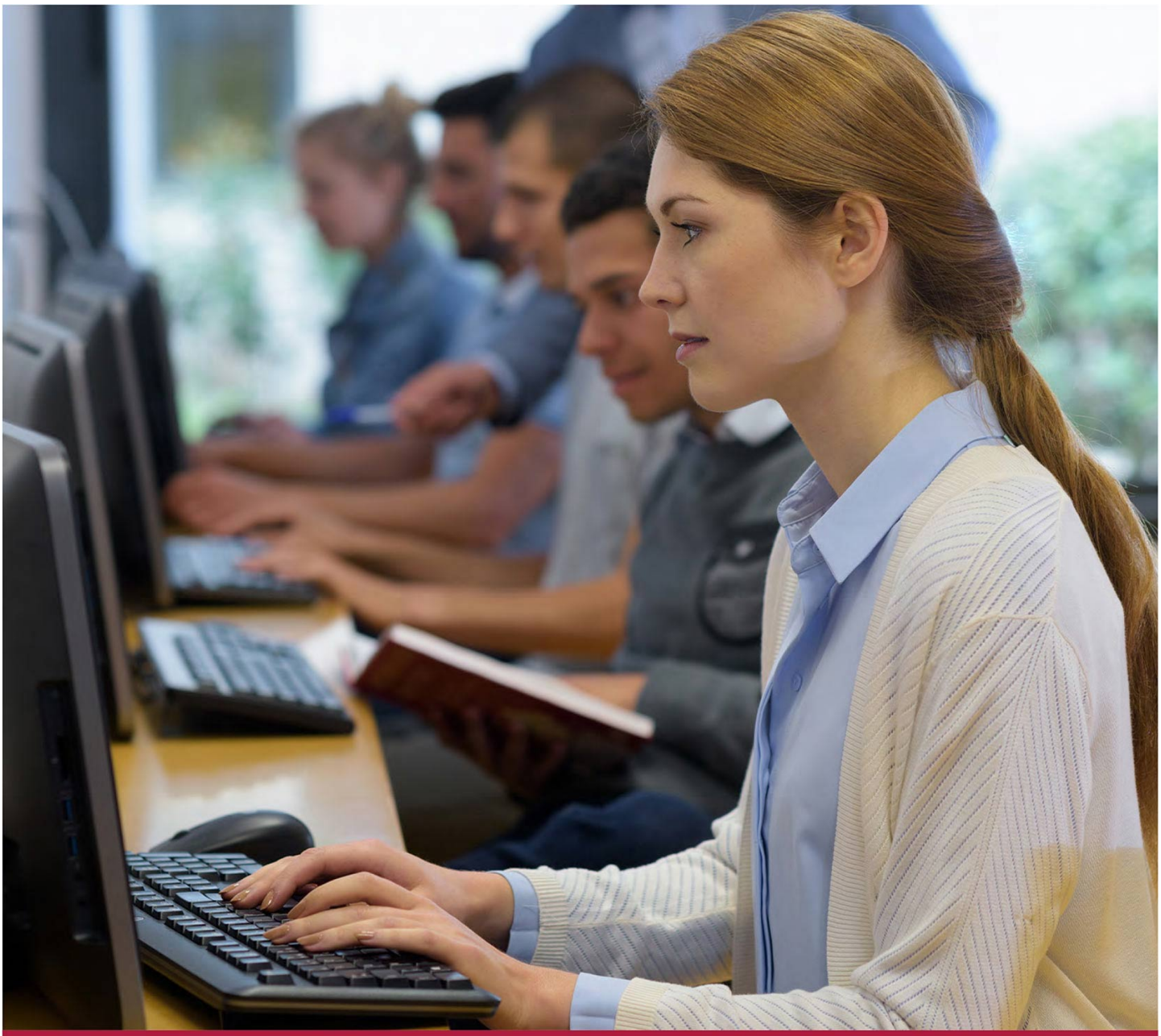
softline учебный центр



PT NAD: проектирование, функциональные возможности и методики расследования атак

Код курса: ПТ75

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

PT NAD: проектирование, функциональные возможности и методики расследования атак

Код курса: ПТ75

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

О курсе

Программа курса включает в себя изучение системы PT Network Attack Discovery (PT NAD), которая предназначена для обнаружения атак. Слушатели подробно рассмотрят функции системы и механизмы поиска и фильтрации данных об атаках. Программа содержит полную информацию о настройке уведомлений, структуре правил и использовании API. На практических примерах участники изучат правила обнаружения сетевых атак, научатся создавать собственные правила, разберут типовые сценарии действий злоумышленников и узнают, как их расследовать.

Подробная информация

Профиль аудитории:

- консультант-аналитик
- аналитик ИБ
- эксплуатация SOC L1 или Оператор системы
- эксплуатация SOC L2-L3 или Специалист по работе с системой
- те, кто готовится сдать сертификацию PT NAD (PT-NAD-CP)

Предварительные требования:

- иметь опыт работы с ОС Linux, Windows и Network
- пройти модули обучения по PT NAD на уровень Certified Specialist (CS)
- иметь опыт работы с MaxPatrol SIEM или другими системами SIEM, PT MultiScanner или PT Sandbox, с системами IDS, IPS или NGFW и другими продуктами Positive Technologies

По окончании курса слушатели смогут:

- репутационные списки, которые применяются в PT NAD, чем они отличаются друг от друга и в каких случаях они могут вызывать ложные срабатывания
- как создавать собственные правила для атак
- что такое ложные срабатывания и чем они вызваны
- некоторые распространенные ошибки, которые допускают специалисты при проведении

расследований
- как нужно поступать с ложными срабатываниями
- как реагировать на инциденты
- содержимое качественного отчета об инциденте
- как из сотен и тысяч отображаемых в интерфейсе атак выбрать именно те, которые следует проверить первыми
- на что обратить внимание при расследовании
- как и для чего можно применять запросы через API
- расследование атак в PT NAD

Программа курса

Модуль 1. Репутационные списки и правила

Модуль 2. Создание собственных правил

Модуль 3. Распространенные ошибки

Модуль 4. Типовые срабатывания

Модуль 5. Примеры атак

Модуль 6. Реагирование на инциденты

Модуль 7. Вы впервые открыли интерфейс «боевого» PT NAD

Модуль 8. Проведение расследования

Модуль 9. API

Модуль 10. 8 примеров расследований

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.