Startel
Dé IT-opleider

Microsoft Information Protection Administrator (SC-400)

Deze training biedt een diepgaand begrip van hoe je gevoelige informatie effectief kunt beschermen en beheren met behulp van de beveiligingstechnologieën van Microsoft.

Algemene omschrijving

De training: “Microsoft Information Protection Administrator (SC-400)” is essentieel voor ICT-professionals die zich willen specialiseren in het beheren van informatiebescherming binnen hun organisatie. Deze training biedt een diepgaand begrip van hoe je gevoelige informatie effectief kunt beschermen en beheren met behulp van de beveiligingstechnologieën van Microsoft.

Door deel te nemen aan deze training zul je over de nieuwste middelen en praktijken leren om datalekken te voorkomen en te reageren op beveiligingsincidenten. De training: “Microsoft Information Protection Administrator (SC-400)” omvat verschillende kerngebieden, zoals het classificeren, bestempelen en beschermen van gevoelige informatie, het beheren van databestuur en het implementeren van volledige informatiebeschermingsstrategieën.

In deze training leer je ook te werken met Microsoft 365 Compliance Center, Microsoft Information Protection (MIP), en andere relevante technologieën. De training is ontworpen om jou niet alleen theoretische kennis te bieden, maar ook praktische vaardigheden die direct toepasbaar zijn jouw dagelijkse werkzaamheden.

Doelgroep

De training: “Microsoft Information Protection Administrator (SC-400)” is bijzonder relevant voor diegenen die verantwoordelijk zijn voor het beheren, implementeren en monitoren van informatiebeveiligingsbeleid en -praktijken.

Deze training biedt jou een uitstekende mogelijkheid om jouw vaardigheden te verfijnen in het gebruik van Microsoft 365 Compliance Center en Microsoft Information Protection, essentiële hulpmiddelen voor moderne informatiebeveiliging.

Deze training is met name geschikt voor de volgende mensen:

- **Compliance Officers en Data Protection Officers**
  - Compliance Officers en Data Protection Officers zullen veel voordeel hebben aan het

volgen van deze training. De training biedt diepgaand inzicht in hoe gevoelige informatie geclassificeerd, bestempeld en beschermd kan worden binnen een organisatie. Dit is cruciaal voor het voldoen aan wettelijke vereisten en het waarborgen van de naleving van regelgeving zoals de AVG (GDPR). De training voorziet jou van de benodigde kennis en vaardigheden om jouw werk effectiever uit te voeren en het risico op datalekken te beperken.

- **Netwerk- en systeembeheerders**
  - Netwerk- en systeembeheerders die betrokken zijn bij het beheren van netwerk- en systeembeveiliging zullen deze training waardevol vinden. Deze training helpt jou om beter te begrijpen hoe informatiebeveiliging geïntegreerd kan worden in de dagelijkse ICT-beheerprocessen. Dit versterkt jouw vermogen om proactief te handelen tegen beveiligingsrisico's en om een robuuste en veilige ICT-omgeving te onderhouden.
- **ICT-consultants en projectmanagers**
  - ICT-consultants en projectmanagers die aan projecten werken die gerelateerd zijn aan gegevensbescherming en naleving zullen veel baat hebben bij het volgen van deze training. De training biedt jou een gedegen basiskennis en praktische vaardigheden die essentieel zijn bij het adviseren van klanten of het leiden van projecten op het gebied van informatiebeveiliging en gegevensbeheer. Het verkrijgen van het certificaat versterkt jouw geloofwaardigheid en expertise in de ogen van potentiële klanten en werkgevers.

Leerdoelen

Door deze training te volgen zul je de volgende kennis en vaardigheden verkrijgen:

- Het uitleggen en gebruiken van sensitivity labels.
- Het maken van een beleid voor Data Loss Prevention (DLP).
- Berichten beveiligen in Office 365.
- Beschrijven van het proces voor de information governance-configuratie.
- Het definiëren van sleutelbegrippen in verband met Microsofts information- en governance-oplossingen.
- Het uitleggen van de Content explorer en de Activity explorer.
- Het beschrijven hoe je gevoelige soorten informatie gebruikt en trainable classifiers.
- DLP-rapportages beoordelen en analyseren.
- DLP policy-overtredingen identificeren en beperken.
- Het beschrijven van de integratie van DLP met Microsoft Cloud App Security (MCAS).
- Het gebruiksklaar maken van Endpoint DLP
- Het beschrijven van record management
- Event driven retention configureren.
- Een file plan importeren.
- Retentiebeleid en labels configureren.
- Het maken van custom keyword dictionaries
- Het implementeren van document fingerprinting.

Voorkennis

Voordat je deelneemt aan de training: “Microsoft Information Protection Administrator (SC-400)” is het belangrijk dat je over basiskennis beschikt van Microsoft Security en nalevingstechnologieën. Deze kennis vormt de basis voor het begrijpen van de geavanceerde onderwerpen die in deze training worden behandeld en is cruciaal voor het effectief beheren van informatiebeveiliging binnen een Microsoft-omgeving.

- **Basiskennis van informatiebeveiligingsconcepten**
  - Een goede basis in informatiebeveiligingsconcepten is essentieel voor het volgen van deze training. Dit omvat een begrip van de basisprincipes van gegevensbescherming, risicobeheer en de verschillende bedreigingen en kwetsbaarheden die de beveiliging van gevoelige informatie kunnen beïnvloeden.
- **Kennis van cloud computing**
  - Een goed begrip van cloud computing is een belangrijke voorwaarde voor het volgen van deze training. Deelnemers moeten bekend zijn met de basisprincipes van clouddiensten, waaronder openbare, private en hybride cloudmodellen, evenals de rol die deze spelen in moderne informatiebeveiligingsstrategieën.
- **Inzicht in Microsoft 365-producten en diensten**
  - Kennis van Microsoft 365-producten en diensten is een belangrijk element voor het volgen van deze training. Dit begrip stelt deelnemers in staat om de specifieke hulpmiddelen en functies die worden gebruikt voor informatiebeveiliging en naleving binnen het Microsoft 365-ecosysteem, effectief te benutten.

Onderwerpen

Module 1: Implement Information Protection in Microsoft 365

Organizations require information protection solutions to protect their data against theft and accidental loss. Learn how to protect your sensitive information. Learn how Microsoft 365 information protection and governance solutions help you protect and govern your data, throughout its lifecycle – wherever it lives, or wherever it travels. Learn about the information available to help you understand your data landscape and know your data. Learn how to use sensitive information types to support your information protection strategy. Learn about how sensitivity labels are used to classify and protect business data while making sure that user productivity and their ability to collaborate are not hindered.

Lessons:

- Introduction to information protection and governance in Microsoft 365.
- Classify data for protection and governance.
- Create and manage sensitive information types.
- Describe Microsoft 365 encryption.
- Deploy message encryption in Office 365.
- Configure sensitivity labels.
- Apply and manage sensitivity labels.

Lab: Implement Information Protection

- Assign permissions for compliance.
- Manage Office 365 message encryption.
- Manage Sensitive Information Types.
- Manage Trainable Classifiers.
- Manage Sensitivity Labels.

After completing this module, students will be able to:

- Describe Microsoft’s approach to information protection and governance.
- List the components of the Data Classification solution.
- Describe how to use sensitive information types and trainable classifiers.

- Implement document fingerprinting.
- Create custom keyword dictionaries.
- Deploy message encryption in Office 365.

Module 2: Implement Data Loss Prevention in Microsoft 365

In this module we discuss how to implement data loss prevention techniques to secure your Microsoft 365 data. Learn how to discover, classify, and protect sensitive and business-critical content throughout its lifecycle across your organization. Learn how to configure and implement data loss prevention policies and integrate them with Microsoft Cloud App Security. Learn how to respond to and mitigate data loss policy violations.

Lessons:

- Prevent Data loss in Microsoft 365.
- Implement Endpoint data loss prevention.
- Configure DLP policies for Microsoft Cloud App Security and Power Platform.
- Manage DLP policies and reports in Microsoft 365.

Lab: Implement Data Loss Prevention

- Manage DLP policies.
- Mange Endpoint DLP.
- Test DLP policies.
- Mange DLP reports.

After completing this module, students will be able to:

- Describe the information protection configuration process.
- Articulate deployment and adoption best practices.
- Describe the integration of DLP with Microsoft Cloud App Security (MCAS).
- Configure policies in Microsoft Cloud App Security.
- Review and analyze DLP reports.
- Identify and mitigate DLP policy violations.
- Mitigate DLP violations in MCAS.

Module 3: Implement Information Governance in Microsoft 365

In this module you will learn how to plan and implement information governance strategies for an organization. Learn how to manage your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't. Learn how to manage retention for Microsoft 365, and how retention solutions are implemented in the individual Microsoft 365 services. Learn how to use intelligent classification to automate and simplify the retention schedule for regulatory, legal, and business-critical records in your organization.

Lessons:

- Govern information in Microsoft 365.
- Manage data retention in Microsoft 365 workloads.
- Manage records in Microsoft 365.

Lab: Implement Information Governance

- Configure Retention Labels.
- Implement Retention Labels.
- Configure Service-based Retention.
- Use eDiscovery for Recovery.
- Configure Records Management.

After completing this module, students will be able to:

- Describe the information governance configuration process.
- Articulate deployment and adoption best practices.
- Describe the retention features in Microsoft 365 workloads.
- Configure retention settings in Microsoft Teams and SharePoint Online.
- Implement retention for Exchange Mailbox items.
- Recover content protected by retention settings.
- Regain protected items from Exchange Mailboxes.
- Describe the records management configuration process.