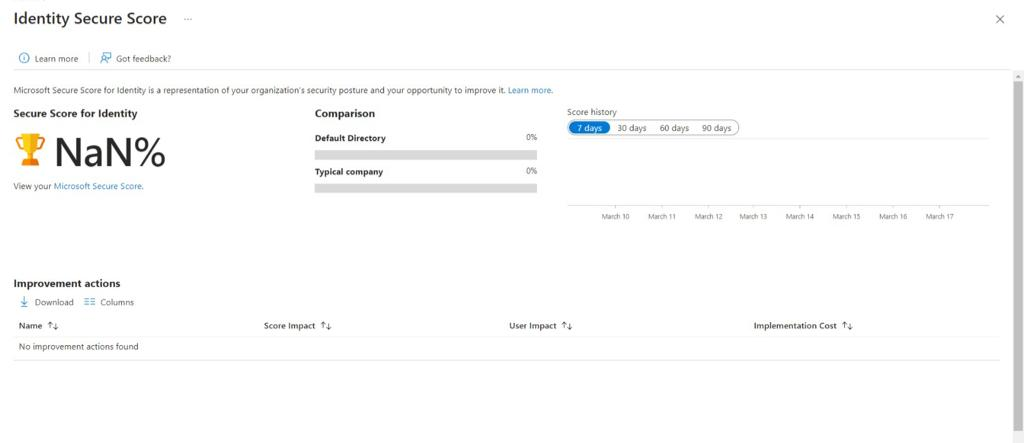
**MANAGING NETWORK/SECURITY RISK**

**ASSIGNMENT – 2**

**Keerthi Moparthi**

**2868921**



**INTRODUCTION**

With Azure Active Directory (Azure AD), a solution for control identities and approach to resources in the cloud, organizations can securely manage user identities and resource access. In Azure AD, the identity score is a metric that measures how well your organization manages identity and access. A higher identity score indicates a more secure identity posture. This article will discuss how to improve the identity score of your Azure AD tenant.

**ENABLE MULTI FACTOR AUTHENTICATION(MFA**):

Multi-factor authentication increases authentication process by requiring users to provide various forms of identification. To significantly raise the identity score of every user in your Azure AD tenant, MFA should be turned on. To activate MFA, access Azure portal, select Azure AD, Users, and Multi-factor authentication.

**IMPLEMENT CONDITIONAL ACCESS POLICIES**

Conditional Access Policies enable organizations to define conditions under which users are allowed to access resources. By implementing Conditional Access Policies, you can restrict access to sensitive resources and data based on location, device, and other criteria. Implementing Conditional Access Policies can help improve your identity score by reducing the risk of unauthorized access to sensitive data.

**ENABLE PASSWORD LESS AUTHENTICATION**:

A secure authentication mechanism that does away with the necessity for users to memorize passwords is password less authentication. Users are instead verified using hardware tokens or biometric characteristics. The danger of password-related threats like phishing and credential stuffing can be decreased by enabling password less authentication for your Azure AD tenant, which can raise your identity score.

**MONITOR SIGN – IN ACTIVITY**:

Monitoring sign-in activity can help detect suspicious activity and potential security breaches. Azure AD provides sign-in logs that can be used to track sign-in activity and identify anomalies. By monitoring sign-in activity, you can take proactive measures to prevent security incidents and improve your identity score.

**ENABLE RISK BASED CONDITIONAL ACCESS POLICIES**:

Risk-Based Conditional Access Policies use Azure AD's Identity Protection feature to assess the risk associated with a user's sign-in attempt and apply appropriate access policies. By enabling Risk-Based Conditional Access Policies, you can improve your identity score by reducing the risk of unauthorized access to sensitive data.

**CONCLUSION**:

To guarantee the security of the data and resources in your company, you must raise the identity score of your Azure AD tenant. You can considerably raise your identity score and lower the likelihood of security incidents by adhering to the best practices described in this article. A higher identity score and a more secure identity posture can be attained by implementing MFA, Conditional Access Policies, password less authentication, tracking sign-in behaviour, and activating Risk-Based Conditional Access Policies.