Cyber Shujaa

Cloud Security Specialist

Assignment 23: Configure and manage threat protection by using Microsoft Defender for Cloud

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Introduction

In this module, we will be equipped with the skills to configure and manage comprehensive threat protection using Microsoft Defender for Cloud.

Enable workload protection services in Microsoft Defender for Cloud

Workload protection services in Microsoft Defender for Cloud offer security alerts powered by Microsoft Threat Intelligence and advanced protections for various workloads. The Cloud workload dashboard includes sections for Defender for Cloud coverage, security alerts, advanced protection capabilities, and insights into security matters relevant to users' subscriptions.
Key capabilities include:

- Protecting cloud servers with Microsoft Defender for Endpoint and other tools.
- Identifying threats to storage resources through advanced detection capabilities.
- Protecting cloud databases with attack detection and response.
- Securing containers with environment hardening and vulnerability assessments.
- Providing insights into application infrastructure weaknesses.
- Managing real-time security alerts and incidents to respond to threats effectively.

Each capability is linked to specific Defender plans that guide users in implementing the necessary security controls for their workloads.

Defender for Servers

Defender for Servers in Microsoft Defender for Cloud enhances security for machines by providing actionable recommendations to improve security posture and protect against real-time threats. It supports multicloud and on-premises environments, allowing for centralized management and reporting of security data.

The service integrates with Defender for Endpoint and Defender Vulnerability Management, enabling features like agentless scanning, threat detection, and compliance assessments. There are two plans available: Plan 1 focuses on endpoint detection and response (EDR) capabilities, while Plan 2 includes additional features such as agentless vulnerability scanning and malware detection.

Defender for Storage

Microsoft Defender for Storage is a security solution designed to protect Azure storage accounts from potential threats such as malicious file uploads, sensitive data exfiltration, and data corruption. It utilizes advanced threat detection capabilities powered by Microsoft Threat Intelligence, Microsoft Defender Antivirus, and Sensitive Data Discovery. Key features include activity monitoring, sensitive data threat detection (currently in preview), and malware scanning. The service can be enabled at the subscription or resource level, ensuring that all existing and newly created storage accounts are automatically protected, with the option to exclude specific accounts.

The benefits of Defender for Storage include improved malware protection through near real-time scanning of uploaded content, enhanced threat detection for sensitive data, and the ability to detect suspicious activities from entities without identities. The service operates without the need for enabling diagnostic logs and provides frictionless enablement at scale. Pricing is based on the number of protected storage accounts, with additional charges for malware scanning based on the volume of data scanned. This flexibility allows organizations to manage their security coverage effectively while controlling costs.

Malware scanning for Defender for Cloud Storage

The Malware Scanning feature in Microsoft Defender for Storage protects Azure Blob Storage from malicious content by performing near real-time scans using Microsoft Defender Antivirus. This agentless solution allows for simple setup and automation at scale, helping organizations meet security and compliance requirements. It scans all file types, including archives, and can delete or quarantine suspicious files based on predefined triggers. The service generates detailed security alerts when malware is detected, ensuring comprehensive protection for storage accounts.

Key use cases for Malware Scanning include web applications, content protection, compliance adherence, third-party data integration, collaborative platforms, data pipelines, and ensuring the integrity of machine learning training data. The service is designed to operate without retaining scanned content. It supports various methods for providing scan results, including blob index tags and Microsoft Defender for Cloud security alerts, Azure Event Grid, and Azure Log Analytics Workspace. Additionally, it features cost control mechanisms, allowing organizations to set monthly scanning limits and manage expenses effectively while ensuring robust malware protection

Detect threats to sensitive data

Sensitive data threat detection helps prioritize and examine security alerts based on the sensitivity of data at risk. This feature enhances data protection by detecting exposure events and suspicious activities. It is powered by an agentless sensitive data discovery engine that scans resources for sensitive data, integrated with Microsoft Purview's sensitive information types and classification labels.

Sensitive data threat detection is enabled by default with Defender for Storage and can be managed in the Azure portal. It supports various Blob storage accounts and requires relevant permissions for activation. Alerts generated from this feature provide insights into sensitivity scanning and operations performed on sensitive data resources. Additionally, organizations can customize sensitivity settings through Microsoft Purview, including creating custom sensitive information types and sensitivity labels.

Implement and manage Microsoft Defender Vulnerability Management

Vulnerability assessment for Azure is powered by Microsoft Defender Vulnerability Management. This solution allows security teams to discover and remediate vulnerabilities in container images without requiring configuration or agent deployment. It specifically supports scanning images in the Azure Container Registry (ACR), and images from other registries must be imported into ACR.

Images in ACR are scanned for vulnerabilities shortly after being added and rescanned every 24 hours. The assessment includes scanning OS packages and language-specific packages, and it provides exploitability information for vulnerabilities. Recommendations and vulnerability reports are generated for images in ACR and those running in Azure Kubernetes Service (AKS).

Log analytics workspaces

A Log Analytics workspace is a centralized data store for collecting log data from both Azure and non-Azure resources and applications. It allows users to manage log data effectively through Azure Monitor features, including insights experiences, alerts, and automatic actions. The workspace supports integration with other Azure services like Microsoft Sentinel and Logic Apps, as well as Microsoft tools such as Power BI and Excel. Users can create custom tables for non-Azure data and manage access, retention, and costs associated with the data stored in these tables.

Data retention in a Log Analytics workspace is divided into interactive and long-term retention, allowing users to retrieve and visualize data as needed. Access to the workspace is controlled through specific permissions, and insights into workspace usage and performance can be monitored. Additionally, data collection rules enable filtering and transformation of data before ingestion, optimizing the workspace for specific business needs without incurring direct costs for

workspace maintenance. However, charges apply for data ingestion and retention based on the table plan.

Deploy Azure Monitor Agent

The Azure Monitor Agent is a tool designed to collect monitoring data from the guest operating systems of Azure and hybrid virtual machines (VMs). It delivers this data to Azure Monitor, which can be utilized by various services, including Microsoft Sentinel and Microsoft Defender for Cloud.

Installation of the Azure Monitor Agent can be performed through various methods, allowing it to be deployed on VMs in Azure, other clouds, or on-premises environments. It collects data from local logs and performance metrics, providing comprehensive monitoring capabilities. The agent can be installed individually or at scale using Azure Policy, and it may be automatically installed when enabling certain features that require it.

Data collection is managed through data collection rules (DCRs), where users define the types of data to be collected, transformations, and the destination for this data. A DCR can encompass multiple data sources, allowing for flexible and centralized management of data collection across different machines. While there is no cost to use the Azure Monitor Agent itself, charges may apply for the data that is ingested and stored.

Connect to your Azure Subscription

Microsoft Defender for Cloud on Azure subscriptions is a cloud-native application protection platform that integrates security measures for cloud applications. It includes capabilities such as DevSecOps, cloud security posture management (CSPM), and cloud workload protection. Users can access foundational CSPM features for free for the first 30 days, after which charges apply based on the selected plans.

Just-in-time machine access

Just-in-time machine access is a feature provided by Defender for Servers Plan 2 in Microsoft Defender for Cloud, designed to reduce the attack surface of virtual machines (VMs) by limiting the number of open management ports, such as RDP or SSH. This feature addresses the challenge of balancing the need for legitimate user access with the necessity of security, as threat actors often target accessible machines with open ports. By enabling JIT access, organizations can lock down inbound traffic to their VMs, allowing access only when needed while minimizing exposure to potential attacks.

In Azure, enabling just-in-time access involves configuring network security group (NSG) rules to block inbound traffic on specific ports. Defender for Cloud ensures that “deny all inbound traffic” rules are established for the selected ports, thereby protecting the management ports of

Azure VMs from unauthorized access. When a user requests access, Defender for Cloud checks their permissions and, if approved, temporarily allows inbound traffic from the specified IP address for a defined period. After the time expires, the NSGs revert to their previous state, ensuring that connections already established remain uninterrupted.

In AWS, just-in-time access functions similarly by revoking rules in the attached EC2 security groups for the selected ports. When access is requested, Defender for Cloud verifies the user's permissions and, upon approval, creates a new EC2 security group that permits inbound traffic to the specified ports. This temporary access is also time-bound, with the system automatically restoring previous security settings after the specified duration. It is important to note that JIT access does not support VMs protected by Azure Firewalls managed by Azure Firewall Manager.

Container security in Microsoft Defender for Containers

Microsoft Defender for Containers is a cloud-native solution aimed at enhancing the security of containerized assets, including Kubernetes clusters, nodes, workloads, container registries, and images across multicloud and on-premises environments. It focuses on four core domains of container security: security posture management, vulnerability assessment, run-time threat protection, and deployment & monitoring.

Security posture management involves continuous monitoring of cloud and Kubernetes APIs to detect misconfigurations and provide risk assessments. The vulnerability assessment feature offers agentless scanning for vulnerabilities in container images with remediation guidelines. Run-time threat protection provides real-time detection of threats in Kubernetes environments, while deployment & monitoring ensure that Kubernetes clusters are properly monitored and managed. Overall, Microsoft Defender for Containers helps organizations secure their containerized applications effectively.

Defender for container architecture

The architecture of Microsoft Defender for Containers is tailored for various Kubernetes environments, including Azure Kubernetes Service (AKS), Amazon Elastic Kubernetes Service (EKS), Google Kubernetes Engine (GKE), and unmanaged Kubernetes distributions. Defender for Containers protects Kubernetes containers by analyzing audit logs, security events, and cluster configurations. It employs an agentless collection method for audit logs in AKS, EKS, and GKE, while utilizing a Defender agent for runtime protection through Extended Berkeley Packet Filter (eBPF) technology. Key components include the Defender agent, which collects signals from hosts, and Azure Policy for Kubernetes, which enforces policies across clusters.

In each Kubernetes environment, Defender for Containers implements a discovery process based on snapshots taken at intervals. For AKS, the Defender agent is deployed as a DaemonSet on each node, while in EKS and GKE, audit logs are collected agentlessly through their respective cloud services. The architecture also includes the use of Azure Arc-enabled

Kubernetes for connecting clusters to Defender for Cloud, allowing for centralized management and protection. The architecture emphasizes secure access through features like Trusted Access, which enables Azure services to interact with AKS without exposing the Kubernetes API server to unnecessary risks.

Microsoft Defender for Cloud DevOps Security

Microsoft Defender for Cloud provides comprehensive visibility, posture management, and threat protection across multicloud environments, including Azure, AWS, GCP, and on-premises resources. Within this framework, DevOps security utilizes a central console to enable security teams to protect applications and resources from code to cloud across various pipeline environments such as Azure DevOps, GitHub, and GitLab. Key capabilities include unified visibility into the DevOps security posture, strengthening cloud resource configurations throughout the development lifecycle, and prioritizing remediation of critical issues in code through contextual insights and custom workflows.

The DevOps security console allows management of connected environments, offering a high-level overview of discovered issues. Users can onboard Azure DevOps, GitHub, and GitLab environments, customize metrics, and configure pull request annotations. The DevOps inventory table provides detailed information on onboarded resources, including their advanced security status and findings related to codes, secrets, and vulnerabilities. Currently, advanced security information is available for Azure DevOps and GitHub repositories, with specific features like pull request annotations applicable to Azure DevOps only.

DevOps environment security posture

Securing DevOps platforms is essential due to the increasing cyber attacks targeting source code management systems and CI/CD pipelines. Microsoft Defender for Cloud offers DevOps posture management, which provides insights into the security posture throughout the software supply chain lifecycle. It employs advanced scanners to assess security configurations and access controls, helping organizations reduce their attack surface by acting on the recommendations provided. The scanners conduct recurring scans every 24 hours across various resources, including builds, secure files, and repositories, to identify weaknesses and misconfigurations.

The DevOps threat matrix is a comprehensive knowledge base developed to track and defend against relevant attack techniques in DevOps environments, utilizing the MITRE ATT&CK framework. It categorizes various tactics and techniques used by attackers, such as initial access, execution, and privilege escalation, and provides actionable recommendations for enhancing security. By addressing identified vulnerabilities and implementing best practices, organizations can strengthen their DevOps environments against potential threats, ensuring a resilient, zero-trust posture.

Configure the Microsoft Security DevOps GitHub action

Microsoft Security DevOps is a command-line application that integrates static analysis tools into the development lifecycle. It installs, configures, and runs various static analysis tools, including those for security and compliance, enabling deterministic execution across multiple environments. The tools include AntiMalware for scanning malware, Bandit for Python, BinSkim for binaries, ESlint for JavaScript, Template Analyzer for ARM templates, Terrascan for Terraform and Kubernetes, and Trivy for container images and Infrastructure as Code (IaC).

To configure the Microsoft Security DevOps GitHub action, users need to have an Azure subscription and connect their GitHub repositories. The setup involves creating a new workflow in GitHub, naming the workflow file, and copying a sample action workflow into it. After committing the new file, users can verify that the action is running. To view scan results, users can navigate to the Security section in GitHub and filter code scanning alerts by tool, with results also available in Defender for Cloud recommendations.

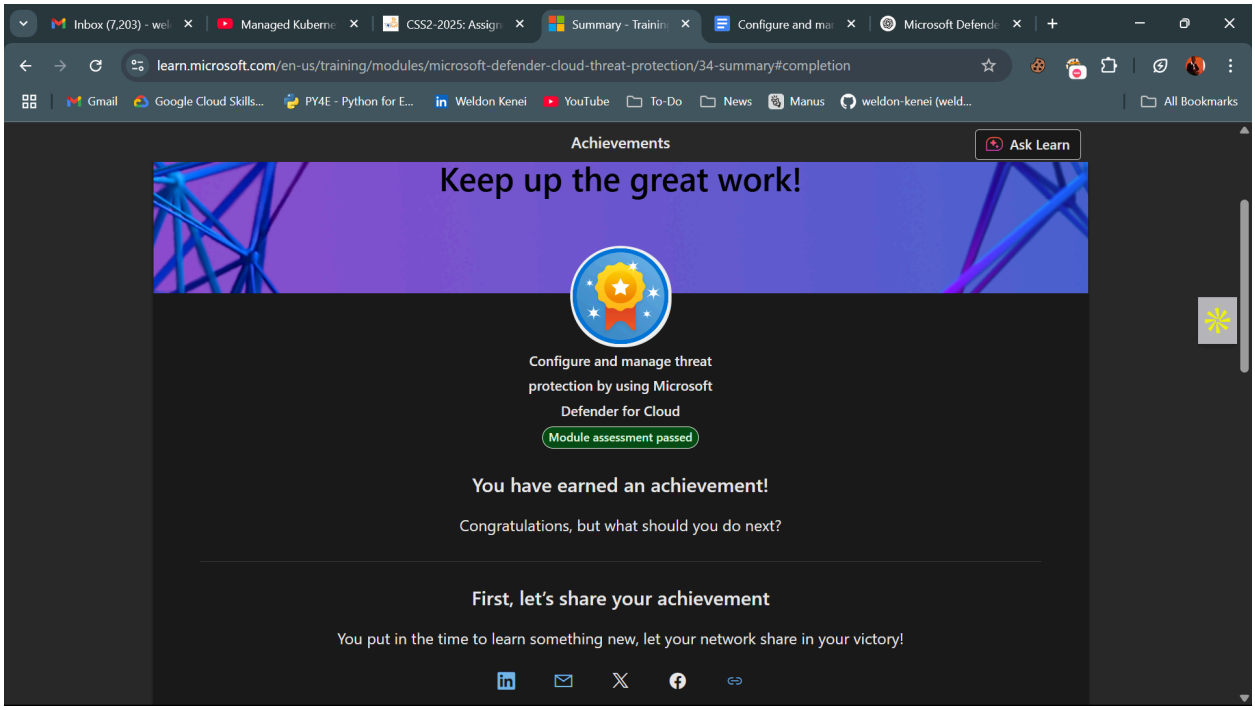
Defender for Cloud AI threat protection

Microsoft Defender for Cloud's AI threat protection identifies threats to generative AI applications in real time and assists in responding to security issues. It works in conjunction with Azure AI Content Safety Prompt Shields and Microsoft's threat intelligence to provide alerts for threats such as data leakage, data poisoning, jailbreak, and credential theft. Currently, this feature is in limited preview, and users should refer to the Supplemental Terms of Use for legal terms applicable to Azure features in preview.

The AI threat protection integrates with Defender XDR, enabling security teams to centralize alerts related to AI workloads in the Defender XDR portal. This integration allows teams to correlate alerts and incidents to gain a comprehensive understanding of attacks, including malicious activities associated with generative AI applications. The feature is available for specific AI services, including Azure OpenAI and Azure AI Model Inference service, but currently supports only text tokens, with image and audio tokens not being scanned.

Conclusion

To conclude, we have learned how to enable workload protection services, configure security for servers, databases, and storage, implement agentless scanning for virtual machines, manage vulnerability assessments for Azure virtual machines, and integrate Microsoft Defender for Cloud DevOps Security with GitHub, Azure DevOps, and GitLab.
https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/NVS7MZBF?sharingId=1C66F93EC0530812


Inbox (7,203) - wel
Managed Kuberne
CSS2-2025: Assign
Summary - Training
Configure and mar
Microsoft Defende
learn.microsoft.com/en-us/training/modules/microsoft-defender-cloud-threat-protection/34-summary#completion
Gmail
Google Cloud Skills...
PY4E - Python for E...
Weldon Kenei
YouTube
To-Do
News
Manus
weldon-kenei (weld...
All Bookmarks
Achievements
Ask Learn
Keep up the great work!
Configure and manage threat protection by using Microsoft Defender for Cloud
Module assessment passed
You have earned an achievement!
Congratulations, but what should you do next?
First, let's share your achievement
You put in the time to learn something new, let your network share in your victory!