

Let's team up for security

A new plan to create more well-skilled
(and well-paid) cybersecurity pros



Introduction:

The cybersecurity challenge—and opportunity

The unrelenting headlines about cyberattacks from ransomware to international cyberwarfare as precursor to invasion remind us of one thing:

The importance and need for highly skilled professionals to defend and secure our critical systems

Trouble is, there simply aren't enough of them

Consider this

Consider this –between 2020 and 2025, there will be a growth of 7 million jobs in security and privacy worldwide¹



Hold this up against an estimated pool of cybersecurity specialists of only 4.2 million

That's a gap of almost 2.8 million unfilled jobs²

And the number of cybersecurity jobs is expected to more than double between now and 2025

2x

Cybersecurity jobs more than double by 2025

The deficit of qualified cybersecurity specialists seems to be expanding

This skills gap is already costing money.

71% of employers have incurred damages because of cyber talent deficit³

And these are great jobs with some of the highest salaries in the tech field

Some are full-time cybersecurity jobs, like a chief information security officer, or CISO.

Others involve a combination of cybersecurity and other IT functions.



¹ Industry Skills Report 2021, Coursera

² A Resilient Cybersecurity Profession Charts the Path Forward, (ISC)2 Cybersecurity Workforce Study, 2021, (ISC)2, 2021

³ 3 Key Statistics from Global Cybersecurity Outlook 2022, Swiss Cyber Institute, March 10, 2022

Skill up for security:

Steps to higher cloud security, compliance, and identity skills

To support your next level of capability and fill one of those open positions, you need a plan

Here are three steps to jumpstart your journey to the security, compliance, and identity skills you need

And, with help from Microsoft Learn, you have the structure and resources you need to empower yourself and your teams as they expand their technical skill sets

1

Familiarize yourself with the skills map and your milestones

- You can find recommended skilling journeys and the tracks for learners in the Security, Compliance, and Identity Journey handbook.

2

Identify the skills, from the basics on, that you need

- Match your planned career direction and next steps with your skilling path
- You'll find that each journey is designed to help identify where to start and where to go based on their specific role or projects.

3

Muster your resources

- After determining which journey is the right fit, find courses, training opportunities, and other important information that sets your team up for success.

Your security, compliance, and identity certification options

1

Microsoft Certified: Security, Compliance, and Identity Fundamentals

For students, business users, or IT professionals

- This fundamentals certification gives you a firm grasp of a range of topics in the rapidly growing field of cybersecurity.
- A first step to advancing to role-based certifications in security operations, identity and access management, and information protection.

3

Microsoft Certified: Identity and Access Administrator Associate

- Gain the skills to design, implement, and operate an organization's identity and access management systems using Azure Active Directory.
- Manage tasks such as providing secure authentication and authorization access to enterprise applications.
- You'll also learn to troubleshoot, monitor, and report on the identity and access environment.

2

Microsoft Certified: Security Operations Analyst Associate

- Collaborate with organizational stakeholders to secure information technology systems for the organization.
- Help reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders.

4

Microsoft Certified: Information Security Administrator Associate

- This certification prepares you to take on responsibility for translating requirements and compliance controls into technical implementation.
- You'll be prepared to assist organizational control owners to become and stay compliant and implement technology that supports policies and controls necessary to sufficiently address regulatory requirements for their organization.

Your security, compliance, and identity certification options

5

Microsoft Certified: Azure Security Engineer Associate

- Manage the security posture, identify and remediate vulnerabilities, perform threat modeling, implementing threat protection, and respond to security incident escalations.
- This course gives you the toolkit to manage security and access, implement platform protection, and to manage your security operations.

6

Microsoft Certified: Cybersecurity Architect Expert

- This certification prepares you to translate cybersecurity strategies into actionable capabilities that protect an organization's assets, business operations, and digital infrastructure.
- You'll be equipped to design and guide the implementation of Zero Trust-aligned security solutions across identity, devices, data, AI, applications, networks, and cloud environments.

Elevate your expertise with Microsoft Applied Skills

1

Microsoft Applied Skills: Get started with identities and access using Microsoft Entra

To earn this Microsoft Applied Skills credential, learners demonstrate the ability to manage identities and access in Microsoft Entra.

As a candidate for this credential, you should be familiar with Microsoft Entra ID.

What you will learn in this assessment

- Perform basic user management tasks
- Perform basic group management tasks
- Perform basic password protection tasks
- Perform basic Self-Service Password Reset (SSPR) tasks
- Perform basic Multifactor authentication tasks
- Perform basic conditional access policy tasks

2

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

To earn this Microsoft Applied Skills credential, learners must demonstrate the ability to implement regulatory compliance controls using the Microsoft cloud security benchmark. Candidates should have experience with Azure IaaS and PaaS, Azure security features, and a basic understanding of compliance standards.

What you will learn in this assessment

- Configure Microsoft Defender for Cloud
- Implement just-in-time (JIT) virtual machine (VM) access
- Implement a Log Analytics workspace
- Mitigate network security risks
- Mitigate data protection risks
- Mitigate endpoint security risks
- Mitigate posture and vulnerability management risks

3

Implement information protection and data loss prevention by using Microsoft Purview

Gain the skills to use Microsoft Purview to improve your data security in Microsoft 365. In this training, you learn how to create sensitive information types, create sensitivity labels, and use auto-labeling policies based on these labels. You also learn how to set up DLP (Data Loss Prevention) policies to safeguard your organization's data.

Prerequisites

- Basic understanding of Microsoft 365 products and services
- Familiarity with Microsoft Purview
- An understanding of the data security concept

What you will learn in this assessment

- Create a custom sensitive information type
- Create and publish a sensitivity label
- Create and assign an auto-labeling policy
- Create a data loss prevention (DLP) policy

4

Defend against cyberthreats with Microsoft Defender XDR

Implement the Microsoft Defender for Endpoint environment to manage devices, perform investigations on endpoints, manage incidents in Defender XDR, and use Advanced Hunting with Kusto Query Language (KQL) to detect unique threats.

Prerequisites

- Experience using the Microsoft Defender portal
- Basic understanding of Microsoft Defender for Endpoint
- Basic understanding of Microsoft Sentinel
- Experience using Kusto Query Language (KQL) in Microsoft Sentinel

What you will learn in this assessment

- Configure a Defender XDR environment
- Manage devices by using Defender for Endpoint
- Use Defender XDR to manage incidents
- Manage investigations on an endpoint
- Perform Advanced Hunting with KQL to detect unique threats

5

Implement retention, eDiscovery, and Communication compliance in Microsoft Purview

Manage data lifecycle, records management, eDiscovery, and communication compliance with Microsoft Purview.

Prerequisites

- Basic understanding of data governance and compliance concepts.
- Familiarity with Microsoft Purview and its interface.
- Knowledge of data lifecycle management principles.
- Experience with eDiscovery processes.
- Awareness of communication compliance requirements.

What you will learn in this assessment

- Create and configure retention labels
- Apply retention labels
- Create and manage retention policies
- Create and configure eDiscovery (Premium) cases
- Implement Communication Compliance
- Monitor and investigate data and activities by using Content search

**Learn how to unlock growth with
Certifications and Applied Skills.**

www.flane.de/microsoft-security-training