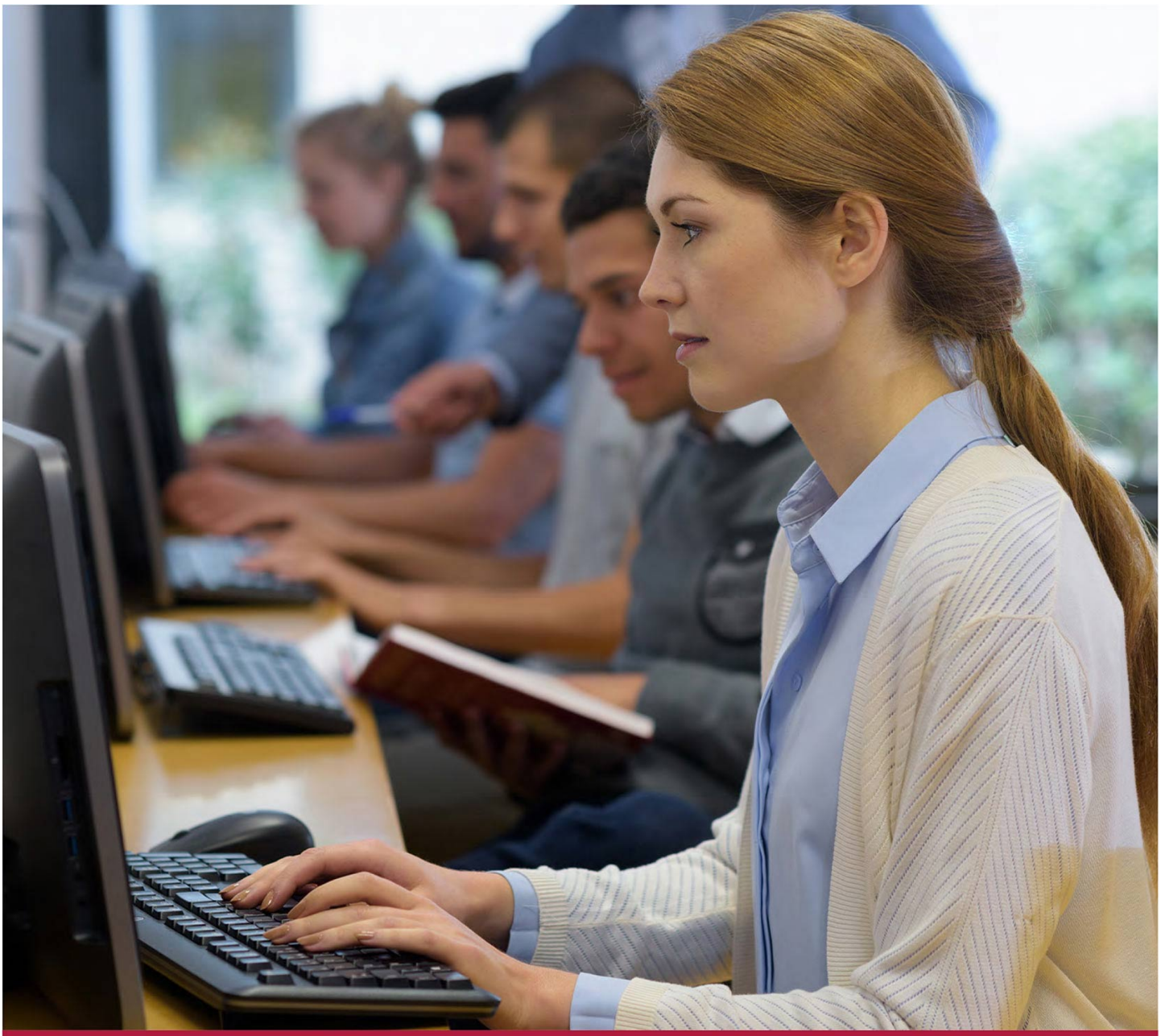
softline учебный центр



PT NAD: базовая архитектура, особенности установки

Код курса: ПТ73

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

PT NAD: базовая архитектура, особенности установки

Код курса: ПТ73

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

О курсе

Базовый курс, посвящённый изучению системы PT Network Attack Discovery (PT NAD), которая предназначена для анализа трафика и выявления атак и аномалий. Программа включает в себя информацию о назначении, архитектуре и функциях PT NAD. Слушатели узнают, как устанавливать, настраивать и использовать систему на практике. Во время обучения участники рассмотрят все аспекты настройки захвата сетевого трафика. Они также разберут различные сценарии использования продукта на практических примерах.

Подробная информация

Профиль аудитории:

- технический пресейл
- консультант-аналитик
- архитектор
- инженер внедрения
- инженер техподдержки
- 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-CS)

Предварительные требования:

- знать основы сетевых технологий
- понимать принципы адресации IPv4
- уметь пользоваться Linux (Debian): работать в командной строке, настраивать сетевые интерфейсы, применять протокол SCP для загрузки файлов на сервер
- 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:

- назначение основных инструментов в веб-интерфейсе продукта
- как выполнять основные действия в пользовательском интерфейсе
- базовую архитектуру PT NAD
- принципы построения многосерверных конфигураций
- схему взаимодействия PT NAD с другими продуктами Positive Technologies
- как легко ориентироваться в базовой архитектуре PT NAD
- различные варианты отображения хранимых данных в PT NAD
- настройку уведомлений по событиям
- настройку отображения событий, показываемых в атаках и ленте активностей
- поиск события, в том числе с использованием фильтров по атрибутам сессий и атак
- какие проблемы могут возникать при работе с веб-интерфейсом PT NAD
- как устранять проблемы, возникающие при работе с веб-интерфейсом PT NAD
- схему лицензирования
- лицензии: инфраструктурные и All-in-one
- выбор необходимых лицензий под поставленные технические задачи
- расчет аппаратной конфигурации системы, отвечающей требованиям заказчика
- как проверять серверы перед установкой PT NAD
- как рассчитывать количество фрагментов индекса Elasticsearch
- как устанавливать PT NAD в односерверном варианте
- как выполнять первичную конфигурацию PT NAD после установки
- брокеры сетевых пакетов и как они могут использоваться для захвата копии трафика
- чем различаются способы захвата копии сетевого трафика с помощью физических и виртуальных TAP, а также функций SPAN/RSPAN/ERSPAN в коммутаторах
- как устроены TAP и что необходимо учитывать при настройке захвата копии трафика с их помощью
- как настраивать захват копии сетевого трафика

Программа курса

Модуль 1. Архитектура PT NAD

Модуль 2. Предназначение PT NAD

Модуль 3. Сравнение NTA-систем с другими решениями

Модуль 4. Как устроен PT NAD

Модуль 5. Сценарии использования

Модуль 6. Анализ трафика

Модуль 7. Какие техники MITRE ATT&CK выявляет PT NAD

Модуль 8. Поставка и лицензирование продукта

Модуль 9. Установка PT NAD AIO

Модуль 10. Пользовательский интерфейс

Модуль 11. Как настроить захват сетевого трафика

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.