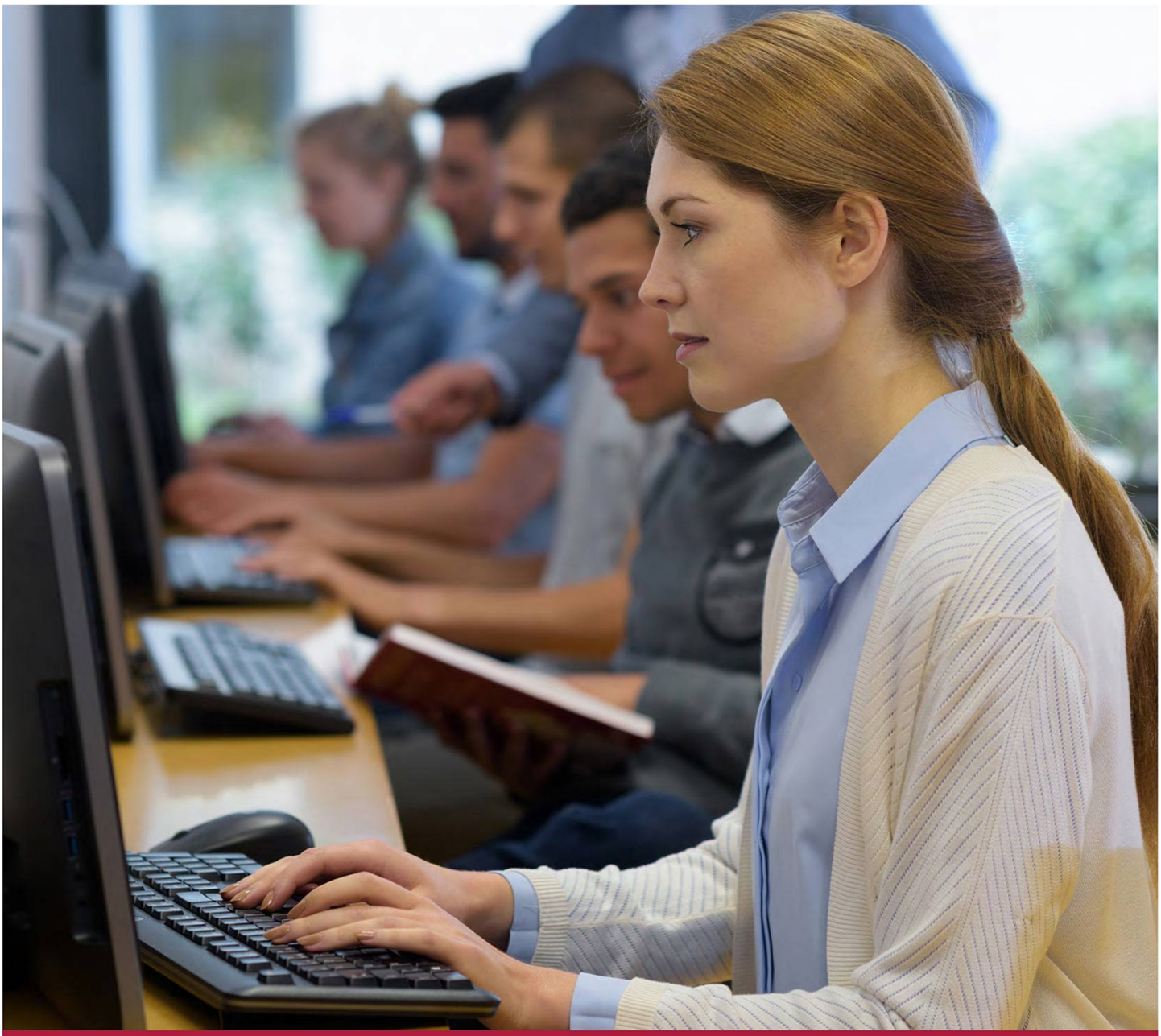
softline учебный центр



Развертывание и администрирование MaxPatrol SIEM

Код курса: ПТ13

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

© Softline, 2024

Развертывание и администрирование MaxPatrol SIEM

Код курса: ПТ13

Длительность	24 ак. часа
Формат	Очно; Дистанционно
Разработчик курса	
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Базовый курс, охватывающий основные возможности системы мониторинга и управления инцидентами информационной безопасности MaxPatrol SIEM и методологию ее использования для автоматизации задач управления событиями информационной безопасности. Рассматриваются вопросы внедрения и эксплуатации MaxPatrol SIEM.

Подробная информация

Профиль аудитории:

- Администраторы безопасности, администраторы корпоративных сетей, специалисты в области информационных технологий, занимающиеся вопросами организации и технологии защиты информации в корпоративных сетях.
- Аудиторы информационной безопасности.
- Консультанты и инженеры, ответственные за построение процессов мониторинга и аудита информационной безопасности.

Предварительные требования:

- Общее представление об архитектуре стека протоколов TCP/IP.
- Практический опыт работы с операционными системами Windows и Linux.
- Базовые знания по сетевым технологиям.
- Общее представление об информационной безопасности и основах построения защищенных корпоративных систем.

По окончании курса слушатели смогут:

- проектировать системы мониторинга и аудита информационной безопасности на базе MaxPatrol с учетом сетевой топологии и особенностей системы управления информационной безопасностью;
- управлять задачами на подключение источников событий и задачами по сбору событий;
- работать с историей событий информационной системы;
- осуществлять администрирование и эксплуатацию системы MaxPatrol SIEM.

© Softline, 2024

Программа курса

Модуль 1. Назначение SIEM-системы.

- Упрощенное внедрение системы.
- Компоненты системы, потоки данных.

Практическая работа 1. Установка системы, первичная настройка компонентов.

Модуль 2. Asset and vulnerability management.

- Метрики CVSSv2, CVSSv3.
- Контекстные метрики.
- БДУ ФСТЭК РФ.

Практическая работа 2. Задачи, профили, активы:

Часть 1. Обнаружение узлов в сети, журналы агента.

Часть 2. Группы активов.

Часть 3. Аудит Windows и Linux.

Часть 4. Назначение контекстных метрик группам.

Часть 5. Топология.

Модуль 3. Пользователи и роли.

- Пользователи и роли.

Практическая работа 3. Пользователи и роли, инфраструктуры.

Модуль 4. Сбор и работа с событиями.

- PDQL и таксономия события.

Практическая работа 4. Сбор событий:

Часть 1. WinEventLog, WMInotification

Часть 2. File via SSH

Часть 3. Checkpoint Gaia 80.10 (необязательная работа)

Часть 4. Kaspersky Security Center (необязательная работа)

Часть 5. Группировка событий

В рамках самостоятельных заданий:

Сбор данных при помощи модуля FileMonitor SMB.

 © Softline, 2024

Работа с системой поиска событий при помощи языка запросов PDQL

Модуль 5. Корреляции.

- Обзор системных правил корреляции.

Практическая работа 5. Корреляции и генераторы

Практическая работа 6. Сбор событий по протоколу syslog

Модуль 6. Инциденты и доставка уведомлений

- Инциденты и доставка уведомлений.

Практическая работа 7. Работа с инцидентами и почтовыми уведомлениями

Часть 1. Работа с автоматически созданным инцидентом.

Часть 2. Самостоятельное создание инцидента.

Модуль 7. Статистика и отчеты

- Статистика и отчеты.

Практическая работа 8. Статистика и отчеты

Часть 1. Статистика

Часть 2. Построение отчетов

Модуль 8. Обзор документации.

- Журналы и решение проблем.

Практическая работа 9. Решение проблем:

Часть 1. Файлы журналов.

Часть 2. Клиент к базе данных Elasticsearch.

Посмотреть расписание курса и записаться на обучение

© Softline, 2024

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!

↓

© Softline, 2024

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.

© Softline, 2024