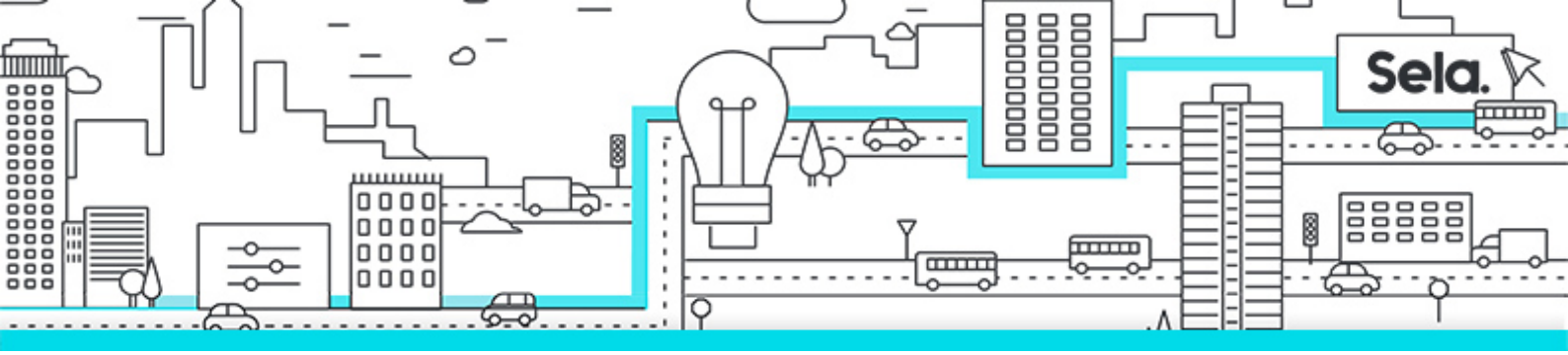
MS101

Microsoft 365 Mobility and Security

college@sela.co.il 03-6176666



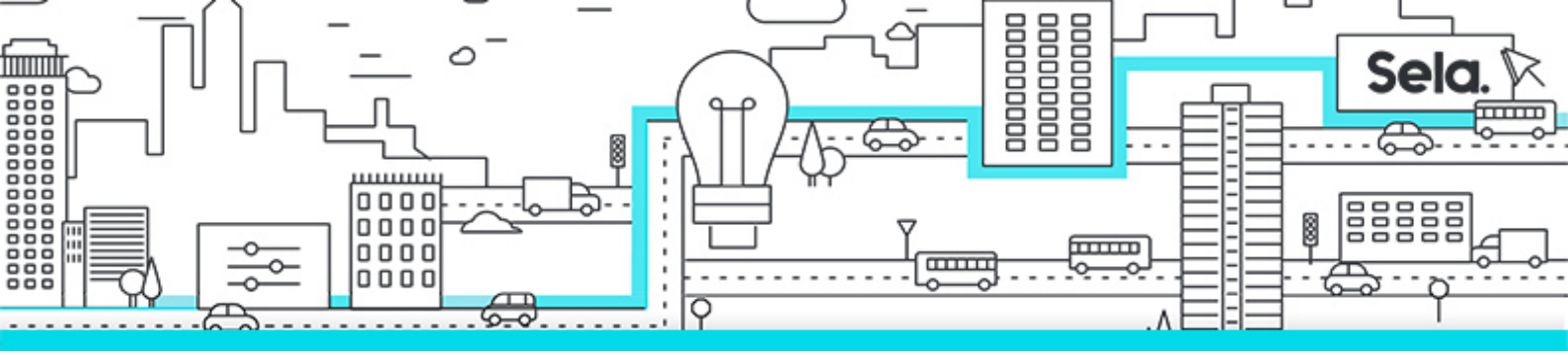
Microsoft 365 Mobility and Security

MS101 - Version: 1

5 days course

Description:

This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 security management, Microsoft 365 compliance management, and Microsoft 365 device management. In Microsoft 365 security management, you will examine all the common types of threat vectors and data breaches facing organizations today, and you will learn how Microsoft 365's security solutions address these security threats. You will be introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You will then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Safe Attachments, and Safe Links. Finally, you will be introduced to the various reports that monitor your security health. You will then transition from security services to threat intelligence; specifically, using Microsoft 365 Defender, Microsoft Defender for Cloud Apps, and Microsoft Defender for Endpoint. With your Microsoft 365 security components now firmly in place, you will examine the key components of Microsoft 365 compliance management. This begins with an overview of all key aspects of data governance, including data archiving and retention, Microsoft Purview message encryption, and data loss prevention (DLP). You will then delve deeper into archiving and retention, paying particular attention to Microsoft Purview insider risk management, information barriers, and DLP policies. You will then examine how to implement these compliance features through the use of data classification and sensitivity labels. You will conclude this section by learning how to manage search and investigation in the Microsoft Purview compliance portal. You will cover Microsoft Purview Audit (Standard and Premium) and Microsoft Purview eDiscovery (Standard and Premium). The course concludes with an in-depth examination of Microsoft 365 device management. You will



begin by planning for various aspects of device management, including preparing your Windows devices for co-management, planning for mobile application management, examining Windows client deployment scenarios, Windows Autopilot deployment models, and planning your Windows client subscription strategy. Finally, you will transition from planning to implementing device management; specifically, your Windows client deployment strategy, Windows Autopilot, Mobile Device Management (MDM), device enrollment to MDM, and endpoint security in Microsoft Intune.

Intended Audience:

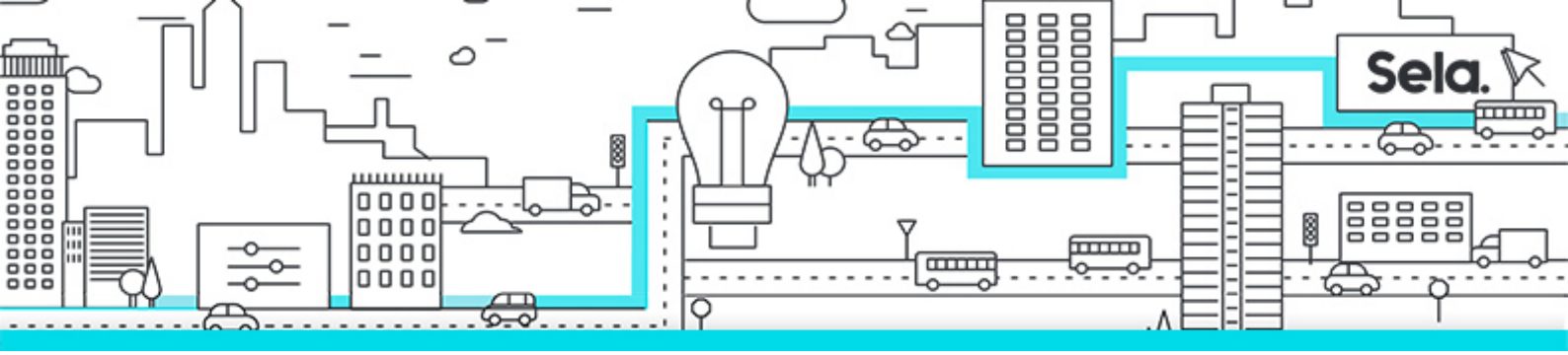
This course is designed for persons who are aspiring to the Microsoft 365 Enterprise Admin role and have completed one of the Microsoft 365 role-based administrator certification paths.

Prerequisites:

• Before attending this course, students must have:
• Completed a role-based administrator course such as Messaging, Teamwork, Security and Compliance, or Collaboration.
• A proficient understanding of DNS and basic functional experience with Microsoft 365 services.
• A proficient understanding of general IT practices.

Topics:

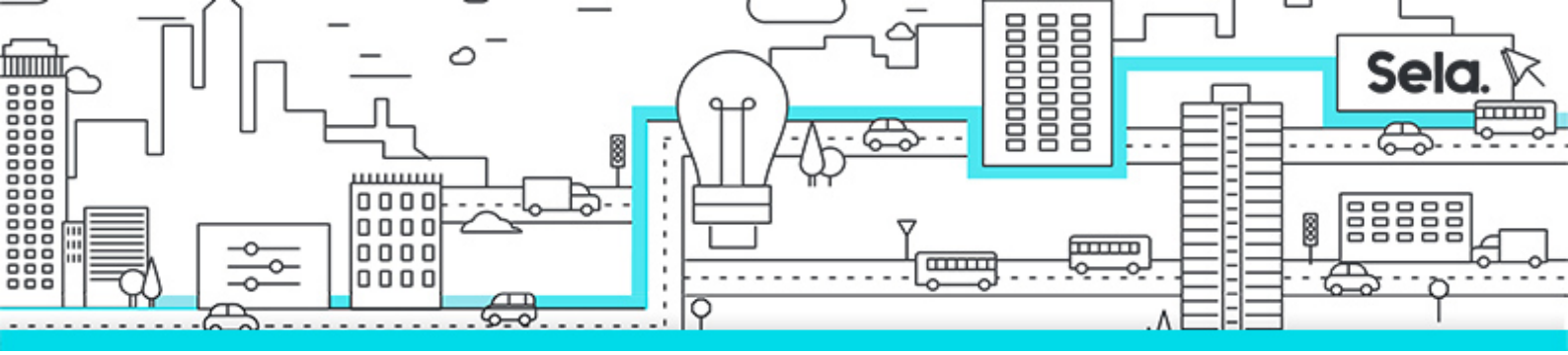
• **Examine threat vectors and data breaches**
- This module examines the types of threat vectors and their potential outcomes that organizations must deal with on a daily basis and how users can enable hackers to access targets by unwittingly executing malicious content.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe techniques hackers use to compromise user accounts through email



- Describe techniques hackers use to gain control over resources
- Describe techniques hackers use to compromise data
- Mitigate an account breach
- Prevent an elevation of privilege attack
- Prevent data exfiltration, data deletion, and data spillage

• **Explore the Zero Trust security model**
- This module examines the concepts and principles of the Zero Trust security model, as well as how Microsoft 365 supports it, and how your organization can implement it.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe the Zero Trust approach to security in Microsoft 365
- Describe the principles and components of the Zero Trust security model
- Describe the five steps to implementing a Zero Trust security model in your organization
- Explain Microsoft's story and strategy around Zero Trust networking

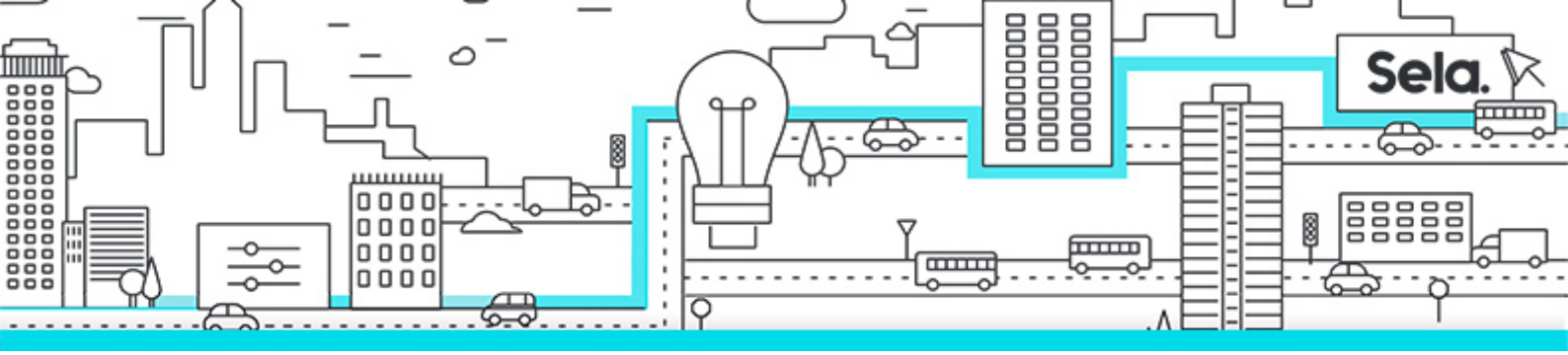
• **Explore security solutions in Microsoft 365 Defender**
- This module introduces you to several features in Microsoft 365 that can help protect your organization against cyberthreats, detect when a user or computer has been compromised, and monitor your organization for suspicious activities.
- Learning objectives
- By the end of this module, you'll be able to:
- Identify the features of Microsoft Defender for Office 365 that enhance email security in a Microsoft 365 deployment
- Explain how Microsoft Defender for Identity identifies, detects, and investigates advanced threats, compromised identities, and malicious insider actions directed at your organization
- Explain how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats
- Describe how Microsoft 365 Threat Intelligence can be beneficial to your



organization’s security officers and administrators
- Describe how Microsoft Cloud App Security enhances visibility and control over your Microsoft 365 tenant through three core areas

• **Examine Microsoft Secure Score**
- This module examines how Microsoft Secure Score helps organizations understand what they've done to reduce the risk to their data and show them what they can do to further reduce that risk.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe the benefits of Secure Score and what kind of services can be analyzed
- Describe how to collect data using the Secure Score API
- Describe how to use the tool to identify gaps between your current state and where you would like to be regarding security
- Identify actions that will increase your security by mitigating risks
- Explain where to look to determine the threats each action will mitigate and the impact it has on users

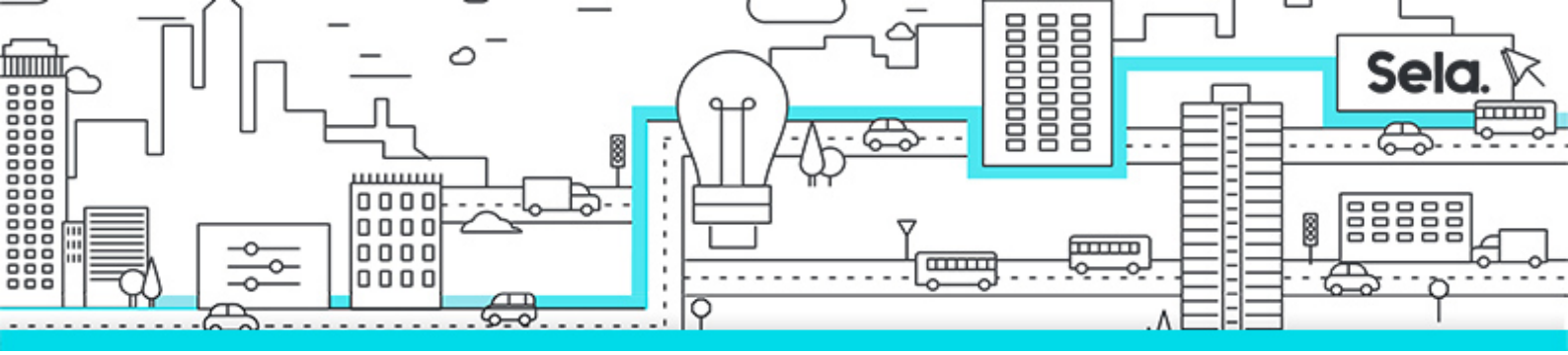
• **Examine Privileged Identity Management**
- This module examines how Privileged Identity Management ensures users in your organization have just the right privileges to perform the tasks they need to accomplish.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how Privileged Identity Management enables you to manage, control, and monitor access to important resources in your organization
- Configure Privileged Identity Management for use in your organization
- Describe how Privileged Identity Management audit history enables you to see all the user assignments and activations within a given time period for all privileged roles
- Explain how Microsoft Identity Manager helps organizations manage the users, credentials, policies, and access within their organizations and hybrid



environments
- Explain how Privileged Access Management provides granular access control over privileged admin tasks in Microsoft 365

• **Examine Azure Identity Protection**
- This module examines how Azure Identity Protection provides organizations the same protection systems used by Microsoft to secure identities.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe Azure Identity Protection (AIP) and what kind of identities can be protected
- Enable the three default protection policies in AIP
- Identify the vulnerabilities and risk events detected by AIP
- Plan your investigation in protecting cloud-based identities
- Plan how to protect your Azure Active Directory environment from security breaches

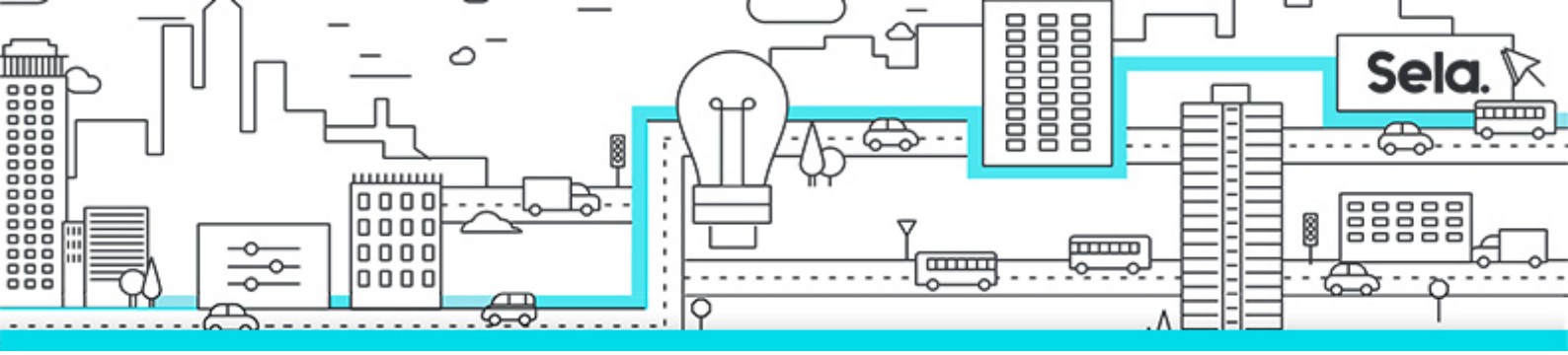
• **Examine Exchange Online Protection**
- This module examines how Exchange Online Protection (EOP) protects organizations from phishing and spoofing. It also explores how EOP blocks spam, bulk email, and malware before they arrive in users' mailboxes.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how Exchange Online Protection analyzes email to provide anti-malware pipeline protection.
- List several mechanisms used by Exchange Online Protection to filter spam and malware.
- Describe other solutions administrators may implement to provide extra protection against phishing and spoofing.
- Understand how EOP provides protection against outbound spam.



- **Examine Microsoft Defender for Office 365**
  - This module examines how Microsoft Defender for Office 365 extends EOP protection by filtering targeted attacks such as zero-day attacks in email attachments and Office documents, and time-of-click protection against malicious URLs.
  - Learning objectives
  - By the end of this module, you'll be able to:
  - Describe how the Safe Attachments feature in Microsoft Defender for Office 365 blocks zero-day malware in email attachments and documents.
  - Describe how the Safe Links feature in Microsoft Defender for Office 365 protects users from malicious URLs embedded in email and documents that point to malicious websites.
  - Create outbound spam filtering policies.
  - Unblock users who violated spam filtering policies so they can resume sending emails.

- **Manage Safe Attachments**
  - This module examines how to manage Safe Attachments in your Microsoft 365 tenant by creating and configuring policies and using transport rules to disable a policy from taking effect in certain scenarios.
  - Learning objectives
  - By the end of this module, you'll be able to:
  - Create and modify a Safe Attachments policy using Microsoft 365 Defender
  - Create a Safe Attachments policy by using PowerShell
  - Configure a Safe Attachments policy
  - Describe how a transport rule can disable a Safe Attachments policy
  - Describe the end-user experience when an email attachment is scanned and found to be malicious

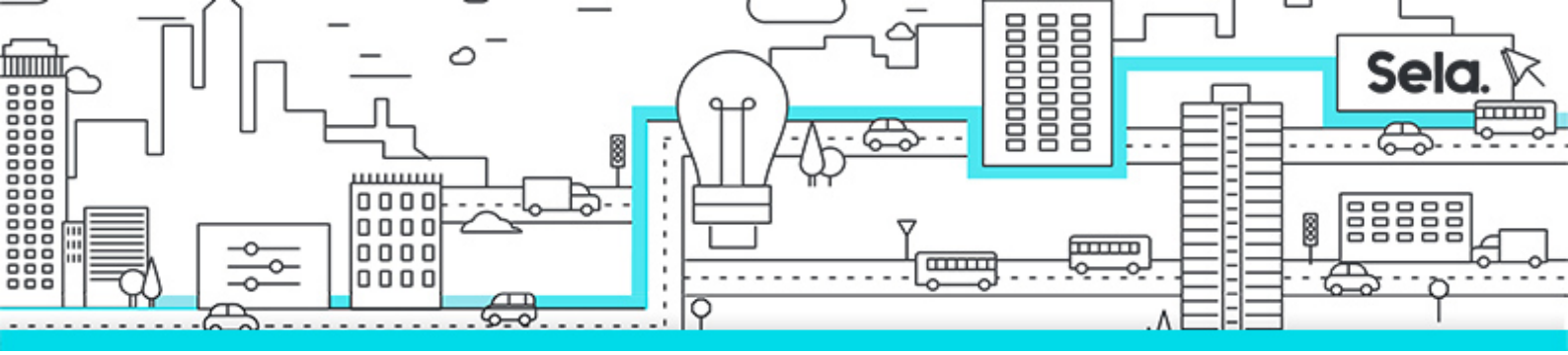
- **Manage Safe Links**
  - This module examines how to manage Safe Links in your tenant by creating and configuring policies and using transport rules to disable a policy from taking



effect in certain scenarios.
- Learning objectives
- By the end of this module, you'll be able to:
- Create and modify a Safe Links policy using Microsoft 365 Defender
- Create a Safe Links policy using PowerShell
- Configure a Safe Links policy
- Describe how a transport rule can disable a Safe Links policy
- Describe the end-user experience when Safe Links identifies a link to a malicious website embedded in email, and a link to a malicious file hosted on a website

• **Explore threat intelligence in Microsoft 365 Defender**
- This module examines how Microsoft 365 Threat Intelligence provides admins with evidence-based knowledge and actionable advice that can be used to make informed decisions about protecting and responding to cyber-attacks against their tenants.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph.
- Create alerts that can identify malicious or suspicious events.
- Understand how the Microsoft 365 Defender's Automated investigation and response process works.
- Describe how threat hunting enables security operators to identify cybersecurity threats.
- Describe how Advanced hunting in Microsoft 365 Defender proactively inspects events in your network to locate threat indicators and entities.

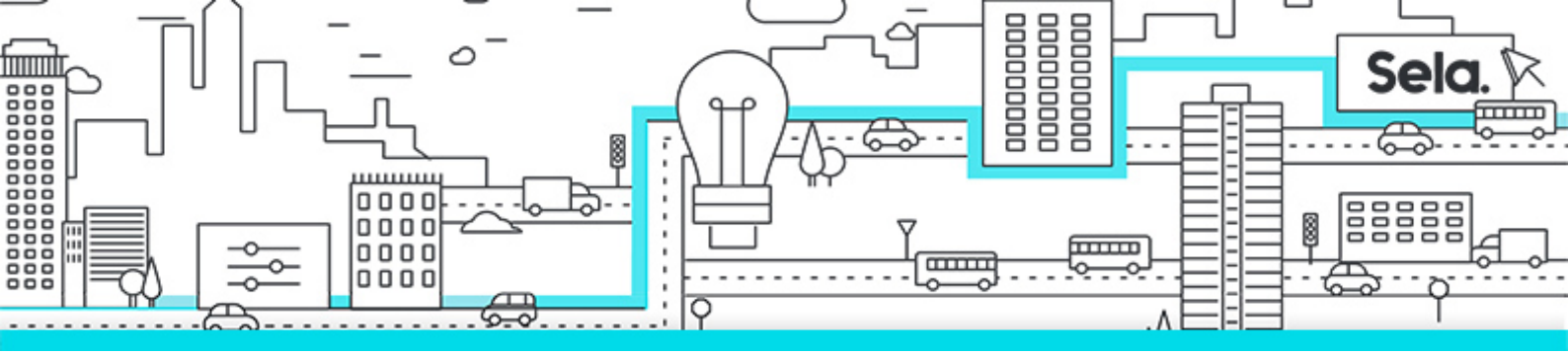
• **Implement app protection by using Microsoft Defender for Cloud Apps**
- This module examines how to implement Microsoft Defender for Cloud Apps, which identifies and combats cyberthreats across all your Microsoft and third-party cloud services.



- Learning objectives
- By the end of this module, you'll be able to:
- Describe how Microsoft Defender for Cloud Apps provides improved visibility into network cloud activity and increases the protection of critical data across cloud applications.
- Explain how to deploy Microsoft Defender for Cloud Apps.
- Control your cloud apps with file policies.
- Manage and respond to alerts that were generated by those policies.
- Configure and troubleshoot Cloud Discovery.
- his module examines how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats by using endpoint behavioral sensors, cloud security analytics, and threat intelligence.
- After completing this module, you'll be able to:
- Describe how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats.
- Onboard supported devices to Microsoft Defender for Endpoint.
- Implement the Threat and Vulnerability Management module to effectively identify, assess, and remediate endpoint weaknesses.
- Configure device discovery to help find unmanaged devices connected to your corporate network.
- Lower your organization's threat and vulnerability exposure by remediating issues based on prioritized security recommendations.

• **Implement threat protection by using Microsoft Defender for Office 365**

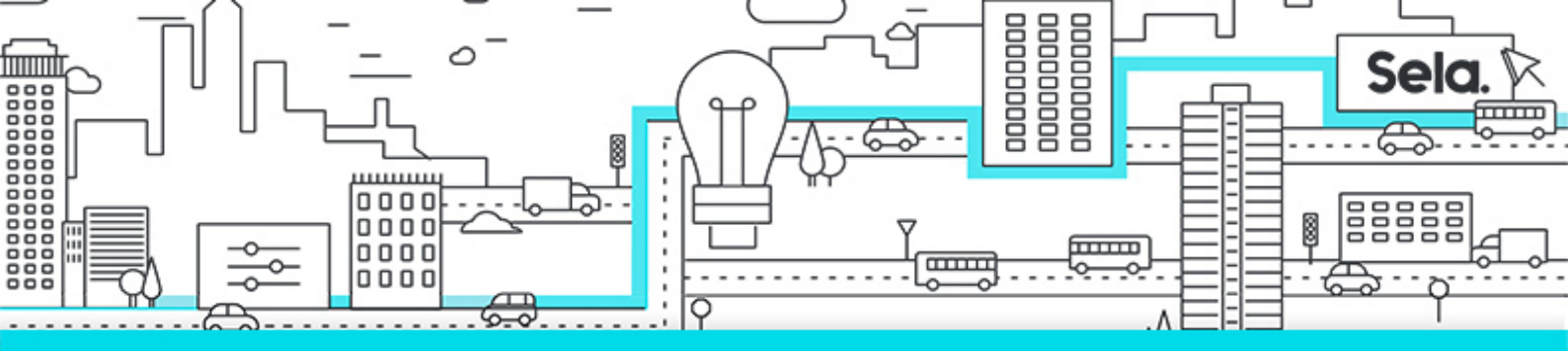
- This module examines the Microsoft Defender for Office 365 protection stack and its corresponding threat intelligence features, including Threat Explorer, Threat Trackers, and Attack simulation training.
- Learning objectives
- After completing this module, you'll be able to:
- Describe the protection stack provided by Microsoft Defender for Office 365.
- Understand how Threat Explorer can be used to investigate threats and help to protect your tenant.



- Describe the Threat Tracker widgets and views that provide you with intelligence on different cybersecurity issues that might affect your company.
- Run realistic attack scenarios using Attack Simulator to help identify vulnerable users before a real attack impacts your organization.

• **Examine governance and compliance solutions in Microsoft Purview**
- This module introduces Microsoft Purview, which is designed to meet the challenges of today's decentralized, data-rich workplace by providing a comprehensive set of solutions that help organizations govern, protect, and manage their entire data estate.
- Learning objectives
- By the end of this module, you'll be able to:
- Protect sensitive data with Microsoft Purview Information Protection.
- Govern organizational data using Microsoft Purview Data Lifecycle Management.
- Minimize internal risks with Microsoft Purview Insider Risk Management.
- Explain the Microsoft Purview eDiscovery solutions.

• **Explore archiving and records management in Microsoft 365**
- This module examines how Microsoft 365 supports data governance by enabling organizations to archive content by using archive mailboxes, and manage their high-value content for legal, business, or regulatory obligations by implementing records management.
- Learning objectives
- By the end of this module, you'll be able to:
- Enable and disable an archive mailbox in the Microsoft Purview compliance portal and through Windows PowerShell.
- Run diagnostic tests on an archive mailbox.
- Learn how retention labels can be used to allow or block actions when documents and emails are declared records.
- Create your file plan for retention and deletion settings and actions.
- Determine when items should be marked as records by importing an existing

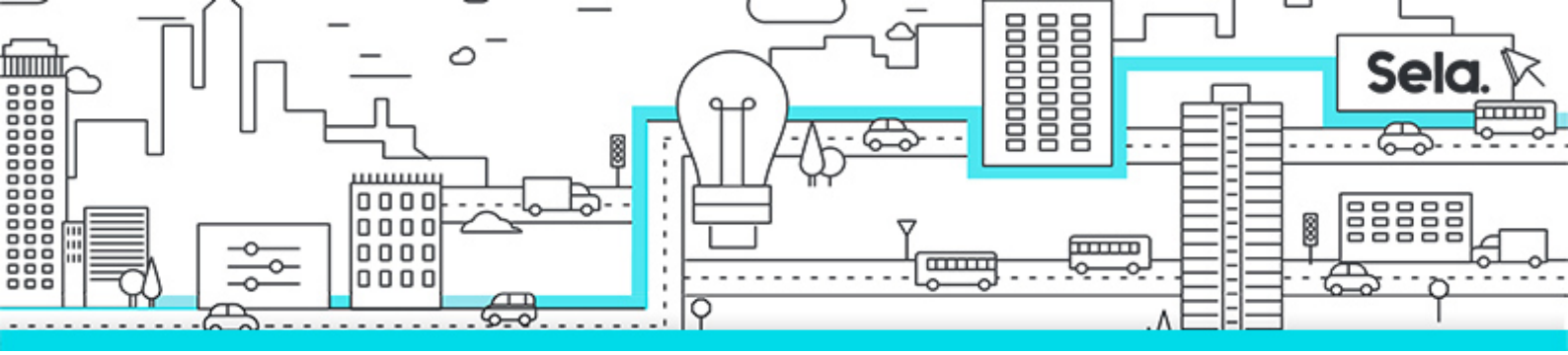


plan (if you already have one) or create new retention labels.
- Restore deleted data in Exchange Online and SharePoint Online.

• **Explore retention in Microsoft 365**
- This module examines how data can be retained and ultimately removed in Microsoft 365 by using data retention policies and data retention labels in retention policies.
- Learning objectives
- By the end of this module, you'll be able to:
- Explain how a retention policies and retention labels work.
- Identify the capabilities of both retention policies and retention labels.
- Select the appropriate scope for a policy depending on business requirements.
- Explain the principles of retention.
- Identify the differences between retention settings and eDiscovery holds.
- Restrict retention changes by using preservation lock.

• **Explore compliance in Microsoft 365**
- This module explores the tools Microsoft 365 provides to help ensure an organization's regulatory compliance, including the Microsoft Purview compliance portal, Compliance Manager, and the Microsoft compliance score.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how Microsoft 365 helps organizations manage risks, protect data, and remain compliant with regulations and standards.
- Plan your beginning compliance tasks in Microsoft Purview.
- Manage your compliance requirements with Compliance Manager.
- Manage compliance posture and improvement actions using the Compliance Manager dashboard.
- Explain how an organization's compliance score is determined.

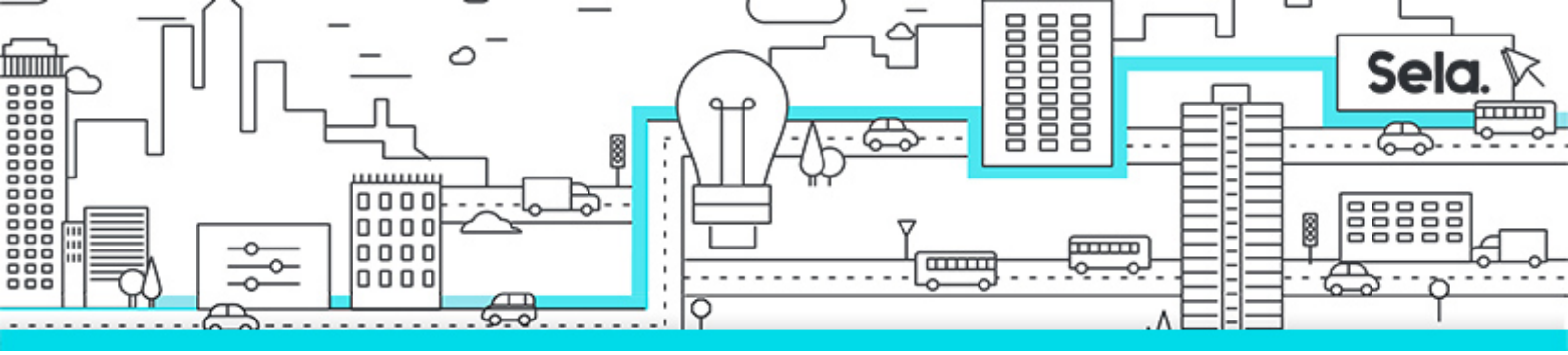
• **Implement Microsoft Purview Insider Risk Management**
- This module examines how Microsoft Purview Insider Risk Management helps



organizations minimize internal risks by enabling them to detect, investigate, and act on malicious and inadvertent activities.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe insider risk management functionality in Microsoft 365.
- Develop a plan to implement the Microsoft Purview Insider Risk Management solution.
- Create insider risk management policies.
- Manage insider risk management alerts and cases.

• **Create information barriers in Microsoft 365**
- This module examines how Microsoft 365 uses information barriers to restrict communication and collaboration in Microsoft Teams, SharePoint Online, and OneDrive for Business.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how information barriers can restrict or allow communication and collaboration among specific groups of users.
- Describe the components of an information barrier and how to enable information barriers.
- Understand how information barrier modes help strengthen who can be added or removed from a Microsoft Team, OneDrive account, and SharePoint site.
- Describe how information barriers prevent users or groups from communicating and collaborating in Microsoft Teams, OneDrive, and SharePoint.

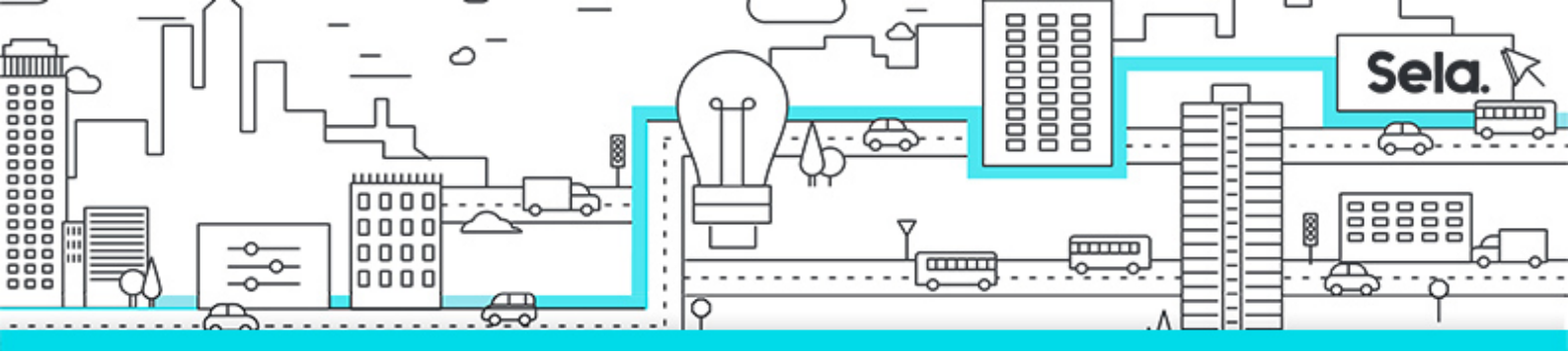
• **Implement Data Loss Prevention policies**
- Intermediate
- Administrator
- Security Engineer
- Solution Architect
- Technology Manager
- Microsoft 365



- Office 365
- This module examines how organizations can use Microsoft Purview Data Loss Prevention to help protect sensitive data and define the protective actions that organizations can take when a DLP rule is violated.
- Learning objectives
- By the end of this module, you'll be able to:
- Create a data loss prevention implementation plan. Implement Microsoft 365's default DLP policy.
- Create a custom DLP policy from a DLP template and from scratch.
- Create email notifications and policy tips for users when a DLP rule applies.
- Create policy tips for users when a DLP rule applies
- Configure email notifications for DLP policies

• **Explore Data Loss Prevention in Microsoft 365**
- This module examines the data loss prevention features in Microsoft 365 that help organizations identify, monitor, report, and protect sensitive data through deep content analysis while helping users understand and manage data risks.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how Data Loss Prevention (DLP) is managed in Microsoft 365
- Understand how DLP in Microsoft 365 uses sensitive information types and search patterns
- Describe how Microsoft Endpoint DLP extends the DLP activity monitoring and protection capabilities.
- Describe what a DLP policy is and what it contains
- View DLP policy results using both queries and reports

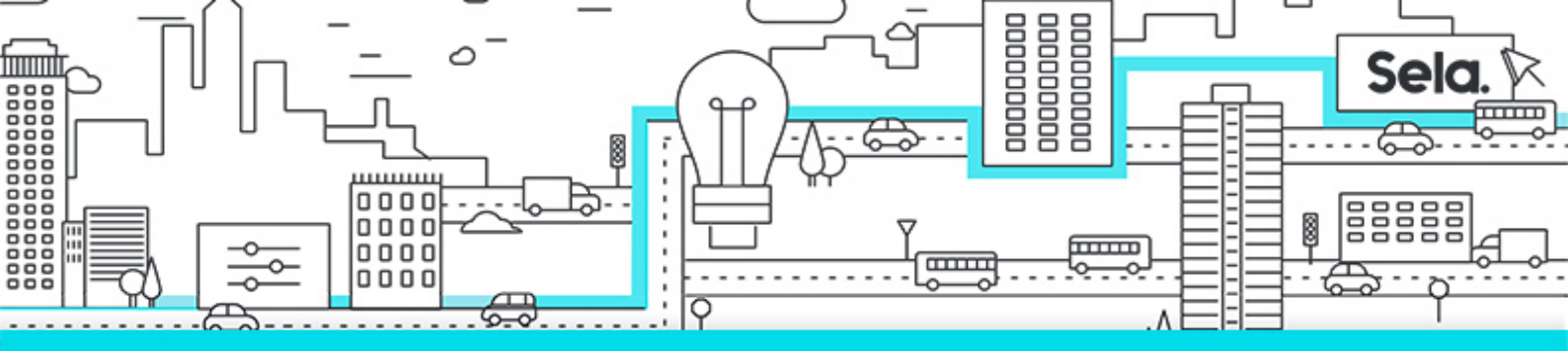
• **Implement data classification of sensitive information**
- This module introduces you to data classification in Microsoft 365, including how to create and train classifiers, view sensitive data using Content explorer and Activity explorer, and implement Document Fingerprinting.
- Learning objectives



- By the end of this module, you'll be able to:
- Explain the benefits and pain points of creating a data classification framework.
- Identify how data classification of sensitive items is handled in Microsoft 365.
- Understand how Microsoft 365 uses trainable classifiers to protect sensitive data.
- Create and then retrain custom trainable classifiers.
- Analyze the results of your data classification efforts in Content explorer and Activity explorer.
- Implement Document Fingerprinting to protect sensitive information being sent through Exchange Online.

• **Explore sensitivity labels**
- This module examines how sensitivity labels from the Microsoft Purview Information Protection solution let you classify and protect your organization's data, while making sure that user productivity and collaboration isn't hindered.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how sensitivity labels let you classify and protect your organization's data
- Identify the common reasons why organizations use sensitivity labels
- Explain what a sensitivity label is and what they can do for an organization
- Configure a sensitivity label's scope
- Explain why the order of sensitivity labels in your admin center is important
- Describe what label policies can do

• **Implement sensitivity labels**
- This module examines the process for implementing sensitivity labels, including applying proper administrative permissions, determining a deployment strategy, creating, configuring, and publishing labels, and removing and deleting labels.
- Learning objectives
- By the end of this module, you'll be able to:



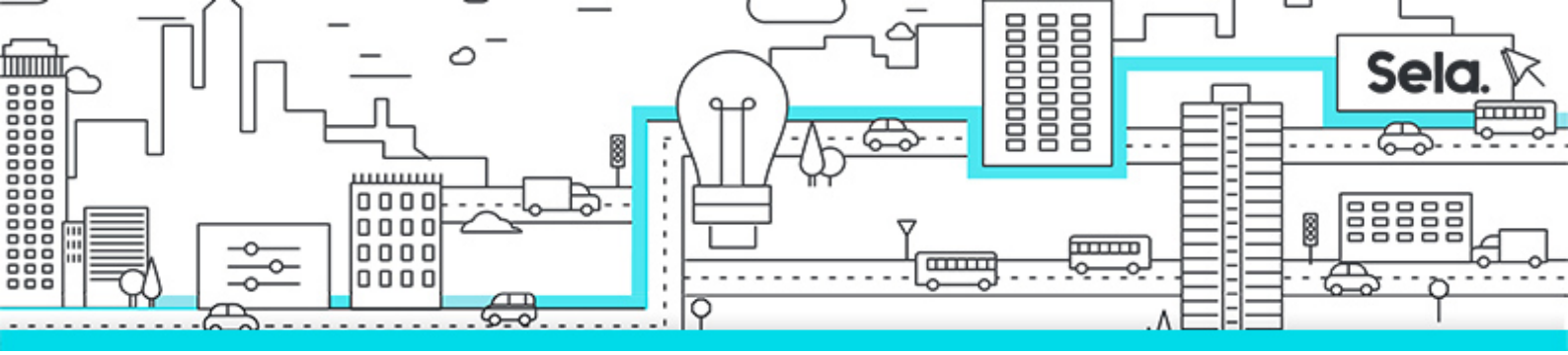
- Describe the overall process to create, configure, and publish sensitivity labels
- Identify the administrative permissions that must be assigned to compliance team members to implement sensitivity labels
- Develop a data classification framework that provides the foundation for your sensitivity labels
- Create and configure sensitivity labels
- Publish sensitivity labels by creating a label policy
- Identify the differences between removing and deleting sensitivity labels

• **Search for content in the Microsoft Purview compliance portal**

- This module examines how to search for content in the Microsoft Purview compliance portal using Content Search functionality, including how to view and export the search results, and configure search permissions filtering.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how to use content search in the Microsoft Purview compliance portal.
- Design and create a content search.
- Preview the search results.
- View the search statistics.
- Export the search results and search report.
- Configure search permission filtering.

• **Manage Microsoft Purview Audit (Standard)**

- This module examines how to search for audited activities using the Microsoft Purview Audit (Standard) solution, including how to export, configure, and view the audit log records that were retrieved from an audit log search.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe the differences between Audit (Standard) and Audit (Premium).
- Identify the core features of the Audit (Standard) solution.
- Set up and implement audit log searching using the Audit (Standard) solution.
- Export, configure, and view audit log records.



- Use audit log searching to troubleshoot common support issues.

• **Manage Microsoft Purview Audit (Premium)**

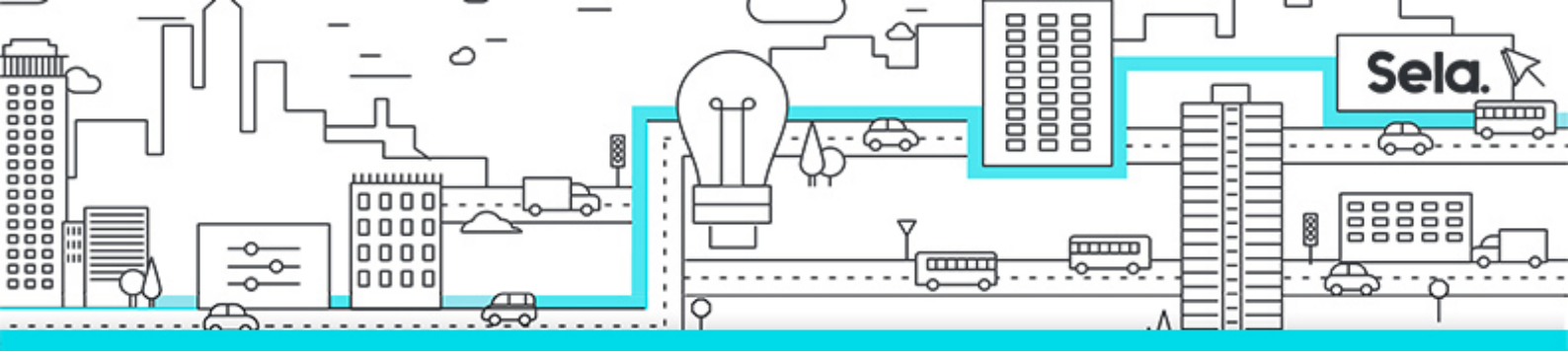
- This module explores the differences between Microsoft Purview Audit (Standard) and Audit (Premium), plus the key functionality in Audit (Premium), including setup requirements, enabling audit logging, creating audit log retention policies, and performing forensics investigations.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe the differences between Audit (Standard) and Audit (Premium).
- Set up and implement Microsoft Purview Audit (Premium).
- Create audit log retention policies.
- Perform forensic investigations of compromised user accounts.

• **Manage Microsoft Purview eDiscovery**

- This module explores how to use Microsoft Purview eDiscovery (Standard) to create an eDiscovery case and a hold for a case, how to manage case content, and how to close, reopen, and delete a case.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how Microsoft Purview eDiscovery (Standard) builds on the basic search and export functionality of Content search.
- Describe the basic workflow of eDiscovery (Standard).
- Create an eDiscovery case.
- Create an eDiscovery hold for an eDiscovery case.
- Search for content in a case and then export that content.
- Close, reopen, and delete a case.

• **Manage Microsoft Purview eDiscovery (Premium)**

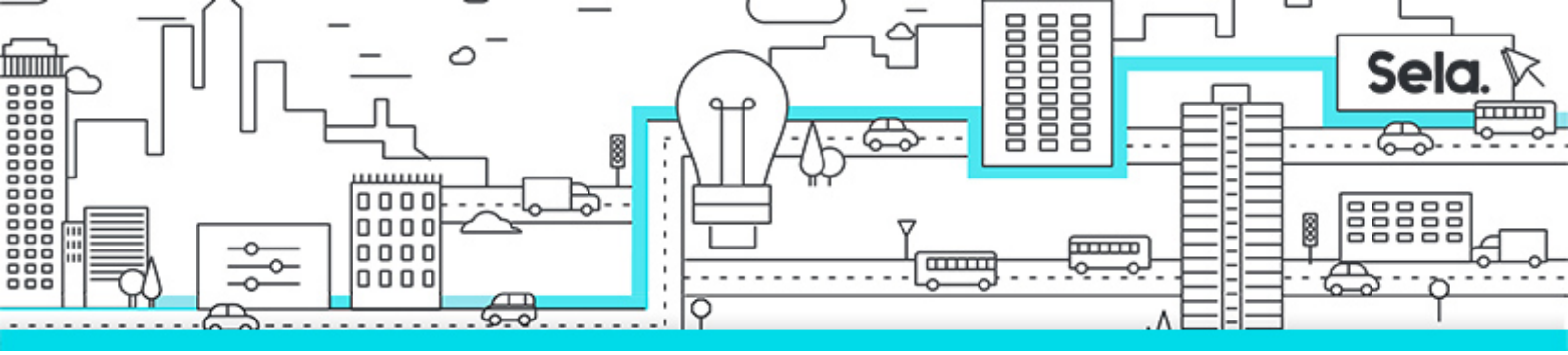
- This module explores how to use Microsoft Purview eDiscovery (Premium) to preserve, collect, analyze, review, and export content that's responsive to an organization's internal and external investigations, and communicate with



custodians involved in a case.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how Microsoft Purview eDiscovery (Premium) builds on eDiscovery (Standard).
- Describe the basic workflow of eDiscovery (Premium).
- Create and manage cases in eDiscovery (Premium).
- Manage custodians and non-custodial data sources.
- Analyze case content and use analytical tools to reduce the size of search result sets.

• **Explore device management using Microsoft Endpoint Manager**
- This module explores the device management features of Microsoft Endpoint Manager, including Microsoft Intune, Configuration Manager, device co-management, and configuration profiles for devices using Intune.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe the device management capabilities found in Microsoft Endpoint Manager.
- Describe how Windows devices can be co-managed in Endpoint Manager using Configuration Manager and Intune.
- Manage devices using Configuration Manager.
- Manage devices using Microsoft Intune.
- Create device profiles in Microsoft Intune.

• **Prepare your Windows devices for Co-management**
- This module examines the steps involved in preparing your existing environment for Co-management, from reviewing Co-management prerequisites to configuring Configuration Manager for Co-management to enrolling Windows 10 devices to Intune.
- Learning objectives
- By the end of this module, you'll be able to:



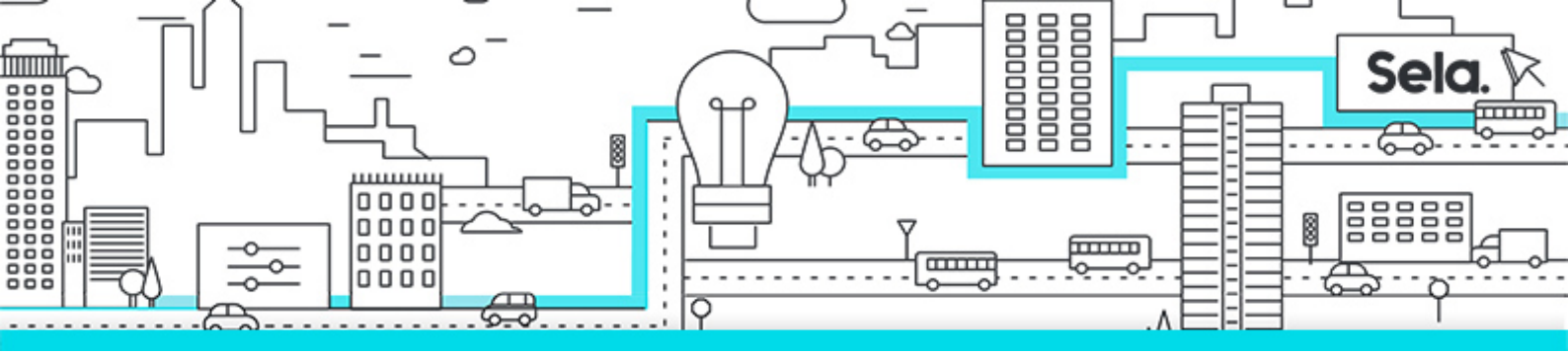
- Describe the prerequisites for using Co-management
- Configure Microsoft Endpoint Configuration Manager for Co-management
- Enroll Windows 10 Devices to Intune

• **Plan for mobile application management in Microsoft Intune**

- This module examines how to plan for mobile application management using Microsoft Intune, with a focus on adding apps to Intune, using app protection policies and app configuration policies, and troubleshooting app protection policy deployment.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe the basic functionality of mobile application management in Microsoft Intune.
- Assess your app requirements and add apps into Intune.
- Protect company data by using app protection policies.
- Implement app configuration policies in Intune to eliminate app setup problems.
- Troubleshoot app protection policy deployment in Intune.

• **Examine Windows client deployment scenarios**

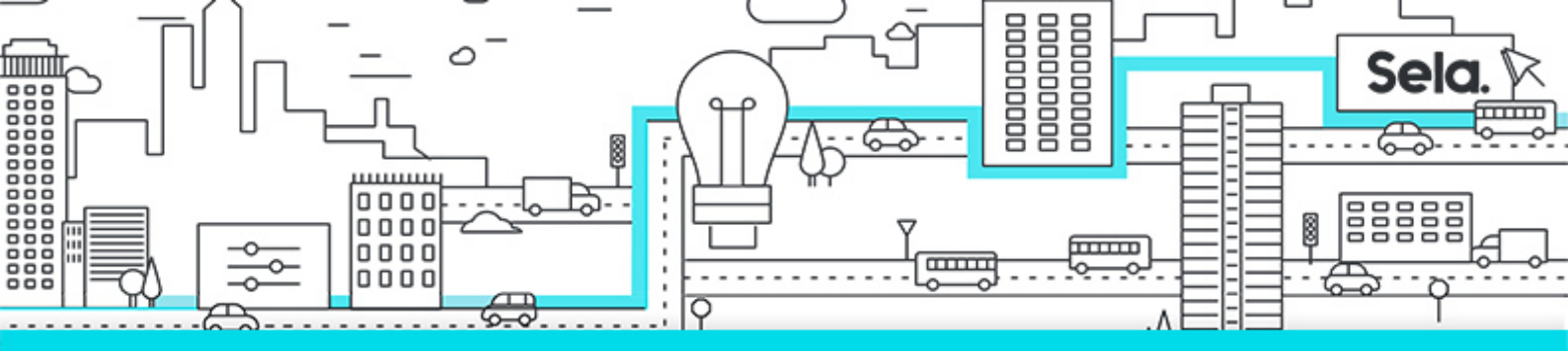
- This module examines the servicing model for Windows as a Service, how to plan for it in your organization, and the Windows 10/11 deployment models, including the modern, dynamic, and traditional deployment methods.
- Learning objectives
- By the end of this module, you'll be able to:
- Explain how the Windows as a Service model continually provides new capabilities and updates while maintaining a high level of hardware and software compatibility.
- Explain how the modern Windows 10/11 deployment model combines both traditional on-premises and cloud services to deliver a streamlined, cost-effective deployment experience.
- Explain how the dynamic Windows 10/11 deployment model can transform the



existing version of Windows 10/11 that's included on a device to a customized version that's used in your company without reinstalling Windows.
- Explain how the traditional Windows 10/11 deployment model is image-based and uses an organization’s on-premises infrastructure.

• **Explore Windows Autopilot deployment models**
- This module examines the Windows Autopilot deployment models and how they enable you to deploy new devices without the need to build, maintain, and apply custom operating system images to the devices.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe the Windows Autopilot deployment requirements.
- Create and assign a Windows Autopilot profile.
- Explain how the Autopilot self-deployment model deploys Windows 10 and 11 with little or no user interaction.
- Explain how the Autopilot pre-provisioned deployment model enables end users to provision new devices by using the preinstalled OEM image and drivers.
- Explain how the Autopilot user-driven deployment model enables new Windows 10 and 11 devices to be transformed from their initial factory state without requiring IT personnel to ever touch the device.
- Deploy BitLocker encryption for Autopiloted devices.

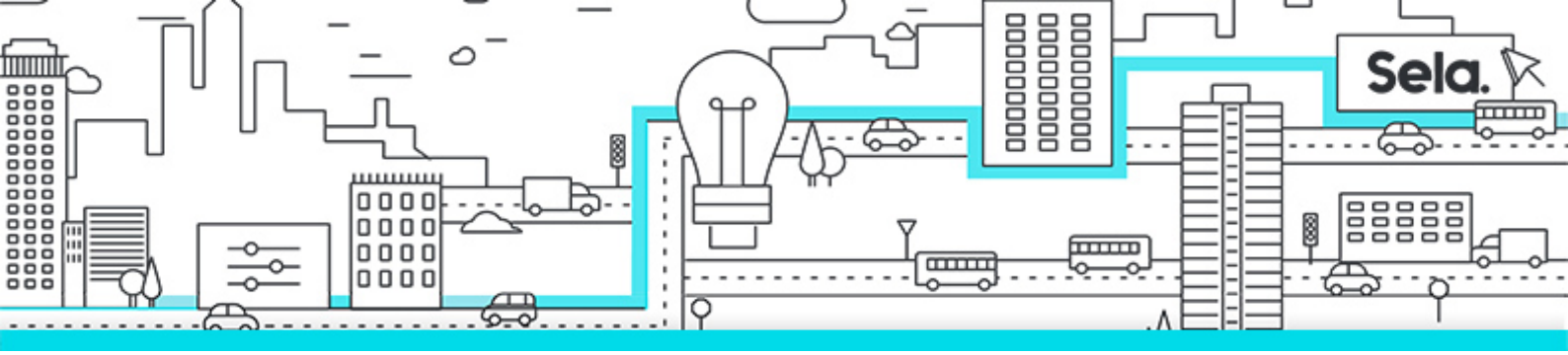
• **Plan your Windows client Subscription Activation strategy**
- This module examines how Windows 10/11 Subscription Activation enables a seamless online upgrade from Windows 10/11 Pro to Windows 10/11 Enterprise, how it provides for automatic subscription activation, and how enterprise licenses can be deployed.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how Windows 10/11 Enterprise E3 subscriptions can be purchased through the Cloud Service Provider channel.
- Configure Virtual Desktop Access for automatic subscription activation on



virtual machines.
- Explain how Windows 10/11 Enterprise licenses can be deployed automatically and without device restart.

• **Explore Mobile Device Management**
- This module examines the built-in capabilities of Mobile Device Management in Microsoft 365, including a comparison of Microsoft's two MDM solutions, policy settings for mobile devices, and controlling email and document access.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe the two MDM authority solutions included in Microsoft 365 - Microsoft Intune and Basic Mobility and Security
- Compare the basic features in Microsoft Intune and Basic Mobility and Security
- Describe the policy settings for mobile devices in Microsoft Intune and Basic Mobility and Security
- Explain how email and document access are controlled on devices managed by MDM

• **Deploy Mobile Device Management**
- This module examines how to deploy Mobile Device Management in Microsoft 365, including activating MDM services, configuring MDM policies, enrolling devices, adding client DNS records, and obtaining an APNS certificate for iOS devices.
- Learning objectives
- By the end of this module, you'll be able to:
- Activate and deploy Mobile Device Management services in Microsoft 365
- Configure domains for MDM by adding DNS records for clients to use Autodiscover when enrolling devices
- Obtain an APNS certificate to enroll and manage iOS devices
- Manage device security policies that can control password settings, encryption settings, and settings that control the use of device features
- Define a corporate device enrollment policy that can limit enrollment and



enable multi-factor authentication

• **Enroll devices to Mobile Device Management**

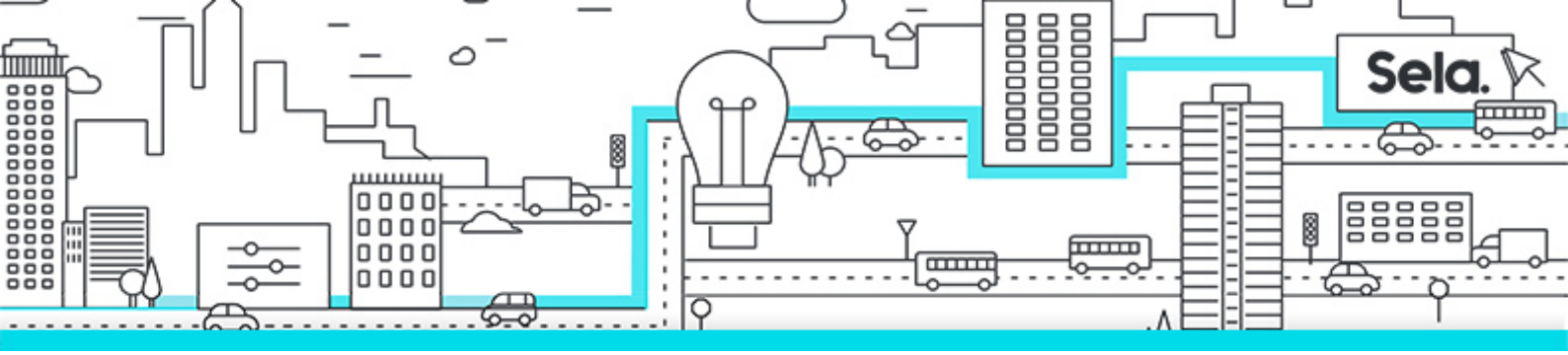
- This module examines device enrollment to MDM, including device enrollment methods, Azure AD joined devices, hybrid Azure AD joined devices, device enrollment methods in Intune, and enrollment for Windows devices.
- Learning objectives
- By the end of this module, you'll be able to:
- Enroll devices to mobile device management in Microsoft Intune.
- Explore the use of Azure AD joined and hybrid Azure AD joined devices.
- Explain how users can enroll their personal devices.
- Describe best practices and capabilities for each device enrollment method.
- Set up enrollment for Windows devices.

• **Manage device compliance**

- This module examines device compliance policies, how organizations effectively use them, how to create policies and configure conditional users and groups, how to build Conditional Access policies, and how to monitor enrolled devices.
- Learning objectives
- By the end of this module, you'll be able to:
- Plan for device compliance by defining the rules and settings that must be configured on a device for it to be considered compliant
- Configure conditional users and groups for deploying profiles, policies, and apps
- Create Conditional Access policies to implement automated access control decisions for accessing your cloud apps
- Monitor enrolled devices to control their Intune activities and compliance status

• **Implement endpoint security in Microsoft Intune**

- This module explores how organizations use Microsoft Intune to implement endpoint security, including the use of device configuration and device



compliance policies, device management, security baselines, and attack surface reduction rules.

- Learning objectives
- By the end of this module, you'll be able to:
- Describe how Microsoft Intune enables organizations to protect their data and devices.
- Understand how endpoint security in Microsoft Intune focuses on device security and risk mitigation.
- Manage devices with endpoint security in Intune.
- Use security baselines to configure Windows devices in Intune.
- Implement attack surface reduction rules to reduce an organization's attack surface.