Cyber Shujaa

Cloud Security Specialist

Assignment 2: SC-900 Learning Path

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Table of Contents

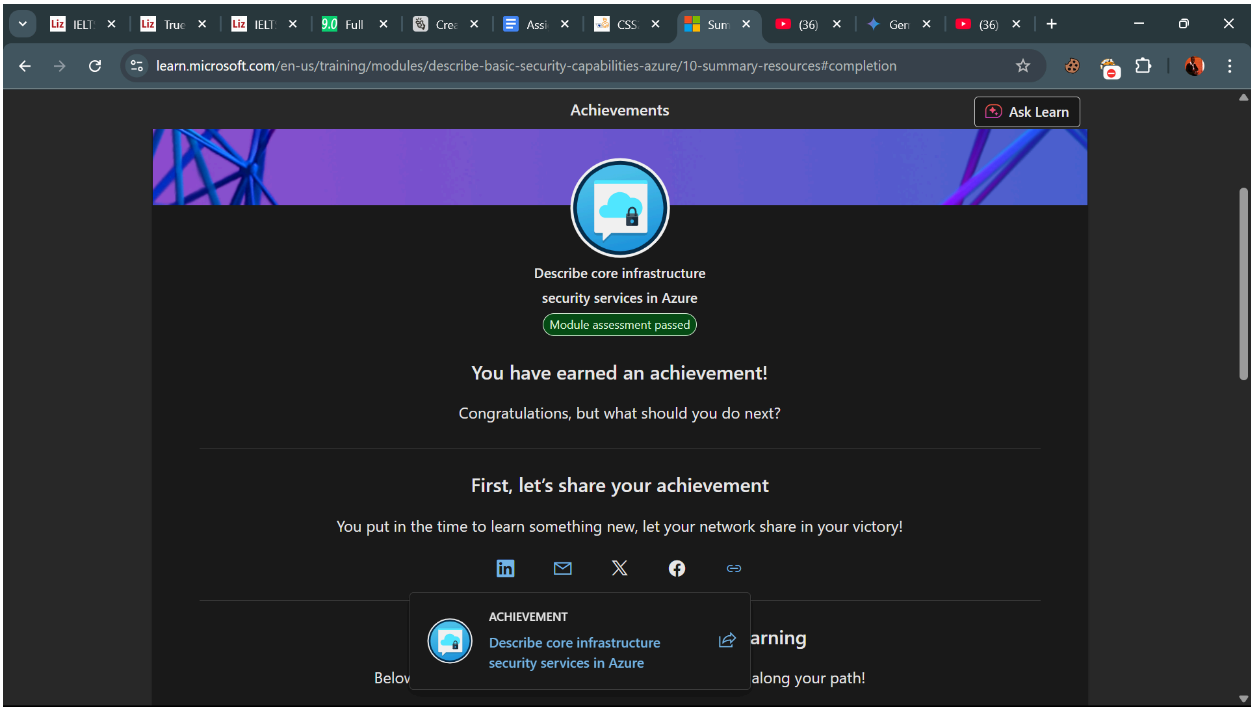
Introduction

In this assignment, we make a continuation of the previous learning path of the AZ 900. We will discuss and learn about the core infrastructure security services in Azure, the security management capabilities in Azure, the security capabilities of Microsoft Sentinel, and the threat protection with Microsoft Defender XDR.

Describe core infrastructure security services in Azure

We've explored the different service offerings provided by Azure, including DDoS protection, Azure Firewall, network security groups, and Azure Bastion to protect access to our systems. We now understand the reasons for and importance of using Azure Key Vault.

Without these security tools, our organization would be vulnerable to data theft, unable to respond swiftly to malicious attacks on our web and data services, and wouldn't meet our security obligations.
https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/ZBQYPVX2?sharingId=1C66F93EC0530812



learn.microsoft.com/en-us/training/modules/describe-basic-security-capabilities-azure/10-summary-resources#completion

Achievements

Describe core infrastructure security services in Azure

Module assessment passed

You have earned an achievement!

Congratulations, but what should you do next?

First, let's share your achievement

You put in the time to learn something new, let your network share in your victory!

ACHIEVEMENT

Describe core infrastructure security services in Azure

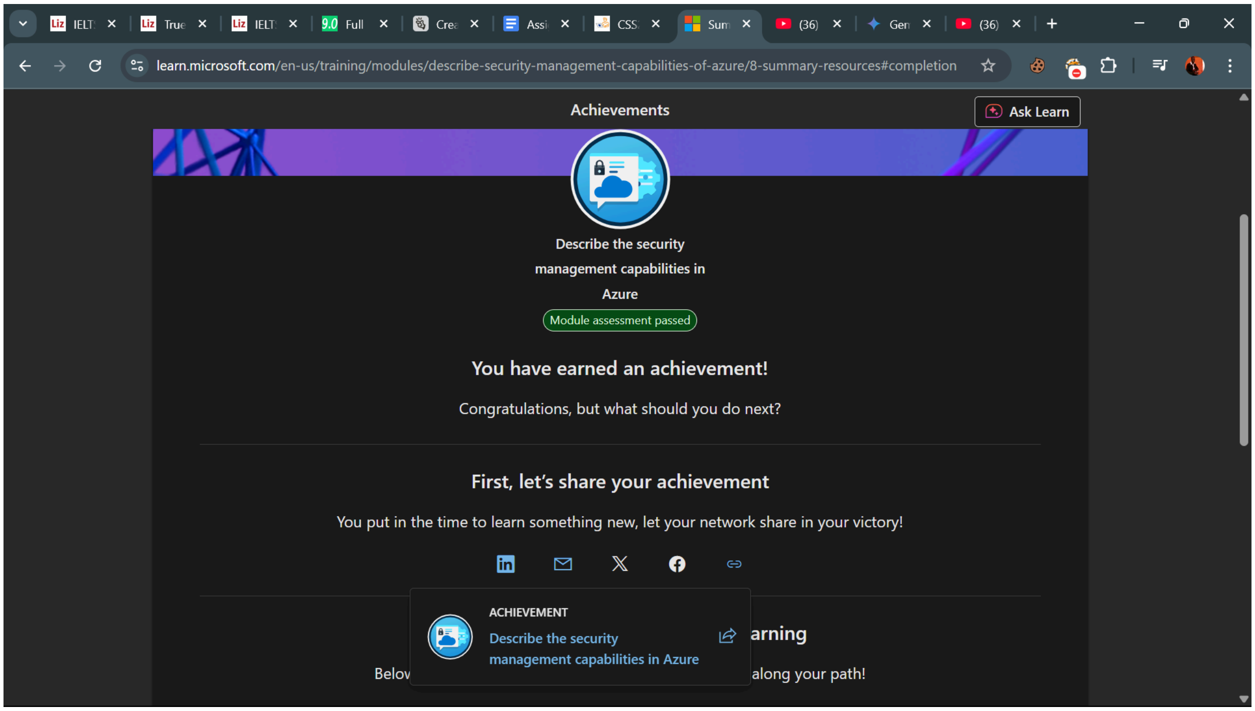
Belov arning

along your path!

Describe the security management capabilities in Azure

We learned about Microsoft Defender for Cloud and how it uses security policies and initiatives to improve cloud security posture. We also learned how each of the three pillars- Defender for DevOps, Cloud Security Posture Management, and Cloud Workload Protection of Microsoft Defender for Cloud protect against cyber threats and vulnerabilities.

https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/URWG2WV3?sharingId=1C66F93EC0530812


IELT
True
IELT
Full
Crea
Assi
CSS
Sum
(36)
Gen
(36)
learn.microsoft.com/en-us/training/modules/describe-security-management-capabilities-of-azure/8-summary-resources#completion
Achievements
Ask Learn

Describe the security management capabilities in Azure

Module assessment passed

You have earned an achievement!

Congratulations, but what should you do next?

First, let's share your achievement

You put in the time to learn something new, let your network share in your victory!

ACHIEVEMENT

Describe the security management capabilities in Azure

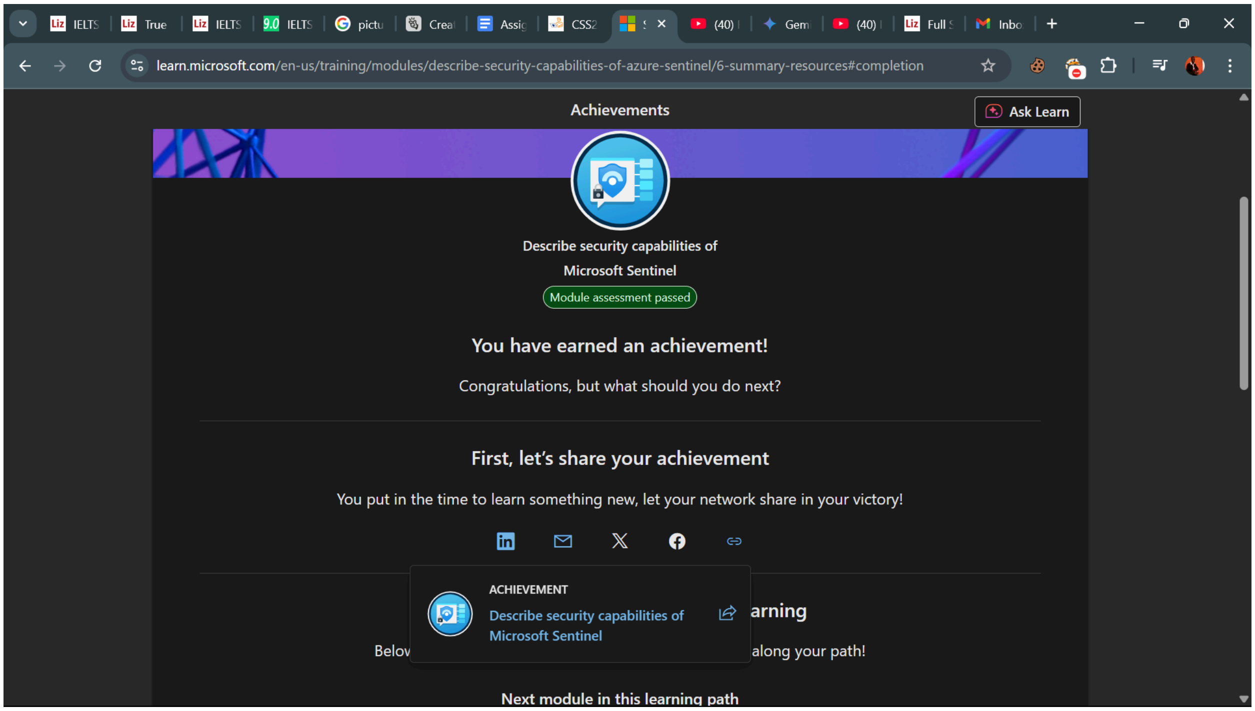
arning

Belov along your path!

Describe the security capabilities of Microsoft Sentinel

In this module, we learned about security information and event management (SIEM) and security orchestration automated response (SOAR). We discovered the key security operation areas that Microsoft Sentinel supports, such as the collection of incident data to response to the incidents and how it integrates with our existing security systems, including Microsoft Security Copilot.

https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/H7XYZ6Y8?sharingId=1C66F93EC0530812



learn.microsoft.com/en-us/training/modules/describe-security-capabilities-of-azure-sentinel/6-summary-resources#completion

Achievements

Ask Learn

Describe security capabilities of Microsoft Sentinel

Module assessment passed

You have earned an achievement!

Congratulations, but what should you do next?

First, let's share your achievement

You put in the time to learn something new, let your network share in your victory!

ACHIEVEMENT

Describe security capabilities of Microsoft Sentinel

arning

Belov

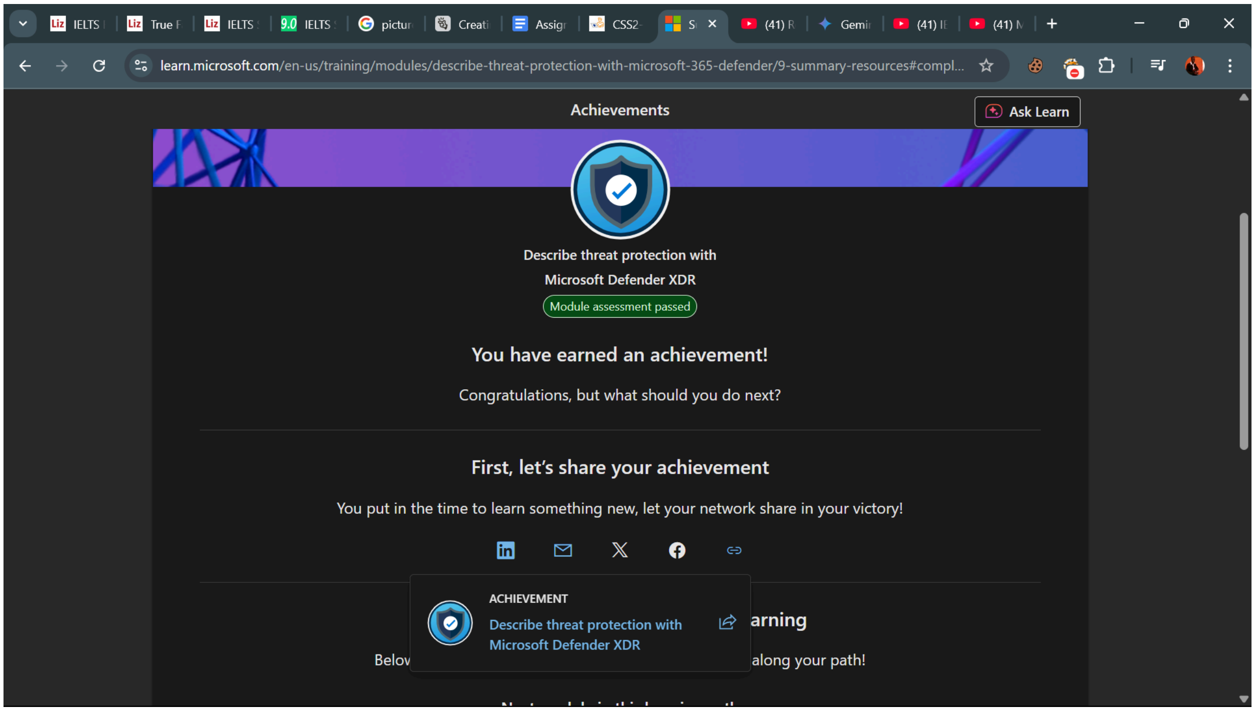
along your path!

Next module in this learning path

Describe threat protection with Microsoft Defender XDR

Extended Detection and Response (XDR) solutions are designed to deliver a holistic, simplified, and efficient approach to protect organizations against advanced attacks. Microsoft Defender XDR delivers a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

In this module, we learned how Microsoft Defender XDR can help protect our organization. We explored each of the different Defender services to understand how they can protect Identity, Office 365, endpoints, and cloud apps. We also explored the capabilities of the Microsoft Defender portal, including Microsoft Secure Score, reports, and incident management.
https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/3AFXTP5H?sharingId=1C66F93EC0530812



learn.microsoft.com/en-us/training/modules/describe-threat-protection-with-microsoft-365-defender/9-summary-resources#compl...

Achievements

Describe threat protection with Microsoft Defender XDR

Module assessment passed

You have earned an achievement!

Congratulations, but what should you do next?

First, let's share your achievement

You put in the time to learn something new, let your network share in your victory!

Describe threat protection with Microsoft Defender XDR

arning

Belov

along your path!

Conclusion

To conclude, we have explored the second part of the learning path of SC-900. Here, we have learned majorly of the Microsoft Defender for the cloud and its capability, the Microsoft Sentinel as a combination of SIEM and SOAR capabilities for monitoring and security orchestraions. We have also dwelled on the Defender for XDR, which leverages specific tools to safeguard identity, Microsoft 365, endpoints, and cloud apps for an organization.