

Аналитик SOC

4 месяца

продолжительность курса

6 проектов



Введение в профессию
“Аналитик SOC”

10 часов

Работа с событиями
безопасности

45 часов

Triage: работа с цепочками
событий безопасности

90 часов

Реагирование на инциденты
безопасности

45 часов

Расследование инцидентов
безопасности

45 часов

Итоговый проект

45 часов

Введение в профессию “Аналитик SOC”

00

[10 часов]

Темы

1. Что такое SOC?

2. Отраслевые специализации
SOC

3. Как выглядит день SOC-
аналитика

Работа с событиями безопасности

01

[3 недели],
[1 проект]

Проект

Вы воспроизведете различные кибератаки, включая kerberoasting и DNS-эксплуатацию, и проанализируете логи для выявления следов атак. Также проведете эмуляцию сетевых атак, таких как сигнатурные атаки и сканирование открытых портов, с анализом сетевых событий. В проекте вы освоите практические навыки выявления угроз и реагирования на инциденты безопасности.

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

Темы

1. Windows-логи

2. Windows-логи в доменной инфраструктуре

3. Linux-логи

4. Логи инфраструктурных сервисов

5. Анализ сети

6. Логи веб-приложений

**[6 недель],
[2 проекта]**

Проект 1

В проекте вы будете эмулировать кибератаки, использовать SIEM для сбора и анализа данных, проводить triage событий, отличать ложные срабатывания, выявлять реальные угрозы и защищать сеть и устройства. Вы получите практические навыки работы с инцидентами и управления цепочками атак.

Проект 2

В этом проекте вы научитесь фильтровать и группировать события, создавать правила корреляции для выявления инцидентов и строить дашборды для мониторинга. Вы будете проверять репутацию объектов с помощью OSINT и анализировать сетевые, аутентификационные и почтовые события для выявления угроз и инцидентов.

В этом модуле вы изучите основные задачи SOC-аналитиков L1/L2, работу с уязвимостями, методы защиты и использование ключевых инструментов SOC, таких как SIEM и SOAR. Вы освоите классификацию событий, реагирование на инциденты и управление цепочками атак. Модуль углубляет знания в области анализа инцидентов и событий безопасности. Вы научитесь фильтровать, группировать и коррелировать события, работать с дашбордами, проверять репутацию объектов, а также анализировать сетевые, аутентификационные и почтовые события. Особое внимание уделяется мониторингу и контролю инцидентов.

Темы

- | | | |
|--------------------------------|----------------------------|--------------------------------------|
| 1. Задачи L1/L2 | 7. От события к инциденту | 13. Анализ сетевых событий |
| 2. Атаки | 8. Правила корреляции | 14. Анализ событий аутентификации |
| 3. Как защищаться от атак? | 9. Принципы поиска событий | 15. Анализ событий доступа |
| 4. Жизненный цикл события | 10. Дашборды | 16. Анализ событий электронной почты |
| 5. Инструментарий SOC L1/L2 | 11. Покрытие мониторингом | |
| 6. Подробное знакомство с SIEM | 12. Проверка объектов | |

Реагирование на инциденты безопасности

03

[3 недели],
[1 проект]

Проект

В проекте вы будете использовать playbook 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.

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.

Темы

1. Возможности по реагированию

2. Инструменты IR

3. Сценарии реагирования: стандартные инциденты

4. Сценарии реагирования: нестандартные инциденты

5. Коммуникации при реагировании

[3 недели],
[1 проект]

Проект

В проекте вы научитесь выдвигать гипотезы на основе сетевых и хостовых событий, проверять их с помощью инструментов для расследования атак и проводить полный анализ инцидента. Вы построите Timeline, соберете артефакты и подготовите отчет с рекомендациями по устранению инцидента.

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 Timeline, анализировать артефакты и готовить отчеты для разных целевых аудиторий.

Темы

1. Использование Mitre для анализа техник и тактик

2. Расследование атак на основе логов

3. Когда требуется расследование

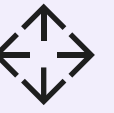
4. Выбор точки старта расследования

5. Timeline расследования

6. Информация для расследования

7. Отчетность

Итоговый проект



[2 недели]

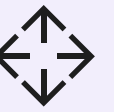
В этом итоговом проекте вы примените все знания и навыки, полученные за время курса. Вы проведете полное расследование сложного инцидента безопасности, начиная с этапа его идентификации. Вы научитесь выдвигать и проверять гипотезы на основе сетевых и хостовых событий, собирать и анализировать артефакты из систем Windows и Linux, строить Timeline атаки, применять методы реагирования и устранять угрозу. В завершение проекта вы подготовите отчет для разных целевых аудиторий с рекомендациями по устранению причин инцидента, опираясь на лучшие практики Incident Response и требования отчетности для CERT.

Воркшопы



Воркшопы проводятся 1 раз за спринт. На воркшопах вы сможете применить полученные знания на практике.

Программа трудоустройства



[4 недели]

Программа становится доступна в конце обучения. В ней мы расскажем о том, как правильно составить резюме, создать портфолио и сделать свой отклик заметнее с помощью сопроводительного письма. Также обсудим процесс подготовки к собеседованию: на какие софт-скиллы и хард-скиллы сделать фокус.