Внедрение и работа в DevSecOps

Длительность курса: 128 академических часов

1 Модель “защита всех слоев” и архитектура Dev|Sec|Ops

1 **Введение в безопасность cloud-native приложений и облачной инфраструктуры**

- Модели безопасности приложений и инфраструктуры
- Отличия традиционной модели от модели защиты в облаке
- Разделение зон ответственности в модели защиты в облаке
- Словарь, термины и объекты используемые в инструментах

Домашние задания

1. Изучить требования которые определяют DevSecOps (написать статью в корпоративный Security Knowledge Base Portal)

---

2 **Обзор архитектуры DevSecOps тулчейна**

- Классификация инструментов используемых в DevSecOps
- Точки внедрения инструментов в CI/CD тулчейн

Домашние задания

1. Изучить существующие Managed Cloud SaaS для CI/CD (GitLab, CircleCI и др) на предмет наличия в них ИБ и подготовить сравнительную таблицу (написать статью в корпоративный Security Knowledge Base Portal)

2 Необходимый базис знаний ИБ

1 **Список видов слабостей исходного программного кода (CWE)**

- Словарь, термины и элементы знаний используемых в CWE
- Использование CWE в инструментах ИБ
- Статистика и тренды изменений CWE за последние годы

Домашние задания

1. Изучить в деталях один из CWE из OWASP/SANS списков для выбранного языка программирования, изучить методы устранения в исходном коде приложения (написать статью в корпоративный Security Knowledge Base Portal)

---

2 **База данных уязвимостей и воздействий в готовых продуктах (CVE)**

- Словарь, термины и элементы знаний используемых в CVE
- Использование CVE в инструментах И
- Статистика и тренды изменений CVE за последние годы

Домашние задания

1. Для ранее изученного CWE составить список наиболее опасных / релевантных CVE, изучить методы устранения трех самых опасных CVE (написать статью в корпоративный Security Knowledge Base Portal)

---

3 **Соответствие стандартам (Compliance) и упрочение конфигурации (Hardening)**

- Основные стандарты, методики, источники информации - ISO, NIST, CIS, PCI DSS, CCM и др.
- Использование Compliance стандартов для упрочения конфигурации (Hardening) инфраструктуры
- Использование Compliance стандартов для упрочения конфигурации (Hardening) стека приложений

Домашние задания

1. Прочитать стандарты NIST 800-53, CIS AWS Foundations Benchmark, CIS AWS Three-tier Web Architecture, CIS Amazon Linux (написать статью в корпоративный Security Knowledge Base Portal с кратким обзором стандартов)

3 Безбарьерное внедрение инструментов ИБ в DevOps

1	**Программа и инструменты начального обучения специалистов при переходе к DevSecOps**	- Области знаний и инструменты для обучения для разработчиков стека приложений - Области знаний и инструменты для обучения для разработчиков облачной инфраструктуры - Области знаний и инструменты для обучения DevOps / SRE инженеров - Области знаний и инструменты для обучения для специалистов по ИБ (аналитиков, пен-тестеров и тп)
2	**Статический анализ на безопасность исходного кода (SAST) - теория и инструментарий**	- Технические требования к SAST для пригодности DevSecOps - Обзор процедуры загрузки приложения AppStack в SAST - Анализ приложения и создание модели угроз (Threat modeling) - Конфигурация SAST на основе данных из модели угроз - Проведение начального сканирования приложения - Анализ результатов и тюнинг конфигурации SAST - Проведение последующих инкрементных сканирований приложения - Автоматизация процесса сканирования и выпуска баг тикетов в CI/CD - Обзор процедуры анализа кода инфраструктуры Cloud Infrastructure (Infrastructure as Code) на примере темплейта AWS CloudFormation и YML Kubernetes

3	**Статический анализ на безопасность исходного кода (SAST) - практика применения и лабораторная работа**	- Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру работы с SAST изученную в рамках вебинара для другого приложения, определить и изучить три самые опасные CWE, определить методы устранения в исходном коде (написать список найденных CWE и методов устранения)
4	**Динамический анализ на безопасность готовых Мобильных и IoT приложений (DAST) - теория и инструментарий**	- Технические требования к DAST для пригодности DevSecOps - Обзор процедуры загрузки приложения в DAST - Технические требования к SAST для пригодности DevSecOps - Анализ приложения и создание модели угроз (Threat modeling) - Конфигурация DAST на основе данных из модели угроз - Проведение начального сканирования приложения - Анализ результатов и тюнинг конфигурации DAST - Проведение последующих инкрементных сканирований приложения - Автоматизация процесса сканирования и выпуска баг тикетов в CI/CD

5	**Динамический анализ на безопасность готовых Мобильных и IoT приложений (DAST) - практика применения и лабораторная работа**	- Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру работы с DAST изученную в рамках вебинара для другого приложения, определить и изучить три самые опасные уязвимости конфигурации или некорректного поведения приложения, определить методы устранения в исходном коде прилож
6	**Интерактивный анализ на безопасность приложений (IAST) - теория и инструментарий**	- Технические требования к IAST для пригодности DevSecOps - Обзор процедуры загрузки приложения в IAST - Конфигурация IAST на основе данных из модели угроз и обнаруженных в SAST CWE - Анализ результатов IAST, сравнение с результатами SAST, уточнение списка возможных атак

7	**Интерактивный анализ на безопасность приложений (IAST) - практика применения и лабораторная работа**	- Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру работы с IAST изученную в рамках вебинара для другого приложения, определить и изучить три самые опасные уязвимости конфигурации или некорректного поведения приложения, определить методы устранения в исходном коде прилож
8	**Анализ на безопасность стороннего и открытого программного обеспечения (SCA) - теория и инструментарий**	- Технические требования к SCA для пригодности DevSecOps и cloud-native security - Обзор процедуры загрузки cloud-native приложения в SCA - Обзор процедуры загрузки инфраструктуры Cloud Infrastructure (Infrastructure as Code) в SCA - Конфигурация SCA на основе требований к соответствию стандартам, допустимых уязвимостей, лицензионной чистоте, и др. - Анализ результатов сканирования cloud-native приложения AppStack - Анализ результатов сканирования инфраструктуры Cloud Infrastructure - Автоматизация процесса сканирования SCA и выпуска баг тикетов в CI/CD

9	**Анализ на безопасность стороннего и открытого программного обеспечения (SCA) - практика применения и лабораторная работа**	- Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру работы с SCA изученную в рамках вебинара для другого среза приложения (части микросервера), определить и изучить три самые опасные уязвимости конфигурации, CVE, лицензионной чистоты. Определить методы устранения в исходн
10	**Тестирование на проникновение (Penetration Testing) - теория и инструментарий**	- Технические требования к Penetration Testing инструментам для пригодности DevSecOps - Обзор процедуры сканирования cloud-native приложения AppStack и инфраструктуры Cloud Infrastructure автоматизированными средствами - Обзор процедуры ручного теста ранее найденных уязвимостей - Обзор процедуры автоматизированного и ручного сканирования REST API - Проведение автоматизированного и ручного тестирования - Анализ результатов тестирования комплекса AppStack (включая REST API + Cloud Infrastructure)

11	**Тестирование на проникновение (Penetration Testing) - практика применения и лабораторная работа**	- Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру работы с Penetration Testing инструментам изученную в рамках вебинара. Сравнить со списком уязвимостей обнаруженных в рамках SAST, DAST, IAST, SCA тестов (написать уточненный список найденных уязвимостей)
12	**Усиление конфигурации и Патчи (Hardening and Pathing) - теория и инструментарий**	- Обзор альтернатив hardening cloud-native приложения AppStack - Обзор альтернатив hardening инфраструктуры Cloud Infrastructure - Анализ результатов сканирования SCA - Проведение ряда изменений конфигурации и патчинг (замена на более усиленный EC2, коррекция конфигурации Kubernetes, Docker engine, Docker Image, патчинг библиотек приложения) - Проведение повторного сканирования SCA для подтверждения успешности проведенных изменений

13	**Усиление конфигурации и Патчи (Hardening and Pathing) - практика применения и лабораторная работа**	Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру hardening изученную в рамках вебинара для другого среза приложения (части микросервера), написать список уязвимостей и соответствующих им проведенных изменений.
14	**Cloud-natice Web-Application Файервол (WAF) - теория и инструментарий**	- Технические требования к Cloud-native Web-Application Firewall инструментам для пригодности DevSecOps - Обзор и сравнение WAF предоставляемых Cloud вендорами и компаниями-экспертами - Особенности и варианты атак на REST API - Обзор методов защиты REST API с помощью специализированных WAF - Создание конфигурации WAF для защиты REST API - Проведение атаки на REST API до и после введения конфигурации WAF

15	**Cloud-natice Web-Application Файервол (WAF) - практика применения и лабораторная работа**	- Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру создания конфигурации WAF для защиты REST API изученную в рамках вебинара для другого REST API, привести WAF конфигурацию и список проведенных тестов.
16	**Система обнаружения / предотвращений вторжений (IDS/IPS) - теория и инструментарий**	- Технические требования к IDS/IPS инструментам для пригодности cloud-native приложений и DevSecOps - Обзор и сравнение IDS/IPS предоставляемых Cloud вендорами и компаниями-экспертами - Обзор методов защиты cloud-native приложений с помощью новейших IDS/IPS, использующих машинное обучение (ML) и подход “white list” - Создание конфигурации IDS/IPS для защиты стека приложения - Проведение атаки на приложение до и после введения конфигурации IDS/IPS - Автоматизация процесса нотификаций IDS/IPS и выпуска баг тикетов в CI/CD - Автоматизация процесса изоляции поврежденной части приложения для последующего анализа с помощью Forensic Analysis

17	**Система обнаружения / предотвращений вторжений (IDS/IPS) - практика применения и лабораторная работа**	- Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру создания конфигурации IDS/IPS для защиты приложения изученную в рамках вебинара для другого среза приложения (части микросервера), написать список атак и соответствующих им проведенных изменений
18	**Мониторинг безопасности приложений и сети, Анализ в реальном времени событий и тревог ИБ (SIEM) - теория и инструментарий**	- Технические требования к SIEM инструментам для пригодности cloud-native приложений и DevSecOps - Обзор и сравнение SIEM предоставляемых Cloud вендорами и компаниями-экспертами - Особенности мониторинга стека cloud-native приложений - Особенности мониторинга инфраструктуры Cloud Infrastructure - Проведение внешней атаки на приложение аналогично вебинару посвященному IDS/IPS - Получение нотификации от SIEM, проведение поиска и анализа по лог файлам для стека приложений и инфраструктуры - Автоматизация процесса нотификаций SIEM и выпуска баг тикетов в CI/CD

19	**Мониторинг безопасности приложений и сети, Анализ в реальном времени событий и тревог ИБ (SIEM) - практика применения и лабораторная работа**	- Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру работы с SIEM, проведение поиска и анализа по лог файлам для стека приложений и инфраструктуры изученную в рамках вебинара для другого набора атак (проведенных преподавателями), написать список атак и соответствующих им
20	**Процедура анализа и автоматизированной реакции на ИБ события (SOAR) - теория и инструментарий**	- Технические требования к SOAR инструментам для пригодности cloud-native приложений и DevSecOps - Обзор и сравнение SOAR предоставляемых Cloud вендорами и компаниями-экспертами - Особенности мониторинга стека cloud-native приложений - Особенности мониторинга инфраструктуры Cloud Infrastructure - Проведение внешней атаки на приложение аналогично вебинару посвященному IDS/IPS - Автоматизация процесса устранения угрозы с помощью SOAR инструмента

21	**Процедура анализа и автоматизированной реакции на ИБ события (SOAR) - практика применения и лабораторная работа**	- Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру работы с SOAR в части автоматизации процесса устранения угрозы
22	**Криминалистическая экспертиза (Forensic Analysis) - теория и инструментарий**	- Технические требования к Forensic Analysis инструментам для пригодности cloud-native приложений и DevSecOps - Обзор и сравнение Forensic Analysis предоставляемых Cloud вендорами и компаниями-экспертами - Проведение внешней атаки на приложение аналогично вебинару посвященному IDS/IPS - Проведение поиска и низко-уровневого анализа воздействия атаки на стек приложения
23	**Криминалистическая экспертиза (Forensic Analysis) - практика применения и лабораторная работа**	- Задачи которые мы решаем и навыки, которые мы приобретаем в данной лабораторной работе - Демо выполнения лабораторной работы Домашние задания 1 Самостоятельно повторить процедуру работы с Forensic Analysis изученную в рамках вебинара для другого набора атак (проведенных преподавателями), написать список атак и соответствующих им следам воздействия на стек приложения

24	**Итоговое обзорное занятие по изученным инструментам**	- Обзор инструментов и их взаимного использования - Best Practice применения каждого инструмента - Как начать использовать и адаптировать инструменты в рабочий процесс

4 План и методика трансформации в DevSecOps

1	**План трансформации и практические шаги при переходе от DevOps к DevSecOps**	- План адаптации инструментов, бизнес-процессов и рабочих ролей - Особенности внедрения инструментов ИБ в CI/CD тулчейн и временные рамки успешного внедрения DevSecOps практики
2	**Коррекция зон ответственности и бизнес-процессов для успешного перехода к DevSecOps**	- Разделение зон ответственности команд - Коррекция бизнес-процессов DevOps для успешного перехода к DevSecOps
3	**Коррекция рабочих ролей для успешного перехода к DevSecOps**	- Изменение существующих ролей и введение новых - Best Practice и примеры из реального проекта трансформации в DevSecOps