



THAILAND

Cyber
Security



 Microsoft Security

Cloud

SECURITY

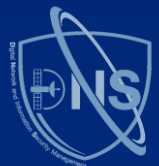
Intensive



Sarah

Saran Hansakul

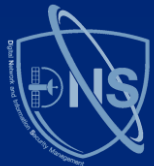
IT & Brand Manager
Rainbow Silver Co.,Ltd.
(AKE AKE Thailand)





1 Overview

Cloud Sec ?
Learning Tips





Cloud?  17788
 SP 800-145

On-demand, Self Service
Broad Network Access
Resource Pooling
Rapid Elasticity
Measured Services

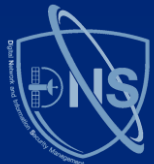
Service

Deployment

IaaS 

PaaS 
vs FaaS ?

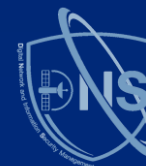
SaaS   





Cloud Sec Engineer
System Netw Audit Specialist/Consults Admin
Engineer Architect Consultant Analyst

Cost \$\$\$?
ROI ?





Search Github Labs with exam code

microsoft github labs **az-500**

SEARCH COPILOT WORK

About 525,000 results

GitHub
<https://github.com/MicrosoftLearning/AZ500-AzureSecurityTechnologies>

AZ500 AzureSecurityTechnologies

Microsoft Azure Security Technologies

66 Watched 810 Starred 786 Forks

Primary language: Bicep License: MIT license

Website: <https://microsoftlearning.github.io/AZ500-AzureSecurityTechnologies/>

Practice / Blogging Actual Hands-on





Files

master

Go to file

> 11

> 12

> 13

> 14

> 15

▼ Instructions

> Archived_Labs

▼ Labs

LAB_01_RBAC.md

LAB_02_NSGs.md

LAB_03_AzureFirewall.md

LAB_04_ConfiguringandSecuri...

LAB_05_SecuringAzureSQLDat...

LAB_06_SecuringAzureStorage...

LAB_07_KeyVaultImplementing...

AZ500-AzureSecurityTechnologies / Instru

serling1962 Update LAB_02_NSGs.md ✓

Name

..

LAB_01_RBAC.md

LAB_02_NSGs.md

LAB_03_AzureFirewall.md

LAB_04_ConfiguringandSecuringAC...

LAB_05_SecuringAzureSQLDatabas...

LAB_06_SecuringAzureStorage.MD

LAB_07_KeyVaultImplementingSec...

LAB_08_Azure Monitor.md

LAB_09_Microsoft Defender for Clo...

LAB_10_Microsoft Sentinel.md

Notifications

Fork 786

Star 810

AZ500-AzureSecurityTechnologies / Instructions / Labs / LAB_01_RBAC.md

Preview

Code

Blame

345 lines (212 loc) · 14.8 KB

Raw

Copy

Download

Edit

More

Student lab manual

Lab scenario

You have been asked to create a proof of concept showing how Azure users and groups are created. Also, how role-based access control is used to assign roles to groups. Specifically, you need to:

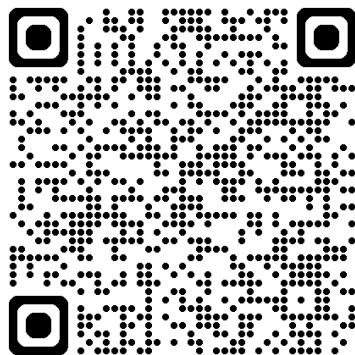
- Create a Senior Admins group containing the user account of Joseph Price as its member.
- Create a Junior Admins group containing the user account of Isabel Garcia as its member.
- Create a Service Desk group containing the user account of Dylan Williams as its member.
- Assign the Virtual Machine Contributor role to the Service Desk group.

For all the resources in this lab, we are using the East US region. Verify with your instructor this is the region to use for class.

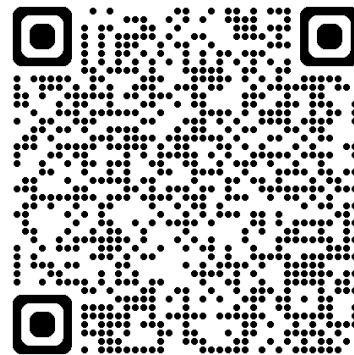
Lab objectives

In this lab, you will complete the following exercises:

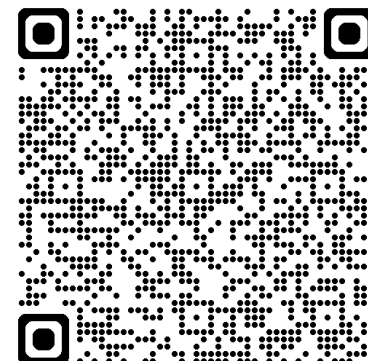
- Exercise 1: Create the Senior Admins group with the user account Joseph Price as its member (the Azure portal).
- Exercise 2: Create the Junior Admins group with the user account Isabel Garcia as its member (PowerShell).
- Exercise 3: Create the Service Desk group with the user Dylan Williams as its member (Azure CLI).
- Exercise 4: Assign the Virtual Machine Contributor role to the Service Desk group.



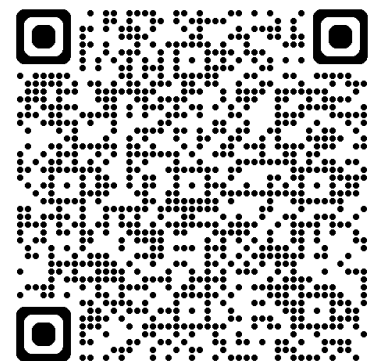
AZ-104 Labs



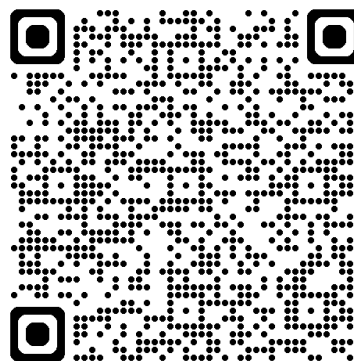
AZ-500 Labs



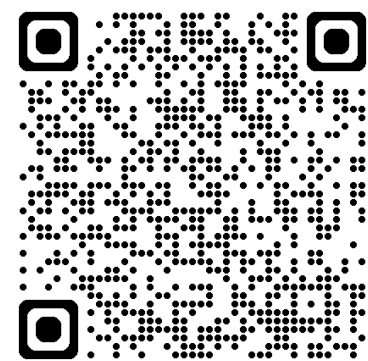
SC-900 Labs



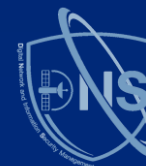
SC-200 Labs



SC-300 Labs



SC-400 Labs



SC-900

SECURITY
COMPLIANCE
IDENTITY



CONCEPT

SOLUTIONS

SECURITY

Cloud Adoption Framework
Shared Responsibility
Defense in Depth
Zero Trust
Encryption vs Hashing

COMPLIANCE

IDENTITY

Authentication vs Authorization
Identity as Perimeter: 4 Pillars – AAA+A
Identity Provider
Directory Service (AD) vs ADaaS
Federation

SC-900

SECURITY
COMPLIANCE
IDENTITY



CONCEPT

SOLUTIONS

IDENTITY (Azure AD)

Identity Control

Identity Types (User/Device/SP/Managed Identity) - External
Identity (B2B/B2C) - Hybrid Identity (Hash/Pass-through/Federated)

Authentication

Methods (Pwd/Passwordless) - MFA - SSPR - Password Protection

Authorization (Access Management)

Conditional Access - AD Role + RBAC

Governance

Entitlement/Access Review/TOU - PIM - Identity Protection

SECURITY

Basic (Network + Resource Lock)
Defender for Cloud
Sentinel
365 Defender
Intune

COMPLIANCE

Service Trust Portal / Privacy (Priva) Purview Compliance (365)

Portal / Compliance Score
Lifecycle (Sensitivity/DLP/Retention/Record)
Insider Risk/Comm.Compli/Info Barrier
eDiscovery/Audit

Purview Governance (Azure)

Portal (Map/Catalog/Estate)
Policy
Blueprint



SC-900

SECURITY
COMPLIANCE
IDENTITY



MS Cloud Adoption Framework

Best Practice from MS
for deploying Azure

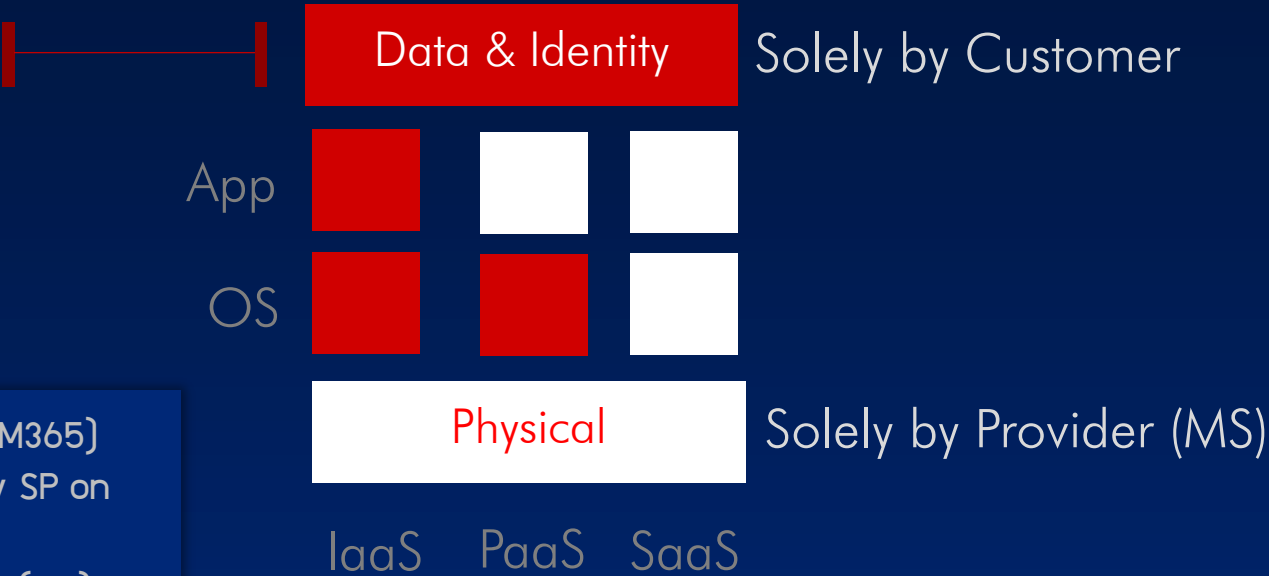
S trategy
P lan
R eady
A dopt
G overn
M anage

SC-900

SECURITY
COMPLIANCE
IDENTITY



Shared Responsibility Model



Q1: SaaS (M365) who apply SP on App?
A: Provider (MS)

Q2: IaaS (VM) who manage Physical network?
A: Provider (MS)

Q3: All cloud types, who is responsible for Data security?
A: Customer

SC-900

SECURITY
COMPLIANCE
IDENTITY



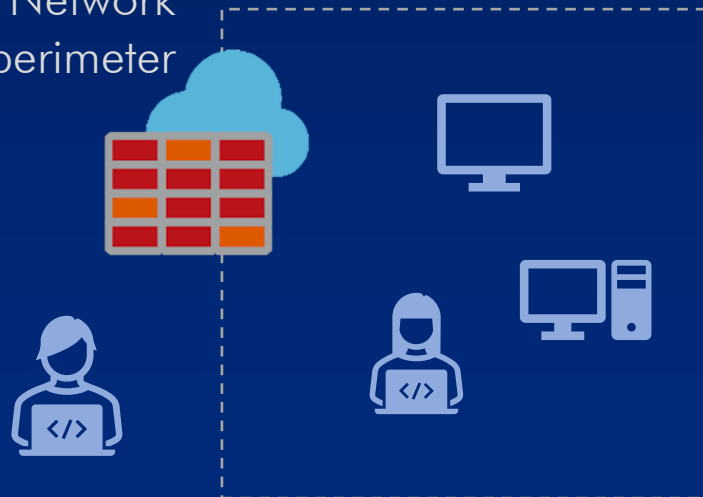
Zero-Trust

Verify explicitly

Least Privileged

Assume Breach

Firewall **cannot**
secure Network
perimeter



Use Identity
as perimeter

SC-900

SECURITY
COMPLIANCE
IDENTITY



6 Key Privacy Principle

Control

Transparency

Security

Strong Legal Protection

No Content-based Targeting

Benefits to you

SC-900

SECURITY
COMPLIANCE
IDENTITY



Encryption

Viewer need "Key"

Digital Signing – prove sender identity

Private Key – for signing

Public Key – for decrypting

Type

at rest – VM disk

in transit – VPN/HTTPS/Email

SC-900

SECURITY
COMPLIANCE
IDENTITY



Authentication



Authorization

Prove identity

Permit access

1st factor Authen:
login page for
Azure/M365 portal

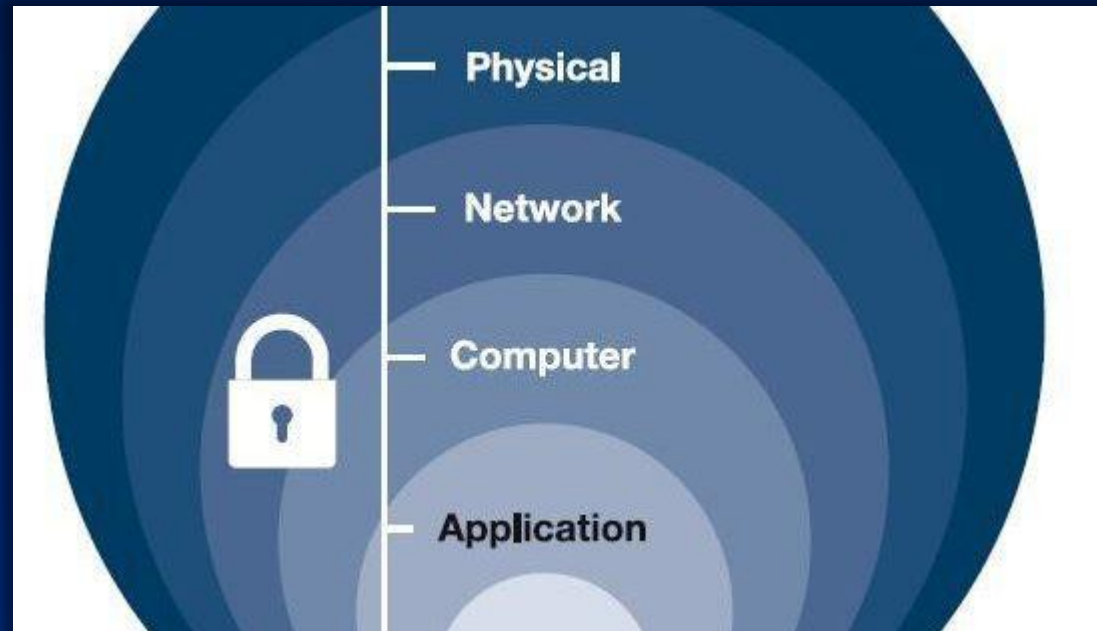
With Conditional
Access, etc. after 1st
factor Authen, e.g.
to force 2nd factor
Authen (MFA)

SC-900

SECURITY
COMPLIANCE
IDENTITY



Defense in Depth — Multilayer defense throughout network



APPLIED SKILLS
Configure SIEM security operations
using Microsoft Sentinel



SaraH
Saran Hansakul





APPLIED SKILLS
Microsoft
Sentinel




← ↻ 🏠 <https://learn.microsoft.com/en-us/credentials/applied-skills/configure-siem-security-operations-using-microsoft-sentinel/results?snapshotId=16389c97-071c-...> A ☆

Microsoft | **Learn** Documentation Training Credentials Q&A Code Samples Assessments Shows

Credentials Browse Credentials Certification Renewals FAQ & Help

[Learn](#) / [Credentials](#) / [Browse Credentials](#) / [Configure SIEM security operations using Microsoft Sentinel](#) /



Applied skills credential earned

Configure SIEM security operations using Microsoft Sentinel

Completed on Oct 29, 2023

[View my credential](#)

Share your achievement: [f](#) [t](#) [in](#) [✉](#)

PASS Assessment date: October 26, 2023

Your overall results: **100%** Pass

75% needed to pass

Performance by task

Love to have?





APPLIED SKILLS
Microsoft
Sentinel

Microsoft | [Learn](#) [Documentation](#) [Training](#) [Credentials](#) [Q&A](#) [Code Samples](#) [Assessments](#) [Shows](#)

SarahAHA

MCID: [REDACTED]

308
Badges

60
Trophies

56
Reputation
points

0
Accepted
answers

0
Following

0
Followers

LEVEL 13

[Activity](#)

[Training](#)

[Challenges](#)

Credentials

[Q&A](#)

[Achievements](#)

[Collections](#)

[Transcript](#)

[Credentials](#) / [View all Applied Skills](#)

Applied Skills [Certifications](#)

Applied Skills Earned

APPLIED SKILLS

Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

Earned on November 2, 2023

[View Credential](#) [Share](#)

APPLIED SKILLS

Configure SIEM security operations using Microsoft Sentinel

Earned on October 26, 2023

[View Credential](#) [Share](#)

 Online Verifiable



APPLIED SKILLS

Microsoft
Sentinel



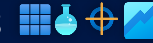
MS Sentinel



Deploy **Step 5**

Content

Hub Solutions



Build on:



Step 4

Log Analytics
Workspace

Set usage >>
Data Retention

Step 1

Assign Sentinel
Roles



IAM
of RG

Step 3

Least Privilege:

- Manage Incident: Sentinel Responder
- "Run" Playbook: Playbook Operator



Windows
Security Events

Configuring...

- Data Collection Rules



Azure
Activity

Configuring...

- Azure Policy
Assignment



Defender
for Cloud

Configuring...

- Bi-directional Sync



Analytics Rules

Set Near Real Time (NRT)
query



Automation

Set Near Real Time (NRT)
query



APPLIED SKILLS
Microsoft
Sentinel



LEARNING PATH

Configure SIEM security operations using Microsoft Sentinel

5 hr 11 min • 6 modules

[Start learning path >](#)

Modules in this learning path



Create and manage Microsoft Sentinel workspaces

34 min • Module • 9 units



Connect Microsoft services to Microsoft Sentinel

26 min • Module • 8 units



Connect Windows hosts to Microsoft Sentinel

26 min • Module • 7 units



Threat detection with Microsoft Sentinel analytics

1 hr 10 min • Module • 9 units



Threat response with Microsoft Sentinel playbooks

1 hr 20 min • Module • 7 units



Configure SIEM security operations using Microsoft Sentinel

1 hr 15 min • Module • 6 units

Online – Open Book

Exercise - Configure SIEM operations using Microsoft Sentinel

15 min

Exercise - Install Microsoft Sentinel Content Hub solutions and data connectors

25 min

Exercise - Configure a data connector Data Collection Rule

10 min

Exercise - Perform a simulated attack to validate the Analytic and Automation rules

15 min





APPLIED SKILLS

Microsoft
Sentinel

Exercise - Configure SIEM operations using Microsoft Sentinel

✓ 100 XP

15 minutes

Now it's your chance to deploy and configure a Microsoft Sentinel workspace.

In this exercise, you'll learn how to create an Azure Log Analytics workspace and Deploy Microsoft Sentinel to the workspace.

Note

To complete this exercise, you will need an [Azure subscription](#).

Launch the exercise and follow the instructions.

[Launch Exercise](#)

Next unit: Exercise - Install Microsoft connectors

[Continue](#)

<https://microsoftlearning.github.io/APL-5001-configure-siem-security-operations-using-microsoft-sentinel/Instructions/Lab01-Exercise01-ConfigureYourMicrosoftSentinelEnvironment.html>

Microsoft

Microsoft Learn

General guidelines

Architecture diagram

Skilling tasks

Exercise instructions

Note: To complete this lab, you will need an [Azure subscription](#), in which you have administrative access.

General guidelines

- When creating objects, use the default settings unless there are requirements to do otherwise.
- Only create, delete, or modify objects to achieve the stated requirements. Do not perform actions that adversely affect your final score.
- If there are multiple approaches to achieving a goal, always choose the one that requires the least administrative effort.

We are currently evaluating the existing security posture of our corporate environment. We need your help in setting up a security information and event management (SIEM) solution to help identify future and ongoing cyber-attacks.

Architecture diagram

Lab 01 - Exercise 01 - Configure your Microsoft Sentinel environment

Task 1: Initialize the Microsoft Sentinel Workspace



Sentinel

MicrosoftLearning/APL-5001-configure-siem-security-operations-using-microsoft-sentinel

Exercise instructions

Task 1 - Create a Log Analytics workspace

Create a Log Analytics workspace, including region option. Learn more about [onboarding Microsoft Sentinel](#).

- In the Azure portal, search for and select [Microsoft Sentinel](#).
- Select **+ Create**.
- Select **Create a new workspace**.
- Select [RG2](#) as the Resource Group.
- Enter a valid name for the Log Analytics workspace.
- Select [West US](#) as the region for the workspace.
- Select **Review + create** to validate the new workspace.
- Select **Create** to deploy the workspace.

Task 2 - Deploy Microsoft Sentinel to a workspace

Deploy Microsoft Sentinel to the workspace.

- Go to **Microsoft Sentinel**.
- Select the workspace you want to add Sentinel to (created in Task 1 step 5).
- Select **Add**.

Task 3 - Assign a Microsoft Sentinel role to a user

Assign a Microsoft Sentinel role to a user. Learn more about [Roles and permissions for working in Microsoft Sentinel](#).

- Go to the Resource group [RG2](#).
- Select **Access control (IAM)**.
- Select **Add** and [Add role assignment](#).
- In the search bar, search for and select the [Microsoft Sentinel Contributor](#) role.






APPLIED SKILLS
Microsoft
Sentinel

Take the assessment

🕒 You will have **2 hr** to complete this assessment.

This assessment will use an interactive lab to evaluate your performance. It will take a few minutes to load the lab, and you may  do other activities while it loads. Your mouse movements and text entered during the lab will be recorded for quality purposes. [Learn more](#)

🔄 **Need accommodations?**
We offer a variety of accommodations to support you. [Learn more](#)

Start

So...why wait?



APPLIED SKILLS
Microsoft
Sentinel

Microsoft | Learn Documentation Training Credentials

Credentials Browse Credentials Certification Renewals FAQ & Help

Learn / Credentials / Browse Credentials / [Secure your services and workloads with Microsoft Sentinel for Cloud Registry compliance controls](#)

To exit full screen, move mouse to top of screen or press **F11**

1 Hr 59 Min Remaining

Instructions 100%

▼ Step 1: Log into the virtual machine (if necessary)

If you were not automatically logged into the virtual machine, you will need to log in with the provided user/pass.

Username: Password:

ENG [Speaker Icon] [Power Icon]

Submit Assessment

Use F11 for full screen, find big monitor

Login to desktop first with provided user/pass

Open Emails

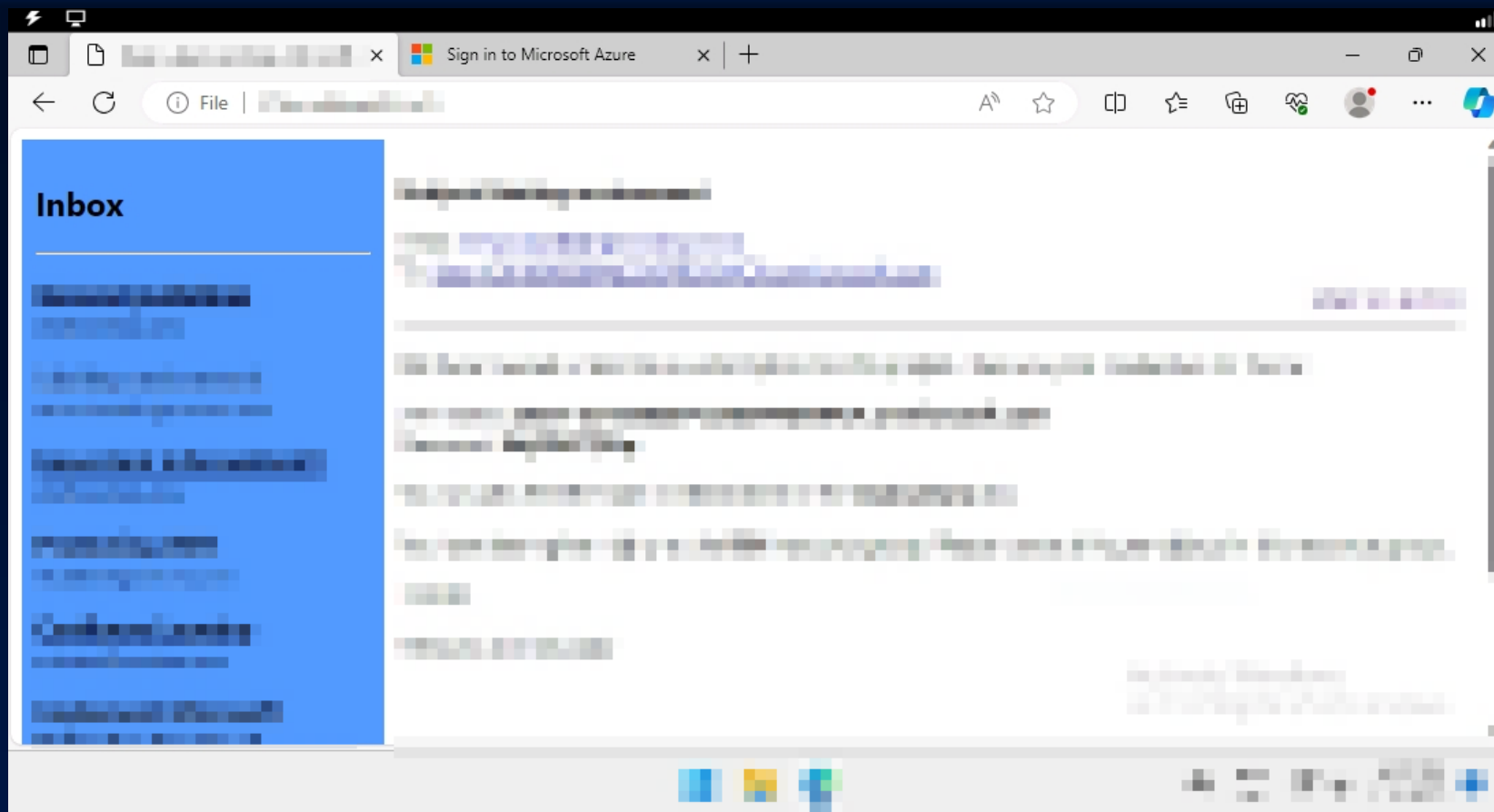
Then scroll direction down to click this.

Submit when every job complete.





APPLIED SKILLS
Microsoft
Sentinel



Direction mail



APPLIED SKILLS

Microsoft



Tips

- Do not wait for processing, open many Azure tabs and go ahead each job.
- Beware of what the direction mail specified: Resource Group, Region, user, resource name, etc.
- Use Default Settings if it is not instructed.
- Do not do unnecessary change.



APPLIED SKILLS
Microsoft
Sentinel

Microsoft | Learn Documentation Training Credentials Q&A Code Samples Assessments Shows

Credentials Browse Credentials Certification Renewals FAQ & Help

Learn /

Still scoring

Your results are still processing. If you don't see a result in 60 seconds, please refresh.

Just refresh every 60 secs.



Congratulations, you've earned a Microsoft Applied Skills credential

Inbox

M

Microsoft
To You

26 Oct

Microsoft

You've earned a Microsoft Applied Skills credential

SarahAHA,

Congratulations! You've earned the Microsoft Applied Skills credential for [Configure SIEM security operations using Microsoft Sentinel](#).

Celebrate your Applied Skills credential through your [Microsoft Learn profile](#), where you can:

← ↻ 🏠 <https://learn.microsoft.com/en-us/credentials/applied-skills/configure-siem-security-operations-using-microsoft-sentinel/results?snapshotId=16389c97-071c-...> ⌵ ☆

Microsoft | Learn Documentation Training Credentials Q&A Code Samples Assessments Shows

Credentials Browse Credentials Certification Renewals FAQ & Help

Learn / Credentials / Browse Credentials / Configure SIEM security operations using Microsoft Sentinel /

Applied skills credential earned

Configure SIEM security operations using Microsoft Sentinel

Completed on Oct 29, 2023

View my credential

Share your achievement: [f](#) [t](#) [in](#) [✉](#)





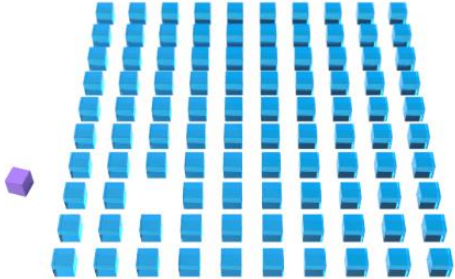
APPLIED SKILLS
Microsoft
Sentinel

Problems and Solutions

Microsoft | **Learn** Documentation Training Credentials Q&A Code Samples Assessments Shows

Credentials Browse Credentials Certification Renewals FAQ & Help

Learn /



Error

Sorry, something went wrong, please try again later

[Go to details page](#)

Do not click!
Just back to the previous page and
keep refreshing.



APPLIED SKILLS
Microsoft
Sentinel

Problems and Solutions

https://learn.microsoft.com/en-us/credentials/applied-skills/secure-azure-services-and-workloads-with-microsoft-defender-for-cloud-regulatory-compliance-...
Learn / Credentials / Browse Credentials / Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls /

Your assessment results for
Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

[Retake](#) You'll be eligible to retake the assessment in:
70 : 46 : 58
HOURS MINUTES SECONDS

FAIL Assessment date: October 26, 2023

Your overall results: **58%** **Fail**
66% needed to pass

Performance by task

- ✓ Configure Microsoft Defender for Cloud
- ✗ Implement just-in-time (JIT) VM access
- ✓ Implement a Log Analytics workspace

Fail? Wait for another 72hrs.
Count from beginning of the lab.

Explore preparation resources to help you earn a Microsoft Applied Skills credential

M Microsoft 26 Oct
To You ...



Retake the assessment to earn a Microsoft Applied Skills credential

SarahAHA,

Thanks for taking the assessment for the Microsoft Applied Skills, [Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls](#). Although you didn't pass this time, we encourage you to try again. We offer resources to help you prepare.





APPLIED SKILLS
Microsoft
Sentinel

Problems and Solutions

Personal Your applied skill results for Micro x +

← ↻ 🏠 🔒 https://learn.microsoft.com/en-us/credentials/applied-skills/configure-siem-security-operations-using-microsoft... ⌵ ☆ 10 🗨️ ⌵

Credentials Browse Credentials Certification Renewals FAQ & Help

Learn / Credentials / Browse Credentials / /

Your assessment results for
Microsoft Certification

[Retake](#) You'll be eligible to retake the assessment in:
70 . 57 . 36
HOURS MINUTES SECONDS

FAIL Assessment date: October 26, 2023

Your overall results: **8%** **Fail**
75% needed to pass

Progress bar showing 8% completion (green segment) out of 75% needed to pass.

Fail but seems buggy (no confirm mail), just go taking again!

Exam Example in SC-900

Security Concepts



have best practices from Microsoft to assist in Azure Development, such as tools and guidances

- A. Resource Lock
- B. Azure Blueprint
- C. MS Cloud Adoption Framework
- D. Azure Blueprint

Answer: **Microsoft Cloud Adoption Framework**

Hint: best practices from **Microsoft**

Exam Example in SC-900

Security Concepts

Microsoft, as cloud provider, is solely responsible for:

- A. Physical Hardware Management
- B. Endpoints Management
- C. Manage user accounts
- D. Manage data stored on Azure

Answer: **Physical Hardware**

Hint: best practices **from Microsoft**

Exam Example in SC-900

Security Concepts

Please answer each question:

1. One of the Zero-trust principle is Assume Breach.
2. Zero-trust means firewall can protect internal network.
3. One of the Zero-trust principle is Verify Explicitly.
4. One of the Zero-trust principle is Least Privilege.

Yes/No

Yes/No

Yes/No

Yes/No

Answer: **Y/N/Y/Y**

Hint: Zero-Trust = Verify Explicitly + Least Privilege + Assume Breach

Exam Example in SC-900

Security Concepts

3 things that are the truth for Zero-Trust:

- A. Network is new Security Perimeter/Boundary
- B. Identity is new Security Perimeter/Boundary
- C. Physical Location is new Security Perimeter/Boundary
- D. Users are always verified their permission explicitly
- E. Apps or other Service Principles are no need to be always verified
- F. Always assume that our system is breached, to actively finding threats. limit segments etc.

Answer: **BDF**

Hint: Zero-Trust = New **Boundary is Identity** (Users/Devices/App/other SPs+Signal)
with **3 principles: Verify Explicitly, Least Privileges, Assume Breach**

Exam Example in SC-900

Security Concepts

Please answer each question:

1. Control is key privacy principle of MS
2. Shared Responsibilities is key privacy principle of MS
3. Least Privilege is key privacy principle of MS
4. Transparency is key privacy principle of MS

Yes/No

Yes/No

Yes/No

Yes/No

Answer: **Y/N/N/Y**

Hint: Control/Transparency/Security/Strong Legal Protection/No Content-based Targeting/Benefits to you

Exam Example in SC-900

Security Concepts



files making data readable/usable only for viewer that has appropriate key.

- A. Hashing
- B. Deduplicating
- C. Encryption
- D. Compressing

Answer: **Encryption**

Hint: Encryption use key to encrypt/decrypt

Exam Example in SC-900

Security Concepts

Please answer each question:

1. Verifying digitally signed docs requires private key of signer
2. Verifying digitally signed docs requires public key of signer
3. Signer uses private key to digitally sign documents.
4. Signer uses public key to digitally sign documents.

Yes/No

Yes/No

Yes/No

Yes/No

Answer: **N/Y/Y/N**

Hint: Asymmetric Encryption: sender uses private key, receiver uses public key.

Exam Example in SC-900

Security Concepts

To place multilayer of defense along network infrastructure, is which security methodology?

- A. Zero-Trust
- B. Key Privacy Principle
- C. CIA: Confidentiality, Integrity, Availability
- D. Defense in Depth

Answer: **Defense in Depth**

Hint: **Multilayer** throughout **Network**

Exam Example in SC-900

Security Concepts

User must be when signing in Azure/M365 portal and then undergo process to identify whether user can access any specific resource.

- A. Authenticated / Authorization
- B. Authorized / Authentication
- C. Accounted / Authentication
- D. Authenticated / Accounting

Answer: **Authenticated** and **Authorization**

Hint: **Authentication** is proving if **signing-in** user authentic. **Authorization** is to authorize/give rights to access/do something to **signed-in** user.