CoBro Consulting

Vulnerability Management

Purpose:

This report details the vulnerability management for CoBro Consulting. The data and network vulnerabilities are assessed through **Microsoft (MS) Azure - Security Center**. Our weekly vulnerability maintenance keeps the MS Azure Cloud Resources secured and provide data availability and integrity to CoBro Consulting users. The following categories are used to assess data and network vulnerabilities for CoBro Consulting:

- Policy and Compliance: Resource policy definitions are used by MS Azure Policy to establish conventions for resources. Each definition describes resource compliance and what effect to take when a resource is non-compliant.
- Resource Security Hygiene covers the following categories below:
    - **RECOMMENDATIONS**: The recommendation.
    - **SECURE SCORE IMPACT**: Based on resources, security, and remediation.
    - **RESOURCE**: Lists the resources to which this recommendation applies.
    - **STATUS BARS**: Describes the severity of that particular recommendation:
        - **High (Red)**: A vulnerability exists with a meaningful resource (such as an application, a VM, or a network security group) and requires attention.
        - **Medium (Orange)**: A vulnerability exists and non-critical or additional steps are required to eliminate it or to complete a process.
        - **Low (Blue)**: A vulnerability exists that should be addressed but does not require immediate attention.
        - **Healthy (Green)**:
        - **Not Available (Grey)**:
- Threat Protection: Detect and investigate advanced attacks on-premises and in the cloud

Platform:

- Microsoft Azure Cloud

Vulnerability Management Tool:

- Microsoft Azure - Security Center

Vulnerability Remediation Schedule: Once a week (Sunday)

- CoBro Consulting MS Azure administrator performs vulnerability checks once a week (Sunday) based on Microsoft Azure - Security Center

- CoBro Consulting MS Azure administrator address particular recommendations from MS Azure - Security Center - Resource Security Hygiene

Approval Process: Requires approval from Chief Information Officer

- CoBro Consulting MS Azure administrators confirm with Chief Information Officer for approval for any changes and remediation within the CoBro Consulting - MS Azure Cloud Resources.

Future consideration:

- Azure Security Center now offers integrated vulnerability assessment with Qualys cloud agents (preview) as part of the Virtual Machine recommendations. If a Virtual Machine does not have an integrated vulnerability assessment solution already deployed, Security Center recommends that it be installed. The solution can be deployed to multiple VMs at one time, and the ability to automatically deploy on new VMs as they are created, will be added soon. Once deployed, the Qualys agent will start reporting vulnerability data to the Qualys management platform, which, in turn, provides vulnerability and health monitoring data back to Security Center. Users can quickly identify vulnerable VMs from the Security Center dashboard. Additional reports and information are available in the Qualys management console, which is linked directly from Security Center.

Sources: Microsoft Azure - Integrated Vulnerability Assessment

_____

Urban Pelicon
CoBro Consulting
Chief Information Officer