Расписание групп

Аналитик SOC 2 линии

Длительность обучения: 3,5 месяца

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

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

Номер недели	Вид	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	2
Неделя 1	Теория	Модуль "Организационная информация"	О программе: структура и форматы Какие компетенции будут приобретены, результаты обученияРабота 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	2,5
Неделя 1	Практика	Практика 1	Проверочное тестирование "Роли и функции SOC-центра"	0,5
		Итого за неделю		**6**
Неделя 2				
Неделя 2	Вебинар	Вебинар 2. Система развития	Матрица компетенций и карьерные треки	2
Неделя 2	Теория	Блок 2. Аудит информационной безопасности Модуль 2.1.Архитектура и механизмы аудита	Аудит типовой ИТ-инфраструктура, Архитектура аудита	3
Неделя 2	Теория	Блок 2. Аудит информационной безопасности Модуль 2.2. Расширенный аудит в ОС Windows	Стандартный и расширенный аудит ОС Windows Подсистема аудита Sysmon Сравнение подсистем аудита в ОС Windows Дополнительные журналы аудита ОС Windows Windows Event Collector, Windows Event Forwarding	3
Неделя 2	Практика	Практика 2	Механизмы аудита Журналы аудита Windows	4
Неделя 2	Теория	Блок 2. Аудит информационной безопасности Модуль 2.3. Расширенный аудит в Linux ОС	Стандарт Syslog Подсистема аудита Auditd Примеры применения аудита ОС Linux в корпоративных сетях	3
		Итого за неделю		**15**
Неделя 3				
Неделя 3	Теория	Блок 2. Аудит информационной безопасности Модуль 2.4. Нестандартный аудит в Linux ОС	Falco, Sysmon for linux и\или другие Дерхенеуровневое сравнение их между собой и с auditd	3
Неделя 3	Практика	Практика 3	Практическое задание "Настройка расширенного аудита"	4
Неделя 3	Теория	Блок 2. Аудит информационной безопасности Модуль 2.5. Расширенный и нестандартный аудит на примере ОС Astra Linux	Настройка подсистемы аудита в Astra Linux	3
Неделя 3	Практика	Практика 4	Практическая работа Настройка подсистемы аудита в Astra Linux	2
Неделя 3	Теория	Блок 2. Аудит информационной безопасности Модуль 2.6. Аудит СЗИ	Подключение источников события KSC и других СЗИ	3
		Итого за неделю		**15**
Неделя 4				
Неделя 4	Вебинар	Вебинар 3. Аудит ИБ	Аудит ИБ Q&A	3
Неделя 4	Теория	Блок 3. Сбор событий с ИТ-систем и СЗИ Модуль 3.1. Подключение источников событий к SIEM	Подключение источников событий к SIEM	6
Неделя 4	Практика	Практика 5 на стенде с оценкой ментора	Подключение источников событий к SIEM	5
		Итого за неделю		**14**
Неделя 5				
Неделя 5	Вебинар	Вебинар 4. СЗИ	Покрытие ИТ-ландшафта СЗИ	3
Неделя 5	Теория	Блок 4. Мониторинг инцидентов Модуль 4.1. Подходы к разработке контента SIEM	- Последовательность обработки событий в SIEM - Контроль и управление EPS (включая агрегацию и фильтрацию) - Знакомство с функционалом корреляции SIEM - Методология структуры контента SIEM - Создание аналитического контента	3

Неделя 5	Теория	Блок 4. Мониторинг инцидентов Модуль 4.2.Работа с контентом SIEM	Методология разработки и эксплуатации контента SIEM - Разработка правил нормализации. Типы событий, парсеры. Регулярные выражения. - Обогащение событий. Источники данных для обогащения. Разработка правил обогащения. - Профилирование активности средствами SIEM. Использование табличных списков. - Влияние контента на производительность SIEM - Генерация отчётов и визуализация в SIEM - Тестирование сценариев	3
Неделя 5	Практика	Практика 6 на стенде с оценкой ментора	Разработка контента SIEM	5
		Итого за неделю		**11**
Неделя 6				
Неделя 6	Вебинар	Вебинар 5. Мониторинг инцидентов	Работа с контентом SIEM	3
Неделя 6	Теория	Блок 4. Мониторинг инцидентов Модуль 4.3.Инструменты дополнительного выявления и расследования инцидентов ИБ	Инструменты дополнительного выявления и расследования инцидентов ИБ - WAF - NTA - EDR - (?)	3
Неделя 6	Практика	Практика 7 на стенде с оценкой ментора	Выявление и расследование инцидентов	5
		Итого за неделю		**11**
Неделя 7				
Неделя 7	Вебинар	Вебинар 6. Работа с SIEM	Базовые, профилирующие и технические правила. Профилирование активности. Обогащение событий.	3
Неделя 7	Теория	Блок 4. Мониторинг инцидентов Модуль 4.4.Обнаружение кибератак	- Разработка инцидентных правил корреляции. Агрегация инцидентов. - Разработка правила Workflow, управление конфигурацией сценария. - Добавление исключений в работу сценария	3
Неделя 7	Теория	Блок 4. Мониторинг инцидентов Модуль 4.5.Детектирование атак	- Методологии атак (Матрица MITRE ATT&CK. Модель Cyber Kill Chain и др) - Web-атаки	3
Неделя 7	Практика	Практика 8 на стенде с оценкой ментора	Детектирование атак с использованием SIEM-системы	5
		Итого за неделю		**14**
Неделя 8				
Неделя 8	Вебинар	Вебинар 7. Атаки и Use Cases	Выявление компьютерных атак. Создание правил, скриптов и механизмов визуализации в SIEM-системе	3
Неделя 8	Теория	Блок 5. Реагирование на инциденты. Модуль 5.1. Реагирование на инциденты	Методологии и инструменты реагирования на инциденты. Механизмы взаимодействия SOC с банковскими и государственными структурами на примере ФинЦЕРТ (Банк России) и НКЦКИ (ГосСОПКА)	3
Неделя 8	Практика	Практика 9 на стенде с оценкой ментора	Реагирование на инциденты	5
		Итого за неделю		**11**
Неделя 9				
Неделя 9	Вебинар	Вебинар 8. Реагирование	Реагирование на инциденты	2
Неделя 9	Теория	Блок 6. Киберразведка и поиск следов взлома корпоративной инфраструктуры Модуль 6.1. Киберразведка (TI)	- OSINT Разведка по открытым источника информации - Инструменты OSINT - Практическое задание - TIP Киберразведка актуальных угрозах с целью прогнозирования вероятных атак и их предотвращения (Threat Intelligence) - Источники аналитики (feeds) и уровни доверия к ним. Подходы по работе с фидами. - Методология и процессы анализа и поиска угроз. Взаимосвязь процессов анализа и поиска угроз с другими процессами	3
	Теория	Блок 6. Киберразведка и поиск следов взлома корпоративной инфраструктуры Модуль 6.2. Разведка киберугроз (TH)	Проактивный поиск следов взлома или функционирования вредоносных программ (Threat hunting)	3
Неделя 9	Практика	Практика 10	Работа с отчётами SIEM-системы и индикаторами компрометации (IoC)	5
Неделя 9	Практика	Практика 11 на стенде с оценкой ментора	Проактивное обнаружение вредоносной деятельности в компьютерных сетях	3
		Итого за неделю		**16**
Неделя 10				
Неделя 10	Вебинар	Вебинар 9. Threat Intelligence и Threat hunting	Threat Intelligence и Threat hunting	2
Неделя 10	Практика	Финальное задание на стенде с оценкой ментора		10
		Итого за неделю		**12**
Неделя 11				
Неделя 11	Вебинар	Вебинар 10. Итоги	Разбор финального задания Подведение итогов	2
		Итого за неделю		**2**
			Итого	**127**