies/bc-azr-networking-1

CKV_AZURE_149
🔹 *File*: `/terraform/main.tf`
🔹 *Resource*: azurerm_linux_virtual_machine.main
🔹 *Guidance*: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/azure-policies/azure-general-policies/ensure-azure-virtual-machine-does-not-enable-password-authentication

CKV_AZURE_119
🔹 *File*: `/terraform/main.tf`
🔹 *Resource*: azurerm_network_interface.honeynetx-vm-nic
🔹 *Guidance*: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/azure-policies/azure-networking-policies/ensure-that-network-interfaces-dont-use-public-ips

Prowler Results (Cloud Configuration)

Scan Summary: - 🔍 Total Checks: 12 - ✅ Passed: 0 - ❌ Failed: 12 - ⚠️ Warnings: 0

Critical Findings

defender_ensure_defender_for_app_services_is_on - high severity
🔹 *Service*: None
🔹 *Region*: None
🔹 *Description*: Ensure That Microsoft Defender for App Services Is Set To 'On'
🔹 *Remediation*: {'Text': 'By default, Microsoft Defender for Cloud is not enabled for your App Service instances. Enabling the Defender security service for App Service instances allows for advanced security defense using threat detection capabilities provided by Microsoft Security Response Center.', 'Url': ''}

defender_ensure_defender_for_arm_is_on - high severity
🔹 *Service*: None
🔹 *Region*: None
🔹 *Description*: Ensure That Microsoft Defender for Azure Resource Manager Is Set To 'On'
🔹 *Remediation*: {'Text': 'Enable Microsoft Defender for Azure Resource Manager', 'Url': ''}

defender_ensure_defender_for_azure_sql_databases_is_on - high severity
🔹 *Service*: None
🔹 *Region*: None
🔹 *Description*: Ensure That Microsoft Defender for Azure SQL Databases Is Set To 'On'
🔹 *Remediation*: {'Text': 'By default, Microsoft Defender for Cloud is disabled for all your SQL database servers. Defender for Cloud monitors your SQL database servers for threats such as SQL injection, brute-force attacks, and privilege abuse. The security service provides action-oriented security alerts with details of the suspicious activity and guidance on how to mitigate the security threats.', 'Url': ''}

defender_ensure_defender_for_containers_is_on - high severity
🔹 *Service*: None
🔹 *Region*: None
🔹 *Description*: Ensure That Microsoft Defender for Containers Is Set To 'On'
🔹 *Remediation*: {'Text': 'By default, Microsoft Defender for Cloud is not enabled for your Azure cloud containers. Enabling the Defender security service for Azure containers allows for advanced security defense against threats, using threat detection capabilities provided by the Microsoft Security Response Center (MSRC).', 'Url': ''}

defender_ensure_defender_for_cosmosdb_is_on - high severity
- *Service*: None
- *Region*: None
- *Description*: Ensure That Microsoft Defender for Cosmos DB Is Set To 'On'
- *Remediation*: {'Text': 'By default, Microsoft Defender for Cloud is not enabled for your App Service instances. Enabling the Defender security service for App Service instances allows for advanced security defense using threat detection capabilities provided by Microsoft Security Response Center.', 'Url': 'Enable Microsoft Defender for Cosmos DB'}

defender_ensure_defender_for_databases_is_on - high severity
- *Service*: None
- *Region*: None
- *Description*: Ensure That Microsoft Defender for Databases Is Set To 'On'

- *Remediation*: {'Text': 'Enable Microsoft Defender for Azure SQL Databases', 'Url': ''}

defender_ensure_defender_for_dns_is_on - high severity
- *Service*: None
- *Region*: None
- *Description*: Ensure That Microsoft Defender for DNS Is Set To 'On'
- *Remediation*: {'Text': 'By default, Microsoft Defender for Cloud is not enabled for your App Service instances. Enabling the Defender security service for App Service instances allows for advanced security defense using threat detection capabilities provided by Microsoft Security Response Center.', 'Url': ''}

defender_ensure_defender_for_keyvault_is_on - high severity
- *Service*: None
- *Region*: None
- *Description*: Ensure That Microsoft Defender for KeyVault Is Set To 'On'
- *Remediation*: {'Text': 'Ensure that Microsoft Defender for Cloud is enabled for Azure key vaults. Key Vault is the Azure cloud service that safeguards encryption keys and secrets like certificates, connection-based strings, and passwords.', 'Url': ''}

defender_ensure_defender_for_os_relational_databases_is_on - high severity
- *Service*: None
- *Region*: None
- *Description*: Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On'
- *Remediation*: {'Text': 'Enabling Microsoft Defender for Open-source relational databases allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).', 'Url': ''}

defender_ensure_defender_for_server_is_on - high severity
- *Service*: None
- *Region*: None

🔹 *Description*: Ensure That Microsoft Defender for Servers Is Set to 'On'
🔹 *Remediation*: {'Text': 'Enabling Microsoft Defender for Cloud standard pricing tier allows for better security assessment with threat detection provided by the Microsoft Security Response Center (MSRC), advanced security policies, adaptive application control, network threat detection, and regulatory compliance management.', 'Url': ''}

defender_ensure_defender_for_sql_servers_is_on - high severity
🔹 *Service*: None
🔹 *Region*: None
🔹 *Description*: Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On'
🔹 *Remediation*: {'Text': 'By default, Microsoft Defender for Cloud is disabled for the Microsoft SQL servers running on virtual machines. Defender for Cloud for SQL Server virtual machines continuously monitors your SQL database servers for threats such as SQL injection, brute-force attacks, and privilege abuse. The security service provides security alerts together with details of the suspicious activity and guidance on how to mitigate to the security threats.', 'Url': ''}

defender_ensure_defender_for_storage_is_on - high severity
🔹 *Service*: None
🔹 *Region*: None
🔹 *Description*: Ensure That Microsoft Defender for Storage Is Set To 'On'
🔹 *Remediation*: {'Text': 'By default, Microsoft Defender for Cloud is disabled for your storage accounts. Enabling the Defender security service for Azure storage accounts allows for advanced security defense using threat detection capabilities provided by the Microsoft Security Response Center (MSRC). MSRC investigates all reports of security vulnerabilities affecting Microsoft products and services, including Azure cloud services.', 'Url': ''}