

Программа курса Обеспечение информационной безопасности

БЛОК №1

7 АКАДЕМИЧЕСКИХ ЧАСОВ

Экспресс киберучения

ЧАСЫ

СРЕДСТВА МОНИТОРИНГА ДЛЯ КИБЕРУЧЕНИЙ

1

Базовые навыки работы со средствами мониторинга, необходимые для успешного прохождения киберучений (интерфейс, ключевые страницы и поля, язык поисковых запросов, механизмы фильтрации и т.д.).

СОВМЕСТНЫЙ РАЗБОР ТЕСТОВОГО КЕЙСА

1

Совместный разбор тестового кейса, направленного на исследование эксплуатации уязвимости веб-приложения.

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

5

Самостоятельное исследование сценария подмены содержимого веб-сайта.

БЛОК №2

29 АКАДЕМИЧЕСКИХ ЧАСОВ

Что вы знали и не знали о SOC

ЧАСЫ

ЧТО ТАКОЕ SOC? ЦЕЛИ И ФУНКЦИИ

1

Задачи и назначение SOC. Миссия и Видение SOC. Операционная модель SOC.

ВИДЫ И ЭВОЛЮЦИЯ SOC-ЦЕНТРОВ

1

In-house SOC, коммерческий SOC, гибридный SOC. Требования к современным SOC-центрам. Fusion Center.

ЛЮДИ – ТЕХНОЛОГИИ – ПРОЦЕССЫ. ПОЧЕМУ ЭТОГО УЖЕ НЕДОСТАТОЧНО?

2

Процессная, организационная и управленческая модели SOC. Архитектура технических средств SOC.

РАСПРЕДЕЛЕНИЕ РОЛЕЙ В SOC. ВОЗМОЖЕН ЛИ И КАКОЙ КАРЬЕРНЫЙ РОСТ В SOC.

1

Ролевая модель SOC. Функции и обязанности каждой роли. Программа обучения и "кузница кадров" в SOC.

ЖИЗНЕННЫЙ ЦИКЛ ИНЦИДЕНТА ИБ

4

Что такое инцидент ИБ. Политика и план реагирования на инциденты. Основные метрики реагирования. Мандат на действия.

КЛЮЧЕВЫЕ ПРОЦЕССЫ SOC

4

Разбор процессов мониторинга и реагирование на инциденты ИБ, пост-анализа.

ТЕХНОЛОГИЧЕСКИЕ ПЛАТФОРМЫ SOC

1

Набор и функции основных технологических средств SOC. Ticketing-система или IRP - как использовать для автоматизации процессов в SOC.

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

15

Создание мандата на полномочия, приоритизация инцидентов, штабные киберучения.

БЛОК №3

50 АКАДЕМИЧЕСКИХ ЧАСОВ

Базовое погружение в особенности осуществления атак

ЧАСЫ

ОСНОВЫ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

6

Атаки на протоколы маршрутизации.

ОСНОВЫ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

4

Основные уязвимости и атаки на Web-приложения, методы защиты Web-приложений; классификация уязвимостей Web-приложений OWASP TOP 10 и Web Application Security Consortium Threat Classification.

ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ

3

Работа с терминалами и интерпретаторами.

ОСНОВЫ БЕЗОПАСНОСТИ WINDOWS

4

Архитектура Windows, службы, реестр, основные процессы, учетные записи, Аутентификация, NTLM, Kerberos, журналы событий.

ОСНОВЫ БЕЗОПАСНОСТИ LINUX

4

Архитектура ядра, файловая система, БД структура каталогов, логи, основные типы событий, основные процессы, Crontab и демоны, пользователи, биты доступа файлов.

OPEN SOURCE РЕШЕНИЯ

4

ELK Stack, Wazuh, TheHive, Arkime, Zeek, Wireshark, Cuckoo Sandbox.

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

25

Поиск флагов, анализ трафика, написание скриптов.

БЛОК №4

41 АКАДЕМИЧЕСКИЙ ЧАС

Глазами атакующего

ЧАСЫ

ВЕБ-АТАКИ

8

- Механизмы возникновения уязвимостей в веб
- Сбор информации и выбор целей
- Автоматизация поиска "Low-Hanging Fruits"
- Поиск, написание и использование эксплойтов
- Фаззинг: файлы и директории, пользователи, параметры
- Уязвимости: SQL-инъекции, Path Traversal, SSRF, RCE и другие

ИНФРАСТРУКТУРНЫЕ АТАКИ

8

Этапы по Cyber Kill-Chain и MITRE ATT&CK.

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

25

Расследования в WAF, NTA, SIEM соответствующих занятию техник атакующих.

БЛОК №5

47 АКАДЕМИЧЕСКИХ ЧАСОВ

Инструменты и продвинутые подходы специалистов по расследованию

ЧАСЫ

РАБОТА С ИНСТРУМЕНТАМИ

6

Продвинутые навыки работы со средствами мониторинга: SIEM, NTA, WAF, Sandbox.

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

4

Анализ почтовых сообщений изучение обратных shell-ов, варианты сетевых соединений с управляющим сервером атакующих, удаленный доступ к скомпрометированной машине: виды, возможности Разведка по открытым источникам (OSINT) в TI, популярные фреймворки пост-эксплуатации: их особенности и способы распознавания. Разбор сценария атаки.

БЕЗОПАСНОСТЬ WINDOWS

4

Сценарии разведки, способы закрепления атакующих, способы обхода UAC, обнаружение ВПО с помощью встроенных инструментов, обфускация, Lateral Movement и др. Разбор сценариев атак.

БЕЗОПАСНОСТЬ LINUX

4

Исследование криптоджекинга, анализ критичных уязвимостей и уязвимостей 0-дня в кроссплатформенных сервисах, изучение методов повышения привилегий в Linux-системах. Разбор сценария атаки.

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

25

Продвинутые расследования в WAF, NTA, SIEM соответствующих занятию техник атакующих.

БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

4

Разбор сценариев атак.

БЛОК №6

28 АКАДЕМИЧЕСКИХ ЧАСОВ

Создание контента SOC

ЧАСЫ

USE CASES

4

Методология создания правил и сценариев мониторинга.

PLAYBOOKS

4

Методология создания сценариев реагирования.

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

20

Написание сценариев мониторинга и реагирования.

Введение в ТІ и ТН

ЧАСЫ

РАБОТА С СЕРВИСАМИ АНАЛИТИКИ УГРОЗ (ТІ)

4

Базовая терминология анализа угроз. Источники аналитики (feeds) и уровни доверия к ним. Подходы по работе с фидами.

ЗНАКОМСТВО С ПЛАТФОРМАМИ ТІ И ТН

2

ОСНОВЫ АНАЛИЗА И ПОИСК АУГРОЗ. ПОСТРОЕНИЕ ГИПОТЕЗ

6

Методология и процессы анализа и поиска угроз. Взаимосвязь процессов анализа и поиска угроз с другими процессами SOC. Поиск угроз и формулировки гипотез. Работа с матрицей ATT&CK, Pyramid of Pain, Yara, Sigma. Работа с Suricata

СОЗДАНИЕ ПРОДУКТОВ АНАЛИТИКИ

3

Методика создания продуктов аналитики. Индикаторы компрометации, тактики и техники нарушителя.

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

20

Упражнения на OSINT, формулирование гипотез, создание продуктов аналитики.

Выпускная работа

Написать самостоятельно сценарий атаки и последовательность по его расследованию. Атаки и правила детектирования. Далее написание контента.