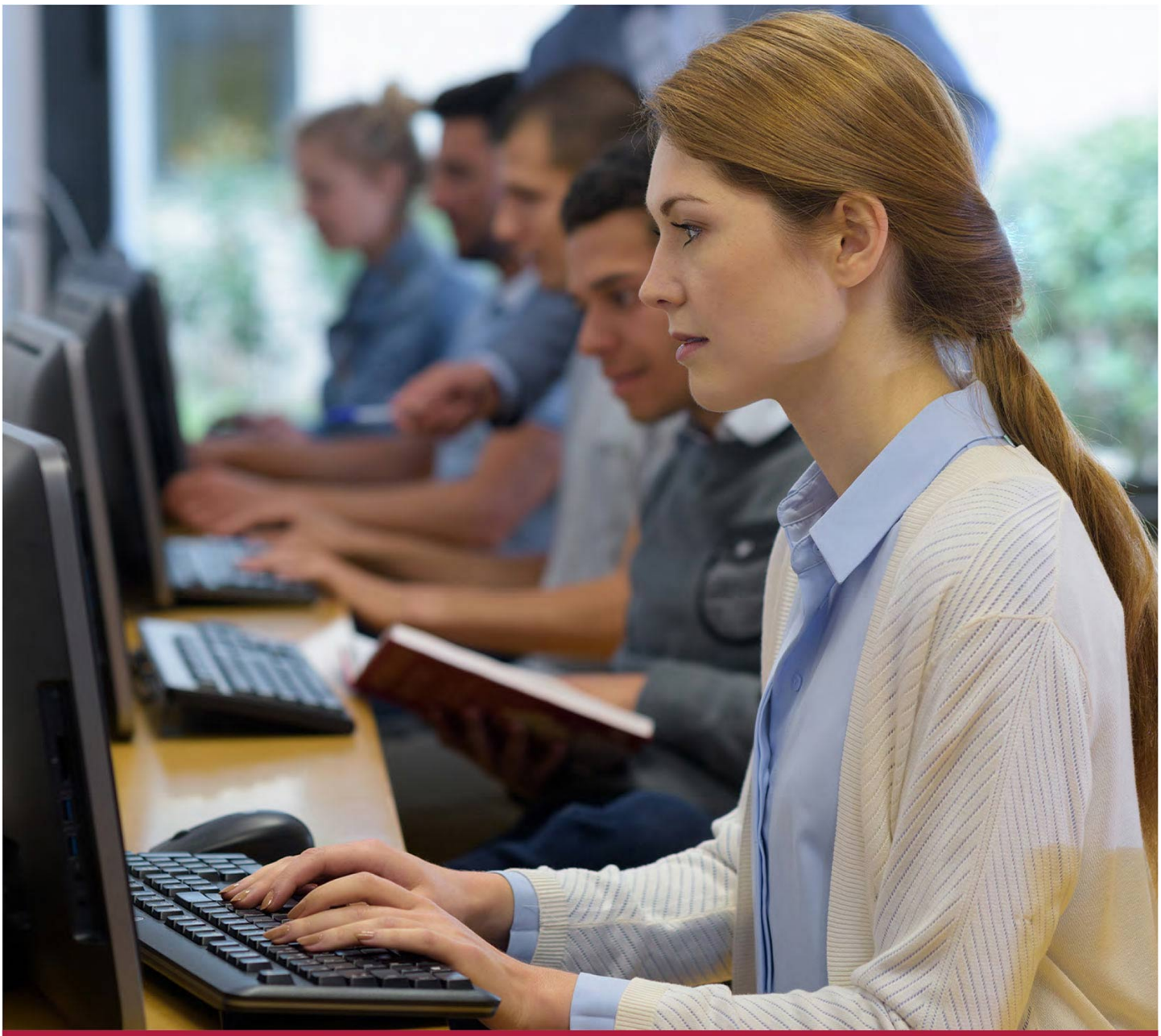
softline учебный центр



Обнаружение атак

Код курса: ИБ-01

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

Обнаружение атак

Код курса: ИБ-01

Длительность	16 ак. часов
Формат	Очно; Дистанционно
Разработчик курса	Softline
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

В двухдневном авторском курсе "Обнаружение атак" под руководством инструктора рассматриваются архитектура и принципы работы систем предотвращения, обнаружения и противодействия атакам.

Подробная информация

Профиль аудитории:

- Руководители и сотрудники служб безопасности, ответственные за обеспечение безопасности компьютерных сетей;
- Руководители и специалисты подразделений информационных технологий, автоматизации и технической защиты информации;
- Администраторы информационной безопасности;
- Аналитики по вопросам компьютерной безопасности, ответственные за анализ состояния информационной безопасности, определение требований к защищенности подсистем автоматизированных систем и путей обеспечения их защиты;
- Системные и сетевые администраторы.

Предварительные требования:

- Базовые знания по основам сетевой безопасности

По окончании курса слушатели смогут:

- Развертывать инфраструктуру обнаружения атак в корпоративной сети
- Выполнять настройку различных средств обнаружения атак
- Управлять механизмами реагирования на события безопасности
- Настраивать взаимодействие систем обнаружения атак с другими средствами защиты
- Организовывать поиск и использовать оперативную информацию о новых уязвимостях в системном и прикладном программном обеспечении

Программа курса

Модуль 1. Необходимость технологии обнаружения атак.

- Обнаружение атак как механизм защиты.

Модуль 2. Терминология.

- События безопасности и уязвимости.
- Атаки.
- Модель традиционной и распределенной атаки.
- Этапы и средства реализации атак.
- Классификация атак.
- Базы данных атак и уязвимостей.
- Инциденты.
- Архитектура системы обнаружения атак

Модуль 3. Источники данных для систем обнаружения атак.

- Принципы работы и варианты подключения сетевых систем обнаружения атак.
- Скрытый режим работы сетевой системы обнаружения атак.
- Обнаружение атак на уровне отдельного узла.
- Network Flow Data как дополнительный источник данных.

Модуль 4. Признаки атак.

- Повтор определенных событий.
- Неправильные команды.
- Использование уязвимостей.
- Несоответствующие параметры сетевого трафика.
- Несоответствие стандартам.
- Непредвиденные атрибуты.

Модуль 5. Методы обнаружения атак.

- Обнаружение аномалий и злоупотреблений.
- Анализ протоколов.
- Построение профиля поведения.

Модуль 6. Механизмы реагирования.

- Варианты оповещений.
- Регистрация.
- Блокировка.
- Особенности использования систем противодействия атакам.

Модуль 7. Специализированные системы обнаружения атак.

- Особенности защиты беспроводных сетей.
- Защита от атак на СУБД и Web-приложения.

Модуль 8. Особенности защиты беспроводных сетей.

- Защита от атак на СУБД и Web-приложения.
- Обнаружение атак и другие защитные механизмы.
- Корреляция.

Модуль 9. Анализ результатов работы систем обнаружения атак.

- Управление инцидентами.

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.