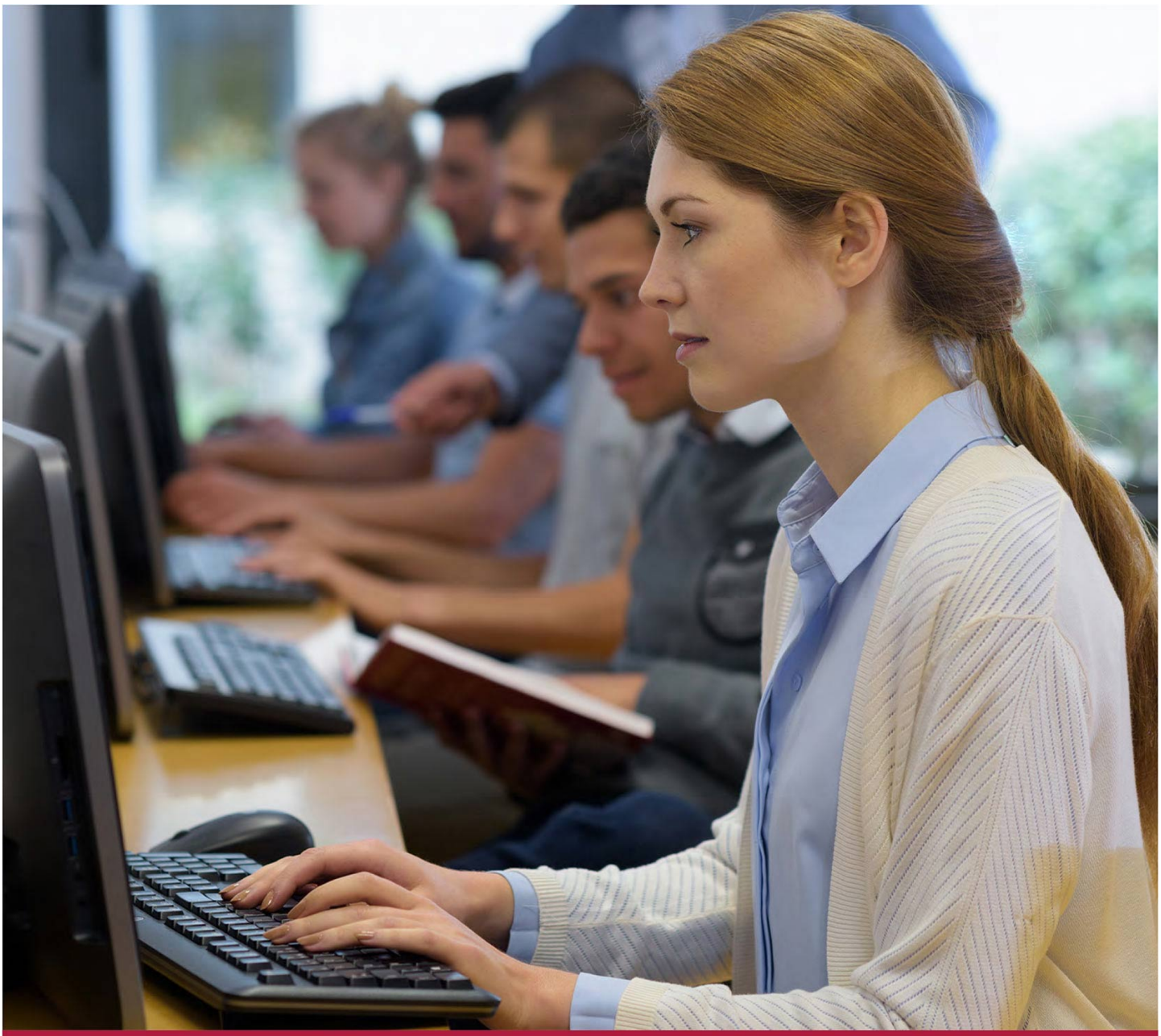
Академия АйТи
a Softline Company



Глубокий траблшутинг подсистемы безопасности PARSEC в инфраструктуре ALD Pro

Код курса: APADV-02

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Глубокий траблшутинг подсистемы безопасности PARSEC в инфраструктуре ALD Pro

Код курса: APADV-02

Длительность	8 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Продвинутый курс по работе с ОС Astra Linux и ALD Pro предназначен для специалистов технической поддержки 2 и 3 линий, системных администраторов и офицеров информационной безопасности, сталкивающихся с неочевидными отказами приложений из-за работы встроенных механизмов защиты PARSEC. Программа построена на глубоком погружении в архитектуру мандатного контроля доступа и обучает использованию специализированных инструментов — таких как psecmon, psecview и журналы parsec-audit — для оперативного выявления причин блокировок. Слушатели научатся отличать сбои, вызванные политиками безопасности, от других типов ошибок, расшифровывать записи в /var/log/audit/audit.log, определять конфликты мандатных меток и быстро восстанавливать работу критичных сервисов без нарушения требований ИБ.

Подробная информация

Профиль аудитории:

- специалисты технической поддержки 2-3 линий, системные администраторы и офицеры ИБ, сталкивающиеся со сложными сбоями ПО из-за работы встроенных механизмов защиты Astra Linux

Цели:

- научиться мгновенно определять, вызван ли сбой приложения механизмами безопасности PARSEC
- освоить чтение и расшифровку специфических логов аудита ИБ Astra Linux для быстрого восстановления сервисов

Предварительные требования:

- опыт администрирования ОС Astra Linux и ALD Pro
- понимание разницы между дискреционным (права rwx) и мандатным (уровни конфиденциальности) доступом

Программа курса

Модуль 1. Инструменты мониторинга и анализ блокировок PARSEC

- Архитектура ядра PARSEC
- Порядок проверки прав доступа операционной системой
- Почему классический Linux-инструментарий не видит блокировки PARSEC
- Обзор утилит psecmon, psecview и механизмов фильтрации событий

Практическая работа:

- Работа с утилитой мониторинга безопасности psecmon в реальном времени
- Намеренная инициализация конфликтов доступа и их фиксация в интерфейсе монитора
- Настройка правил логирования под конкретные задачи аудита

Модуль 2. Траблшутинг сервисов и парсинг журналов аудита

- Структура подсистемы parsec-audit
- Логи безопасности: расшифровка векторов отказа (Access Denied), кодов ошибок и мандатных контекстов в /var/log/audit/audit.log и syslog
- Специфика работы сетевых служб, включая компоненты ALD Pro на разных мандатных уровнях
- Диагностика отказов репликации и аутентификации в домене ALD Pro при включенном МРД.

Практическая работа:

- Лабораторная работа «Поиск сломанного сервиса»: диагностика упавшего приложения (веб-сервер/СУБД), определение нехватки привилегий PARSEC, исправление мандатных меток и восстановление штатной работы службы.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru