

Become a Microsoft Defender for Cloud Ninja

Yuri Diogenes -



Edited by www.phack.tech



https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/become-a-microsoft-defender-for-cloud-ninja/ba-p/1608761?WT.mc_id

Every month we are adding new updates to this article, and you can track it by checking the *red* date besides the topic. If you already study all the modules and you are ready for the *knowledge check*, follow the procedures below:










1. Take the knowledge check [here](#).
2. If you score 80% or more in the knowledge check, request your participation certificate [here](#). If you achieved less than 80%, please review the questions that you got it wrong, study more and take the assessment again.





















Note: it can take up to 24 hours for you to receive your certificate via email.

Module 1 - Introducing Microsoft Defender for Cloud and Microsoft Defender







-  [What is Microsoft Defender for Cloud](#)
-  [Getting Started with Microsoft Defender for Cloud](#)
-  [A new name for multi-cloud security: Microsoft Defender for Cloud](#)
-  [Microsoft Defender for Cloud plans](#)
-  [Microsoft Defender for Cloud Total Economic Impact Study](#)
-  [Introduction to Microsoft Defender for Cloud](#)
-  [Securing the hybrid cloud with Microsoft Defender for Cloud](#)
-  [Hybrid security management across your data center](#)
-  [Understanding Microsoft Defender for Cloud and Microsoft Defender for Cloud plans Pricing](#)
-  [Microsoft Defender for Cloud Data Flow](#)
-  [How Microsoft uses Microsoft Defender for Cloud & Microsoft Defender for Cloud plans](#)
-  [Microsoft Defender for Cloud - Updates from Ignite 2021](#)
-  [Secure sensitive data in your cloud resources](#)
































Module 2 – Planning Microsoft Defender for Cloud

-  [Supported Platforms](#)
-  [Microsoft Defender for Cloud - Use cases](#)
-  [Microsoft Defender for Servers P1 and P2](#)
-  [Microsoft Defender for Cloud Plans](#)
-  [Features for IaaS workloads](#)
-  [Features for PaaS workloads](#)
-  [Built-in RBAC Roles in Microsoft Defender for Cloud](#)
-  [Enterprise Onboarding Guide](#)
-  [Assigning Permissions in Microsoft Defender for Cloud](#)



-  [Design Considerations for Log Analytics Workspace](#)
-  [Microsoft Defender for Cloud Monitoring Agent Deployment Options](#)
-  [Onboarding on-premises machines using Windows Admin Center](#)
-  [Understanding Security Policies in Microsoft Defender for Cloud](#)
-  [Creating Custom Policies](#)
-  [Configuring Microsoft Defender for Cloud Resource Type Pricing with Azure Policy](#)
-  [Centralized Policy Management in Microsoft Defender for Cloud using Management Groups](#)
-  [Planning Data Collection for IaaS VMs](#)
-  [Considerations for Multi-Tenant Scenario](#)
-  [Best Practices for Log Analytics Workspace when using Microsoft Defender for Cloud and Azure Sentinel...](#)
-  [How to Effectively Perform an Microsoft Defender for Cloud PoC](#)
 -  [Microsoft Defender for Cloud PoC Series – Microsoft Defender for Resource Manager](#)
 -  [Microsoft Defender for Cloud PoC Series – Microsoft Defender for Storage](#)
 -  [Microsoft Defender for Cloud PoC Series – Microsoft Defender for DNS](#)
 -  [Microsoft Defender for Cloud PoC Series – Microsoft Defender for App Service](#)
 -  [Microsoft Defender for Cloud PoC Series - Microsoft Defender for Container Registries](#)
 -  [Microsoft Defender for Cloud PoC Series – Microsoft Defender CSPM \(04/2023\)](#)
-  [Grant tenant-wide permissions to yourself](#)
-  [Azure Security Benchmark is now the default policy initiative for Microsoft Defender for Cloud](#)
-  [Protect non-Azure resources using Azure Arc and Microsoft Defender for Cloud](#)


































Module 3 – Enhance your Cloud Security Posture

-  [Overview of Secure Score in Microsoft Defender for Cloud](#)
-  [Azure Secure Score vs. Microsoft Secure Score](#)
-  [Best Practices to improve your secure score](#)
-  [How to calculate your secure score](#)
-  [Secure Score Capabilities](#)
-  [How Secure Score affects your governance](#)
-  [Enhance your Secure Score in Microsoft Defender for Cloud](#)
-  [Security recommendations](#)
-  [Creating Exemptions and Enforcing Policies](#)
-  [Resource exemption](#)

-  [Customizing Endpoint Protection Recommendation in Microsoft Defender for Cloud](#)
-  [How to keep track of Resource Exemptions in Microsoft Defender for Cloud](#)
-  [Deliver a Security Score weekly briefing](#)
-  [Send Microsoft Defender for Cloud Recommendations to Azure Resource Stakeholders](#)
-  [Secure Score Over Time Reports](#)
-  [Secure Score Reduction Alert](#)
-  [Weekly Secure Score Progress Report](#)
-  [Average Time taken to remediate resources](#)
-  [Improved experience for managing the default Azure security policies \(04/2023\)](#)
-  [Security Policy Enhancements in Defender for Cloud \(04/2023\)](#)
-  [Create custom recommendations and security standards \(04/2023\)](#)
-  [Secure Score Overtime Workbook](#)
-  [Automation Artifacts for Secure Score Recommendations](#)
-  [Remediation Scripts](#)
-  [Security Controls in Microsoft Defender for Cloud](#)
 -  [Enable MFA](#)
 -  [Restrict Unauthorized Network Access](#)
 -  [Secure Management Ports](#)
 -  [Secure management ports demo](#)
 -  [Apply adaptive application control](#)
 -  [Enable auditing and logging](#)
 -  [Enable auditing and logging demo](#)
 -  [Remediate security configurations](#)
 -  [Apply system updates](#)
 -  [Enable endpoint protection demo](#)
 -  [Encrypt data in transit](#)
 -  [Encrypt data at rest](#)
 -  [Protect Applications Against DDoS Attacks](#)
 -  [Implement security best practices](#)
- Using Attack Path to prioritize risk (04/2023)
 -  [A Proactive Approach to Cloud Security Posture Management with Microsoft Defender for Cloud](#)
 -  [Prioritize Risk remediation with Microsoft Defender for Cloud Attack Path Analysis](#)











Module 4 – Cloud Security Posture Management Capabilities in Microsoft Defender for Cloud

-  [Overview of the Asset Inventory feature in Microsoft Defender for Cloud](#)
-  [Software inventory filters added to asset inventory](#)










-  [Drive your organization to security actions using Governance experience](#)
-  [Microsoft Defender for Cloud and Azure Security Benchmark](#)
-  [Managing Asset Inventory in Microsoft Defender for Cloud](#)
-  [New Security Baseline recommendation](#)
-  [Overview of Vulnerability Assessment in Microsoft Defender for Cloud](#)
-  [Vulnerability Assessment Deployment Options](#)
-  [Vulnerability Assessment Workbook Template](#)
-  [Vulnerability Assessment for Containers](#)
-  [Microsoft Threat and Vulnerability Management added as vulnerability assessment solution](#)
-  [Exporting Azure Container Registry Vulnerability Assessment in Microsoft Defender for Cloud](#)
-  [Improvements in Continuous Export feature](#)
-  [Implementing Workflow Automation](#)
-  [Workflow Automation Artifacts](#)
-  [Creating Custom Dashboard for Microsoft Defender for Cloud](#)
-  [Using Microsoft Defender for Cloud API for Workflow Automation](#)
-  [Understanding Network Map](#)
-  [Using Adaptive Network Hardening](#)
-  [Identify security vulnerabilities workloads managed by Microsoft Defender for Cloud](#)
-  [Multi Cloud support in Microsoft Defender for Cloud](#)
-  [What you need to know when deleting and re-creating the security connector\(s\) in Defender for Cloud](#)
-  [Connect AWS Account with Microsoft Defender for Cloud](#)
 -  [Custom assessments and standards in Microsoft Defender for Cloud for AWS workloads](#)
 -  [Video Demo - Connecting AWS accounts](#)
 -  [Microsoft Defender for Cloud PoC Series - Multi-cloud with AWS](#)
-  [Connect GCP Account with Microsoft Defender for Cloud](#)
 -  [Protecting Containers in GCP with Defender for Containers](#)
 -  [Custom assessments and standards in Microsoft Defender for Cloud for GCP workloads](#)
 -  [Video Demo - Connecting GCP Accounts](#)
 -  [Microsoft Defender for Cloud PoC Series - Multicloud with GCP](#)
-  [Protection for multi cloud workloads](#)
-  [Azure Monitor Workbooks integrated into Microsoft Defender for Cloud and three templates provided](#)
-  [How to Generate a Microsoft Defender for Cloud exemption and disable policy report](#)
-  [Azure Workbooks in Microsoft Defender for Cloud](#)



































-  [New Network Security Dashboard for Microsoft Defender for Cloud](#)
-  [CSPM Improvements announced at Ignite 2021](#)
-  [Custom assessments and standards in Microsoft Defender for Cloud for AWS workloads](#)
-  [Cloud Security Explorer](#)
-  [Identify and remediate attack paths](#)
-  [Agentless scanning for machines](#)
-  [Cloud security explorer and Attack path analysis](#)
-  [Governance Rules at Scale](#)
-  [Governance Improvements](#)
















Module 5 – Regulatory Compliance Capabilities in Microsoft Defender for Cloud

-  [Regulatory compliance dashboard](#)
-  [Understanding Regulatory Compliance Capabilities in Microsoft Defender for Cloud](#)
-  [Regulatory Compliance dashboard and security benchmark](#)
-  [Adding new regulatory compliance standards](#)
-  [Blueprint samples for regulatory compliance standards](#)
-  [Regulatory Compliance workbook](#)
-  [Regulatory compliance dashboard now includes Azure Audit reports](#)
-  [Azure Security Benchmark v3 integration with Regulatory Compliance dashboard](#)
-  [Latest updates in the regulatory compliance dashboard \(Nov 2022\)](#)
-  [Microsoft cloud security benchmark: Azure compute benchmark is now aligned with CIS!](#)









Module 6 – Cloud Workload Protection Platform Capabilities in Microsoft Defender for Clouds

-  [Enhanced Security in Microsoft Defender for Cloud](#)
-  [Understanding Just-in-Time VM Access](#)
-  [Demystifying Microsoft Defender Once for All](#)
-  [Reducing the Attack Surface with Just-In-Time VM Access](#)
-  [Implementing JIT VM Access](#)
-  [Automate JIT VM Access Deployment with PowerShell](#)
-  [File Integrity Monitoring in Microsoft Defender](#)
-  [Define known-safe applications using Adaptive Application Control](#)
-  [Understanding Threat Protection in Microsoft Defender](#)
-  [Microsoft Defender for Servers](#)
 -  [January 2022 Updates for Defender for Servers](#)

-  [Keep Calm and Deploy Defender for Servers](#)
 -  [Demystifying Defender for Servers \(04/2023\)](#)
-  [Microsoft Defender for Network Layer](#)
-  [Microsoft Defender for AKS](#)
-  [Microsoft Defender for Containers](#)
 -  [January 2022 Updates for Defender for Containers](#)
 -  [Demystifying Microsoft Defender for Containers](#)
 -  [Basics of Defender for Containers](#)
 -  [Secure your Containers from Build to Runtime](#)
 -  [AWS ECR Coverage in Defender for Containers](#)
-  [Microsoft Defender for Storage](#)
 -  [Protect your storage resources against blob-hunting](#)
 -  [Malware Scanning in Defender for Storage \(04/2023\)](#)
-  [Microsoft Defender for SQL](#)
-  [Microsoft Defender for SQL and the Vulnerability Assessment \(VA\)](#)
 -  [New Defender for SQL VA](#)
-  [Microsoft Defender for SQL Anywhere](#)
 -  [Validating Alerts on Microsoft Defender for SQL on machines](#)
-  [Microsoft Defender for KeyVault](#)
-  [Microsoft Defender for AppService](#)
 -  [How Microsoft Defender for App Service works](#)
-  [Microsoft Defender for IoT](#)
-  [Microsoft Defender for Resource Manager and DNS](#)
-  [Microsoft Defender for Resource Manager](#)
-  [Microsoft Defender for DNS](#)
-  [Understanding Security Incident](#)
-  [Overview of Security Alerts in Microsoft Defender for Cloud](#)
-  [Alert Reference Guide](#)
-  ['Copy alert JSON' button added to security alert details pane](#)
-  [Alert Suppression](#)
- [Simulating Alerts in Microsoft Defender for Cloud](#)
 -  [Alert validation](#)
 -  [Simulating alerts for Windows](#)
 -  [Simulating alerts for Linux](#)
 -  [Simulating alerts for Containers](#)
 -  [Simulating alerts for Storage](#)
 - [Simulating alerts for Microsoft Key Vault](#)
 - [Simulating alerts for Microsoft Defender for DNS](#)





-  [Simulating alerts for Microsoft Defender for Resource Manager](#)
-  [Microsoft Defender PoC Series – Microsoft Defender for App Service](#)
-  [Troubleshooting Alerts](#)
-  [Integration with Microsoft Defender for Endpoint](#)
 -  [Auto-provisioning of Microsoft Defender for Endpoint unified solution](#)
-  [Resolve security threats with Microsoft Defender for Cloud](#)
-  [Protect your servers and VMs from brute-force and malware attacks with Microsoft Defender for Cloud](#)
-  [Investigating Microsoft Defender for Cloud alerts using Azure Sentinel](#)
-  [Service Layer Protection - Microsoft Defender for Resource Manager and DNS](#)
-  [Identify vulnerable container images in CI/CD workflows](#)
-  [Azure Arc and Azure Microsoft for Kubernetes](#)
-  [Enhance your CI/CD deployment with Microsoft Defender for ACR](#)
-  [Filter security alerts by IP address](#)
-  [Alerts by resource group](#)
-  [Defender for Servers Security Alerts Improvements](#)

Module 7 – Streaming Alerts and Recommendations to a SIEM Solution

-  [Continuous Export capability in Microsoft Defender for Cloud](#)
-  [Deploying Continuous Export using Azure Policy](#)
-  [Microsoft Defender for Cloud How Azure Sentinel and Microsoft Defender for Cloud Work Together](#)
-  [Connecting Microsoft Sentinel with Microsoft Defender for Cloud](#)
-  [Closing an Incident in Azure Sentinel and Dismissing an Alert in Microsoft Defender for Cloud](#)
-  [Accessing Microsoft Defender for Cloud Alerts in Splunk using Graph Security API Integration](#)
-  [Microsoft Defender and Microsoft Sentinel - Better Together](#)
-  [Microsoft Sentinel bi-directional alert synchronization](#)

Module 8 – Integrations and APIs

-  [Integration with Tenable](#)
-  [Integrate security solutions in Microsoft Defender for Cloud](#)
-  [Defender for Cloud integration with Defender EASM](#)
-  [Defender for Cloud integration with Defender TI](#)
-  [REST APIs for Microsoft Defender for Cloud](#)

-  [Obtaining Secure Score via REST API](#)
-  [Using Graph Security API to Query Alerts in Microsoft Defender for Cloud](#)
-  [Automate\(d\) Security with Microsoft Defender for Cloud and Logic Apps](#)
-  [Automating Cloud Security Posture and Cloud Workload Protection Responses](#)

Module 9 – Defender for DevOps

-  [Overview of Defender for DevOps](#)
-  [Defender for DevOps Interactive Guide](#)
-  [Introduction of Defender for DevOps](#)
-  [Defender for DevOps Appendix from Defender for Cloud Book by MSPress](#)
-  [Configure the Microsoft Security DevOps Azure DevOps extension](#)
-  [Configure the Microsoft Security DevOps GitHub action](#)
-  [Automate SecOps to Developer Communication with Defender for DevOps](#)
-  [Compliance for Exposed Secrets Discovered by Defender for DevOps](#)
-  [Automate Defender for DevOps Recommendation Remediation](#)
-  [DevOps Security Workbook](#)
-  [Remediating Security Issues in Code with Pull Request Annotations](#)
-  [Code to Cloud Security using Microsoft Defender for DevOps \(04/2023\)](#)