VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE ENGINEERING

AND INFORMATION SYSTEMS

MICROSOFT SECURITY, COMPLIANCE AND IDENTITY FUNDAMENTALS

An Industrial Internship Report

submitted by

THILAKRAJ C – 20MIS0401

in partial fulfilment for the award of the degree of

MASTER OF TECHNOLOGY(INTEGRATED)

In

SOFTWARE ENGINEERING

DECLARATION BY THE CANDIDATE

I hereby declare that the Industrial Internship report entitled "**Microsoft Security, Compliance and Identity Fundamentals"** submitted by me to Vellore Institute of Technology, Vellore in partial fulfilment of the requirement for the award of the degree of **Master of Technology (Integrated)** in **Software Engineering** is a record of bonafide industrial trainingundertaken by me under the supervision of **Mr. Harsh Chhabra, Microsoft.**I further declare that the work reported in this report has not beensubmitted and will not be submitted, either in part or in full, for the awardof any other degree or diploma in this institute or any other institute or university.

Signature of the student

NAME: THILAKRAJ C
REG NO: 20MIS0401

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science Engineering and Information Systems

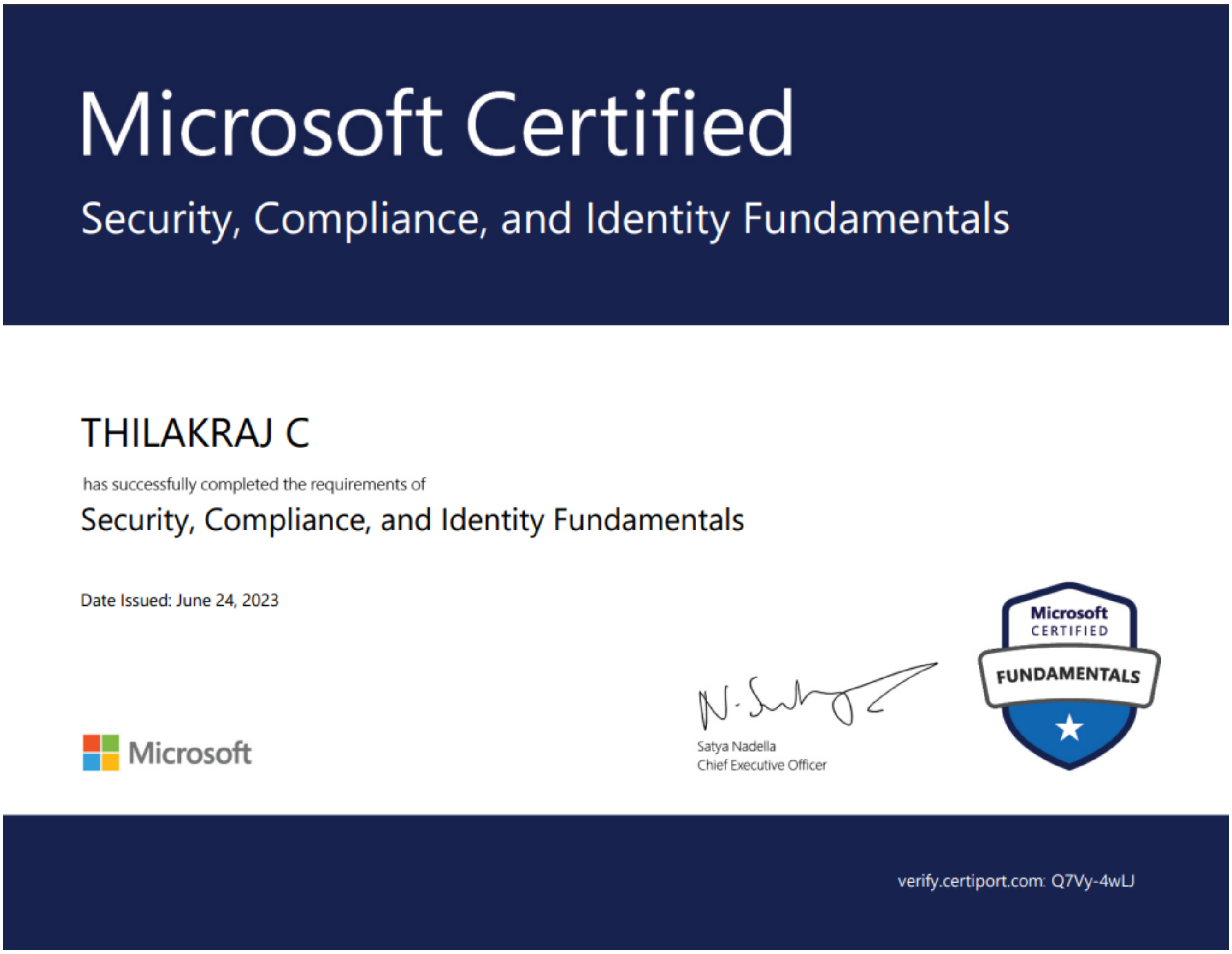
BONAFIDE CERTIFICATE

This is to certify that the Industrial Internship report entitled "**Microsoft Security, Compliance and Identity Fundamentals"** submitted by **THILAKRAJ C (20MIS0401)** to Vellore Institute of Technology, Vellore in partial fulfilment of the requirement for the awardof the degree of **Masters of Technology(Integrated) in Software Engineering** is a record of bonafide Industrial Internship undertaken by him/her under my supervision. The training fulfils the requirements as per the regulations of this Institute and in my opinion, meets the necessary standards for submission. The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Signature of the
Supervisor

SUPERVISOR

CERTIFICATE BY MICROSOFT



Microsoft Certified

Security, Compliance, and Identity Fundamentals

THILAKRAJ C

has successfully completed the requirements of

Security, Compliance, and Identity Fundamentals

Date Issued: June 24, 2023

Microsoft

Satya Nadella
Chief Executive Officer

Microsoft CERTIFIED FUNDAMENTALS

verify.certiport.com: Q7Vy-4wLJ

ACKNOWLEDGEMENT

The opportunity given to me by the university was a great chance for learning and professional development. Therefore, I consider myself a very lucky individual as I was provided with an opportunity to study and develop. I express my deepest thanks to my professors for giving necessary advice and guidance. I am extremely grateful and would like toacknowledge their contributions. I perceive this opportunity as a big milestone in my career development. I will strive to use gained skills andknowledge in the best possible way, and I will continue to work on their improvement, in order to attain desired career objectives. I hope tocontinue cooperation with all of you in the future.

Place : Vellore **THILAKRAJ C**

Date : 01/11/2023

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
1.	**Introduction**	1
	1.1.Synopsis	1
	1.2.Course Outline	2
2.	**About Microsoft Corporation**	2
	2.1. General	2
	2.2. Vision	3
	2.3. Nature	4
3.	**Skill set before training**	5
4.	**In-plant training curriculum**	6
	4.1. Describe security and compliance concepts	6
	4.1.1. Introduction	6
	4.1.2. Describe the shared responsibility model	6
	4.1.3. Describe defense in depth	7
	4.1.4. Describe the Zero Trust model	8
	4.1.5. Describe encryption and hashing	8
	4.1.6. Describe governance, risk and compliance concepts	10
	4.2. Describe the capabilities of Microsoft Entra	10
	4.2.1. Describe the functions and identity types of Microsoft Entra ID	10
	4.2.2. Describe the authentication capabilities of Microsoft Entra ID	11
	4.2.3. Describe access management capabilities of Microsoft Entra ID	13
	4.2.4. Describe the identity protection and governance capabilities of Microsoft Entra	14
	4.3. Describe the capabilities of Microsoft security solutions	15

	4.3.1. Describe core infrastructure security services in Azure	15
	4.3.2. Describe the security management capabilities in Azure	16
	4.3.3. Describe the capabilities in Microsoft Sentinel	17
	4.3.4. Describe threat protection with Microsoft 365 Defender	18
5.	**Application of In-plant training**	19
6.	**Comparison and self-evaluation**	20
	LIST OF FIGURES	
Figure 1	Shared responsibility model	7
Figure 2	Types of encryptions	9
Figure 3	GRC	10
Figure 4	Microsoft Entra Authentication Methods	12
Figure 5	Microsoft Entra Roles	13
Figure 6	Microsoft Entra ID Verification	14
Figure 7	Azure DDoS Protection	15
Figure 8	Web Application Firewall	16
Figure 9	Microsoft Defender for Cloud	17
Figure 10	Azure Sentinel	18
Figure 11	Microsoft defender	18

1. Introduction

1.1. Synopsis

The Microsoft Security, Compliance, and Identity Fundamentals (SC-900) istargeted to familiarize with the fundamentals of security, compliance, and identity(SCI) across cloud based and related Microsoft services. The module introduces some important security and compliance concepts.

As more business data is being accessed from locations outside of the traditional corporate network, security and compliance have become overriding concerns. Organizations need to understand how they can best protect their data, regardless of where it's accessed from, and whether it sits on their corporate network or in the cloud. In addition, organizations need to ensure they're compliant with industry and regulatory requirements to ensure the protection and privacy of data. In the course one shall learn about the shared responsibility model, defense in depth, and Zero Trust model. You'll be introduced to the concepts of encryptionand hashing as ways to protect data. When it comes to security, your organizationcan no longer rely on its network boundary. To allow employees, partners, and customers to collaborate securely, organizations need to shift to an approach whereby identity becomes the new security perimeter. Using an identity provider helps organizations manage that shift and all the aspects of identity security. You'll learn about Microsoft Entra ID, Microsoft's cloud-based identity and access management service. You'll also learn about the identity types supported and howyou can use Microsoft Entra ID to support external users. The traditional network security perimeter is changing as more companies move to either a hybrid cloud environment, with some resources located on-premises and some in the cloud, or a fully cloud-based network solution. Protection of your organization's assets, resources, and data is essential. Threats can come from any direction: for instance,a Denial-of-Service attack on your organization's services, or a hacker trying to access your network by attempting to penetrate your firewall. Azure offers a widearray of configurable security tools that can be customized to give you the securityand control to meet your organization's needs. You will explore many different services and features of Azure that can help protect your networks, assets, and resources, including DDoS protection, Azure Firewall, network security groups, and more.

You’ll also learn about Azure Key Vault and why you would use this feature to keep secrets safe. Microsoft Cloud services are built on a foundation oftrust, security, and compliance. The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about Microsoft security, privacy, and compliance practices. Microsoft also helps organizations meet their privacy requirements, with Microsoft Priva. Priva helps organizations safeguard personal data and build a privacy-resilient workplace. You’ll learn about the Service Trust Portal and resources it provides, including audit reports, security assessments, and compliance guides that enable organizations to manage compliance. You'll learn about Microsoft's commitment to privacy and its privacy principles. Lastly, you'lllearn about Microsoft Priva, which helps organizations meet their privacy goals.

1.2. Course Outline

To achieve the course objective to familiarize with the fundamentals of security, compliance, and identity (SCI) the course explores the following,

- Describe the concepts of security, compliance, and identity
- Describe the capabilities of Microsoft identity and access management solutions
- Describe the capabilities of Microsoft Security solutions
- Describe the capabilities of Microsoft compliance solutions

2. About Microsoft Corporation

2.1. General

Microsoft was founded in 1975. Our mission is to enable people and businesses throughout the world to realize their full potential by creating technology that transforms the way people work, play, and communicate. We develop and marketsoftware, services, and hardware that deliver new opportunities, greater convenience, and enhanced value to people's lives. Microsoft does business worldwide and have offices in more than 100 countries.

The company generates revenue by developing, licensing, and supporting awide range of software products and services, by designing and selling hardware, and by delivering relevant online advertising to a global customer audience. In addition to selling individual products and services, we offer suites of products and services. Microsoft enables digital transformation for the era of an intelligent cloudand an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more. Microsoft set up its India operations in1990. Microsoft in India offers its global cloud services from local data centers toaccelerate digital transformation across Indian start-ups, businesses, and government agencies.

2.2. Vision

Microsoft's vision is "to help people and businesses throughout the world realize their full potential." This vision statement shows that the company presents its computing products as tools that people and business organizations can use for their personal or organizational development. Microsoft's corporate vision statement has the following components:

- Value proposition: To help realize their full potential
- Target market: People and businesses throughout the world

The corporate vision's components are directly related to the components of the corporate mission statement, indicating that Microsoft focuses on its value proposition and target market. For example, the vision statement specifies that thecompany's value proposition is that its information technology products can help customers realize their full potential. This emphasis on helping and satisfying customers agrees with the strategic objective of addressing the concerns of customers as a stakeholder group in Microsoft's corporate social responsibility strategy and stakeholder management approaches. This means that individual usersand organizations are a focus in the product development strategy of the technology business.

Microsoft's corporate vision statement also specifies the target market. In stating "people and businesses throughout the world," the technology company defines its target market as composed of every person and business organization inthe world. In this way, the corporate vision describes a business condition where Microsoft continues as one of the leading global providers of computer technologyand related online services to customers around the world. Maintaining this marketposition requires competitive advantages for success despite competing firms alsooperating in the information technology and Internet services market. In this regard, the business strengths detailed in the SWOT analysis of Microsoft Corporation support the fulfillment of the corporate vision statemen

2.3. Nature

The products include operating systems for personal computers ("PCs"), servers, phones, and other intelligent devices; server applications for distributed computingenvironments; productivity applications; business solution applications; desktop and server management tools; software development tools; video games; and online advertising. We also design and sell hardware including the Xbox 360 gaming and entertainment console, Kinect for Xbox 360, Xbox 360 accessories, and Microsoft PC hardware products.

We provide consulting and product and solution support services, and we train and certify computer system integrators and developers. We also offer cloud-based solutions that provide customers with software, services and content over the Internet by way of shared computing resources located in centralized data centers. Cloud revenue is earned primarily from usage fees and advertising.

Examples of cloud-based computing services we offer include:

- Microsoft Office 365, an online suite that enables people to work from virtually anywhere at any time with simple, familiar collaboration and communication solutions, including Microsoft Office, Exchange, SharePoint, and Lync.
- Xbox LIVE service, which enables online gaming, social networking, andaccess to a wide range of video, gaming, and entertainment content.
- Microsoft Dynamics CRM Online customer relationship management services for sales, service, and marketing professionals provided through afamiliar Microsoft Outlook interface.
- Bing, our Internet search engine that finds and organizes the answers people need so they can make faster, more informed decisions.
- Skype, which allows users to connect with friends, family, clients, and colleagues through a variety of devices; and
- The Azure family of platform and database services that help developers connect applications and services in the cloud or on premise.

These services include Windows Azure, a scalable operating system with computing, storage, hosting, and management capabilities, and Microsoft SQL Azure,a relational database.

We also conduct research and develop advanced technologies for future software and hardware products and services. We believe that we will continue to grow andmeet our customers' needs by delivering compelling, new, high-value solutions through our integrated software, hardware, and services platforms, creating new opportunities for partners, improving customer satisfaction, and improving our service excellence, business efficacy, and internal processes.

3. Skill set before training

I have worked extensively on learning Python Development. I had also built a sound knowledge of DBMS, OS, Networks, and other core Computer Science Subjects before the course. I learned a lot while at the university and in between my vacations.Most of the basics I learned were through online courses and by being a part of technical clubs. I also learned about a variety of technologies, while working on the variousprojects that were a part of the core computer science subjects offered by my university. Before the course, I possessed the following skills:

- Core Computer Science Subjects: I had built a strong foundation in Computer Science, through the various core subjects offered by the university. The various subjects include OS, DBMS & Networks. I also worked on skills needed in the Software Engineering processes.
- Data Structures & Algorithms: I had extensively learned about the various data structures & the most popular algorithms associated with various tasks such assorting, recursion, etc. This learning can be majorly attributed to the courses atVIT.
- Python development: As a Python developer, I possess a comprehensiveskillset that includes proficiency in Python programming, web development using Django and Flask, data analysis, and visualization. I'm experienced in machine learning, database integration, scripting for automation, and version control with Git. I pride myself on my problem-solving abilities, dedication tocontinuous learning, and collaborative approach, making me a versatile asset in the world of software development.

4. In-plant Training Curriculum

The preparation for the SC-900 exam: Microsoft Security, Compliance and Identity Fundamentals teach about the core concepts that are foundational to security, compliance and identity solutions including shared responsibilities, zero trust, data residency, the role of identity providers and more. The learning path followed in the course is as follows:

4.1. Describe security and compliance concepts

4.1.1. Introduction

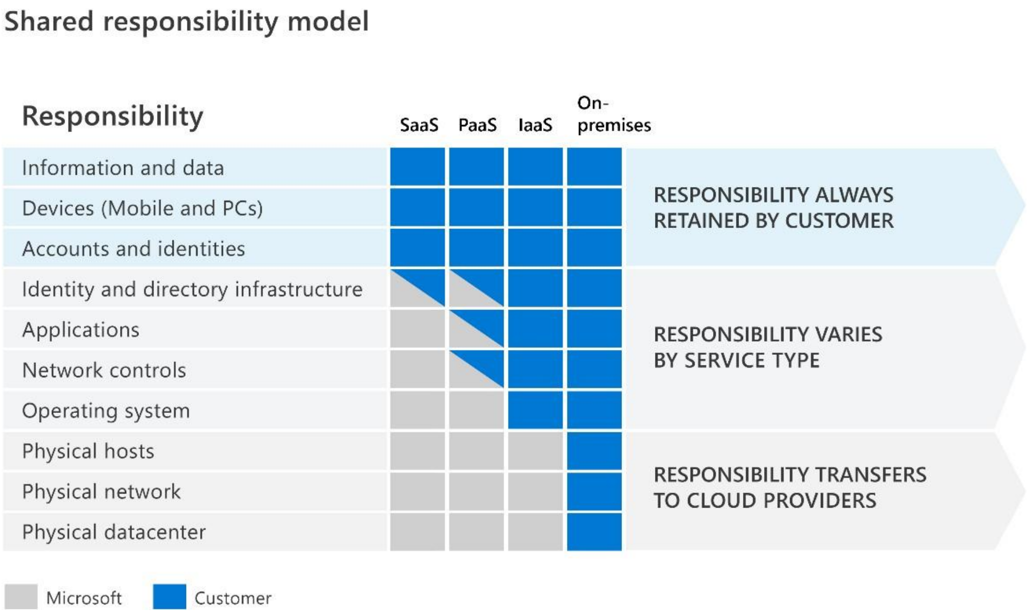
You'll learn about the shared responsibility model, defense in depth, and ZeroTrust model. You'll be introduced to the concepts of encryption and hashing as ways to protect data. Lastly, you'll learn about concepts that relate to compliance. After completing this module, you'll be able to:

- Describe the shared responsibility and the defense in-depth securitymodels.
- Describe the Zero-Trust model.
- Describe the concepts of encryption and hashing.
- Describe some basic compliance concepts.

4.1.2. Describe the shared responsibility model

In organizations running only on-premises hardware and software, the organization is 100 percent responsible for implementing security and compliance. With cloud-based services, that responsibility is shared between the customer and the cloud provider. The shared responsibility model identifieswhich security tasks are handled by the cloud provider, and which security tasks are handled by you, the customer. The responsibilities vary depending onwhere the workload is hosted:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- On-premises datacenter



Shared responsibility model

Responsibility	SaaS	PaaS	IaaS	On-premises	
Information and data	🟦	🟦	🟦	🟦	RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦	
Accounts and identities	🟦	🟦	🟦	🟦	
Identity and directory infrastructure	◪	◪	🟦	🟦	RESPONSIBILITY VARIES BY SERVICE TYPE
Applications	⬜	◪	🟦	🟦	
Network controls	⬜	◪	🟦	🟦	
Operating system	⬜	⬜	🟦	🟦	
Physical hosts	⬜	⬜	⬜	🟦	RESPONSIBILITY TRANSFERS TO CLOUD PROVIDERS
Physical network	⬜	⬜	⬜	🟦	
Physical datacenter	⬜	⬜	⬜	🟦	

⬜ Microsoft 🟦 Customer

Figure 1: Shared responsibility model

4.1.3. Describe defense in depth

Defense in depth uses a layered approach to security, rather than relying on a single perimeter. A defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. Each layer provides protection so that, if one layer is breached, a subsequent layer will prevent an attacker getting unauthorized access to data. Example layers of security might include:

- Physical security such as limiting access to a datacenter to only authorized personnel.
- Identity and access security controls, such as multifactor authenticationor condition-based access, to control access to infrastructure and change control.
- Perimeter security of your corporate network includes distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.

- Network security, such as network segmentation and network access controls, to limit communication between resources.
- Compute layer security such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.
- Application layer security to ensure applications are secure and free of security vulnerabilities.
- Data layer security including controls to manage access to business and customer data and encryption to protect data.

4.1.4. Describe the Zero Trust model

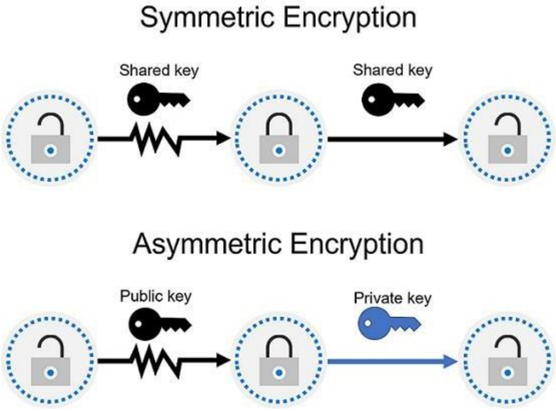
Zero Trust assumes everything is on an open and untrusted network, even resources behind the firewalls of the corporate network. The Zero Trust modeloperates on the principle of “trust no one, verify everything.” The Zero Trust model has three principles which guide and underpin how security is implemented. These are: verify explicitly, least privilege access, and assume breach.

- Verify explicitly. Always authenticate and authorize based on theavailable data points, including user identity, location, device, service or workload, data classification, and anomalies.
- Least privileged access. Limit user access with just-in-time and just- enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.
- Assume breach. Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.

4.1.5. Describe encryption and hashing

One way to mitigate against common cybersecurity threats is to encrypt sensitive or valuable data. Encryption is the process of making data unreadableand unusable to unauthorized viewers. To use or read encrypted data, it must be decrypted, which requires the use of a secret key. There are two top-level types of encryptions: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt the data. Asymmetric encryption uses a public key and private key pair. Either key can encrypt data, but the key used to encrypt can't be used to decrypt encrypted data. To decrypt, you need a paired key. For example, if the public key is used to encrypt, then only the corresponding private key can be used to decrypt. Asymmetric encryption is used for things such accessing sites on the internet using the HTTPS protocol and electronic data signing solutions. Encryption may protect data at rest, or intransit.

Figure 2: Types of encryptions



Hashing uses an algorithm to convert text to a unique fixed-length value calleda hash. Each time the same text is hashed using the same algorithm, the same hash value is produced. That hash can then be used as a unique identifier of itsassociated data. Hashing is different to encryption in that it doesn't use keys, and the hashed value isn't subsequently decrypted back to the original. Hashingis often used to store passwords. When a user enters their password, the same algorithm that created the stored hash creates a hash of the entered password. This is compared to the stored hashed version of the password. If they match, the user has entered their password correctly. This is more secure than storingplain text passwords, but hashing algorithms are also known to hackers.Because hash functions are deterministic (the same input produces the same output), hackers can use brute-force dictionary attacks by hashing the passwords. For every matched hash, they know the actual password. Tomitigate this risk, passwords are often "salted". This refers to adding a fixed- length random value to the input of hash functions to create unique hashes forsame input.

4.1.6. Describe governance, risk and compliance concepts

Organizations face increasing complexity and change in regulatory environments, calling for a more structured approach for managinggovernance, risk, and compliance (GRC). As organizations establish GRC competency they can establish a framework that includes implementing specific policies, operational processes, and technologies. A structured approach for managing GRC helps organizations reduce risk and improve compliance effectiveness. An important prerequisite to establishing GRC competency is understanding the key terms.

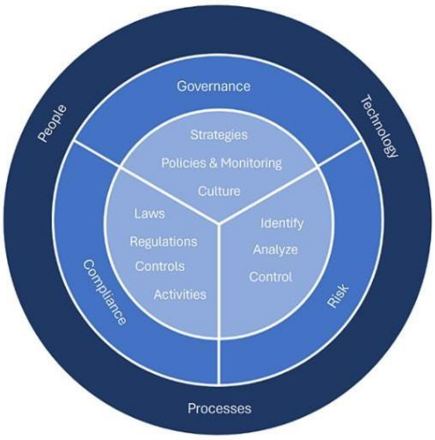


Figure 3: GRC

4.2. Describe the capabilities of Microsoft Entra

4.2.1. Describe the functions and identity types of Microsoft Entra ID:

Microsoft Entra ID, formerly Azure Active Directory, is Microsoft's cloud-based identity and access management service. Organizations use Microsoft Entra ID to enable their employees, guests, and others to sign in and access the resources they need, including:

- Internal resources, such as apps on your corporate network and intranet,and cloud apps developed by your own organization.
- External services, such as Microsoft Office 365, the Azure portal, andany SaaS applications used by your organization.

In Microsoft Entra ID, there are different types of identities that are supported. The terms you'll hear and are introduced in this unit are user identities, workload identities, device identities, external identities, and hybrid identities. Hybrid identity is accomplished through provisioning andsynchronization.

- Inter-directory provisioning is provisioning an identity between two different directory services systems. For a hybrid environment, the most common scenario for inter-directory provisioning is when a useralready in Active Directory is provisioned into Microsoft Entra ID.
- Synchronization is responsible for making sure identity information for your on-premises users and groups is matching the cloud.

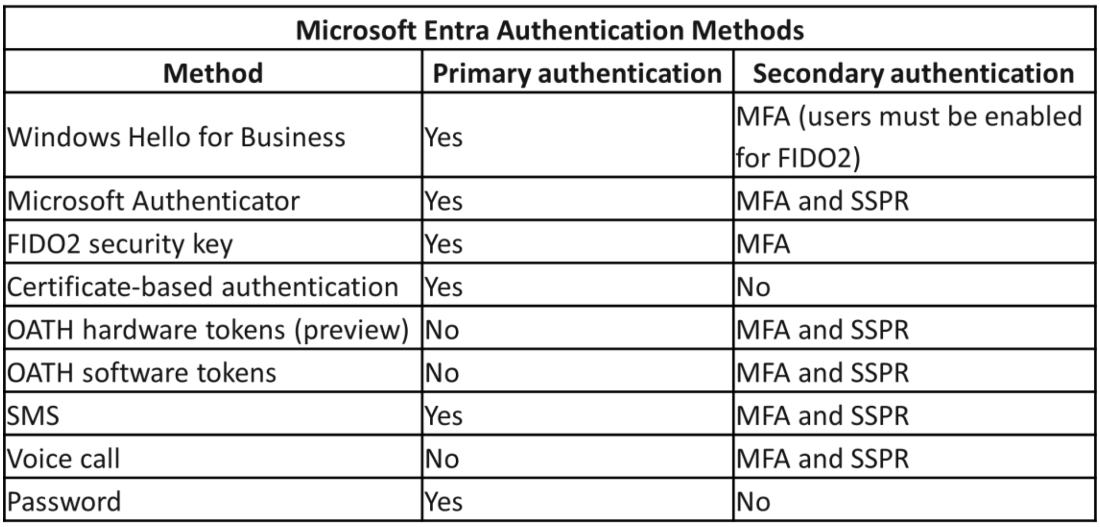
Microsoft Entra ID External Identities refers to all the ways you can securely interact with users outside of your organization. The following capabilities make up External Identities:

- B2B collaboration
- B2B direct connect
- Microsoft Entra External ID for customers (preview)
- Microsoft Entra ID multi-tenant organization

4.2.2. Describe the authentication capabilities of Microsoft Entra ID

Passwords are the most common form of authentication, but they have manyproblems, especially if used in single-factor authentication, where only oneform of authentication is used. If they're easy enough to remember, they're easyfor a hacker to compromise. Strong passwords that aren't easily hacked aredifficult to remember and affect user productivity when forgotten. MicrosoftEntra Identity certificate-based authentication (CBA) enables customers toallow or require users to authenticate directly with X.509 certificates againsttheir Microsoft Entra Identity, for applications and browser sign-in. CBA issupported only as a primary form of passwordless authentication. X.509 certificates, which are part of the public key infrastructure (PKI), are digitallysigned documents that bind an identity (an individual, organization, website)to its public key. Some authentication methods can be used as the primary factor when you sign in to an application or device

Other authentication methods are only available as a secondary factor when you use Microsoft EntraMultifactor Authentication or SSPR. While that information is called-out in the text that describes each authentication method, the following table summarizeswhen an authentication method can be used during a sign-in event.



Microsoft Entra Authentication Methods		
Method	**Primary authentication**	**Secondary authentication**
Windows Hello for Business	Yes	MFA (users must be enabled for FIDO2)
Microsoft Authenticator	Yes	MFA and SSPR
FIDO2 security key	Yes	MFA
Certificate-based authentication	Yes	No
OATH hardware tokens (preview)	No	MFA and SSPR
OATH software tokens	No	MFA and SSPR
SMS	Yes	MFA and SSPR
Voice call	No	MFA and SSPR
Password	Yes	No

Figure 4: Microsoft Entra Authentication Methods

Security defaults are a set of basic identity security mechanisms recommendedby Microsoft. When enabled, these recommendations are automatically enforced in your organization. The goal is to ensure that all organizations havea basic level of security enabled at no extra cost. These defaults enable some of the most common security features and controls, including:

- Enforcing Microsoft Entra multifactor authentication registration for all users.
- Forcing administrators to use multifactor authentication.
- Requiring all users to complete multifactor authentication when needed.

Self-service password reset (SSPR) is a feature of Microsoft Entra that allowsusers to change or reset their password, without administrator or help desk involvement. SSPR has several key benefits for organizations and users:

- SSPR reduces IT support costs by enabling users to reset passwords ontheir own.
- SSPR allows users to get back to work faster and be more productive.

- Administrators can change settings to accommodate new security requirements and roll these changes out to users without disrupting their sign-in.
- SSPR includes robust audit logs that are available from an API, enabling data to be imported to a Security Incident and Event Monitoring (SIEM) system of choice.

4.2.3. Describe access management capabilities of Microsoft Entra ID

Conditional Access is a feature of Microsoft Entra that provides an extra layerof security before allowing authenticated users to access data or other assets. Conditional Access is implemented through policies that are created andmanaged in Microsoft Entra ID. A Conditional Access policy analyses signalsincluding user, location, device, application, and risk to automate decisions forauthorizing access to resources (apps and data).

Microsoft Entra roles control permissions to manage Microsoft Entra resources. For example, allowing user accounts to be created, or billing information to be viewed. Microsoft Entra supports built-in and custom roles.Managing access using roles is known as role-based access control (RBAC). Microsoft Entra built-in and custom roles are a form of RBAC in that MicrosoftEntra roles control access to Microsoft Entra resources. This is referred to as Microsoft Entra RBAC.

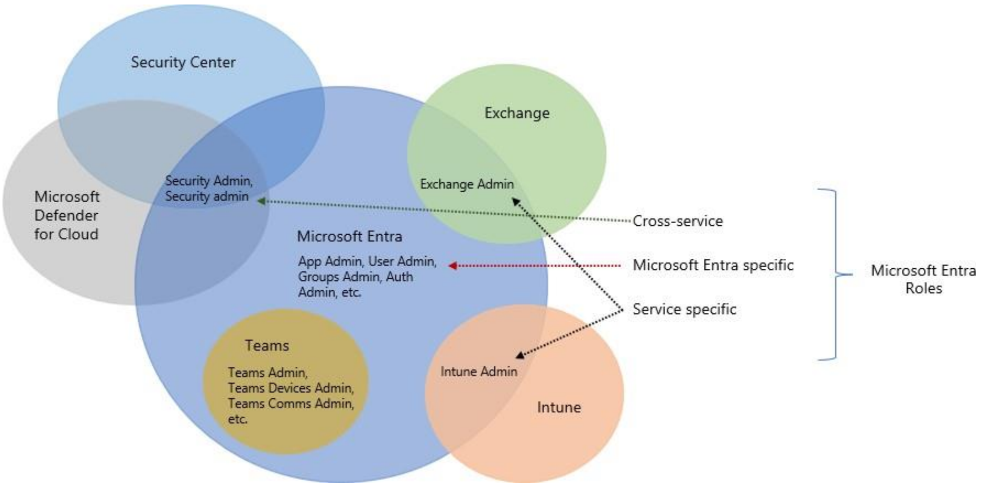

Security Center
Microsoft Defender for Cloud
Security Admin, Security admin
Exchange
Exchange Admin
Cross-service
Microsoft Entra
App Admin, User Admin, Groups Admin, Auth Admin, etc.
Microsoft Entra specific
Service specific
Microsoft Entra Roles
Teams
Teams Admin, Teams Devices Admin, Teams Comms Admin, etc.
Intune Admin
Intune

Figure 5: Microsoft Entra Roles

4.2.4. Describe the identity protection and governance capabilities ofMicrosoft Entra

Microsoft Entra ID Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people havethe right access to the right resources. ID Governance gives organizations theability to do the following tasks:

- Govern the identity lifecycle.
- Govern access lifecycle.
- Secure privileged access for administration.

Microsoft Entra access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment. Regular access reviews ensure that only the right people have access toresources. Excessive access rights are a known security risk. However, when people move between teams, or take on or relinquish responsibilities, access rights can be difficult to control. Entitlement management is an identitygovernance feature that enables organizations to manage the identity and access lifecycle at scale. Entitlement management automates access request workflows, access assignments, reviews, and expiration. PIM reduces the chance of a malicious actor getting access by minimizing the number of peoplewho have access to secure information or resources. By time-limiting authorized users, it reduces the risk of an authorized user inadvertently affecting sensitive resources. PIM also provides oversight for what users are doing with their administrator privileges. Microsoft Entra Verified ID is a managed verifiable credentials service based on open standards. Verified ID automates verification of identity credentials and enables privacy-protected interactions between organizations and users.

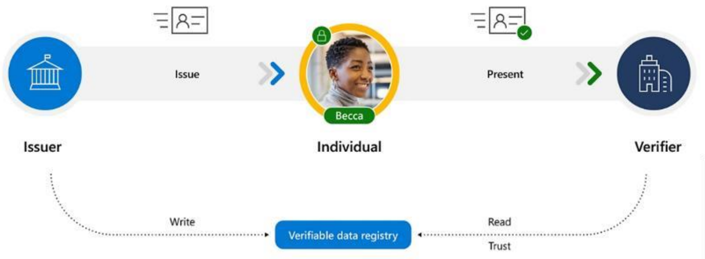


Figure 6: Microsoft Entra ID Verification

4.3. Describe the capabilities of Microsoft security solutions

The traditional network security perimeter is changing as more companies move to either a hybrid cloud environment, with some resources located on-premises and some in the cloud, or a fully cloud-based network solution. Protection of your organization's assets, resources, and data is essential. Threats can come from any direction: for instance, a Denial-of-Service attack on your organization’s services,or a hacker trying to access your network by attempting to penetrate your firewall.Azure offers a wide array of configurable security tools that can be customized togive you the security and control to meet your organization's needs.

4.3.1. Describe core infrastructure security services in Azure

The Azure DDoS Protection service is designed to help protect your applications and servers by analyzing network traffic and discarding anythingthat looks like a DDoS attack.

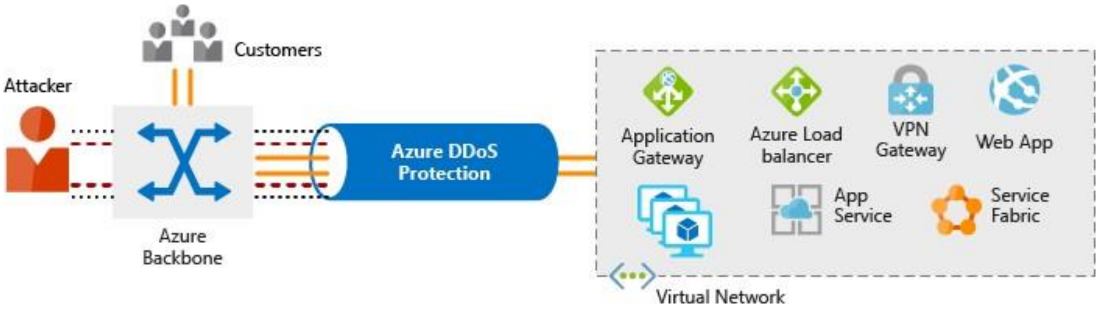


Figure 7: Azure DDoS Protection

Azure Firewall is a managed, cloud-based network security service that provides threat protection for your cloud workloads and resources running in Azure. You can deploy Azure Firewall on any virtual network but the best approach is to use it on a centralized virtual network. All your other virtual and on-premises networks will then route through it. The advantage of this model is the ability to centrally exert control of network traffic for all your VNets across different subscriptions. Web Application Firewall (WAF) providescentralized protection of your web applications from common exploits and vulnerabilities. A centralized WAF helps make security management simpler, improves the response time to a security threat, and allows patching a known vulnerability in one place, instead of securing each individual web application.

A WAF also gives application administrators better assurance of protection against threats and intrusions.

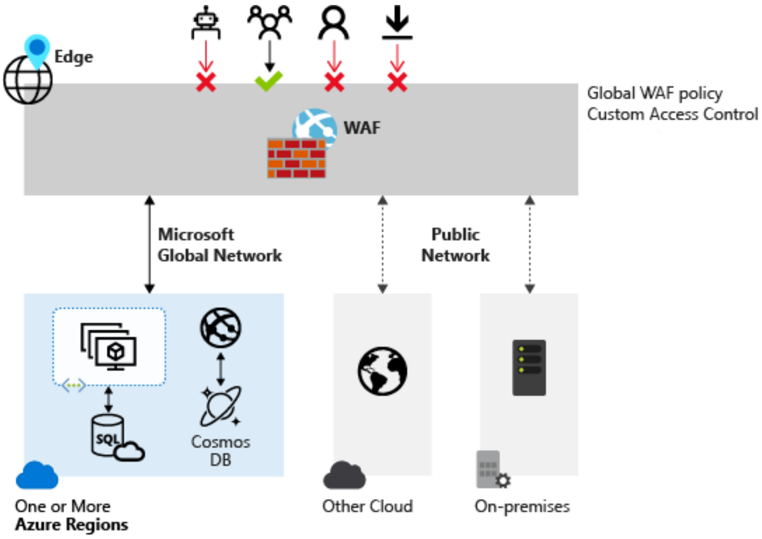


Figure 8: Web Application Firewall

Segmentation is about dividing something into smaller pieces. An organization, for example, will typically consist of smaller business groups such as human resources, sales, customer service, and more. In an office environment, it's common to see each business group have their own dedicatedoffice space, while members of the same group share an office. This enables members of the same business group to collaborate, while maintaining separation from other groups to address the confidentiality requirements of each business. Azure Bastion is a service you deploy that lets you connect to avirtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside yourvirtual network. Azure Bastion provides secure and seamless RDP and SSH connectivity to your virtual machines directly from the Azure portal using Transport Layer Security (TLS). When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special clientsoftware.

4.3.2. Describe the security management capabilities in Azure

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.

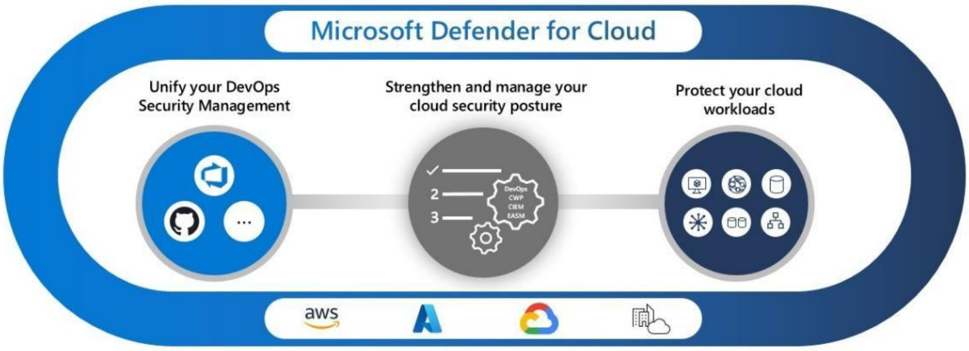

Microsoft Defender for Cloud
Unify your DevOps Security Management
Strengthen and manage your cloud security posture
Protect your cloud workloads
2
3
DevOps
CWP
CIEM
EASM
aws

Figure 9: Microsoft Defender for Cloud

The central feature in Microsoft Defender for Cloud that provides visibility to your current security posture is secure score. Defender for Cloud continually assesses your cross-cloud resources for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

4.3.3. Describe the capabilities in Microsoft Sentinel

A SIEM system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents.A SOAR system takes alerts from many sources, such as a SIEM system. The SOAR system then triggers action-driven automated workflows and processesto run security tasks that mitigate the issue.

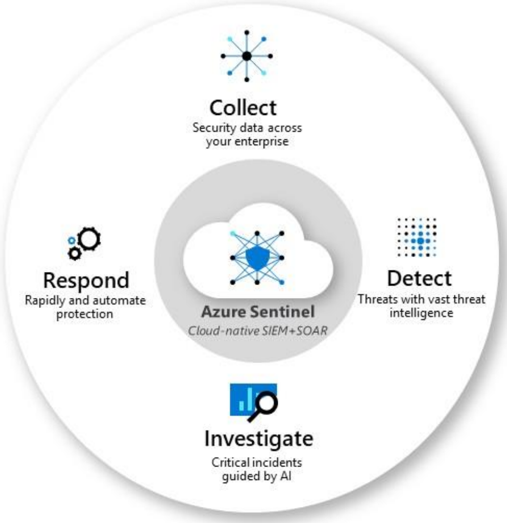

Collect
Security data across your enterprise
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI
Respond
Rapidly and automate protection
Azure Sentinel
Cloud-native SIEM+SOAR

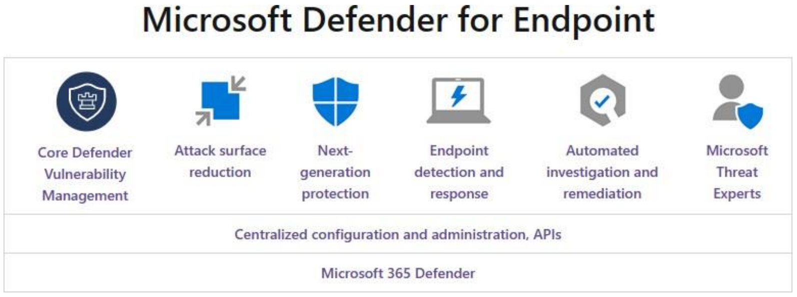
Figure 10: Azure Sentinel

The center of Microsoft Security Copilot is the prompt bar that allows securityanalysts to ask questions in natural language. You use the prompt bar to tell copilot what insights you want from your security data.

4.3.4. Describe threat protection with Microsoft 365 Defender

Microsoft 365 Defender is an enterprise defense suite that protects against sophisticated cyberattacks. With Microsoft 365 Defender, you can natively coordinate the detection, prevention, investigation, and response to threats across endpoints, identities, email, and applications. Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints including laptops, phones, tablets, PCs, access points, routers, and firewalls. It does so by preventing, detecting, investigating, and responding to advancedthreats. Microsoft Defender for Endpoint embeds technology built into Windows 10 and beyond, and Microsoft cloud services.

Figure 11: Microsoft defender


Microsoft Defender for Endpoint
Core Defender Vulnerability Management
Attack surface reduction
Next-generation protection
Endpoint detection and response
Automated investigation and remediation
Microsoft Threat Experts
Centralized configuration and administration, APIs
Microsoft 365 Defender

5. Application of In-plant training

Undertaking the Microsoft Security, Compliance, and Identity Fundamentals course has been a transformative experience from a first-person perspective. It has equipped me with a comprehensive understanding of key concepts that are criticalin today's digital landscape. The course has enabled me to dive deep into Microsoft's array of security solutions. I've become proficient in using Azure Active Directory, Microsoft Defender, and the Microsoft 365 Security Center to protect data, identities, and applications. With this knowledge, I can proactively defend against cyber threats and unauthorized access, a skill that is invaluable in the current era of persistent cybersecurity risks.

Navigating compliance requirements and regulations was previously a daunting task, but this course has demystified it for me. I now have a clear understanding of how to address complex regulations like GDPR and HIPAA andhow Microsoft tools can be leveraged to ensure compliance. This knowledge is vital for businesses in regulated industries, and it allows me to contribute significantly to risk mitigation and legal adherence. Identity and access management are central to security, and I've honed my skills in this area, primarily through Azure Active Directory. This knowledge empowers me to manage who has access to an organization's resources and data, a crucial aspect of security anddata protection. This course has been instrumental in shaping me into a cybersecurity expert. It's not just about understanding the tools but also comprehending the underlying principles of security. I've learned how to assess risks, develop security strategies, and respond effectively to security incidents, making me a more valuable asset to any organization.

The knowledge gained through this course has significantly improved my career prospects. I now have the confidence and skills to pursue a wide range of roles, from IT administrator to security analyst or compliance officer. This versatility opens up various opportunities and allows me to explore different careerpaths within the tech industry.

The course has transformed me into a compliance management resource. Understanding the intricacies of regulatory requirements, particularly GDPR and HIPAA, equips me to guide organizations in ensuring they meet legal standards.

This expertise is essential for businesses operating in highly regulated sectors, andI can assist them in avoiding penalties and reputational damage.

I've learned to use Microsoft's security tools efficiently, which not only improves security but also helps organizations save on costs. This can be a key selling point for organizations looking to optimize their security strategies while managing their budgets effectively.

The course is highly practical, offering hands-on experience and real-world scenarios. This approach has been invaluable in applying theoretical knowledge to actual security and compliance challenges, making me better prepared for the complexities of the professional world.

The Microsoft Security, Compliance, and Identity Fundamentals course has notonly broadened my skill set but has also given me a competitive edge in the job market. It's been an investment in my career, enabling me to explore roles in IT, security, and compliance more confidently. As technology continues to evolve, theinsights and skills I've acquired in this course will remain relevant, allowing me tostay ahead of emerging threats and regulatory changes while harnessing Microsoft's cutting-edge solutions for securing digital environments.

6. Comparison and Self-evaluation

Microsoft Security, Compliance and Identity Fundamentals teach about the core concepts that are foundational to security, compliance and identity solutionsincluding shared responsibilities, zero trust, data residency, the role of identity providers and more. I also learnt about Microsoft azure, Microsoft 365, MicrosoftFirewall and defender that gave me a better insight on my day-to-day security features available for me. I learnt about various Microsoft security tool and how they can turn as a selling point for the organizations.