Оглавление

Предисловие 16

Благодарности 20

О книге 22

Структура издания 22

О коде 24

От издательства 24

Об иллюстрации на обложке 25

Об авторе 25

Глава 1. Безопасность в DevOps 26

1.1. Методология DevOps 27

1.1.1. Непрерывная интеграция 30

1.1.2. Непрерывная поставка 30

1.1.3. Инфраструктура как сервис 30

1.1.4. Культура и доверие 32

1.2. Безопасность в DevOps 33

1.3. Непрерывная безопасность ... 35
1.3.1. Безопасность на основе тестирования ... 37
1.3.2. Мониторинг и реагирование на атаки ... 40
1.3.3. Оценка рисков и усиление безопасности ... 45
Резюме ... 46

Часть I. Пример применения уровней безопасности к простому DevOps-конвейеру

Глава 2. Выстраивание базового DevOps-конвейера ... 49
2.1. Реализация схемы ... 50
2.2. Репозиторий кода: GitHub ... 52
2.3. CI-платформа CircleCI ... 52
2.4. Репозиторий контейнеров Docker Hub ... 56
2.5. Инфраструктура среды эксплуатации Amazon Web Services ... 59
2.5.1. Трехуровневая архитектура ... 60
2.5.2. Настройка доступа к AWS ... 61
2.5.3. Virtual Private Cloud ... 62
2.5.4. Создание уровня баз данных ... 64
2.5.5. Создание первых двух уровней с помощью Elastic Beanstalk ... 66
2.5.6. Развертывание контейнера в ваших системах ... 70
2.6. Обзор безопасности ... 73
Резюме ... 74

Глава 3. Уровень безопасности 1: защита веб-приложений ... 75
3.1. Защита и тестирование веб-приложений ... 76
3.2. Атаки на сайты и безопасность контента ... 81
3.2.1. Межсайтовые сценарии и политика безопасности контента ... 81
3.2.2. Подделка межсайтовых запросов ... 89
3.2.3. Кликджекинг и защита плавающих фреймов ... 93
3.3. Методы аутентификации пользователей ... 95
3.3.1. Базовая HTTP-аутентификация ... 95
3.3.2. Обслуживание паролей ... 98

3.3.3. Поставщики идентификации ... 99
3.3.4. Безопасность сессий и cookie-файлов ... 105
3.3.5. Тестирование аутентификации ... 106
3.4. Управление зависимостями ... 106
3.4.1. Golang-вендоринг ... 107
3.4.2. Система управления пакетами Node.js ... 108
3.4.3. Требования Python ... 109
Резюме ... 111

Глава 4. Уровень безопасности 2: защита облачной инфраструктуры ... 112
4.1. Защита и тестирование облачной инфраструктуры: deployer ... 113
4.1.1. Настройка deployer ... 114
4.1.2. Настройка уведомлений между Docker Hub и deployer ... 115
4.1.3. Тестирование инфраструктуры ... 116
4.1.4. Обновление среды invoicer ... 117
4.2. Ограничение сетевого доступа ... 118
4.2.1. Тестирование групп безопасности ... 119
4.2.2. Налаживание доступа между группами безопасности ... 121
4.3. Создание безопасной точки доступа ... 123
4.3.1. Генерирование SSH-ключей ... 124
4.3.2. Создание хоста-бастиона в EC2 ... 126
4.3.3. Внедрение двухфакторной аутентификации с помощью SSH ... 128
4.3.4. Отправка уведомлений о доступе ... 134
4.3.5. Рассуждения о группах безопасности ... 137
4.3.6. Открытие доступа для групп безопасности ... 143
4.4. Управление доступом к базе данных ... 145
4.4.1. Анализ структуры базы данных ... 146
4.4.2. Роли и права доступа в PostgreSQL ... 147
4.4.3. Определение минимальных прав доступа для приложения invoicer ... 149
4.4.4. Определение прав доступа в deployer ... 154
Резюме ... 157

Глава 5. Уровень безопасности 3: защита каналов взаимодействия 158
5.1. Что такое защита каналов взаимодействия 159
5.1.1 Ранняя симметричная криптография 160
5.1.2. Алгоритм Диффи — Хеллмана и RSA 161
5.1.3. Инфраструктуры открытых ключей 164
5.1.4. SSL и TLS 165
5.2. Обзор SSL/TLS 166
5.2.1. Цепочка доверия 167
5.2.2. Установление TLS-соединения 168
5.2.3. Совершенная прямая секретность 170
5.3. Настройка приложений на использование HTTPS 171
5.3.1. Получение сертификата AWS 171
5.3.2. Получение сертификата Let's Encrypt 172
5.3.3. Применение HTTP на AWS ELB 174
5.4. Модернизация HTTPS 177
5.4.1. Тестирование TLS 179
5.4.2. Реализация руководств Mozilla Modern 181
5.4.3. HSTS: строгая защита транспорта 183
5.4.4. HPKP: закрепление открытых ключей 185
Резюме 188

Глава 6. Уровень безопасности 4: защита конвейера поставки 189
6.1. Распределение доступа к инфраструктуре управления кодом 193
6.1.1. Управление правами доступа в GitHub-организации 194
6.1.2. Управление правами доступа в GitHub и CircleCI 196
6.1.3. Подпись коммитов и меток с помощью Git 199
6.2. Управление доступом к хранилищу контейнеров 203
6.2.1. Управление правами доступа в пределах Docker Hub и CircleCI 203
6.2.2. Подписание контейнеров с помощью Docker Content Trust 206
6.3. Распределение прав доступа для управления инфраструктурой 207
6.3.1. Управление правами доступа с помощью ролей и политик AWS 208
6.3.2. Распределение закрытых данных в системах среды эксплуатации ... 212
Резюме 220

Часть II. Выявление аномалий и защита сервисов от атак

Глава 7. Сбор и хранение журналов ... 223
7.1. Сбор данных журналов из систем и приложений ... 226
7.1.1. Сбор журналов от систем ... 228
7.1.2. Сбор журналов приложения ... 232
7.1.3. Журналирование инфраструктуры ... 237
7.1.4. Сбор журналов от GitHub ... 240
7.2. Потоковая передача событий журналов с помощью брокеров сообщений ... 242
7.3. Обработка событий потребителями журналов ... 245
7.4. Хранение и архивация журналов ... 249
7.5. Анализ журналов ... 251
Резюме ... 255

Глава 8. Анализ журналов для выявления вторжений и атак ... 256
8.1. Архитектура уровня анализа журналов ... 257
8.2. Выявление атак с помощью строковых сигнатур ... 264
8.3. Статистические модели для обнаружения вторжений ... 269
8.3.1. Скользящие окна и циклические буферы ... 269
8.3.2. Скользящее среднее ... 272
8.4. Применение географических данных для обнаружения вторжений ... 276
8.4.1. Составление географического профиля пользователей ... 277
8.4.2. Вычисление расстояний ... 280
8.4.3. Нахождение области обычных соединений пользователя ... 281
8.5. Выявление аномалий в известных паттернах ... 283
8.5.1. Подпись пользовательского агента ... 283
8.5.2. Аномальный браузер ... 283
8.5.3. Паттерны взаимодействия ... 284
8.6. Отправка уведомлений администраторам и конечным пользователям ... 284
8.6.1. Информирование администраторов об угрозах безопасности ... 285
8.6.2. Как и когда уведомлять пользователей ... 289
Резюме ... 291

Глава 9. Обнаружение вторжений ... 292
9.1. Семь фаз вторжения: цепочка вторжения ... 293
9.2. Что такое указатели на вторжение ... 296
9.2.1. Правила Snort ... 297
9.2.2. Yara ... 298
9.2.3. OpenIOC ... 299
9.2.4. STIX и TAXII ... 301
9.3. Сканирование конечных точек на наличие IOC ... 303
9.3.1. Обзор инструментов ... 304
9.3.2. Сравнение инструментов для исследования безопасности конечных точек ... 312
9.3.3. Безопасность конечных точек и контейнеры ... 313
9.4. Исследование сетевого трафика с помощью Suricata ... 316
9.4.1. Установка Suricata ... 318
9.4.2. Наблюдение за сетью ... 318
9.4.3. Написание правил ... 320
9.4.4. Использование предопределенных наборов правил ... 321
9.5. Обнаружение вторжений в журналах аудита системных вызовов ... 322
9.5.1. Уязвимость выполнения ... 323
9.5.2. Обнаружение исполнения вредоносного кода ... 324
9.5.3. Мониторинг файловой системы ... 326
9.5.4. Отслеживание невероятного ... 327
9.6. Человеческий фактор в обнаружении аномалий ... 328
Резюме ... 330

Глава 10. Карибское вторжение: практический пример реагирования на инцидент ... 331
10.1. Карибское вторжение ... 333
10.2. Идентификация ... 334
10.3. Изоляция ... 337
10.4. Искоренение ... 340
10.4.1. Сбор артефактов цифрового расследования в AWS ... 342
10.4.2. Фильтрация исходящего трафика в IDS ... 343
10.4.3. Ловля IOC с помощью MIG ... 348

10.5. Восстановление ... 351
10.6. Извлечение уроков и преимущества подготовки ... 353
Резюме ... 356

Часть III. Усиление безопасности в DevOps

Глава 11. Оценка рисков ... 359
11.1. Что такое управление рисками ... 360
11.2. Триада CIA ... 363
11.2.1. Конфиденциальность ... 364
11.2.2. Целостность ... 366
11.2.3. Доступность ... 367
11.3. Определение основных угроз для организации ... 369
11.4. Количественное измерение влияния рисков ... 371
11.4.1. Финансы ... 371
11.4.2. Репутация ... 372
11.4.3. Продуктивность ... 372
11.5. Выявление угроз и измерение уязвимости ... 373
11.5.1. Фреймворк моделирования угроз STRIDE ... 373
11.5.2. Фреймворк моделирования угроз DREAD ... 375
11.6. Быстрая оценка рисков ... 377
11.6.1. Сбор информации ... 379
11.6.2. Определение словаря данных ... 381
11.6.3. Выявление и измерение рисков ... 382
11.6.4. Составление рекомендаций ... 387
11.7. Запись и отслеживание рисков ... 388
11.7.1. Принятие, отклонение и передача рисков ... 389
11.7.2. Регулярный пересмотр рисков ... 390
Резюме ... 391

Глава 12. Тестирование безопасности ... 392
12.1. Обеспечение наблюдения за безопасностью ... 393
12.2. Аудит внутренних приложений и сервисов ... 395
12.2.1. Сканеры веб-приложений ... 396

12.2.2. Фаззинг ... 400
12.2.3. Статический анализ кода ... 403
12.2.4. Аудит облачной инфраструктуры ... 405
12.3. Красные команды и внешнее тестирование на проникновение ... 411
12.3.1. Предложение о найме ... 411
12.3.2. Техническое задание ... 414
12.3.3. Аудит ... 415
12.3.4. Обсуждение результатов ... 415
12.4. Программы по отлову багов ... 416
Резюме ... 419

Глава 13. Непрерывная безопасность ... 420
13.1. Практика и повторение: 10 000 часов защиты ... 421
13.2. Год первый: внедрение безопасности в DevOps ... 422
13.2.1. Не судите слишком рано ... 424
13.2.2. Тестируйте все и отслеживайте процессы ... 424
13.3. Год второй: подготовка к худшему ... 426
13.3.1. Избегайте дублирования инфраструктуры ... 426
13.3.2. Выстроить или купить? ... 427
13.3.3. Вторжение ... 428
13.4. Год третий: управление изменениями ... 429
13.4.1. Пересмотрите приоритеты в безопасности ... 430
13.4.2. Постоянное совершенствование ... 430