Microsoft ADC Cybersecurity Skilling Program

Week 1 Assignment

Student Name: Vincent Onchieku Collins

Student ID: ADC-CSS02-25052

Introduction

This week I worked through the SC-900 Learning Path: Microsoft Security, Compliance, and Identity Fundamentals. It consisted of six core modules that introduced me to essential concepts in Microsoft Entra ID, security, and compliance. These modules helped lay the foundation for understanding how identity and access management work within Microsoft environments and why they are crucial in today's cybersecurity landscape.

The modules I completed are:

1. Describe security and compliance concepts
2. Describe identity concepts
3. Describe the function and identity types of Microsoft Entra ID
4. Describe the authentication capabilities of Microsoft Entra ID
5. Describe the access management capabilities of Microsoft Entra ID
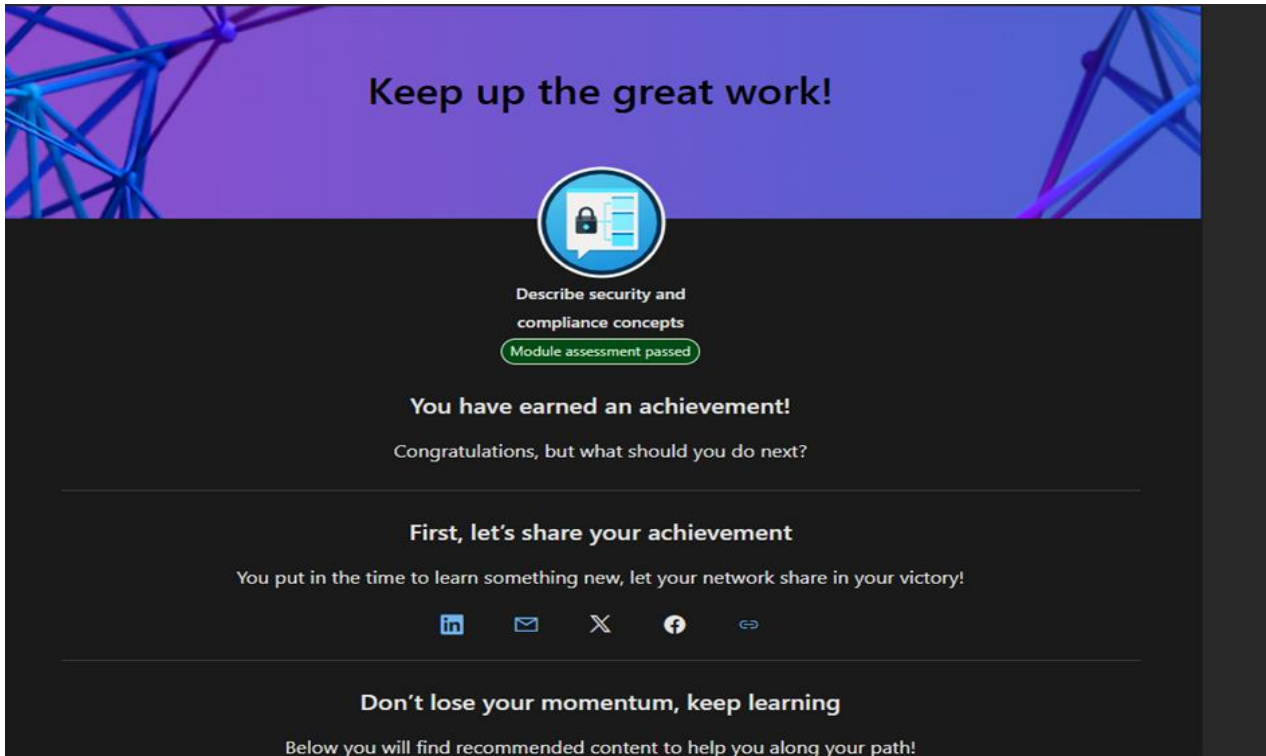6. Describe the identity protection and governance capabilities of Microsoft Entra

Tasks Completed

1. Describe security and compliance concepts

This module delved into common security and compliance concepts that are foundational to Microsoft solutions. Topics I explored include the shared responsibility model, the Zero Trust model, as well as methods of securing data such as encryption and hashing. I also learned about governance, risk, and compliance (GRC) frameworks, data residency, and data sovereignty.

I completed the module assessment and passed as shown below. I shared my achievement on LinkedIn to start building my professional visibility.

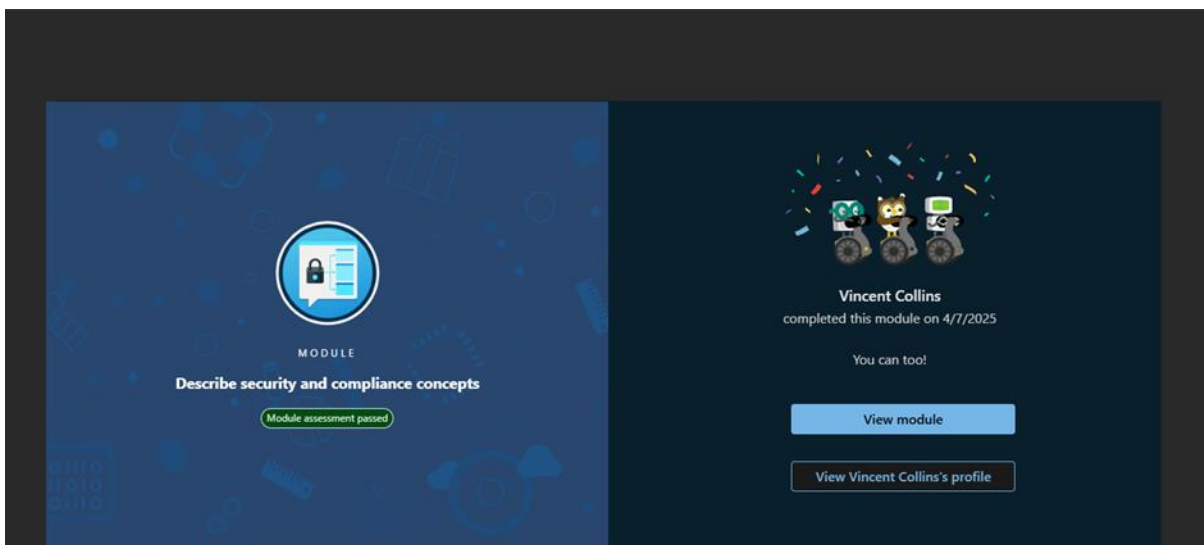**Verification link:** https://learn.microsoft.com/en-us/users/vincentcollins-8814/achievements/w2x8fs6n

2. Describe identity concepts

This module covered key concepts of authentication, authorization, and why identity is a critical foundation of modern security strategies. I learned about identity providers, the difference between Microsoft Entra ID and Active Directory, and the roles these platforms play in identity management. I also explored federated identity, single sign-on (SSO), and how identities enable secure collaboration across organizations.

I completed the module assessment and passed as shown below. I shared my achievement on LinkedIn and started building my visibility.

Verification link: https://learn.microsoft.com/en-us/users/vincentcollins-8814/achievements/w2x8raqn
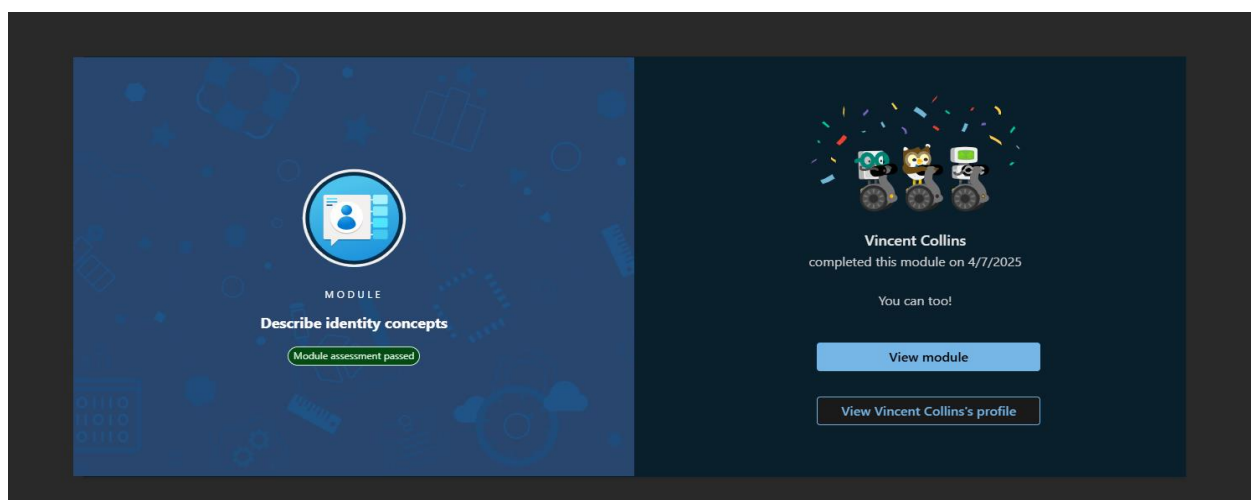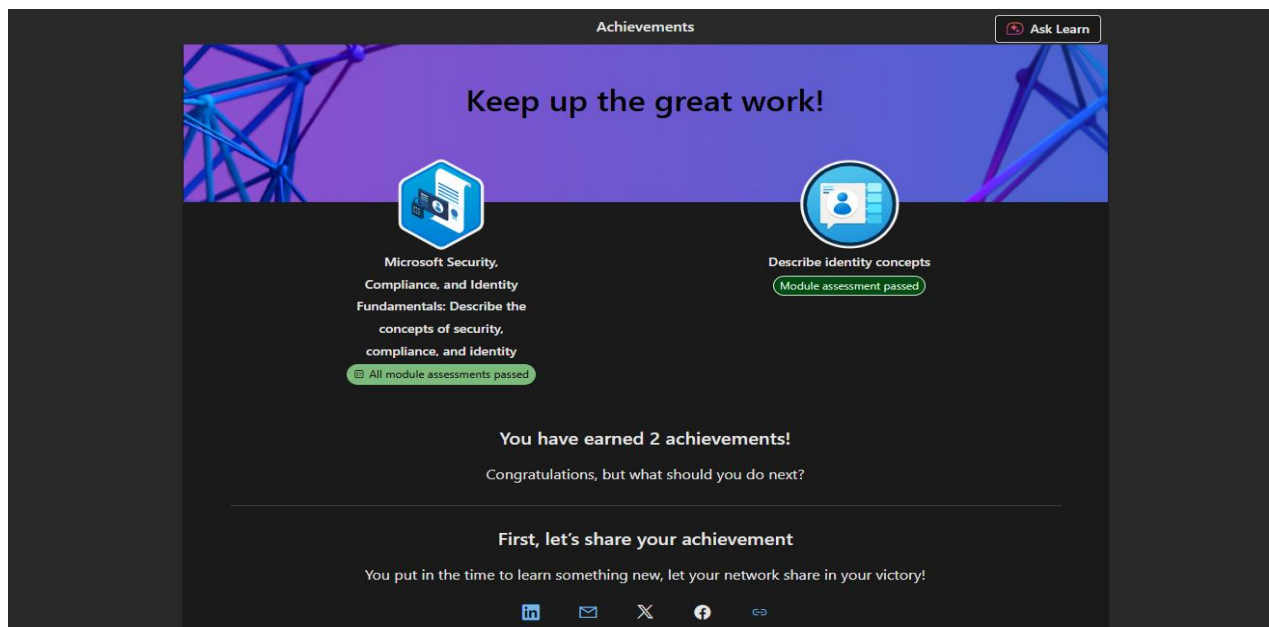
3. Describe the function and identity types of Microsoft Entra ID

In this module, I explored the core functions of Microsoft Entra ID, including identity provisioning, device registration, and the different types of identities it supports such as user, service principal, and managed identities. I also gained clarity on how Microsoft Entra ID supports hybrid identity scenarios and integrates with on-premises Active Directory.

I completed the module assessment and passed as shown below. I shared my achievement on LinkedIn and started building my visibility.

Verification link: https://learn.microsoft.com/en-us/users/vincentcollins-8814/achievements/bcs6m43d
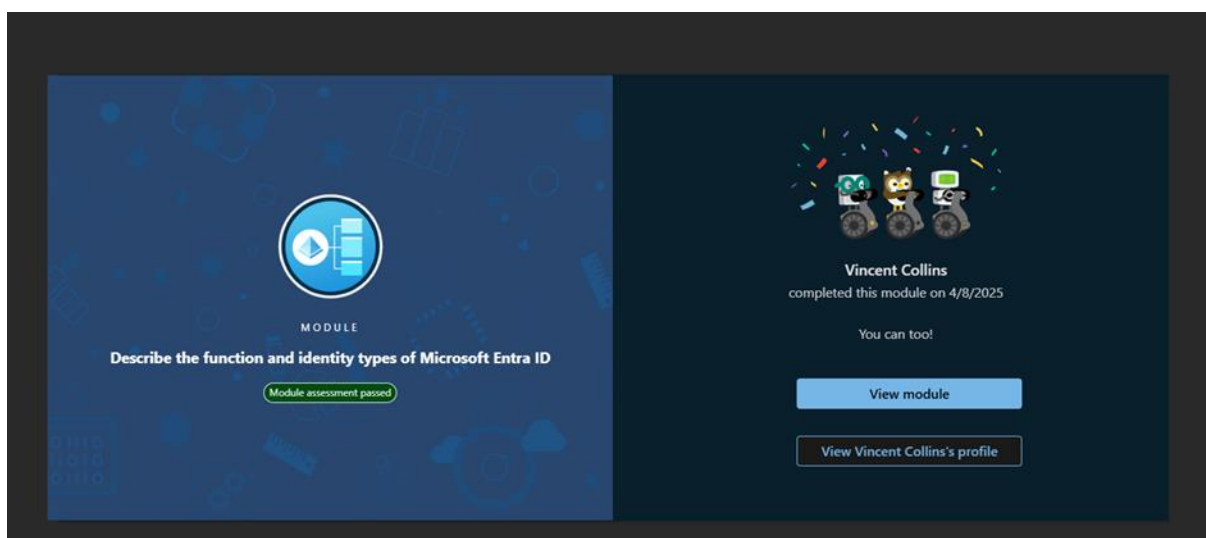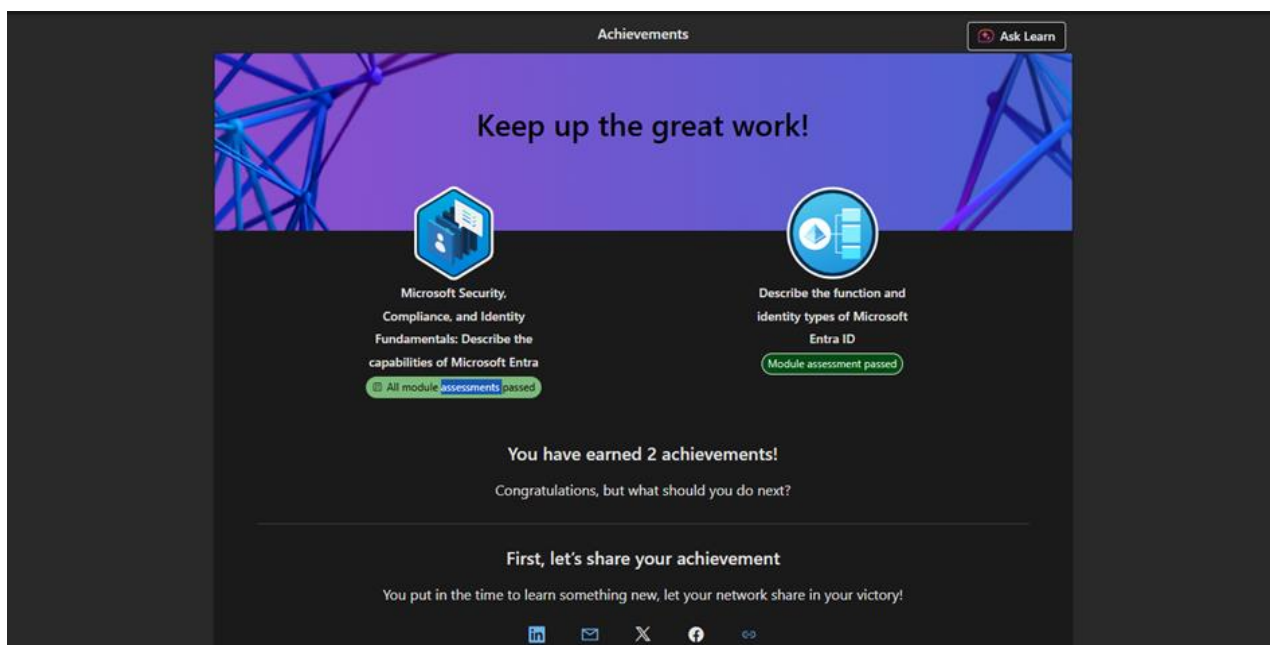
4. Describe the authentication capabilities of Microsoft Entra ID

This module gave me a deep dive into authentication methods supported by Microsoft Entra ID, including password-based, multi-factor authentication (MFA), Windows Hello, and FIDO2 security keys. I also understood how risk-based authentication works and how Conditional Access policies can be used to enhance authentication security.

I completed the module assessment and passed as shown below. I shared my achievement on LinkedIn and started building my visibility.

Verification link: https://learn.microsoft.com/en-us/users/vincentcollins-8814/achievements/w2x87pdn
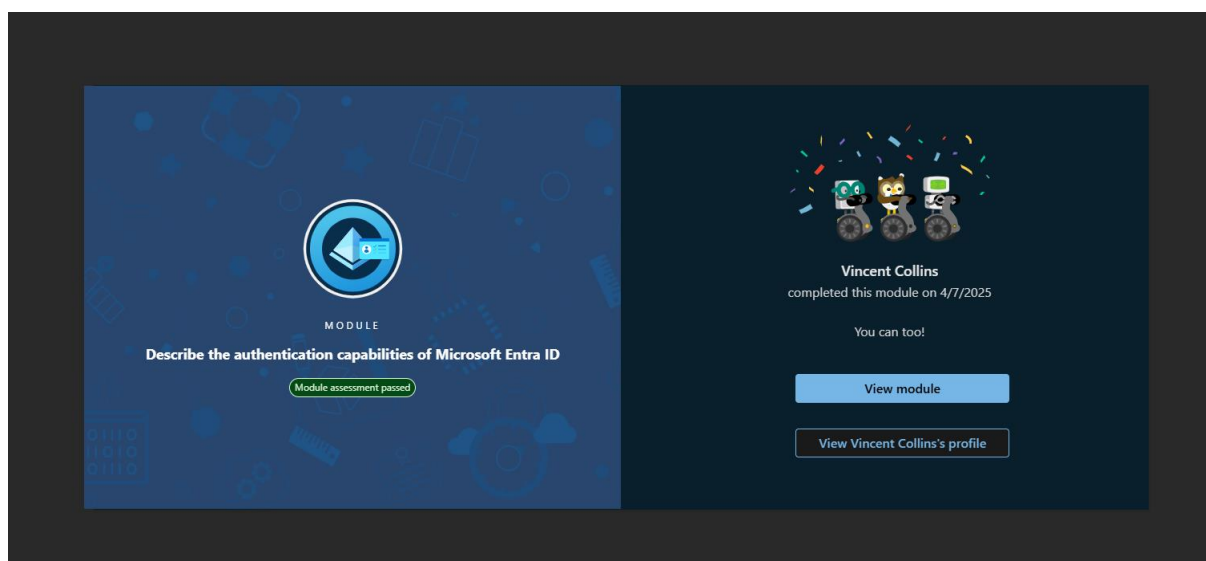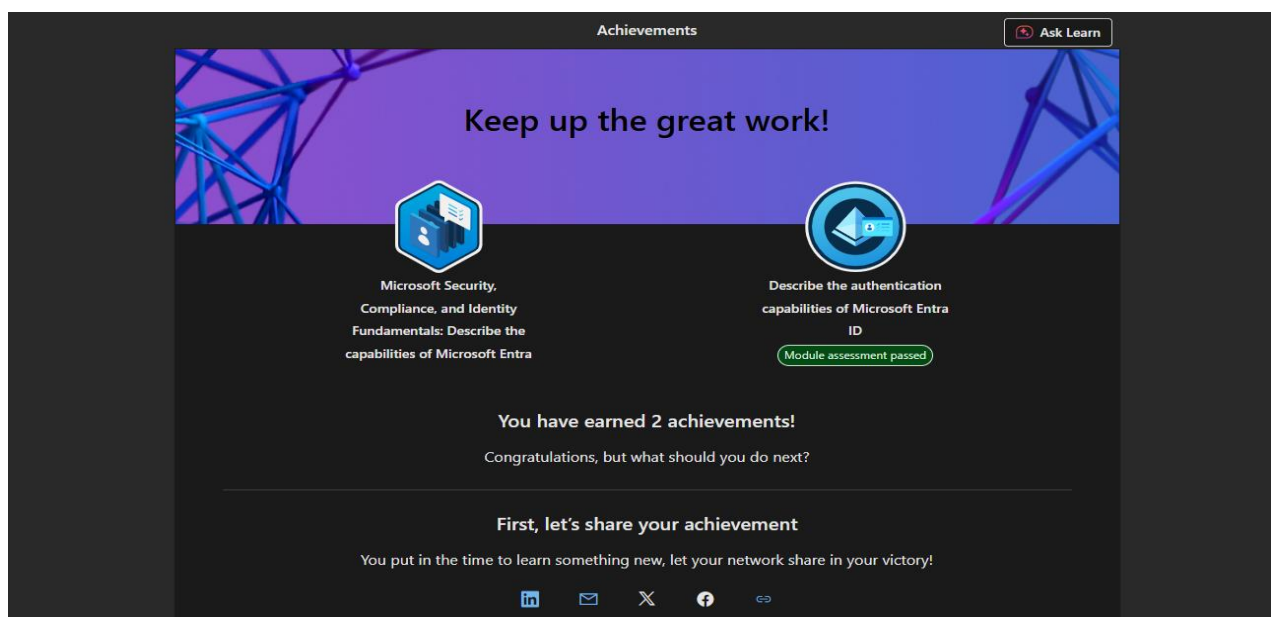
5. Describe access management capabilities of Microsoft Entra ID

In this module, I learned about access control mechanisms including role-based access control (RBAC), Microsoft Entra groups, entitlement management, and Privileged Identity Management (PIM). These capabilities allow organizations to enforce the principle of least privilege and monitor high-risk permissions.

I completed the module assessment and passed as shown below. I shared my achievement on LinkedIn to start building my professional visibility.

Verification link: https://learn.microsoft.com/en-us/users/vincentcollins-8814/achievements/fmrnv8zx
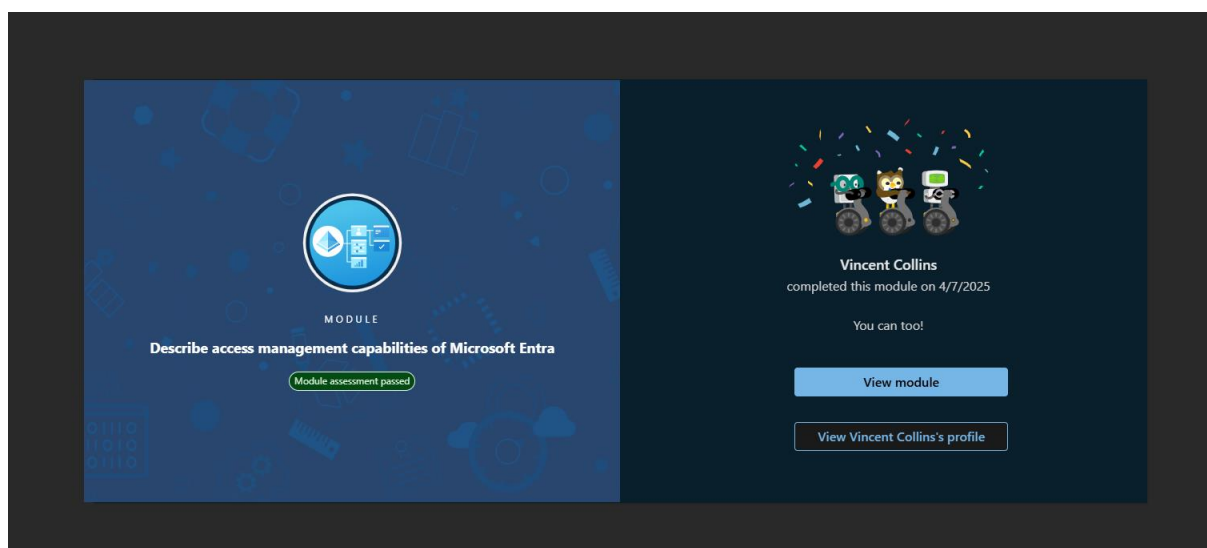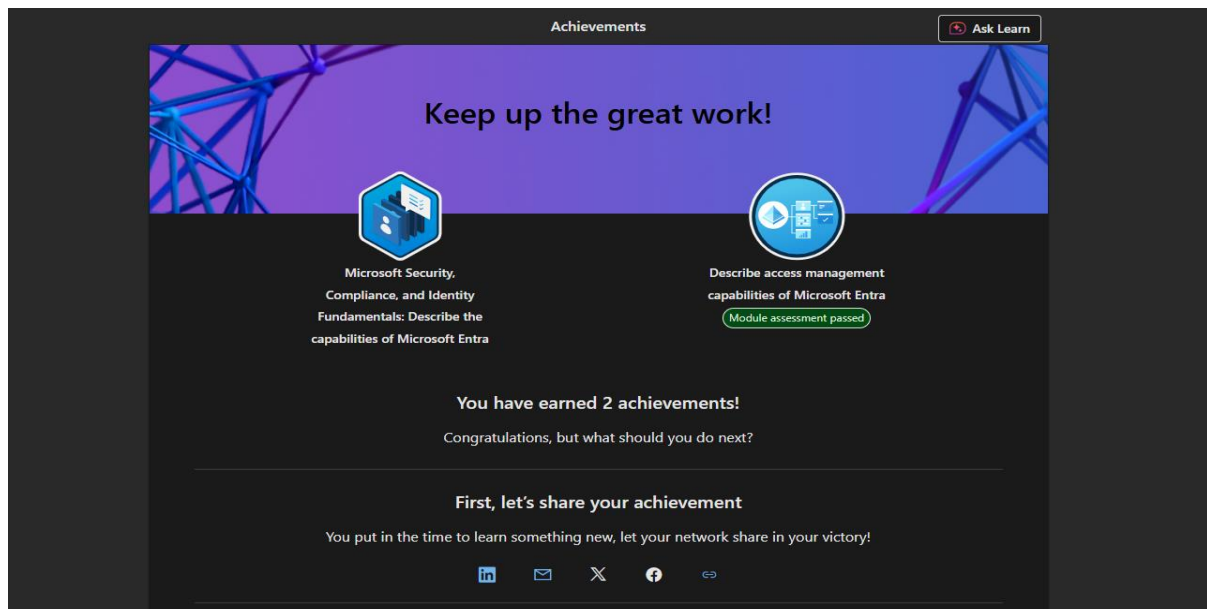
6. Describe the identity protection and governance capabilities of Microsoft Entra

The final module introduced advanced capabilities such as Microsoft Entra Identity Protection, which detects and responds to risky sign-ins, and governance features like access reviews, terms of use, and lifecycle management. I found the features for automated identity governance especially useful in maintaining compliance and security across an organization.

I completed the module assessment and passed as shown below. I shared my achievement on LinkedIn to start building my professional visibility.

Verification link: https://learn.microsoft.com/en-us/users/vincentcollins-8814/achievements/7kvabnaz
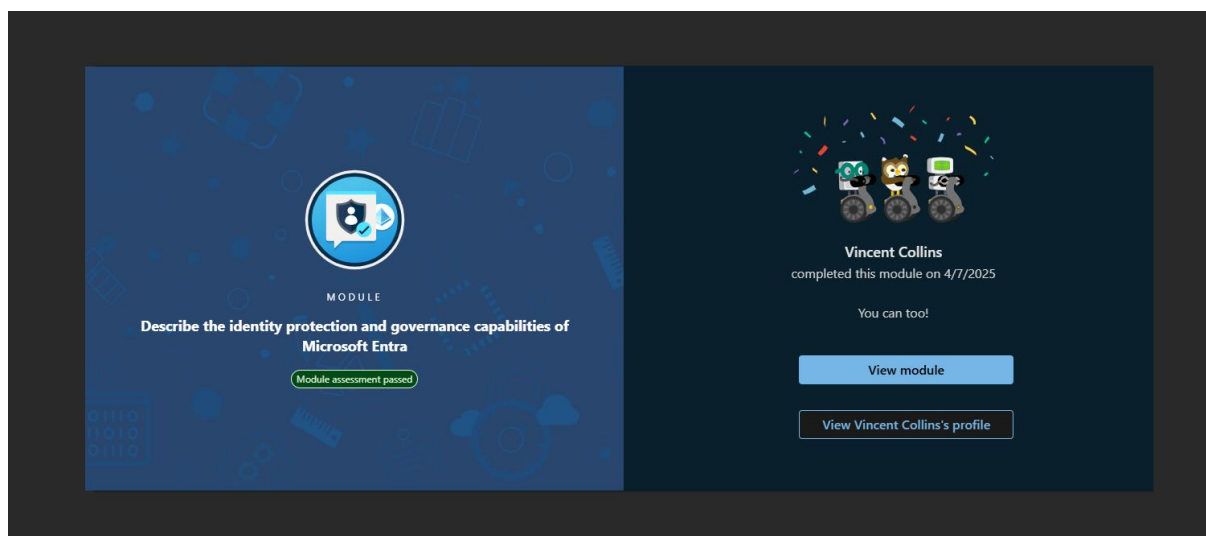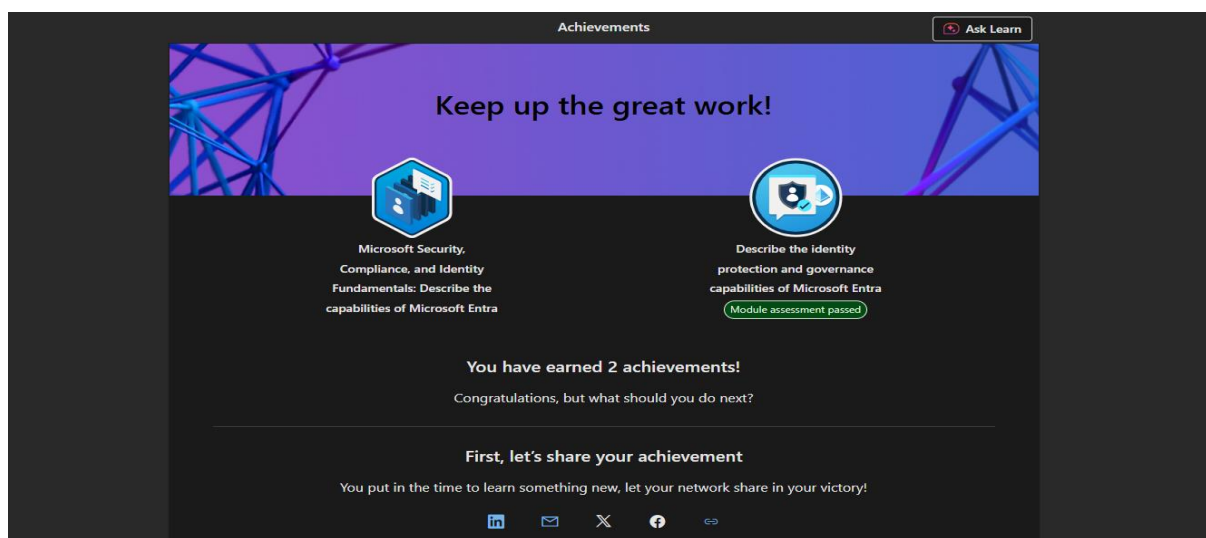
Conclusion

This week I gained a strong foundational understanding of security, compliance, and identity within Microsoft cloud environments. The SC-900 learning path introduced me to both core concepts and real-world tools used to manage and secure identities and data. This was my first full Microsoft Learn path, and I'm excited about how much I've learned already. I look forward to building on this foundation in upcoming weeks and sharing my learning journey publicly as I progress toward certification.