ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «РОСТОВСКИЙ ЦЕНТР ПОВЫШЕНИЯ КВАЛИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ»

«УТВЕРЖДАЮ»
Директор
ЧОУ ДПО «РЦПК ИТС»

_____ С.Д. Мармоленко

«___»_____2022 г.

Программа дополнительного профессионального образования

«Развертывание системы мониторинга предприятия»

Ростов-на-Дону

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая программа дополнительного образования «Развертывание системы мониторинга предприятия» (далее - программа) разработана ООО «Солар Секьюрити», компания группы ПАО «Ростелеком»с учётом требований: Федерального закона от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», «Доктрины информационной безопасности Российской Федерации», утвержденной Указом Президента РФ № 646 от 05.12.2016 г., Федерального закона от 28.12.2010 г. № 390-ФЗ «О безопасности», Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», «Методических рекомендаций по разработке программ профессиональной переподготовке и повышения квалификации специалистов, работающих в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры. противодействия иностранным техническим разведкам и технической защите информации», утвержденных ФСТЭК России 04.04.2015 г. и примерной программы повышения квалификации, разработанной Минтруда Российской Федерации (письмо Минтруда РФ от 09.09.2013 г.).

2 ЦЕЛЬ РЕАЛИЗАЦИИ ПРОГРАММЫ

Целью обучения по программе является изучение специалистами современных способов управления инцидентами информационной безопасности, получение навыков работы с множеством источников событий аудита ИБ, получение навыков работы в SIEM-системе на продвинутом уровне, получение навыков написания контента для выявления инцидентов ИБ.

Обучающиеся по программе повышения квалификации готовятся к осуществлению следующих профессиональной видов деятельности: аналитик мониторинга Security Operations Center.

Объектами профессиональной деятельности обучающихся являются корпоративные сети.

Поставленная цель достигается решением следующих задач:

Предподготовка по введению в аудит ИБ, категориям и приоритетам событий, архитектурам и механизмам аудита, расширенному аудиту ОС Windows, технологиям Windows Event Forwarding и Windows Event Collector, Sysmon. Также, изучаются типовые корпоративные инфраструктуры в контексте аудита источников в ней.

Изучение и практическая отработка навыков по работе с типовыми источниками событий аудита (ОС Windows, ОС Linux, приложения), практика применения аудита в корпоративных сетях;

Изучение методологии SOC – линии, экспертиза, метрики, процессы.

Изучение последовательности обработки событий в SOC.

Изучение языка написания контента XP в PT MP SIEM. Изучение методологии работы с контентом, структуры контента. Изучение формул нормализации, правил обогащения, правил корреляции.

Навыки контроля за состоянием мониторинга ИБ в корпоративной сети. Ведение статистики срабатываний правил корреляции. Профилирование активности. Работа с исключениями.

Также изучаются другие аспекты работы SOCи аспекты роли аналитика SOC.

3 ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ ПОСТУПАЮЩЕГО НА ОБУЧЕНИЕ

Уровень образования лица, поступающего на обучение:среднеепрофессиональное или высшее образование по специальностям в области информационной безопасностии/или информационных технологий.

Наличие опыта работы по специальности как минимум 2 года.

Желательно наличие первичных навыков работы с SIEM-системами и расследованием инцидентов ИБ.

4 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

В данном курсе собраны лучшие практики подготовки аналитиков SOC, которые обладают широким набором знаний и навыков, способны работать с SIEM-системой на уровне контента для выявления инцидентов ИБ в корпоративной сети.

На курсе будет использоваться MaxPatrol SIEM, при этом, полученные знания можно будет применять в работе с любой другой SIEM-системой.

Знания, умения и навыки, полученные в ходе прохождения программы «Развёртывание системы мониторинга предприятия», являются необходимыми и достаточными для того, чтобы приступить к работе младшего аналитикаSOC с потенциалом профессионального роста до старшего аналитика SOC.

Слушатель по итогам обучения должен:

а) знать:

- Методологию SOC, метрики;
- Подходы к разработке контента, управлению контентом SIEM;
- Компоненты SIEM, их функционал, жизненный цикл события в SIEM;
- Особенности решений класса XDR;

б) уметь:

- Проводить анализ источника событий на предмет его полезности, определить категории событий от источника;
- Подключать источник событий к SIEM-системе

- Написать правило корреляции и сопутствующий контент, направленный на выявление отдельной угрозы ИБ;
- Сформировать карточку сценария выявления инцидента ИБ;

в) иметь навыки:

- Инвентаризации источников событий в корпоративной сети;
- Приоритезации и категорирования типов событий и источников;
- Оценивать активность на предмет её соответствия тактикам и техникам матрицы MITRE;
- Вносить исключения в работу правила корреляции.

5 ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Компьютерный класс ЧОУ ДПО «РЦПК ИТС» оснащен компьютерным оборудованием, проектором, доступом в сеть Интернетдля проведения лекционных и практических занятий.

Формирование профессиональных компетенций обеспечивается широким использованием в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, ролевых игр, разбора конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Программа повышения квалификации предусматривает проведение занятий в соответствии с целевыми установками программы, которые обеспечивают требуемый уровень усвоения учебного материала. Знания приобретаются путем прослушивания лекций в формате семинаров и вебинаров(с использованием системы проведения вебинаров), а также в ходе самостоятельного изучения материалов на платформе для дистанционного обучения (LMS). Практические навыки и умения слушатели курса в индивидуальном порядке и в составе групп получают при выполнении практическихи лабораторных работ, для чего предоставляется защищенный доступ с компьютеров ЧОУ ДПО «РЦПК ИТС», рабочих мест или домашних компьютеров к Киберполигону, на котором развернут тренировочный стенд с MaxPatrol SIEM. Для оперативного ответа на вопросы и соответствующих обсуждений используется групповой чат в Телеграм.

Для обучающихся обеспечивается доступ к информационным справочным и поисковым системам по тематике информационной безопасности.

Изменения и дополнения вносятся в программу постоянно, по мере актуализации ИБ-угроз и появления новых инструментов их мониторинга и предотвращения.

С целью текущего контроля знаний в ходе практических занятий проводятся выборочные опросы и используются различные приёмы тестирования.

Преподаватели, осуществляющие обучение по данной программе, имеют образование, соответствующее профилю преподаваемой дисциплины

(в сфере защиты информации), конкретный опыт реализации разработок и иной формы практической деятельности в области информационной безопасности, непосредственно в Security Operations Center.

6 ФОРМЫ АТТЕСТАЦИИ И ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Контрольно-проверочные мероприятия включают посещаемость и принятие активного участия на онлайн-занятиях, прохождение курсов и выполнение тестов в СДО. Освоение обучающимися программы повышения квалификации завершается итоговой аттестацией в форме теста по теоретическим вопросам и выполнения итогового практического задания.

Критерии оценки результатов финального практического задания: хронология и детализация описания, логика повествования, интерпретация активности, наличие релевантных выводов и рекомендаций. Преимуществом будет указание фильтров поиска, которые использовались для расследования, и скриншотов (при их целесообразности).

Курсы и тесты по базовым темам организованы таким образом, чтобы выровнять различия в компетенциях обучающихся, чтобы группа обучающихся проходила программу, исключая возможную неуспеваемость отдельных обучающихся.

Также, занятия подразумевают наличие самостоятельных заданий, которые выполняются в свободное время от занятий. Качество и количество выполненных заданий учитываются при подготовкесводного отчёта о проведённом обучении.

Для проведения контрольно-проверочных занятий образовательным учреждениемразработаны тестовые задания, включающие вопросы для тестирования (не менее 30 вопросов для итогового теста).

Для успешного прохождения тестирования и получения оценки «зачтено» необходимо набрать не менее 70 баллов.

Ответ на вопрос считается правильным, если он является полным.

Тест включает в себя вопросы, направленные как на контроль знаний, так и на проверку полученных навыков работы. Во время тестирования запрещается пользоваться какой-либо литературой.

При проведении тестирования с использованием электронных форм контроля и оценки у каждого слушателя есть три попытки напрохождение тестирования. Время на одну попытку - 120 минут. По окончанию попыткислушатель может видеть результаты теста и полученные баллы. Также имеется возможность просмотра отчета, показывающегоошибки при прохождении теста. Оценка выставляется по последней попытке.

Лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдаются удостоверения о повышении квалификации.

Лицам, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы повышения квалификации и (или) отчисленным

из организации, выдается справка об обучении или о периоде обучения, по установленному образцу.

7 УЧЕБНЫЙ ПЛАН ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

7.1 Уровень образования лица, поступающего на обучение – среднее профессиональное / высшее образование по специальностям в области информационной безопасности или информационных технологий.

7.2 Срок обучения: 116 часов

7.3Форма обучения:

смешанная — часть времени отводится аудиторному обучению в очном формате, также занятия проводятся с использованием дистанционных технологий обучения в соответствии с действующей нормативной базой.

7.4 План учебного процесса.

№ п/п	Наименование учебных модулей, тем	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
1	2	3	4	5	6	7	8	9	10	11
1.	**Сбор событий ИБ**	**6**	**0**	**0**	**0**	**0**	**0**	**0**	**6**	**-**
1.1	Цели аудита.	1,5	0	0	0	0	0	0	1,5	
1.2	Категории и приоритеты событий	1,5	0	0	0	0	0	0	1,5	
1.3	События кибербезопасности	2	0	0	0	0	0	0	2	
1.4	Архитектура и механизмы аудита	1	0	0	0	0	0	0	1	
2	**Расширенный аудит в ОС Microsoft Windows**	**13,5**	**6**	**5,5**	**0,5**	**0**	**4,5**	**0**	**3**	
2.1	Лабораторнаяработа "Advanced OS Windows audit"	2	0	0	0	0	2	0	0	
2.2	Подсистема аудита Sysmon	4,5	2	2	0	0	0	0	2,5	
2.3	Сравнение стандартного аудита ОС Windows и Sysmon	1,5	1,5	1,5	0	0	0	0	0	
2.4	Дополнительные журналы аудита ОС Windows	2	2	2	0	0	0	0	0	
2.5	Windows Event Collector	3,5	0,5	0	0,5	0	2,5	0	0,5	
3	**Расширенный аудит в Linux ОС**	**3**	**3**	**1,5**	**1,5**	**0**	**0**	**0**	**0**	
3.1	Аудит Syslog	0,5	0,5	0,5	0	0	0	0	0	
3.2	Подсистема аудита Auditd	2	2	0,5	1,5	0	0	0	0	

3.3	Примеры применения аудита ОС Linux в корпоративных сетях	0,5	0,5	0,5	0	0	0	0	0	
4	**Сбор событий с типовых ИТ систем и средств защиты информации**	**17**	**10**	**0**	**1**	**9**	**0**	**0**	**7**	
4.1	Аудит типовой корпоративной ИТ-инфраструктуры	5	0	0	0	0	0	0	5	
4.2	Аудит типовой ИБ-инфраструктуры	2	0	0	0	0	0	0	2	
4.3	Настройка аудита источников	4,5	4,5	0	0,5	4	0	0	0	
4.4	Механизмы и транспорты передачи/получения событий	1,5	1,5	0	0,5	1	0	0	0	
4.5	Подключение источников к SIEM	3	3	0	0	3	0	0	0	
4.6	Диагностика и решение проблем при подключении источников к SIEM	1	1	0	0	1	0	0	0	
5	**Базовые подходы к разработке контента SIEM**	**31,5**	**31,5**	**15,5**	**5**	**11**	**0**	**0**	**0**	
5.1	Задачи L3 и L4 в Security Operations Center, компетенции	0,5	0,5	0,5	0	0	0	0	0	
5.2	Реестр сценариев	1	1	1	0	0	0	0	0	
5.3	Статистика, Customer KB	1,5	1,5	1,5	0	0	0	0	0	
5.4	Последовательность обработки событий	1,5	1,5	1,5	0	0	0	0	0	
5.5	Иерархия правил корреляции	5	5	5	0	0	0	0	0	
5.6	Инцидентные правила корреляции	3	3	3	0	0	0	0	0	
5.7	Правило типа Workflow	1,5	1,5	1,5	0	0	0	0	0	
5.8	Синтаксис языка XP	3	3	0	3	0	0	0	0	
5.9	Нормализация событий	1	1	0	1	0	0	0	0	
5.10	Практическое задание по нормализации событий	7	7	0	1	6	0	0	0	
5.11	Влияние контента на производительность SIEM	1	1	1	0	0	0	0	0	
5.12	Перенос контента между инсталляциями	0,5	0,5	0,5	0	0	0	0	0	
5.13	Генерация отчетов средствами MP SIEM	2,5	2,5	0	0	2,5	0	0	0	
5.14	Визуализация в MP SIEM	2,5	2,5	0	0	2,5	0	0	0	
6	**Практика обнаружения кибератак**	**37**	**37**	**4**	**9**	**24**	**0**	**0**	**0**	
6.1	Рабочий процесс обработки инцидента ИБ	1	1	1	0	0	0	0	0	
6.2	Мониторинг обработки событий и EPS, фильтры событий	0,5	0,5	0,5	0	0	0	0	0	
6.3	Практическое задание по написанию базовых и профилирующих правил	12	12	1	1	10	0	0	0	
6.4	Практическое задание по написанию инцидентных правил	9	9	0	1	8	0	0	0	
6.5	Добавление исключений	2	2	0	2	0	0	0	0	
6.6	Практика по внесению исключений в правила	6	6	0	1	5	0	0	0	
6.7	System Health	0,5	0,5	0,5	0	0	0	0	0	
6.8	Методология расследования инцидентов	4	4	0	4	0	0	0	0	
6.9	Анализ уведомлений об инцидентах	2	2	1	0	1	0	0	0	
7	**Решение класса XDR: защита от кибератак**	**8**	**10**	**0**	**5**	**3**	**0**	**0**	**0**	
7.1	Администрирование KATA	2	3	0	1	1	0	0	0	
7.2	Анализ событий KATA	3	3	0	2	1	0	0	0	
7.3	Реагирование на инциденты ИБ с использованием данных инструментов	3	4	0	2	1	0	0	0	

8	**Итоговая аттестация**	**4**	**-**	**-**	**-**	**4**	**-**	**-**	**-**	**Финальное практическое задание; Тест**
	Итого:	**116**	**97,5**	**26,5**	**22**	**47**	**4,5**	**0**	**16**	

8 КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Сроки проведения занятий	Количество рабочих недель	Количество занятий в неделю	Количество занятий в курсе	Продолжительность занятия (в часах)	Сроки итоговой аттестации
Устанавливаются решением руководителя учреждения по мере формирования групп	5	5	29	6 (40 минут отводится на обед)	в конце 5-й недели

9 РАБОЧАЯ ПРОГРАММА УЧЕБНОГО КУРСА

9.1 Содержание учебных модулей, тем.

Тема № 1. Сбор событий ИБ

В данном разделе необходимо рассмотреть цели сбора событий ИБ, какие типы событий будут полезны с точки зрения кибербезопасности.

Тема № 2. Расширенный аудит в ОС Microsoft Windows.

Необходимо рассмотреть особенности работы с событиями в Windows, включая серверные и пользовательские версии ОС, сравнение стандартных логов и Sysmon, продвинутый аудит на контроллерах домена. Слушатели курса должны узнать о различных архитектурах централизованного сбора событий ИБ, Windows Event Forwarding и механизмах конфигурации источников событий.

Тема № 3. Расширенный аудит в Linux ОС.

В данном разделе необходимо сделать обзор основных возможностей в ОС Linux, рассматриваются особенности конфигурации, возможности расширенного аудита. Слушатели должны на практике познакомятся с механизмами конфигурации источников событий и построению архитектуры централизованного сбора событий ИБ.

Тема № 4. Сбор событий с типовых ИТ систем и средств защиты информации.

Помимо операционных систем, важными источниками событий ИБ являются различные ИТ системы и средства защиты информации. В данном разделе должны быть рассмотрены основные типы событий, которые будут интересны для SOC, и особенности их сбора, доставки и нормализации в SIEM.

Тема № 5. Базовые подходы к разработке контента SIEM.

В данном разделе необходимо рассмотреть полный жизненный цикл события ИБ в MaxPatrol SIEM: от его сбора и нормализации, до его обогащения, корреляции и создания инцидента. Также необходимо рассмотреть вопросы профилирования активности и добавление её в исключения правил корреляции, разработка отчетов на основе ранее созданных профилей и разработка дашбордов», разработка отчетов на основе ранее созданных профилей и разработка дашбордов.

Тема № 6. Практика обнаружения кибератак.

В данном разделе необходимо рассмотреть примеры кибератак, способы их обнаружения, основные инструменты киберпреступников. Рассказать о классификации атак на примере кейсов SOC. Рассказать о способах детектирования сетевых атак, специфических атак на инфраструктуру компаний, инструментах злоумышленников. Рассмотреть нетиповые кейсы — расследование и решение.

Тема № 7. Решение класса XDR: защита от кибератак.

В данном разделе необходимо рассмотреть вопросы администрирования KasperskyAntiTargetedAttack, анализ событий KasperskyAntiTargetedAttack, реагирование на КИ с использованием данных инструментов.

9.2 Учебно-методическое и информационное обеспечение учебного курса

Основная литература:

1. "Синтаксис языка запросов PDQL", PositiveTechnologies, 151 стр, 2022 г.
2. "Руководство разработчика", PositiveTechnologies, 281 стр, 2022 г.
3. "Настройка источников", PositiveTechnologies, 1342стр, 2022 г.
4. Управление инцидентами и событиями информационной безопасности. URL: https://safe-surf.ru/specialists/article/5236/611719/
5. NIST Incident Response: Your Go-To Guide to Handling Cybersecurity Incidents. URL: https://www.auditboard.com/blog/nist-incident-response/
6. NIST Incident Response Plan: Building Your Own IR Process Based on NIST Guidelines. URL: https://www.cynet.com/incident-response/nist-incident-response/
7. NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide. Paul Cichonski, Thomas Millar, Tim Grance, Karen Scarfone. August 2012. URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
8. ISO/IEC 27035-2:2016. Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response. URL: https://www.iso.org/standard/62071.html
9. ISO/IEC 27035-3:2020. Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations. URL: https://www.iso.org/standard/74033.html

10. Проект стандарта. Руководство по реагированию на инциденты в сфере информационных и компьютерных технологий. URL: https://fstec.ru/en/component/attachments/download/3042
11. Проект стандарта. ОБНАРУЖЕНИЕ, ПРЕДУПРЕЖДЕНИЕ И ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК И РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ. URL: https://fstec.ru/en/component/attachments/download/2770
12. The 7 stages of effective incident response. URL: https://www.atlassian.com/incident-management/incident-response
13. THE USE OF AUDIT TRAILS IN SECURITY SYSTEMS: GUIDELINES FOR EUROPEAN BANKS. European Payments Council, 2 June 2010, 34 pages
14. Twenty Critical Controls for Effective Cyber Defense:Consensus Audit Guidelines. NIST. August 10, 2009. 49 pages.
15. Windows Event Logging and Forwarding. Australian Cyber Security Centre. January 2019. 19 pages.

Дополнительнаялитература:

1. DISRUPTING THE CYBER KILL CHAIN: HOW TO CONTAIN USE OF TOOLS AND PROTOCOLS, CrowdStrike White Paper, 6 pages, 2020
2. Silence Moving into the darkside, Group-IB, 87 страниц, Сентябрь 2018
3. COBALT STRIKES BACK: AN EVOLVING MULTINATIONAL THREAT TO FINANCE, Positive Technologies, 19 pages, 2017
4. ISO/IEC 27035-2:2016. Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response. URL: https://www.iso.org/standard/78974.html
5. ISO/IEC 27035-3:2020. Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations. URL: https://www.iso.org/standard/74033.html
6. NIST Special Publication 800-61. Computer Security Incident Handling Guide. / Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone / August 2012

9.3 Материально-техническое обеспечение учебного курса

Наименование специализированных аудиторий, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Специализированный учебный класс ЧОУ ДПО «РЦПК ИТС»	Лекции, вебинары, дистанционное обучение, практические занятия, лабораторные работы	Автоматизированное рабочее место преподавателя и компьютерный класс, принтер. Проектор LCD. Экран. LMS. Система для проведения вебинаров. Стенд MaxPatrol SIEM на Киберполигоне. Групповой чат в Телеграм.

9.4 Примерные вопросы контроля знаний

1. Какой из компонентов PT MaxPatrol SIEM осуществляет сбор событий с источников?
2. Как распределяются задачи и компетенции между линиями SOC?
3. Какие стадии проходит событие от генерации события на конечной системе до закрытия инцидента после этапа реагирования?
4. Какая активность происходит в процессе подключения с помощью утилиты PsExec?
5. Какие транспорты могут использоваться для сбора событий средствами SIEM?
6. Как происходит написание и тестирование формулы нормализации в SIEM?
7. Какую роль играет обогащение событий в MPSIEM?
8. Какие категории правил корреляции могут встречаться в SIEM? Какие цели выполняет каждая категория правил?
9. Чем профиль отличается от списка исключений?
10. Каким образом KATAполучает источники данных для анализа?