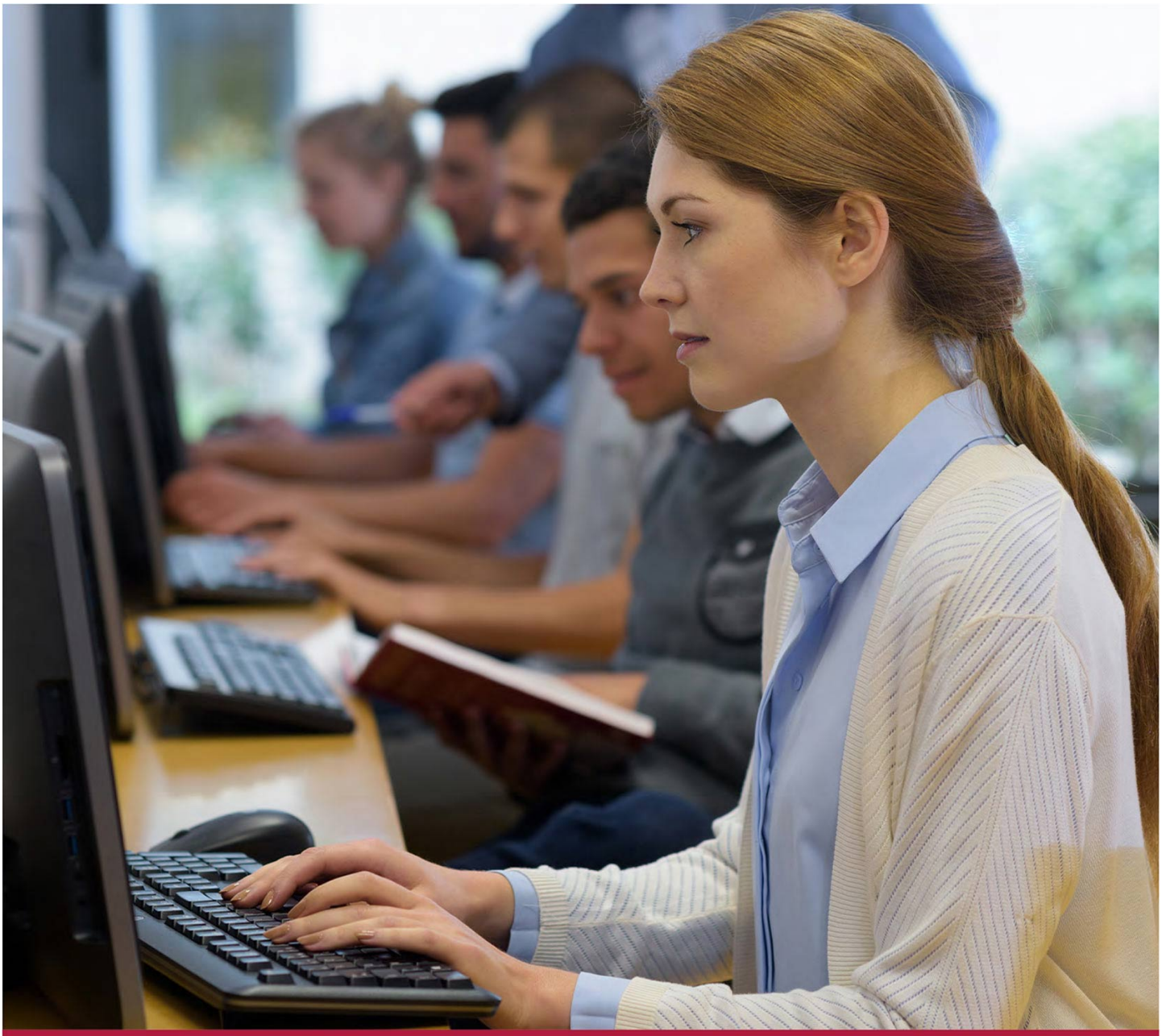
softline®

Учебный центр Softline



Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы (закрытый контур)

Код курса: Inf-01

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

Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы (закрытый контур)

Код курса: Inf-01

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

О курсе

Целью курса является изучение теоретических и практических аспектов сбора требований при организации корпоративной защиты от внутренних угроз информационной безопасности, правовых и организационных аспектов легитимизации использования автоматизированных систем по контролю информационных потоков (DLP систем), а также получение профессиональных компетенций в области последующей настройки и работы с DLP системой.

Подробная информация

Профиль аудитории:

Желающие получить профессиональные компетенции в области настройки и работы с DLP системой.

Предварительные требования:

Обязательно наличие знаний и практических навыков на уровне администратора либо продвинутого пользователя:

- владение инструментами управления файлами, директориями, процессами из командной строки ОС Linux;
- умение конфигурировать СХД (разделы и логические тома) в ОС Linux;
- навыки конфигурирования файловых систем, файловых атрибутов в ОС Linux;
- знание семиуровневой модели OSI, правил построения сетей, принципов маршрутизации;
- навыки управления статическими маршрутам (Static Routes), NAT в ОС Linux;
- опыт написания shell-скриптов для задач системного администрирования, а также умение разбираться в скриптах, написанных другими пользователями;
- опыт настройки системных логов, включая удалённое логирование;
- понимание принципов и режимов работы SMTP-relay и HTTP-proxy;
- опыт настройки и понимание принципов работы HTTP-proxy SQUID, SSL-Bump, ICAP;
- опыт настройки сервисов POSTFIX, NTP, SSH;
- опыт написания DDL и DML запросов к PostgreSQL и Oracle DB;

- опыт администрирования PostgreSQL и Oracle DB через CLI;
- опыт создания резервной копии БД;
- опыт восстановления резервной копии БД;
- опыт управления сервисами Microsoft Active Directory;
- опыт выявления и исправления проблем с DNS, DHCP;
- опыт управления учётными записями пользователей в домене;
- опыт настройки и администрирования Объектов Групповых Политик (GPO);
- опыт установки и диагностирования проблем распространения ПО через GPO.

Желательно наличие сертификатов:

- Red Hat® Certified System Administrator (RHCSA®) и выше или LPIC-101 и выше;
- Oracle Certified Associate и выше;
- MCSA или MCSE по Windows Server 2012 или 2016;
- Администратор PostgreSQL;
- Postgres Plus Associate Certification и выше;
- MCSA Windows 10.

По окончании курса слушатели будут:

уметь:

- владеть комплексом типовых технических мероприятий по конфигурированию и обслуживанию InfoWatch Traffic Monitor и его модулей;
- реализовывать последовательность действий и мероприятий по анализу бизнес процессов и созданию концепции настройки DLP системы;

знать:

- теоретические аспекты и практическую реализацию последовательности действий и мероприятий по обеспечению защиты хозяйствующего субъекта от внутренних угроз информационной безопасности;
- правовые и организационные аспекты легитимизации использования DLP систем;
- особенности аналитической поддержки организации корпоративной защиты от внутренних угроз информационной безопасности на примере нефтяной, банковской, страховой, строительной, телекоммуникационной, фармакологической отраслей, а также розничных продаж;
- этапы установки InfoWatch Traffic Monitor и его модулей.

Программа курса

Модуль 1. Развертывание InfoWatch Traffic Monitor

Спецификация оборудования, необходимого для развертывания системы. Способы установки InfoWatch Traffic Monitor. Поэтапная установка InfoWatch Traffic Monitor. Техническая архитектура InfoWatch Traffic Monitor. Первоначальная настройка InfoWatch Traffic Monitor.

Модуль 2. Развертывание InfoWatch Device Monitor

Поэтапная установка InfoWatch Device Monitor из дистрибутива. Первоначальная настройка InfoWatch Device Monitor. Установка агента InfoWatch Device Monitor.

Модуль 3. Типовые технические мероприятия по конфигурированию и обслуживанию InfoWatch Traffic Monitor

Обслуживание сервера Traffic Monitor: загрузка лицензии, работа с конфигурационными файлами, проверка и очистка места, работа с лог файлами, диагностика возможных проблем. Обслуживание схемы базы данных Traffic Monitor: PostgreSQL DataBase. Настройка подсистемы мониторинга.

Модуль 4. Типовые технические мероприятия по конфигурированию и обслуживанию InfoWatch Device Monitor

Работа с журналом логов. Проверка соединения с сервером InfoWatch Traffic Monitor. Проверка соединения с Базой Данных.

Модуль 5. Обзор аналитических работ

Цели аналитических работ. План аналитических работ. Сбор требований для настройки автоматизированной системы. Анализ требований. Подготовка концепции настройки DLP системы. Оценка результата аналитических работ.

Модуль 6. Практикум по настройке и использованию DLP системы

Предварительная настройка: теги, статусы, периметры, веб ресурсы, файловые типы, создание групп. Настройка технологий контентного анализа, объектов защиты, политик информационной безопасности. Настройка областей видимости и ролей. Мониторинг с использованием запросов и отчетов. Консультации с наставником в формате вопрос-ответ. Подведение итогов по результатам выполнения заданий.

Модуль 7. Правовые и организационные аспекты легитимизации использования DLP системы.

Законодательство и DLP: неприкосновенность частной жизни, личной и семейной тайны; тайна связи и переписки; требования закона о персональных данных и приказов ФСТЭК; защита коммерческой тайны; специальные технические средства. Организационные меры внедрения DLP-системы.

Модуль 8. Выполнение кейсов по настройке составных модулей DLP системы

Анализ требований к защищаемым данным, предъявляемых компаниями нефтяной, банковской, страховой, строительной, телекоммуникационной, фармакологической отраслей, а также розничных продаж. Подготовка концепции настройки политик информационной безопасности. Настройка автоматизированной системы. Тестирование системы на основе предоставленных в рамках кейсов примеров документов. Консультации с наставником в формате вопрос-ответ. Подведение итогов по результатам выполнения заданий.

Экзамен. Подведение итогов обучения

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 **17 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 Касперсокого, 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 и презентации