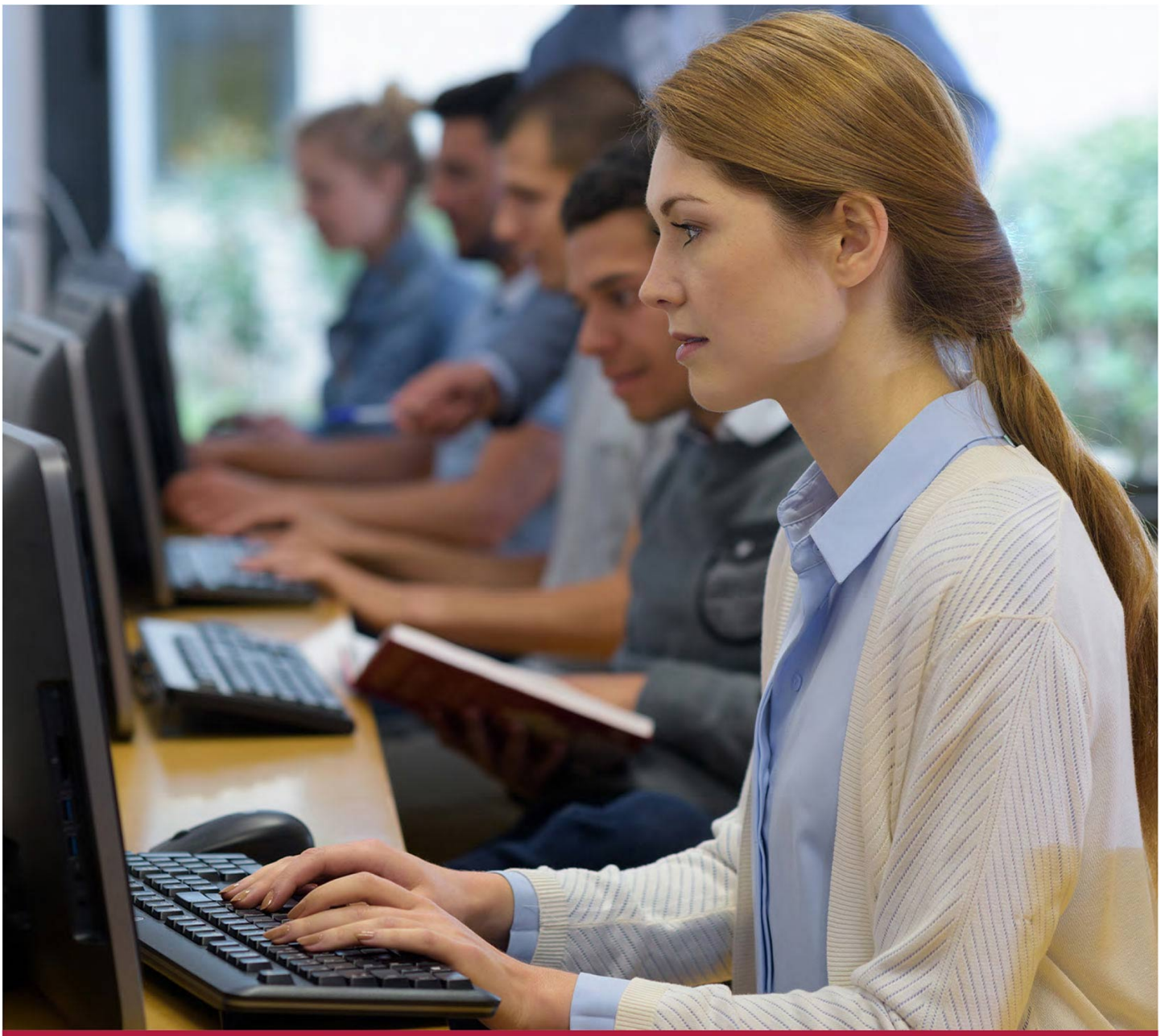
softline учебный центр



Администратор безопасности Microsoft 365

Код курса: MS-500T00

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

Администратор безопасности Microsoft 365

Код курса: MS-500T00

Длительность	32 ак. часа
Формат	Очно; Дистанционно
Разработчик курса	Microsoft
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

В данном курсе слушатели изучат способы обеспечения безопасности доступа пользователей к ресурсам организации. Курс описывает защиту паролей многофакторную аутентификацию, включение Azure Identity Protection, настройку и использование Azure AD Connect, а также знакомит слушателей с условным доступом в Microsoft 365. Слушатели изучат технологии защиты от угроз, которые помогают защищать окружения Microsoft 365. Отдельное внимание в курсе уделено векторам угроз и решениям Microsoft для устранения угроз. В рамках курса слушатели изучат оценки безопасности (Secure Score), защиту Exchange Online, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection и управление угрозами. Также в курсе изучаются технологии защиты информации, которые помогают обеспечить безопасность окружения Microsoft 365. Дополнительно курс затрагивает права управляемого контента, шифрование сообщений, а также заголовки, политики и правила, которые обеспечивают защиту от потери данных и защиту информации.

Подробная информация

Профиль аудитории:

Курс администратор безопасности Microsoft 365 будет одинаково полезен корпоративным администраторам Microsoft 365, лицам, принимающим решения, и прочим администраторам рабочих нагрузок, отвечающим за планирование и реализацию стратегий безопасности, а также обеспечивающих соответствие решений политике организации и требованиям регуляторов.

Предварительные требования:

- Понимание базовых концепций Microsoft Azure.
- Опыт работы с устройствами под управлением Windows
- Опыт работы с Office 365.
- Понимание основ аутентификации и авторизации.
- Понимание основ компьютерных сетей.
- Опыт управления мобильными устройствами.

По окончании курса слушатели смогут:

- Администрировать доступ пользователей и групп в Microsoft
- Описать и управлять возможностями Azure Identity Protection.
- Планировать и внедрять Azure AD Connect.
- Управлять синхронизированными идентификаторами.
- Описать и использовать условный доступ.
- Описать векторы угроз кибер-атак.
- Описать решения безопасности для Microsoft
- Использовать оценки безопасности Microsoft (Secure Score) для оценки состояния безопасности.
- Настраивать различные службы защиты от угроз для Microsoft
- Настраивать Advanced Thread Analytics.
- Планировать и разворачивать безопасность мобильных устройств.
- Внедрять управление правами на доступ к информации.
- Обеспечивать безопасность сообщений в Office
- Настраивать политики предотвращения потери данных (DLP).
- Разворачивать и управлять безопасность облачных приложений.
- Внедрять защиту информации Windows для устройств.
- Планировать и разворачивать систему архивации и хранения данных.
- Создавать и управлять расследованиями eDiscovery.
- Управлять запросами данных

Программа курса

Модуль 1 «Защита пользователей и групп».

- Концепции управления идентификаторами и доступом.
- Безопасность нулевого доверия (Zero Trust).
- Учетные записи в Microsoft
- Роли администратора и группы безопасности в Microsoft
- Управление паролями в Microsoft 365.
- Лабораторная работа. Инициализация пробной версии клиента.
- Лабораторная работа. Настройка управления привилегированной идентификацией.

Модуль 2 «Синхронизация идентификаторов».

- Введение в синхронизацию идентификаторов.
- Планирование Azure AD Connect.
- Применение Azure AD Connect.
- Управление синхронизированными идентификаторами.
- Введение в федеративные идентификаторы.
- Лабораторная работа. Применение синхронизации идентификаторов.

Модуль 3 «Управление доступом».

- Условный доступ.
- Управление доступом устройств.
- Управление доступом на базе ролей (RBAC).

- Решения для внешнего доступа.
- Лабораторная работа. Использование условного доступа для включения многофакторной аутентификации (MFA).

Модуль 4 «Безопасность в Microsoft 365».

- Векторы угроз и бреши данных.
- Принципы и стратегии безопасности.
- Решения безопасности в Microsoft 365.
- Оценка безопасности Microsoft (Secure Score).
- Лабораторная работа. Использование оценки безопасности Microsoft.

Модуль 5 «Продвинутая защита от угроз (ATP)».

- Защита Exchange Online.
- Продвинутая защита от угроз Office
- Управление безопасными приложениями.
- Управление безопасными ссылками.
- Azure Advanced Thread Protection.
- Microsoft Defender Advanced Thread Protection.
- Лабораторная работа. Управление службами безопасности Microsoft

Модуль 6 «Управление угрозами».

- Использование дашборда безопасности.
- Исследование и ответные действия на угрозы Microsoft
- Azure Sentinel для Microsoft
- Настройка продвинутой аналитики угроз.
- Лабораторная работа. Использование симулятора атак.

Модуль 7 «Мобильность».

- Планирование управления мобильными приложениями.
- Планирование управления мобильными устройствами (MDM).
- Развертывание управления мобильными устройствами (MDM).
- Регистрация устройств для
- Лабораторная работа. Настройка Azure AD для Intune.

Модуль 8 «Защита информации».

- Концепции защиты информации.
- Защита информации
- Продвинутая защита информации.
- Защита информации
- Лабораторная работа. Применение защиты информации Azure и защиты информации Windows.

Модуль 9 «Управление правами и шифрованием».

- Управление правами (IRM).

- Обеспечение безопасности многоцелевого расширения почты в интернете.
- Шифрование сообщений Microsoft 365.
- Лабораторная работа. Настройка шифрования сообщений Office

Модуль 10 «Защита от потери данных (DLP)».

- Описание защиты от потери данных (DLP).
- Политики защиты от потери данных (DLP).
- Настройка политик DLP.
- Создание политик DLP для защиты документов.
- Типы политик.
- Лабораторная работа. Применение политик защиты от потери данных (DLP).

Модуль 11 «Безопасность облачных приложений».

- Описание безопасности облачных приложений.
- Использование безопасности облачных приложений.

Модуль 12 «Соответствие в Microsoft 365».

- Планирование требований соответствия.
- Построение этических стен в Exchange Online.
- Управление хранением почты.
- Устранение неисправностей обслуживания данных.

Модуль 13 «Архивация и хранение».

- Архивация в Microsoft 365.
- Хранение в Microsoft 365.
- Политики хранения в центре соответствия Microsoft
- Архивация и хранение в Exchange.
- Управление записями в
- Лабораторная работа. Соответствие и хранение.

Модуль 14 «Поиск контента и исследование».

- Поиск контента.
- Исследование журнала аудита.
- Расширенный поиск
- Лабораторная работа. Управление поиском и исследованиями.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!

Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **18 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline
Вы можете узнать из профайла.