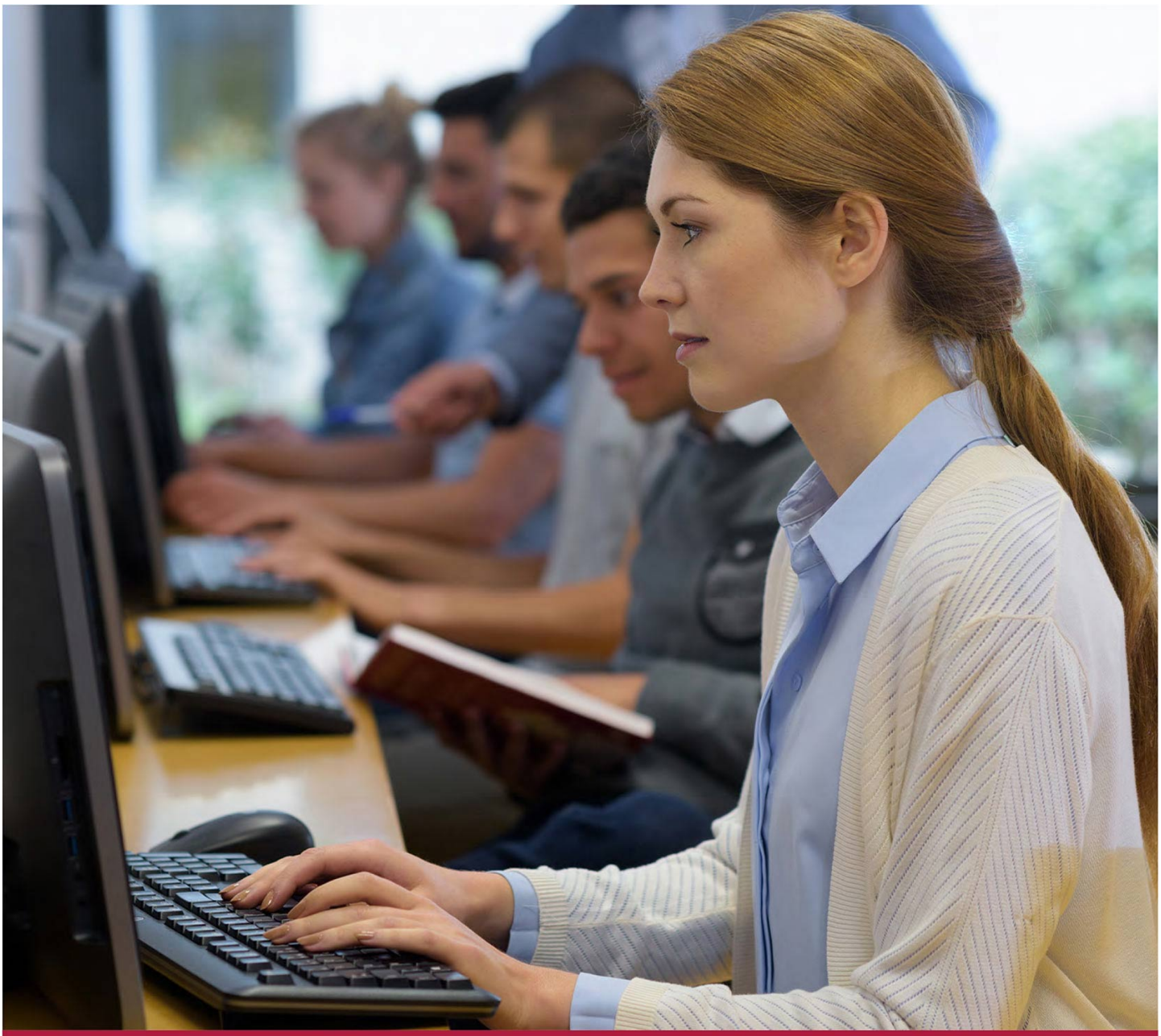
Академия АйТи
a Softline Company



Аналитик киберугроз

Код курса: TI

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

Аналитик киберугроз

Код курса: TI

Длительность	40 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

В условиях эскалации кибератак и появления новых инструментов в арсенале злоумышленников процесс анализа киберугроз (Threat Intelligence, TI) перестал быть факультативной практикой и превратился в критический фундамент современной информационной безопасности. Развитие компетенций в области киберразведки позволяет специалистам не просто реагировать на инциденты, а предвидеть действия противника, фильтровать информационный шум и минимизировать усталость аналитиков от ложных срабатываний. Ключевой парадигмой зрелой ИБ-культуры является интеграция TI именно в начало процессов защиты, а не использование его исключительно как постфактум-инструмента для расследования уже случившихся нарушений. На этапах проектирования архитектуры и моделирования угроз данные разведки обеспечивают реалистичную оценку рисков, позволяя выстраивать оборону под конкретные тактики злоумышленников, а не под абстрактные чек-листы соответствия. Это знание напрямую трансформирует управление уязвимостями и настройку систем детектирования, заставляя приоритезировать устранение тех брешей, которые активно эксплуатируются целевыми группировками в реальном времени.

Подробная информация

Профиль аудитории:

- Аналитики SOC
- Специалисты реагирования на инциденты
- Специалисты информационной безопасности
- Системные и сетевые администраторы и инженеры, касающиеся вопросов обеспечения информационной безопасности инфраструктуры

Предварительные требования:

- Базовые навыки администрирования Linux
- Понимание основ программирования на Python
- Понимание базовых концепций обеспечений информационной безопасности

По окончании курса слушатели изучат:

- Проектировать автоматические конвейеры обработки киберразведданных;
- Создавать скрипты на Python для парсинга и обогащения индикаторов компрометации (IOC);
- Выявлять скрытую инфраструктуру атакующих с помощью графового анализа и Maltego;
- Применять структурированные аналитические методики (ACH, Diamond Model);
- Развертывать и настраивать связку платформ MISP и OpenCTI;
- Интегрировать данные Threat Intelligence в процессы SOC, SIEM и SOAR;
- Разрабатывать проактивные правила детектирования угроз (YARA, Sigma)

Программа курса

Модуль 1. Фундамент Threat Intelligence и нормативный контекст

- Сущность и задачи Threat Intelligence (TI).
- Таксономия кибератак: индикаторы компрометации (IOC), тактики, техники и процедуры (TTP).
- Анатомия целевых атак (APT) и модель Cyber Kill Chain.
- Этапы разведывательного цикла (Intelligence Cycle).
- Правовое регулирование TI в РФ: КИИ (ФЗ-187), приказы и методики ФСТЭК России.
- Профессиональный трек и компетенции CTI-аналитика.
- Лабораторная работа: «Разработка аналитической записки по актуальной киберугрозе».

Модуль 2. Технологии сбора данных и разведка по открытым источникам

- Методология и инструменты OSINT в интересах ИБ.
- Специфика теневого сегмента сети (Dark Web): мониторинг форумов, маркетплейсов и каналов утечек.
- Классификация и архитектура платформ Threat Intelligence Platform (TIP).
- Стандарты обмена данными об угрозах (STIX/TAXII).
- Лабораторная работа: «Развертывание TIP-платформы (MISP), агрегация и тегирование индикаторов».

Модуль 3. Тактический анализ и систематизация киберугроз

- Валидация, скоринг и обогащение полученных IOC.
- Практическое применение фреймворка MITRE ATT&CK для маппинга действий атакующих.
- Отечественные аналоги и базы данных угроз (БДУ ФСТЭК, классификаторы НКЦКИ).
- Профилирование группировок киберпреступников.
- Лабораторная работа: «Реконструкция сценария сложной атаки с использованием матрицы MITRE ATT&CK».

Модуль 4. Исследование артефактов и базовый анализ вредоносного ПО

- Жизненный цикл вредоносного программного обеспечения (ВПО).
- Методы статического экспресс-анализа (сигнатуры, хэши, строки, PE-заголовок).
- Динамический анализ ВПО: изоляция, запуск в песочницах, мониторинг поведения в системе и сети.
- Лабораторная работа: «Базовый поведенческий анализ вредоносного файла в изолированной лабораторной среде».

Модуль 5. Синергия TI с операционным центром безопасности (SOC) и Threat Hunting

- Интеграция фидов данных (TI-feeds) в контур защиты: SIEM, SOAR, EDR, XDR.
- Разработка правил детектирования (Sigma, Yara) на основе данных TI.
- Проактивный поиск скрытых угроз (Threat Hunting): гипотезы, методики, поиск аномалий.
- Роль аналитика TI в процедурах реагирования на инциденты (Incident Response).
- Комплексный кейс-стади: «Обогащение SIEM-системы индикаторами TI и разработка сценария реагирования».

Модуль 6. Стратегические коммуникации, отчетность и внешнее взаимодействие

- Построение технических, тактических и стратегических отчетов для разных аудиторий.
- Методы визуализации связей и графов атак.
- Регламенты и форматы обмена данными с российскими центрами: ГосСОПКА, НКЦКИ, ФинЦЕРТ.
- Взаимодействие с международными CERT и коммерческими ИБ-альянсами в современных реалиях.
- Практическая работа: «Подготовка аналитического доклада и дашборда для топ-менеджмента (CISO/CEO)».

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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