RoboMate Azure Security Assessment Report

CopyRights © RoboMate v3.6 - Developed by Marco Fekry

Report Date: 3/9/2025 4:57:50 AM

Tenant Name: PaySky **Subscription Name: GIM-HUB-UAT-SUBSCRIPTION**

Tenant ID: 5e13e6b6-73e3-4cc1-858c-05f973561678 **Subscription ID: 18a165d1-9372-47bd-ae54-02ec32e9e65b**

Introduction

RoboMate Azure Security Assessment Report has been collected and populated throught the RoboMate Cloud Automation

The report is based on evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or an organization using Microsoft Cybersecurity refrence Architecture

Contents

1- RoboMate Azure Security Assessment Report Summary
2- RoboMate Azure Security Assessment Detailed Resources Report Summary
3- RoboMate Azure Security Operating Systems / Databases Assessment Report Summary

RoboMate Azure Security Assessment Report Summary

The below RoboMate Azure Security Assessment Report Summary represents the current security assessment Findings and recommendations to the current environment

Target-Security-Area	Findings	Severity
Identity	A maximum of 3 Owners should be designated for subscriptions	High
Identity	Reissue authenticators for changed groups and accounts	High
Identity	Guest accounts with write permissions on Azure resources should be removed	High
Identity	Disabled accounts with owner permissions on Azure resources should be removed	High
Identity	Disabled accounts with read and write permissions on Azure resources should be removed	High
Identity	Guest accounts with owner permissions on Azure resources should be removed	High
Identity	Guest accounts with read permissions on Azure resources should be removed	High
Identity	The Unknown Azure Scoped type is Subscriptions while it should be limited to the intended resources permissions	High
Azure Monitor	Azure Monitor is a recommended insights solution for Virtual Machines to keep track of Virtual Machine Insights	Medium
Defender For Cloud Recommendations	3 High Severity Defender for Cloud Recommendations Detected	High
Microsoft Sentinel	Microsoft Sentinel SEIM and SOAR Should be Enabled on All Available Data Sources	High
Azure Firewall	Azure Firewall is recommended to secure your Workloads , Or else use an Azure Marketplace Security Appliance (GIM-FGT-UAT with fortinet VM security appliance detected)	High
Web Application Firewall	AZ-WAF-UAT-GIM Application Gateway Web Application Firewall RuleSetType OWASP rule Upgrade is recommended to Microsoft_BotManagerRuleSet in order to secure youe WAF Traffic	High
Web Application Firewall	AZ-AG-UAT-GIM Application Gateway Web Application Firewall Mode should be configured to Prevent Application Gateway Threats	High
Web Application Firewall	AZ-AG-UAT-GIM AppLication Gateway Diagnostics should be configured to keep track of our traffic insights and threats	High
Azure DDOS	Azure DDOS is recommended to secure your Public IPs from Denial of Service Attacks	High
Azure Bastion	Azure Bastions is recommended to secure your Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses	Low
Purview	Azure Purview Accounts is recommended to help address the fragmentation of data across organizations, the lack of visibility that hampers data protection and governance	Low
Copilot	Microsoft Security Copilot is recommended to improve security outcomes at machine speed and scale, while remaining compliant to responsible AI principles.	Low
Defender EASM	Defender EASM is recommended to continuously discovers and maps your digital attack surface to provide an external view of your online infrastructure	Low

RoboMate Azure Security Assessment Detailed Resources Report Summary

The below RoboMate Azure Security Assessment Report Summary represents the current security assessment Findings and recommendations to the current environment resources

Target-Security-Area	Findings	Severity
Virtual Machines	GIM-FGT-UAT Virtual Machine Disabled Linux Patch Mode detected, It is recommended to turn Patch Mode On	High
Virtual Machines	GIM-FGT-UAT Virtual Machine Disabled Linux Assessment Mode detected, It is recommended to turn Assessment Mode On	High
Virtual Machines	GIM-FGT-UAT Virtual Machine No Trusted Launch detected, It is recommended to enable Trusted Launch for Virtual machine security	High
Virtual Machines	GIM-FGT-UAT Virtual Machine Disks Encryption is recommended to secure your data	High
Virtual Machines	GIM-FGT-UAT Virtual Machine Disks Replication is recommended for High Availability of your workloads	High
Network Security Groups	GIM-FGT-UAT Network Security Group * source detected, It is recommended to harden the Source address prefix for a public IP attached to a virtual machine	High
Subscriptions	Azure Subscription Diagnostic Settings is recommended to to keep Subscription Activity Logs for Auditing and Investigations	Low
Diagnostic Settings	No Azure Diagnostic Settings for Virtual Networks . It is recommended to to keep Virtual Networks Logs for Auditing and Investigations	Low
Diagnostic Settings	No Azure Diagnostic Settings for Public Ips . It is recommended to to keep Public Ips Logs for Auditing and Investigations	Low
Diagnostic Settings	No Azure Diagnostic Settings for Network Security Groups . It is recommended to to keep Network Security Groups Logs for Auditing and Investigations	Low

RoboMate Azure Security Operating Systems / Databases Assessment Report Summary

The below RoboMate Azure Security Assessment Report Summary represents the current Operating Systems / Databases assessment Findings and recommendations to the current environment

RoboMate Azure Security Assessment Report

CopyRights © RoboMate v3.6 - Developed by Marco Fekry