Аналитик SOC

Пояснения к словам иностранного происхождения

Здесь собраны пояснения к словам иностранного происхождения, которые используются в программе курса, но пока не включены в словарную норму русского языка.

01 Кому подойдёт курс

- Разработчикам
- DevOps-специалистам
- Сетевым инженерам
- Системным администраторам
- Тем, у кого небольшой опыт в кибербезопасности

Что нужно знать:

- Основы работы сетевых протоколов: DNS, HTTP, DHCP, SMB
- Архитектуру операционных систем Windows и Linux
- Архитектуру современных веб-приложений
- Работу с командной строкой в операционных системах Windows и Linux

02 Чему научитесь на курсе

Какие знания и навыки освоите

- Выявлять хакеров по их действиям и следам
- Обрабатывать инциденты безопасности
- Соблюдать этические принципы работы с информацией
- Подключать источники для сбора событий безопасности
- Анализировать события безопасности в SIEM и выстраивать цепочки атак
- Разбирать атаки с точки зрения специалиста центра мониторинга
- Реагировать на выявленные угрозы и атаки
- Регистрировать и документировать инциденты безопасности
- Работать с полным циклом реагирования на инциденты в системе IRP/SOAR

03 Как проходит курс

- Теория на платформе Практикума
- Практика на индивидуальных виртуальных машинах, развёрнутых в облаке
- Доступ из любой точки мира в удобное время
- Воркшопы и вебинары с опытными наставниками
- Практические проекты, приближенные к реальности

Что вас ждёт

Документ о полном прохождении курса

Практика, основанная на решении реальных рабочих задач

Программа от экспертов из Яндекса и других крупных компаний

Аналитик SOC

4 месяца

продолжительность курса

6 проектов

с обратной связью от экспертов

10 ЧАСОВ

00

Введение в профессию «Аналитик SOC»

3 НЕДЕЛИ

01

Работа с событиями безопасности

6 НЕДЕЛЬ

02

Triage: работа с цепочками событий безопасности

3 НЕДЕЛИ

03

Реагирование на инциденты безопасности

3 НЕДЕЛИ

04

Расследование инцидентов безопасности

3 НЕДЕЛИ

05

Итоговый проект

Введение в профессию «Аналитик SOC» 00

10 часов

Работа с событиями безопасности 01

3 недели
1 проект

Модуль научит вас эффективно анализировать логи различных систем — от Windows и Linux до веб-приложений и инфраструктурных сервисов.
Вы освоите работу с логами файрволов, IDS и сетевого трафика, а также научитесь выявлять с их помощью атаки и угрозы.

Содержание

Темы

1. Windows-логи
2. Windows-логи в доменной инфраструктуре
3. Linux-логи
4. Логи инфраструктурных сервисов
5. Анализ сети
6. Логи веб-приложений

Проект

Вы проведёте серию атак в тестовой среде и научитесь распознавать действия злоумышленника в логах. В проекте вы освоите практические навыки выявления угроз и реагирования на инциденты безопасности.

Triage: работа с цепочками событий безопасности 02

6 недель
2 проекта

В этом модуле вы разберёте ключевые задачи аналитиков L1 и L2, познакомитесь с основными понятиями SOC — событиями, инцидентами и атаками — и научитесь проводить триаж и первичный анализ. Вы изучите типы и цепочки атак (Kill Chain, MITRE ATT&CK, TTP) и поймёте, как строится логика атакующих. Далее вы узнаете, как защищаться от атак с помощью технических, организационных и физических методов, а также как детектировать их средствами защиты.

Завершающая часть спринта посвящена ключевым инструментам SOC — SIEM, SOAR, CMDB, EDR и IRP. Вы разберётесь в принципах их работы, взаимодействии между ними и роли каждого в процессе мониторинга и расследования инцидентов.

Содержание

Темы

1. Задачи L1/L2
2. Атаки
3. Как защищаться от атак?
4. Ключевые инструменты SOC: SIEM, SOAR, CMDB, EDR, IRP
5. Подробное знакомство с SIEM
6. Правила корреляции
7. Принципы поиска событий
8. Дашборды
9. Покрытие мониторингом
10. Проверка объектов

Проект 1

В этом проекте вы проведёте расследование целевой атаки с использованием инструментов SOC. Вы проанализируете артефакты атаки, сопоставите события с тактиками и техниками MITRE ATT&CK, определите вектор компрометации и предложите меры реагирования.

Проект 2

В этом проекте вы научитесь работать с ELK, правилами корреляции, дашбордами Kibana, а также с практикой документирования расследований. Вы проведёте расследование инцидента информационной безопасности, используя ELK. Научитесь выявлять аномалии в логах, создавать правила корреляции и визуализировать данные в дашбордах.

Реагирование на инциденты безопасности 03

3 недели
1 проект

В этом модуле вы освоите ключевые методы и инструменты для реагирования на инциденты. Узнаете, как SOC взаимодействует с IT, научитесь использовать SOAR и ручные методы реагирования, а также координировать действия в стандартных и нестандартных сценариях. Особое внимание уделено командной работе и коммуникации при реагировании на инциденты.

Содержание

Темы

1. Возможности по реагированию
2. Инструменты IR
3. Сценарии реагирования на стандартные инциденты
4. Сценарии реагирования на нестандартные инциденты
5. Коммуникации при реагировании

Проект

В проекте вы будете использовать плейбук для реагирования на стандартные инциденты, автоматизировать действия с помощью SOAR и разбирать ошибки SOC при реагировании. Вы научитесь координировать действия в нестандартных ситуациях, собирать дополнительную информацию и эффективно общаться с командой через выбранные каналы связи.

Расследование инцидентов безопасности

04

3 недели
1 проект

В этом модуле вы узнаете, как проводить расследование атак и полный цикл работы с инцидентами. Вы научитесь выдвигать и проверять гипотезы на основе сетевых и хостовых событий, выбирать точки старта для расследования, строить таймлайн, анализировать артефакты и готовить отчёты для разных целевых аудиторий.

Содержание

Темы

1. Методология и структура расследования инцидента
2. Источники, артефакты и данные в рамках расследования
3. Анализ артефактов и построение гипотез
4. Завершение расследования и подготовка отчёта

Проект

В проекте вы проведёте полный цикл расследования инцидента информационной безопасности: от формулировки гипотез и анализа цифровых следов до построения таймлайна, подготовки отчётов и предложений по улучшению мониторинга. Научитесь применять результаты расследования для автоматизации процессов: создавать правила корреляции и плейбуки реагирования.

Итоговый проект 05

3 недели

В этом итоговом проекте вы примените все знания и навыки, полученные за время прохождения курса. Вы выполните полноценное расследование сложного многоэтапного инцидента, обнаруженного в инфраструктуре компании Demo Lab. Работа охватывает все ключевые компетенции SOC-аналитика: от анализа логов и построения таймлайна до написания правил корреляции, конфигурации мониторинга и подготовки отчётности.

Воркшопы

Воркшопы проводятся один раз за спринт. На воркшопах вы сможете применить полученные знания на практике.