Расписание групп

Аналитик SOC L1 линии

Длительность обучения: 4 месяца

Объем программы: 120 ак.часов Форматы: лонгриды, видео, тестирования с автопроверкой, практические кейсы на инфраструктуре Киберполигона с оценкой от менторов, вебинары с экспертами

Доступ к LMS открыт круглосуточно, модули открываются по расписанию и доступны в течение 2-х месяцев после завершения обучения. Ведущие эксперты и и менторы:

Номер недели	Формат	Название	Содержание	Время, (ак.ч.)
Неделя 1				
Неделя 1	Вебинар	Вебинар 1. Установочная встреча	О программе Знакомство с командой и экспертами Работа с LMS и Киберполигоном	1
Неделя 1	Теория	Модуль "Организационная информация"	О программе: структура и форматы Какие компетенции будут приобретены, результаты обучения Работа с платформамиСоветы по обучению	1
Неделя 1	Теория	Модуль 1. Центр мониторинга и реагирования на инциденты	Задачи SOC-центра Структура современного SOCРолевая модель Линии мониторинга в Security Operations Center	3
Неделя 1	Практика	Практика 1	Проверочное тестирование	0,5
		Итого за неделю		**6**
Неделя 2				
Неделя 2	Вебинар	Вебинар 2. Система развития	Матрица компетенций Карьерные треки в ИБ	2
Неделя 2	Теория	Блок 2. Безопасность ОС. Модуль 2.1. Архитектура ОС	Архитектура ОС и файловая система	1
Неделя 2	Теория	Блок 2. Безопасность ОС. Модуль 2.2. Безопасность в ОС Windows	Исполняемые файлы и процессы Portable Executable Внедрение кода, Управление доступом, Реестр ОС Windows	3
Неделя 2	Теория	Блок 2. Безопасность ОС. Модуль 2.3. Анализ журналов в ОС Windows	Аудит по журналам ОС, Работа с событиями, Интерпретация события аудита, Анализ события, Работа с событиями Sysmon	3
Неделя 2	Практика	Практика 2	Проверочное тестирование	2
Неделя 2	Практика	Практика 3 на стенде с самопроверкой	Анализ запущенных процессов	1,3
Неделя 2	Практика	Практика 4 на стенде с самопроверкой	Расследование активности по журналу Power Shell с самопроверкой	2
		Итого за неделю		**14**
Неделя 3				
Неделя 3	Теория	Блок 2. Безопасность ОС. Модуль 2.4. Безопасность в ОС Linux	Безопасность Linux: файловая система, работа с утилитами эксплуатации уязвимостей. Анализ журналов Linux, интерпретация событий аудита Linux	3
Неделя 3	Теория	Блок 2. Безопасность ОС. Модуль 2.5. Анализ журналов в ОС Linux	Журналы аудита Linux, Интерпретация событий аудита ОС Linux, auditd, iptables	1
Неделя 3	Вебинар	Вебинар 3. Анализ журналов	Журналы событий: их значимость в аудите ИБ, журналы и интерпретация событий. Атаки на ОС	2
Неделя 3	Практика	Практика 5 на стенде с оценкой ментора	Безопасность Linux	1
Неделя 3	Практика	Практика 6 на стенде с оценкой ментора	Расследование инцидента по журналам событий ОС Linux и IDS Suricata и дампу сетевого трафика	2
		Итого за неделю		**10**
Неделя 4				
Неделя 4	Вебинар	Вебинар 4. Q&A	Q&A-сессия по модулям 2 и 3 Разбор практических заданий	2
Неделя 4	Теория	Блок 3. Безопасность сетей Модуль 3.1. Сетевая модель	Сетевая модель OSI.	3
Неделя 4	Теория	Блок 3. Безопасность сетей Модуль 3.2. Протоколы и технологии безопасности	Сетевая безопасность: протоколы и технологии.	3
Неделя 4	Теория	Блок 3. Безопасность сетей Модуль 3.3. Сетевые атаки	Сетевые атаки в соответствии с уровнями модели OSI.	3
Неделя 4	Теория	Блок 3. Безопасность сетей Модуль 3.4. Методы анализа событий в сетевом трафике	Методы анализа событий в сетевом трафике	2
Неделя 4	Практика	Практика 7	Проверочное тестирование	2
Неделя 4	Практика	Практика 8 на стенде с оценкой ментора	Протоколы безопасности	2
		Итого за неделю		**17**
Неделя 5				
Неделя 5	Вебинар	Вебинар 5. Атаки на сети	Обзор последних атак на сети и подходы к обеспечению безопасности сетей Современные/актуальные сетевые атаки на корпоративную инфраструктуру Подходы к обеспечению безопасности сети предприятия / сетевой инфраструктуры Q&A-сессия	2
Неделя 5	Теория	Блок 4. Средства защиты информации Модуль 4.1. Сетевые средства защиты	Сетевые средства защиты	3
Неделя 5	Теория	Блок 4. Средства защиты информации Модуль 4.2. Хостовые и комплексные средства защиты	Хостовые и комплексные средства защиты	3
Неделя 5	Практика	Практика 9 на стенде с оценкой ментора	NTA	3
Неделя 5	Практика	Практика 10 на стенде с оценкой ментора	EDR	2
		Итого за неделю		**13**

Неделя 6-7				
Неделя 6-7	Теория	Блок 5. Безопасность корпоративной инфраструктуры Модуль 5.1. Централизованное управление корпоративной IT-инфраструктурой	Строение корпоративной инфраструктуры, Домены в корпоративной IT-инфре, Типовые сервисы в корпоративной сети, Протоколы в доменах AD, Групповые политики	3
Неделя 6-7	Теория	Блок 5. Безопасность корпоративной инфраструктуры Модуль 5.2. Атаки на домены Active Directory	Простейшие атаки, Разведка в доменах АД, Атаки на протокол NTLM, Атаки на протокол Kerberos, Атаки на контроллеры домена, Другие типы атак	3
Неделя 6-7	Практика	Практика 11 на стенде с оценкой ментора	Настройка групповых политик AD	2
Неделя 6-7	Практика	Практика 12 на стенде с оценкой ментора	Мониторинг КИС	2
Неделя 6-7	Вебинар	Вебинар 6. СЗИ в ИТ-инфраструктуре	ИТ-инфраструктура и СЗИ: какие СЗИ используются для каких задач	2
		Итого за неделю		**12**
Неделя 8				
Неделя 8	Теория	Блок 6. Вредоносное ПО Модуль 6.1. Вредоносное ПО	Анализ вредоносного программного обеспечения. Обеспечение безопасности при удалённом администрировании. Разведка по открытым источникам для целей обеспечения информационной безопасности	2
Неделя 8	Практика	Практика 13 на стенде с оценкой ментора	Реализация атаки на сетевую инфраструктуру с использованием PsExec»	1
Неделя 8	Теория	Блок 7. Безопасность Web-технологий Модуль 7.1. Безопасность Web-технологий	Механизмы защиты веб-приложений. Применение WAF для защиты веб-приложений	3
Неделя 8	Практика	Практика 14 на стенде с оценкой ментора	Обеспечение безопасности сети с использованием WAF	2
		Итого за неделю		**8**
Неделя 9				
Неделя 9	Вебинар	Вебинар 7. Уязвимости	Атаки на веб-системы в соответствии с методологией OWASP Top 10	2
Неделя 9	Теория	Блок 8. Мониторинг инцидентов Модуль 8.1. SIEM-система	SIEM-система:архитектура,интерфейс, мониторинг доступности источников событий	3
Неделя 9	Практика	Практика 15 на стенде с оценкой ментора	Анализ инцидента	2
		Итого за неделю		**7**
Неделя 10				
Неделя 10	Вебинар	Вебинар 8. Мониторинг	Мониторинг доступности источников событий и работоспособности SIEM	2
Неделя 9	Теория	Блок 8. Мониторинг инцидентов Модуль 8.2. Средства мониторинга	NTA, Security Optional, Suricata, Zeek, Системы мониторинга, Проведение расследований	3
Неделя 10	Практика	Практика 16 на стенде с оценкой ментора	NTA и WAF для мониторинга инцидентов	2
		Итого за неделю		**7**
Неделя 11				
Неделя 11	Вебинар	Вебинар 9. Использование SIEM-системы для мониторинга и реагирования на инциденты информационной безопасности	Расследование в консоли SIEM типовой активности в корпоративной сети	2
Неделя 11	Теория	Блок 9. Реагирование на инциденты Модуль 9.1. Реагирование на инциденты	Методологии реагирования на инциденты Инструменты реагирования Работа по плейбукам и реагирование на типовые инциденты	4
Неделя 11	Практика	Практика 17 на стенде с оценкой ментора	Реагирование на типовые инциденты	3
		Итого за неделю		**9**
Неделя 12				
Неделя 12	Вебинар	Вебинар 10. Проведение расследования инцидентов информационной безопасности с применением SIEM-системы	Методология расследования инцидентов ИБ в SIEM	2
Неделя 12	Теория	Блок 10. Расследование инцидентов Модуль 10.1. Расследование инцидентов	Эксплуатация уязвимостей, матрица MITRE ATT&CK и MITRE D3F3ND, модель Cyber Kill Chain Индикаторы компрометацииОбзор отраслевых отчетов	4
Неделя 12	Практика	Практика 18 на стенде с оценкой ментора	Расследование инцидентов	3
		Итого за неделю		**9**
Неделя 13				
Неделя 13	Практика	Финальное задание на стенде с оценкой ментора		10
		Итого за неделю		**10**
Неделя 14				
Неделя 14	Вебинар	Вебинар 11. Итоговый вебинар	Разбор финального задания Итоги программы	2
		Итого за неделю		**2**
			Итого	**124**