| | |
|---|---|
| **Mögliche Trainingslösung:** | SALTZ-Seminar |
| **Seminarsprache:** | Englisch |
| **Dauer** | 5 Tage |

## Übersicht

Dieser Kurs behandelt drei zentrale Elemente der Microsoft 365-Unternehmensverwaltung - Microsoft 365-Sicherheitsverwaltung, Microsoft 365-Konformitäts-Verwaltung und Microsoft 365-Geräteverwaltung. Im Microsoft 365-Sicherheitsmanagement untersuchen Sie alle gängigen Arten von Bedrohungsvektoren und Datenverstößen, mit denen Unternehmen heute konfrontiert sind, und Sie erfahren, wie die Sicherheitslösungen von Microsoft 365 diese Sicherheitsbedrohungen angehen.
Sie werden mit dem Microsoft Secure Score sowie mit dem Azure Active Directory Identitätsschutz vertraut gemacht. Anschließend erfahren Sie, wie Sie die Sicherheitsdienste von Microsoft 365 verwalten können, einschließlich Exchange Online Protection, Advanced Threat Protection, Safe Attachments und Safe Links.
Schließlich werden Sie mit den verschiedenen Berichten zur Überwachung Ihrer Sicherheit vertraut gemacht. Anschließend werden Sie von den Sicherheitsdiensten zu den Bedrohungsinformationen übergehen; insbesondere werden Sie das Sicherheits-Dashboard und die erweiterte Bedrohungsanalyse verwenden, um potenziellen Sicherheitsverletzungen einen Schritt voraus zu sein.

Da Ihre Microsoft 365-Sicherheitskomponenten nun fest installiert sind, werden Sie die Schlüsselkomponenten des Microsoft 365-Konformitäts-Managements untersuchen. Dies beginnt mit einem Überblick über alle Schlüsselaspekte der Datenverwaltung, einschließlich Datenarchivierung und -aufbewahrung, Verwaltung von Informationsrechten, Secure Multipurpose Internet Mail Extension (S/MIME), Office 365-Nachrichtenverschlüsselung und Data Loss Prevention (DLP).

Anschließend werden Sie sich eingehender mit der Archivierung und Aufbewahrung befassen, wobei Sie sich insbesondere mit dem in -place Records Management in SharePoint, der Archivierung und Aufbewahrung in Exchange und den Aufbewahrungsrichtlinien im Sicherheits- und Konformitäts- Center befassen. Nachdem Sie nun die Schlüsselaspekte der Data Governance verstanden haben, werden Sie untersuchen, wie diese umgesetzt werden können, einschließlich des Aufbaus von ethischen Mauern in Exchange Online, der Erstellung von DLP-Richtlinien aus eingebauten Vorlagen, der Erstellung von benutzerdefinierten DLP-Richtlinien, der Erstellung von DLP-Richtlinien zum Schutz von Dokumenten und der Erstellung von Richtlinientipps.

Anschließend konzentrieren Sie sich auf die Verwaltung der Data Governance in Microsoft 365, einschließlich der Verwaltung der Datenaufbewahrung in E-Mails, der Fehlerbehebung bei Aufbewahrungsrichtlinien und Richtlinientipps, die fehlschlagen, sowie der Fehlerbehebung bei sensiblen Daten.

Anschließend lernen Sie, wie Sie Azure Information Protection und Windows Information Protection einrichten. Sie werden diesen Abschnitt abschließen, indem Sie lernen, wie Sie die Suche und Untersuchung verwalten, einschließlich der Suche nach Inhalten im Sicherheits- und Konformitäts-Center, der Prüfung von Protokolluntersuchungen und der Verwaltung der erweiterten eDiscovery.Der Kurs schließt mit einer eingehenden Prüfung der Verwaltung von Microsoft 365-Geräten ab.
Sie beginnen mit der Planung verschiedener Aspekte der Geräteverwaltung, einschließlich der Vorbereitung Ihrer Windows 10-Geräte für die gemeinsame Verwaltung. Sie lernen den Übergang vom Configuration Manager zu Intune und werden in den Microsoft Store for Business and Mobile Application Management eingeführt.
An diesem Punkt werden Sie von der Planung zur Einrichtung des Gerätemanagements übergehen, insbesondere zu Ihrer Windows 10-Bereitstellungsstrategie. Dazu gehört das Erlernen der Einrichtung von Windows Autopilot, Windows Analytics und Mobile Device Management (MDM). Bei der Untersuchung von MDM werden Sie lernen, wie man es einsetzt, wie man Geräte für MDM anmeldet und wie man die Konformität der Geräte verwaltet

## Voraussetzungen

- Abschluss eines rollenbasierten Administratorkurses wie z.B. Nachrichtenvermittlung, Teamwork, Sicherheit und Compliance oder Zusammenarbeit.
- Ein fundiertes Verständnis von DNS und grundlegenden Funktionserfahrungen mit Microsoft 365-Diensten.
- Ein fundiertes Verständnis allgemeiner IT-Praktiken.

## Zielgruppe

Dieser Kurs richtet sich an Personen, die die Microsoft 365 Enterprise-Administratorrolle anstreben und einen der Microsoft 365-Zertifizierungspfade für rollenbasierte Administratoren abgeschlossen haben.

## Erworbene Qualifikationen

- Microsoft 365 Security Metrics
- Microsoft 365 Security Services
- Microsoft 365 Threat Intelligence
- Datenverwaltung in Microsoft 365
- Archivierung und Aufbewahrung im Office 365
- Datenverwaltung in Microsoft 365 Intelligence
- Suche und Ermittlungen
- Geräteverwaltung
- Windows 10-Bereitstellungsstrategien
- Verwaltung mobiler Geräte

## Agenda

**Modul 1: Einführung in die Microsoft 365 Sicherheitsmetriken**

In diesem Modul untersuchen Sie alle gängigen Arten von Bedrohungsvektoren und Datenverletzungen, mit denen Unternehmen heute konfrontiert sind, und erfahren, wie die Sicherheitslösungen von Microsoft 365 diese Sicherheitsbedrohungen angehen, einschließlich des Zero Trust-Ansatzes. Sie werden in den Microsoft Secure Score, das Privileged Identity Management sowie in den Azure Active Directory-Identitätsschutz eingeführt.

**Lektionen**

- Bedrohungsvektoren und Datenverletzungen
- Das Zero Trust-Modell
- Sicherheitslösungen in Microsoft 365
- Einführung in Microsoft Secure Score
- Privilegierte Identitätsverwaltung
- Einführung in Azure Active Directory Identity Protection

- **Lab: Einrichten eines Mandanten und PIM**
- Initialisieren Sie Ihren Microsoft 365-Mandanten
- PIM-Ressourcen-Workflows

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Beschreiben Sie verschiedene Techniken, die Hacker anwenden, um Benutzerkonten per E-Mail zu gefährden
- Beschreiben Sie Techniken, mit denen Hacker die Kontrolle über Ressourcen erlangen
- Beschreiben Sie Techniken, mit denen Hacker Daten kompromittieren
- Beschreiben Sie den Zero Trust-Sicherheitsansatz in Microsoft 365.
- Beschreiben Sie die Komponenten der Zero Trust-Sicherheit.
- Beschreiben und fünf Schritte zum Implementieren eines Zero Trust-Modells in Ihrer Organisation.
- Erläutern Sie das Zero Trust-Netzwerk

- Die Arten von Bedrohungen auflisten, die mit EOP und Office 365 ATP vermieden werden können.
- Beschreiben Sie, wie Microsoft 365 Threat Intelligence Ihrem Unternehmen zugute kommen kann
- Überwachen Sie Ihre Organisation durch Audits und Warnungen
- Beschreiben Sie, wie ASM die Sichtbarkeit und Kontrolle Ihres Mandanten in drei Kernbereichen verbessert
- Die Vorteile von Secure Score beschreiben und welche Arten von Diensten analysiert werden können.
- Beschreiben Sie, wie Daten mit Hilfe der Secure Score-API erfasst werden
- Wissen, wo Sie Maßnahmen identifizieren können, die Ihre Sicherheit erhöhen, indem Sie Risiken minimieren
- Erklären Sie, wie Sie die Bedrohungen ermitteln, die durch jede Aktion gemindert werden und welche Auswirkungen sie auf die Verwendung hat
- Erläutern Sie PIM (Privileged Identity Management) in der Azure-Verwaltung
- Konfigurieren Sie PIM für die Verwendung in Ihrer Organisation
- PIM-Rollen prüfen
- Erläutern Sie Microsoft Identity Manager
- Erläutern Sie die Verwaltung privilegierter Zugriffe in Microsoft 365
- Beschreiben Sie Azure-Identitätsschutz und die Art der Identitäten, die geschützt werden können
- Erfahren Sie, wie Sie den Azure-Identitätsschutz aktivieren
- Wissen, wie man Schwachstellen und Risikoereignisse identifiziert
- Planen Sie Ihre Untersuchung zum Schutz von Cloud-basierten Identitäten
- Planen Sie, wie Sie Ihre Azure Active Directory-Umgebung vor Sicherheitsverletzungen schützen können

**Modul 2: Verwaltung Ihrer Microsoft 365 Sicherheitsdienste**

In diesem Modul wird die Verwaltung der Microsoft 365-Sicherheitsdienste untersucht, einschließlich Exchange Online Protection, Advanced Threat Protection, Safe Attachments und Safe Links. Sie werden mit den verschiedenen Berichten zur Überwachung Ihrer Sicherheit vertraut gemacht.

**Lektionen**

- Einführung in den Exchange Online Protection
- Einführung in Advanced Threat Protection
- Verwalten sicherer Anhänge
- Verwalten sicherer Links
- Monitoring und Berichte

- **Labor : Microsoft 365 Security Services verwalten**
- Implementieren Sie eine Richtlinie für sichere Anhänge
- Implementieren Sie eine Safe Links-Richtlinie

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Die Anti-Malware-Pipeline beschreiben, während E-Mails von Exchange Online Protection analysiert werden.
- Nennen Sie verschiedene Mechanismen zum Filtern von Spam und Malware
- Beschreiben Sie zusätzliche Lösungen zum Schutz vor Phishing und Spoofing
- Beschreiben Sie die Vorteile der Spoof Intelligence-Funktion
- Beschreiben, wie sichere Anhänge verwendet werden, um Zero-Day-Malware in E-Mail-Anhängen und Dokumenten zu blockieren.
- Beschreiben Sie, wie sichere Links Benutzer vor schädlichen URLs schützen, die in E-Mails und Dokumente eingebettet sind
- Erstellen und ändern Sie eine Richtlinie für sichere Anhänge im Security & Compliance Center
- Erstellen Sie mit Hilfe von Windows PowerShell eine Richtlinie für sichere Anhänge
- Konfigurieren Sie eine Richtlinie für sichere Anhänge, um bestimmte Aktionen auszuführen
- Verstehen, wie eine Transportregel verwendet werden kann, um die Funktion für sichere Anhänge zu deaktivieren
- Beschreiben Sie die Endbenutzererfahrung, wenn ein E-Mail-Anhang gescannt und als bösartig eingestuft wird

- Erstellen und ändern Sie eine Richtlinie für sichere Links im Security & Compliance Center
- Erstellen Sie mit Hilfe von Windows PowerShell eine Richtlinie für sichere Links
- Verstehen, wie eine Transportregel verwendet werden kann, um die Funktion für sichere Links zu deaktivieren
- Beschreiben Sie die Endbenutzererfahrung, wenn Safe Links einen Link zu einer schädlichen Website oder Datei identifiziert
- Beschreiben Sie, wie Berichte Aufschluss darüber geben, wie EOP und ATP Ihr Unternehmen schützen
- Verstehen Sie, wo Sie auf von EOP und ATP generierte Berichte zugreifen können
- Verstehen, wie Sie auf detaillierte Informationen aus Berichten zugreifen können, die von EOP und ATP erstellt wurden

**Modul 3: Microsoft 365 Threat Intelligence**

In diesem Modul werden Sie von den Sicherheitsdiensten zu den Bedrohungsinformationen übergehen; insbesondere werden Sie das Sicherheits-Dashboard und die erweiterte Bedrohungsanalyse verwenden, um potenziellen Sicherheitsverletzungen einen Schritt voraus zu sein.

**Lektionen**

- Übersicht über Microsoft 365 Threat Intelligence
- Verwenden des Sicherheits-Dashboards
- Konfigurieren der erweiterten Bedrohungsanalyse
- Richten Sie die Sicherheit Ihrer Cloud-Anwendung ein

- **Lab: Implementieren Sie Threat Intelligence**
- Führen Sie mit dem Angriffssimulator einen Spear Phishing-Angriff durch
- Führen Sie Passwortangriffe mit dem Angriffssimulator durch
- Bereiten Sie sich auf Warnrichtlinien vor
- Implementieren Sie eine Mailbox-Berechtigungsbenachrichtigung
- Implementieren Sie einen SharePoint-Berechtigungsalarm
- Testen Sie den Standard-eDiscovery-Alert

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Verstehen Sie, wie Bedrohungsinformationen vom Microsoft Intelligent Security Graph unterstützt werden
- Beschreiben Sie, wie das Bedrohungs-Dashboard Sicherheitsbeauftragten auf C-Ebene zugute kommen kann
- Beschreiben Sie, wie man mit dem Threat Explorer Bedrohungen untersuchen und Ihren Mandanten schützen kann
- Beschreiben Sie, wie das Sicherheits-Dashboard die wichtigsten Risiken, globalen Trends und die Schutzqualität anzeigt
- Beschreiben, was die erweiterte Bedrohungsanalyse (ATA) ist und welche Anforderungen für die Bereitstellung erforderlich sind.
- Konfigurieren fortgeschrittener Bedrohungsanalysen.
- Verwalten Sie die ATA-Services
- Beschreiben der Cloud-App-Sicherheit.
- Erläutern, wie die Cloud-App-Sicherheit bereitgestellt wird.
- Kontrollieren Ihrer Cloud-Apps mit Richtlinien.
- Problembehandlung für die Cloud-App-Sicherheit

**Modul 4: Einführung in Data-Governance in Microsoft 365**

Dieses Modul untersucht die wichtigsten Komponenten des Microsoft 365 Compliance-Managements. Dies beginnt mit einem Überblick über alle Schlüsselaspekte der Datenverwaltung, einschließlich Datenarchivierung und -aufbewahrung, Verwaltung von Informationsrechten, Secure Multipurpose Internet Mail Extension (S/MIME), Office 365-Nachrichtenverschlüsselung und Data Loss Prevention (DLP).

**Lektionen**

- Einführung in die Archivierung in Microsoft 365
- Einführung in die Aufbewahrung in Microsoft 365
- Einführung in die Verwaltung von Informationsrechten
- Einführung in die sichere Mehrzweck-Internet-Mail-Erweiterung
- Einführung in die Office 365-Nachrichtenverschlüsselung
- Einführung in den Schutz vor Datenverlust

- **Lab: Implementieren Sie die Nachrichtenverschlüsselung und IRM**
- Konfigurieren Sie die Microsoft 365-Nachrichtenverschlüsselung und Verwaltung von Informationsrechten

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Grundlegendes zur Datenverwaltung in Microsoft 365
- Den Unterschied zwischen In-Place-Archivierung und Datensatzverwaltung beschreiben.
- Erläutern, wie Daten in Exchange archiviert werden.
- Vorteile von In-Place Dokumentenmanagement in SharePoint
- Erläutern Sie den Unterschied zwischen Message Records Management (MRM) in Exchange und Retention in SCC.
- Verstehen Sie, wie MRM in Exchange funktioniert
- Listen Sie die Arten von Aufbewahrungstags auf, die auf Postfächer angewendet werden können
- Verschiedene Microsoft 365-Verschlüsselungsoptionen beschreiben
- Verstehen Sie, wie IRM in Exchange verwendet werden kann
- Konfigurieren Sie den IRM-Schutz für Exchange-Mails
- Erläutern Sie, wie IRM in SharePoint verwendet werden kann
- Wenden Sie den IRM-Schutz auf SharePoint-Dokumente an
- Ermitteln Sie die Unterschiede zwischen IRM-Schutz und AIP-Klassifizierung
- Die Verwendung von S / MIME beschreiben.
- Erklären Sie, was digitale Signaturen sind
- Setzen Sie eine digitale Signatur auf eine Nachricht
- Verstehen Sie, wie die Nachrichtenverschlüsselung funktioniert
- Führen Sie die Verschlüsselung einer Nachricht durch
- Führen Sie die Entschlüsselung einer Nachricht durch
- Verstehen Sie die Zusammenarbeit von gleichzeitigem Signieren und Verschlüsselung
- Erläutern Sie, was dreifach verpackte Nachrichten sind
- Beschreiben Sie, wann Sie die Office 365-Nachrichtenverschlüsselung verwenden können
- Erläutern Sie die Funktionsweise der Office 365-Nachrichtenverschlüsselung
- Prävention von Datenverlust (DLP) beschreiben.
- Verstehen Sie, welche vertraulichen Informationen und Suchmuster DLP verwendet
- Wissen, was eine DLP-Richtlinie ist und was sie enthält
- Erkennen, wie Aktionen und Bedingungen für DLP zusammenwirken
- Drücken Sie aus, wie Aktionen Funktionen zum Senden von E-Mails zu Übereinstimmungen enthalten
- Zeigen Sie den Benutzern Richtlinientipps an, wenn eine DLP-Regel gilt
- Verwenden von Richtlinienvorlagen, um DLP-Richtlinien für häufig verwendete Informationen zu implementieren.
- Erklären Sie den Dokumentfinger
- Verstehen, wie DLP zum Schutz von Dokumenten in Windows Server FCI verwendet wird

**Modul 5: Archivierung und Aufbewahrung im Microsoft 365**

Dieses Modul befasst sich eingehender mit der Archivierung und Aufbewahrung, wobei der Verwaltung von In-Place-Datensätzen in SharePoint, der Archivierung und Aufbewahrung in Exchange sowie den Aufbewahrungsrichtlinien im Sicherheits- und Compliance-Center besondere Aufmerksamkeit gewidmet wird.

**Lektionen**

- In-Place Dokumentenverwaltung in SharePoint
- Archivierung und Aufbewahrung im Austausch
- Retentionsrichtlinien im SCC

- **Labor: Archivierung und Aufbewahrung einrichten**
- Konformität initialisieren
- Konfigurieren von Aufbewahrungstags und Richtlinien

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Verstehen Sie den Prozess der Datensatzverwaltung
- Erstellen Sie einen Dateiplan für Ihre Organisation
- Beschreiben Sie zwei Methoden zum Konvertieren aktiver Dokumente in Datensätze
- Beschreiben Sie die Vorteile von direktem Records-Management
- Konfigurieren Sie des direkten Records-Managements für Ihre Organisation
- Aktivieren und Deaktivieren der direkten Archivierung
- Erstellen nützlicher Aufbewahrungstags.
- Erstellen Sie Aufbewahrungsrichtlinien, um Aufbewahrungs-Tags zu gruppieren
- Weisen Sie Postfächern Aufbewahrungsrichtlinien zu
- Zuweisen von Berechtigungen und Skripten zum Exportieren und Importieren von Aufbewahrungs-Tags
- Exportieren Sie alle Aufbewahrungsrichtlinien und Tags aus einer Organisation
- Importieren Sie alle Aufbewahrungsrichtlinien und Tags in ein Unternehmen
- Erklären Sie, wie eine Aufbewahrungsrichtlinie funktioniert
- Erstellen Sie eine Aufbewahrungsrichtlinie
- Verwalten Sie Einstellungen für Aufbewahrungsrichtlinien

**Modul 6: Implementierung von Data-Governance in Microsoft 365 Intelligence**

In diesem Modul wird untersucht, wie die wichtigsten Aspekte der Datenverwaltung implementiert werden, einschließlich der Erstellung ethischer Wände in Exchange Online, der Erstellung von DLP-Richtlinien aus integrierten Vorlagen, der Erstellung benutzerdefinierter DLP-Richtlinien, der Erstellung von DLP-Richtlinien zum Schutz von Dokumenten sowie der Erstellung von Richtlinientipps.

**Lektionen**

- Bewertung Ihrer Compliance-Bereitschaft
- Implementierung von Compliance Center-Lösungen
- Aufbau ethischer Mauern in Exchange Online
- Erstellen einer einfachen DLP-Richtlinie aus einer integrierten Vorlage
- Erstellen einer benutzerdefinierten DLP-Richtlinie
- Erstellen einer DLP-Richtlinie zum Schutz von Dokumenten
- Arbeiten mit Richtlinientipps

- **Labor : DLP-Richtlinien implementieren**
- DLP-Richtlinien verwalten
- Testen Sie die MRM- und DLP-Richtlinien

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Beschreiben Sie das Microsoft 365 Compliance Center und den Zugriff darauf
- Beschreiben Sie den Zweck und die Funktion der Compliance-Bewertung
- Erläutern Sie die Komponenten der Ermittlung einer Compliance-Bewertung für ein Unternehmen
- Erläutern Sie, wie Bewertungen zur Formulierung von Compliance-Bewertungen verwendet werden
- Erläutern Sie, wie Microsoft 365 zur Bewältigung der globalen Datenschutzbestimmungen beiträgt
- Beschreiben Sie Insider-Risikomanagementfunktionen in Microsoft 365
- Konfigurieren Sie Richtlinien für das Insider-Risikomanagement

- Erläutern Sie die Kommunikationskonformitätsfunktionen in Microsoft 365
- Beschreiben, was eine ethische Mauer in Exchange ist und wie sie funktioniert.
- Erklären Sie, wie Sie in Exchange eine ethische Mauer erstellen
- Identifizieren Sie Best Practices für den Aufbau und die Arbeit mit ethischen Mauern in Exchange
- Grundlegendes zu verschiedenen integrierten Vorlagen für DLP-Richtlinien
- Bestimmen Sie, wie die richtigen Speicherorte für eine DLP-Richtlinie ausgewählt werden
- Konfigurieren von korrekten Regeln zum Schutz von Inhalten.
- Aktivieren und überprüfen Sie die DLP-Richtlinie fachgerecht
- Beschreiben, wie vorhandene Regeln von DLP-Richtlinien geändert werden.
- Erklären Sie, wie Sie einer DLP-Regel benutzerdefinierte Bedingungen und Aktionen hinzufügen und diese ändern können
- Beschreiben Sie, wie Benutzerbenachrichtigungen und Richtlinientipps geändert werden
- Konfigurieren einer Option zur Benutzerübersteuerung für eine DLP-Regel.
- Erläutern Sie, wie Vorfallberichte durch einen Verstoß gegen die DLP-Regel gesendet werden
- Beschreiben Sie, wie man mit verwalteten Eigenschaften für DLP-Richtlinien arbeitet
- Erläutern, wie SharePoint Online gecrawlte Eigenschaften aus Dokumenten erstellt.
- Beschreiben Sie, wie eine verwaltete Eigenschaft aus einer gecrawlten Eigenschaft in SharePoint Online erstellt wird
- Erläutern Sie, wie man eine DLP-Richtlinie mit Regeln erstellt, die für verwaltete Eigenschaften über PowerShell gilt
- Beschreiben Sie die Benutzererfahrung, wenn ein Benutzer eine E-Mail oder Website mit vertraulichen Informationen erstellt
- Erläutern Sie das Verhalten in Office-Apps, wenn ein Benutzer vertrauliche Informationen eingibt

**Modul 7: Verwalten von Data Governance in Microsoft 365**

Dieses Modul konzentriert sich auf die Verwaltung der Datenverwaltung in Microsoft 365, einschließlich der Verwaltung der Aufbewahrung in E-Mails, der Fehlerbehebung bei Aufbewahrungsrichtlinien und fehlgeschlagenen Richtlinientipps sowie der Fehlerbehebung bei vertraulichen Daten. Anschließend lernen Sie, wie Sie Azure Information Protection und Windows Information Protection einrichten.

**Lektionen**

- Verwalten der Aufbewahrung in E-Mails
- Problembehebung bei Data Governance
- Implementierung des Azure Information Protection
- Erweiterte Funktionen von AIP implementieren
- Implementieren von Windows Informationsschutz

- **Labor : AIP und WIP implementieren**
- Azure-Informationsschutz implementieren
- Implementieren von Windows Informationsschutz

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Bestimmen Sie, wann und wie Aufbewahrungs-Tags in Postfächern verwendet werden sollen
- Weisen Sie einem E-Mail-Ordner eine Aufbewahrungsrichtlinie zu
- Fügen Sie E-Mail-Nachrichten und Ordnern optionale Aufbewahrungsrichtlinien hinzu
- Entfernen Sie eine Aufbewahrungsrichtlinie aus einer E-Mail-Nachricht
- Erklären Sie, wie das Retentionsalter der Elemente berechnet wird.
- Reparieren Sie Aufbewahrungsrichtlinien, die nicht wie erwartet funktionieren
- Grundlegendes dazu, wie man systematisch Fehler beheben kann, wenn eine Aufbewahrungsrichtlinie anscheinend fehlschlägt
- Führen Sie Richtlinientests im Testmodus mit Richtlinientipps durch
- Beschreiben Sie, wie DLP-Richtlinien durch Nachrichtenverfolgung überwacht werden
- Beschreiben Sie die erforderlichen Planungsschritte für die Verwendung von AIP in Ihrem Unternehmen

- Konfigurieren und Anpassen von Beschriftungen
- Erstellen Sie Richtlinien zum Veröffentlichen von Etiketten
- Planen Sie eine Bereitstellung des Azure Information Protection-Clients
- Konfigurieren erweiterter AIP-Diensteinstellungen für Rechtsmanagementdienst (RMS) -Vorlagen.
- Automatische und empfohlene Kennzeichnung implementieren
- Aktivieren Sie die Super-User-Funktion für Verwaltungsaufgaben
- Erstellen Sie Ihren Mandantenschlüssel für die Verschlüsselung
- Stellen Sie den AIP-Scanner für die Kennzeichnung vor Ort bereit
- Planen Sie die Bereitstellung des RMS-Connectors für die Verbindung von Servern vor Ort
- Beschreiben Sie WIP und wofür es verwendet wird
- Planen Sie die Bereitstellung von WIP-Richtlinien
- Implementieren Sie WIP-Richtlinien mit Intune und SCCM
- Implementieren Sie WIP-Richtlinien in Windows-Desktop-Apps

**Modul 8: Suche und Ermittlungen verwalten**

In diesem Modul wird dieser Abschnitt zur Datenverwaltung abgeschlossen, indem untersucht wird, wie Suche und Untersuchung verwaltet wird, einschließlich der Suche nach Inhalten im Sicherheits- und Compliance-Center, der Prüfung von Protokolluntersuchungen und der Verwaltung des erweiterten eDiscovery.

**Lektionen**

- Suchen nach Inhalten im Sicherheits- und Compliance-Center
- Prüfung von Log-Untersuchungen
- Verwalten des erweiterten eDiscovery

- **Labor : Suche und Untersuchungen verwalten**
- Implementieren Sie eine Datenanfrage für eine betroffene Person
- Untersuchen Ihrer Microsoft 365-Daten

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Verwendung der Inhaltssuche beschreiben.
- Gestalten Sie Ihre Inhaltssuche Konfigurieren der Filterung der Suchberechtigung.
- Erklären Sie, wie man nach Daten von Drittanbietern sucht
- Beschreiben Sie, wann man Skripte für erweiterte Suchvorgänge verwenden sollte
- Beschreiben Sie, was Überwachungsprotokolle und Berechtigungen sind, die zum Durchsuchen des Office 365-Überwachungsprotokolls erforderlich sind
- Konfigurieren von Überwachungsrichtlinien.
- Kriterien für die Suche im Überwachungsprotokoll eingeben.
- Anzeigen, Sortieren und Filtern von Suchergebnissen
- Exportieren Sie Suchergebnisse in eine CSV-Datei
- Durchsuchen Sie das einheitliche Überwachungsprotokoll mit Windows PowerShell
- Beschreiben Sie Advanced eDiscovery
- Konfigurieren Sie Berechtigungen für Benutzer in Advanced eDiscovery
- Erstellen Sie Fälle in Advanced eDiscovery
- Suchen und Vorbereiten von Daten für Advanced eDiscovery

**Modul 9: Gerätemanagement planen**

Dieses Modul bietet eine eingehende Prüfung der Microsoft 365-Geräteverwaltung. Sie beginnen mit der Planung verschiedener Aspekte der Geräteverwaltung, einschließlich der Vorbereitung Ihrer Windows 10-Geräte für die gemeinsame Verwaltung. Sie lernen den Übergang vom Configuration Manager zu Microsoft Intune und werden in den Microsoft Store for Business and Mobile Application Management eingeführt.

**Lektionen**

- Einführung in das Co-Management
- Windows 10-Geräte für das Co-Management vorbereiten
- Übergang vom Configuration Manager zu Intune
- Einführung in Microsoft Store for Business -Verwaltung mobiler Anwendungen planen

- **Labor : Implementierung des Microsoft Store for Business**
- Microsoft Store für Unternehmen konfigurieren.
- Verwalten des Microsoft Store for Business

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Beschreiben Sie die Vorteile von Co-Management
- Planen Sie die Co-Management-Strategie Ihres Unternehmens
- Beschreiben Sie die Hauptfunktionen des Configuration-Managers
- Beschreiben Sie, wie Azure Active Directory Co-Management ermöglicht
- Identifizieren Sie die Voraussetzungen für die Verwendung von Co-Management
- Konfigurieren Sie Configuration Manager für Co-Management
- Registrieren Sie Windows 10-Geräte für Intune
- Ändern Sie Ihre Co-Management-Einstellungen
- Übertragen Sie Workloads an Intune
- Überwachen Sie Ihre Co-Management-Lösung
- Überprüfen Sie die Konformität für gemeinsam verwaltete Geräte
- Beschreiben sie die Funktionen und Vorteile des Microsoft Store for Business
- Microsoft Store für Unternehmen konfigurieren.
- Verwalten Sie die Einstellungen für den Microsoft Store for Business

**Modul 10: Planen Ihrer Windows 10-Bereitstellungsstrategie**

Dieses Modul konzentriert sich auf die Planung Ihrer Windows 10-Bereitstellungsstrategie, einschließlich der Implementierung von Windows Autopilot und Windows Analytics, sowie auf die Planung Ihres Windows 10-Abonnementaktivierungsdienstes.

**Lektionen**

- Windows 10-Bereitstellungsszenarien
- Implementierung und Verwaltung von Windows Autopilot
- Planen Ihrer Windows 10-Abonnementaktivierungsstrategie
- Windows 10-Aktualisierungsfehler beheben
- Einführung in die Windows-Analytik

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Planung für Windows as a Service
- Planen Sie eine moderne Bereitstellung
- Planen Sie eine dynamische Bereitstellung
- Planen Sie eine traditionelle Bereitstellung
- Beschreiben Sie die Windows Autopilot-Anforderungen
- Autopilot konfigurieren
- Erstellen und Zuweisen eines Autopilot-Profils
- Autopilot bereitstellen und validieren
- Beschreiben Sie Autopilot Selbst-Bereitstellungen, erstklassige Bereitstellungen und benutzergesteuerte Bereitstellungen
- Stellen Sie die BitLocker-Verschlüsselung für autopilotierte Geräte bereit
- Grundlegendes zu Windows 10 Enterprise E3 in CSP
- Konfigurieren Sie VDA für die Abonnementaktivierung

- Stellen Sie Windows 10 Enterprise-Lizenzen bereit
- Beschreiben allgemeiner Korrekturen für Windows 10-Aktualisierungsfehler
- Verwenden Sie SetupDiag
- Fehlerbehebung bei Aktualisierungsfehlern
- Beschreiben Sie die Windows-Fehlerberichterstattung
- Grundlegendes zu Aktualisierungs-Fehlercodes und das Lösungsverfahren
- Beschreiben Sie Windows Analytics
- Beschreiben Sie den Gerätezustand
- Beschreiben Sie die Aktualisierungs-Konformität
- Bestimmen Sie die Bereitschaft zur Aktualisierung

**Modul 11: Verwaltung mobiler Geräte umsetzen**

Dieses Modul konzentriert sich auf das Mobile Device Management (MDM). Sie erfahren, wie man es bereitstellt, Geräte bei MDM registriert und die Gerätekonformität verwaltet.

**Lektionen**

- Verwaltung mobiler Geräte planen
- Bereitstellen der Verwaltung mobiler Geräte
- Geräte bei MDM registrieren
- Geräte-Compliance verwalten

- **Labor : Geräte mit Intune verwalten**
- Geräteverwaltung aktivieren
- Azure AD für Intune konfigurieren
- Intune-Richtlinien erstellen
- Registrieren eines Windows 10-Geräts
- Verwalten und Überwachen eines Geräts im Intune

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Geräte mit MDM verwalten.
- MDM für Office 365 und Intune vergleichen
- Grundlegendes zu Richtlinieneinstellungen für mobile Geräte
- Steuern Sie E-Mail- und Dokumentenzugriff
- Aktivieren Sie mobile Geräteverwaltungs-Services
- Mobilgerätemanagement bereitstellen
- Domänen für MDM konfigurieren.
- Konfigurieren Sie ein APNs-Zertifikat für iOS-Geräte
- Verwalten von Gerätesicherheitsrichtlinien.
- Registrierungsrichtlinie für Unternehmensgeräte definieren
- Geräte bei MDM registrieren
- Grundlegendes zum Apple-Geräteregistrierungsprogramm
- Grundlegendes zu Registrierungsregeln
- Konfigurieren einer Manager-Rolle für die Geräteanmeldung.
- Beschreiben Sie Überlegungen zur Multi-Faktor-Authentifizierung
- Planen der Gerätekonformität
- Bedingte Benutzer und Gruppen konfigurieren.
- Richtlinien für den bedingten Zugang erstellen
- Registrierte Geräte überwachen