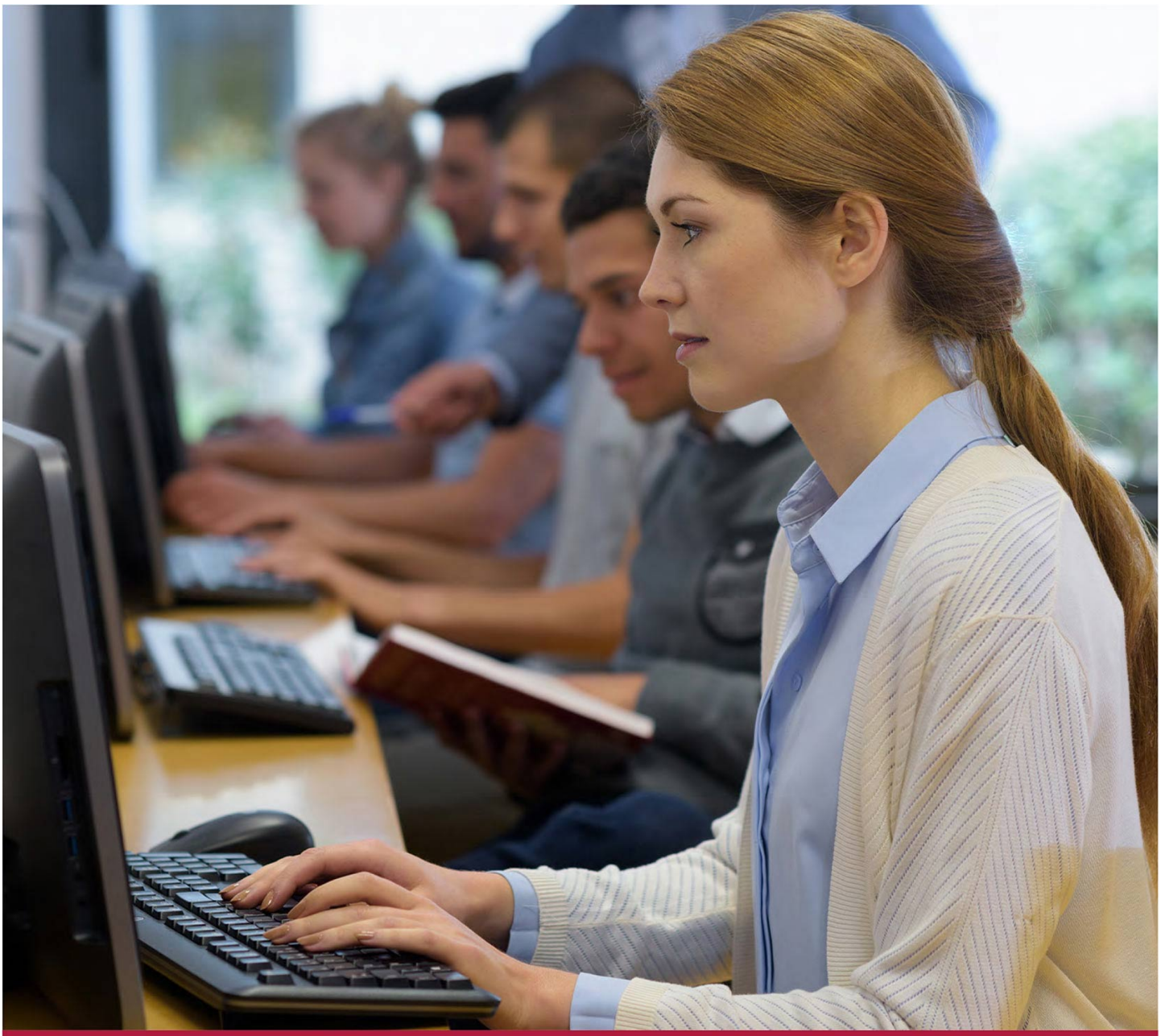
softline учебный центр



Управление событиями безопасности на базе решений компании Positive Technologies

Код курса: ПТ15

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

© Softline, 2024

Управление событиями безопасности на базе решений компании Positive Technologies

Код курса: ПТ15

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

О курсе

Расширенный курс, готовящий специалистов к самостоятельной работе с системой MaxPatrol SIEM, включая полноценную работу с источниками событий, включая сбор и нормализацию событий с произвольных источников. В курсе рассматриваются вопросы написания собственных правил корреляции, работу с табличными списками и вопросы диагностики работоспособности 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:

- Знания об архитектуре и принципах работы системы MaxPatrol SIEM, а также методологии применения MaxPatrol SIEM для мониторинга событий информационной безопасности и управления инцидентами на базе MaxPatrol SIEM

По окончании курса слушатели смогут:

- подключать сбор событий с любого источника;
- настраивать централизованное обновление MaxPatrol в распределенных сетях;
- писать собственные правила корреляции;
- восстанавливать работоспособность системы MaxPatrol SIEM в случае сбоев.

© Softline, 2024

Программа курса

Модуль 1. Нормализация событий.

Описание таксономии.

Практическая работа 1. Написание правила нормализации событий нестандартного источника. Построение графа нормализации.

Модуль 2. Корреляция, модельная корреляция.

Язык создания правил корреляции.

Практическая работа 2. Модификация системных правил корреляции.
Практическая работа 3. Создание собственных правил корреляции.

Модуль 3. Работа с табличными списками.

Работа с табличными списками.

Практическая работа 4. Создание правил корреляции с использованием табличных списков.

Модуль 4. Маршрутизация данных внутри системы.

Диагностика работоспособности системы.

Практическая работа 5. Поиск неисправностей в системе.

Модуль 5. Резервное копирование и восстановление компонент MP SIEM.

Резервное копирование и восстановление компонент MP SIEM.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

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

© Softline, 2024

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