Cyber Shujaa

Cyber Shujaa

Cloud Security Specialist

Assignment 21 -AZ-500 Learning Path: Secure Posture Management

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Introduction

In this module, we will gain the knowledge and skills needed to manage and enhance the security posture of our cloud environment using Microsoft Defender for Cloud, ensuring proactive identification and remediation of security risks.

Implement Microsoft Defender for Cloud

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities.

Defender for Cloud combines the capabilities of:

- A development security operations (DevSecOps) solution that unifies security management at the code level across multicloud and multiple-pipeline environments
- A cloud security posture management (CSPM) solution that surfaces actions that you can take to prevent breaches
- A cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads

Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory

Microsoft Defender for Cloud aims to help users understand and improve their security posture through the Secure Score feature, which assesses cross-cloud resources for security issues and aggregates findings into a single score.

Users can enhance their score by remediating security recommendations grouped into controls. To see a score improvement, all recommendations for a single resource must be addressed. Only built-in recommendations affect the score, and users are encouraged to disable inapplicable recommendations.

Assess compliance against security frameworks and Microsoft Defender for Cloud

Microsoft Defender for Cloud assists organizations in assessing compliance against various security frameworks by utilizing its regulatory compliance dashboard. This dashboard continuously evaluates the hybrid cloud environment, analyzing risk factors based on the controls and best practices of the selected compliance standards.

When Defender for Cloud is enabled on an Azure subscription, it automatically assigns the Microsoft cloud security benchmark, which is informed by established standards such as the Center for Internet Security (CIS), Payment Card Industry (PCI) Data Security Standards (DSS), and the National Institute of Standards and Technology (NIST).

The dashboard provides insights into compliance status, allowing users to monitor gaps and improve their compliance posture over time by acting on recommendations and remediating identified issues.

Add industry and regulatory standards to Microsoft Defender for Cloud

The Microsoft cloud security benchmark (MCSB) is essential for adding industry and regulatory standards to Microsoft Defender for Cloud. It provides a comprehensive framework that helps organizations improve their security posture by offering prescriptive best practices and recommendations tailored for cloud environments.

The MCSB focuses on cloud-centric control areas and draws input from various industry standards, including the Cloud Adoption Framework, Azure Well-Architected Framework, and the CISO Workshop.

To implement these standards, organizations can utilize the MCSB to automate control monitoring across different cloud platforms, including AWS. This feature allows for a consistent user experience in monitoring compliance and security across multi-cloud environments.

Ultimately, adding industry and regulatory standards to Microsoft Defender for Cloud through the MCSB enables organizations to maintain a robust security posture while minimizing the overhead associated with managing multiple compliance frameworks.

Add custom initiatives to Microsoft Defender for Cloud

A security initiative is a collection of Azure Policy definitions grouped towards a specific goal. By default, every subscription in Microsoft Defender for Cloud is assigned the Microsoft cloud security benchmark, which provides a set of guidelines for security best practices.

We can customize this initiative by enabling or disabling individual policies within it. Additionally, we can create our custom initiatives by defining specific Azure Policy rules that align with our organization's security requirements. This customization allows us to tailor our security posture according to our organization's needs, ensuring compliance with desired security configurations and addressing any compliance gaps effectively.

Connect hybrid cloud and multi-cloud environments to Microsoft Defender for Cloud

Connecting hybrid cloud and multi-cloud environments to Microsoft Defender for Cloud is crucial to maintain a unified security posture across diverse IT landscapes. With Azure Arc-enabled servers for non-Azure machines, the Native Cloud Connector, and the Classic Connector, you can extend the capabilities of Microsoft Defender for Cloud to non-Azure resources. This integration empowers you to monitor, detect, and respond to security threats comprehensively.

Users can connect non-Azure machines through Azure Arc-enabled servers, the Native Cloud Connector, or directly with Microsoft Defender for Endpoint. Azure Arc-enabled servers allow non-Azure machines to be treated as Azure resources, enabling comprehensive monitoring and security recommendations.

Additionally, to protect workloads in Amazon Web Services (AWS), users must establish a connection between AWS accounts and Defender for Cloud, ensuring proper permissions and configurations are in place. The document outlines the prerequisites and steps necessary for successful integration, including the use of the Log Analytics agent and other security extensions.

Implement and use Microsoft Defender External Attack Surface Management

Microsoft Defender External Attack Surface Management (Defender EASM) continuously discovers and maps your digital attack surface to provide an external view of your online infrastructure. This visibility enables security and IT teams to identify unknowns, prioritize risk, eliminate threats, and extend vulnerability and exposure control beyond the firewall. Attack Surface Insights are generated by leveraging vulnerability and infrastructure data to showcase the key areas of concern for your organization.

Defender EASM employs proprietary discovery technology that recursively searches for infrastructure connected to known legitimate assets, uncovering previously unknown properties. It supports the discovery of various asset types, including domains, hostnames, IP addresses, and SSL certificates. Additionally, it offers dashboards that provide insights into vulnerabilities and compliance, allowing users to manage their assets effectively and customize their views based on specific needs.

Conclusion

To conclude, we have learned how to effectively manage and enhance your organization's security posture by utilizing Microsoft Defender for Cloud, including identifying and addressing security risks through Secure Score and Inventory, assessing compliance against security frameworks, customizing security standards, connecting hybrid and multi cloud environments, and monitoring external assets for comprehensive threat protection.