

Информационная безопасность

Громкие атаки 2024

«Даже одна утечка может
включать миллионы жертв»



С начала 2024 года

510 млн

записей о россиянах утекло в сеть

500 млн

из этих записей были скомпрометированы в результате
одного! киберинцидента

Громкие атаки 2024 / ГАС «Правосудие»

6 октября 2024 атака группировки «Во Team» на государственную автоматизированную систему «Правосудие»:

▲ Способ

- Вирус-шифровальщик

Выкуп злоумышленники не требовали
Нарушено свойство информации – **доступность**

▲ Результат

- Суды откатились на **20 лет назад**
- Обмен документами в бумажном виде

▲ Последствия

- Восстановительные работы
- Финансовые затраты

☐ Об успешной атаке хакеры выпускают заявление: **«ворота были открыты...»**

Громкие атаки 2024 / Dr. Web

~ 09 сентября 2024 Атака группировки «DumpForums» на внутреннюю инфраструктуру компании, горизонтальное перемещение

▲ Скомпрометированы:

- Корпоративный **GitLab**
- Корпоративная почта
- **Confluence**
- **Jenkins**
- **Redmine**

▲ Результат

- Утечка данных сотрудников и клиентов
- Нарушено свойство информации – **конфиденциальность**

▲ Последствия

- Восстановительные работы
- Репутационный ущерб
- Финансовые затраты
- Юридические последствия за возможную утечку данных пользователей

- ☐ Об успешной атаке хакеры выпускают заявление: **«Мы проникли в локальную сеть, изначально спланировав всё...»**

Громкие атаки 2024 / СДЭК

26 мая 2024 атака хакерской группировки «Head Mare»

▲ Способ

- Вирус-шифровальщик

Выкуп злоумышленники
не требовали
Нарушено свойство
информации – **доступность**

▲ Результат

- Зашифрованы все данные, включая резервные копии
- Полный паралич работы СДЭК

▲ Последствия

- Репутационный ущерб
- Финансовые потери
- Восстановительные работы

- ☐ Об успешной атаке хакеры выпускают заявление: **«Сисадмины слишком слабы..... А политики безопасности не оправдали себя ...»**



Громкие атаки 2024. Причины и цели

Цели

- Не материальны, злоумышленники не требуют выкуп
- Нанесение максимального ущерба и простой инфраструктуры

Причины

- Dr.Web – спланированная и хорошо подготовленная атака профессиональной группировки
- ГАС «Правосудие», СДЭК – отсутствие системы безопасности и уязвимости в системе безопасности, заражение вредоносным ПО; инсайд или переход по вредоносной ссылке. Хактивизм

«Три кита» информационной безопасности

Конфиденциальность

свойство информации, гарантирует, что доступ к информации имеют только определенные лица

Целостность

свойство информации, гарантирует, что только определенные лица могут менять информацию

Доступность

свойство информации, гарантирует, что лица, имеющие доступ к информации, в нужный момент смогут получить доступ

Что такое информационная безопасность

Информационная безопасность —

комплекс мер, направленных на защиту
конфиденциальности, целостности
и доступности

! Информационная безопасность — это **всегда процесс**

Основные термины

1. **Угроза ИБ** – возможное случайное или преднамеренное негативное воздействие на сеть, программное и аппаратное обеспечение
2. **Уязвимость** – недостаток в ПО или информационной системе, который может быть использован для реализации угрозы
3. **Инцидент ИБ** – одно или несколько негативных событий, нарушающих безопасность информации (конфиденциальность, целостность, доступность)
4. **Недопустимое событие** – событие, возникшее в результате кибератаки и которое делает невозможным достижение операционных или стратегических целей предприятия или приводит к существенному нарушению ее основной деятельности



Основные термины

- 5. **Поверхность атаки** – область информационной системы которая может быть подвергнута негативному воздействию; порты, сервисы и службы, веб-приложения, API, человек...
- 6. **Вектор атаки** – средства или пути по которым злоумышленник может скомпрометировать целевое устройство.
- 7. **Атака** – действия злоумышленника направленные на нарушение свойств информации: конфиденциальности, целостности, доступности.



Ландшафт угроз 2024



Киберугрозы и тенденции 2024

Атаки на IT инфраструктуру российских компаний и государственного сектора:

- Атаки с целью хищения конфиденциальных данных
- DDoS атаки
- Компрометация служб удаленного доступа RDP, VPN
- Фишинговые рассылки вредоносного ПО
- Атаки на цепочки поставок (подрядчики, зависимости)
- Шпионское ПО, RAT (Remote Access Trojan)
- Сокращение времени от опубликования сведений об уязвимости до ее эксплуатации

Киберугрозы и тенденции 2024

Отчет F.A.C.C.T.

Мотивация киберпреступников

- Нанесение максимального ущерба российским компаниям и гос. сектору
- Монетизация ущерба – больше не является приоритетом

Популярные техники

- Эксплуатация известных уязвимостей
- Компрометация служб удаленного доступа
- Заражение легитимного ПО
- Атаки на цепочки поставок

Атака на цепочку поставок

SSC — software supply chain attacks



Основная цель (клиент) – хорошо защищена, атака требует серьезной подготовки и вложений

- Долго
- Дорого
- Шансы на успех не понятны



Разработчик ПО (поставщик) – есть шансы успешной атаки

Основная цель SSC

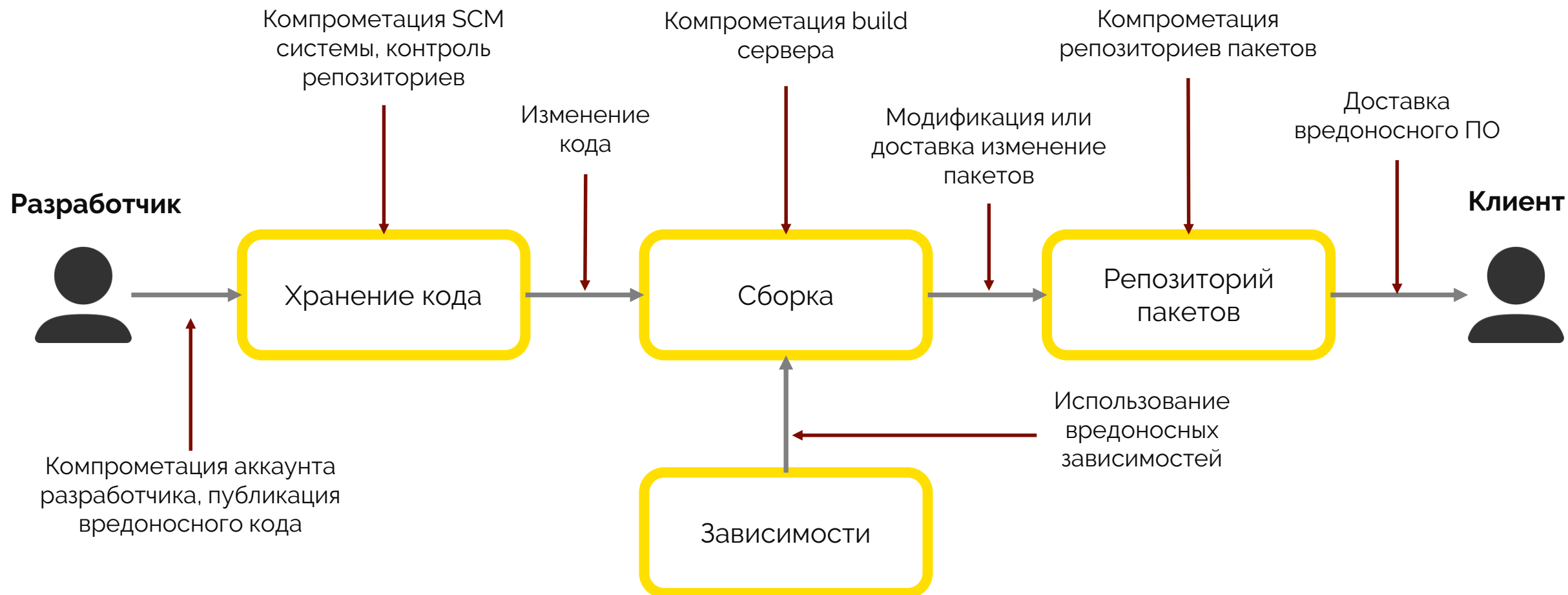
- доступ к исходным кодам
- доступ к процессам сборки
- доступ к механизмам обновления допустимого ПО

Под угрозой атак SSC

- разработчик ПО
- поставщик ПО

Атака на цепочку поставок

Атака SSC охватывает весь жизненный цикл разработки



Атака на цепочку поставок

Методы атак SSC

Заражение вредоносным ПО:

Шпионское ПО, для кражи учетных данных у сотрудников

Социальная инженерия:

Поддельные приложения, письма, ссылки, Fake Boss....

Brute Force:

Перебор паролей SSH, RDP

Уязвимости в ПО:

SQL injection, эксплойты

Уязвимости в конфигурации:

Проблемы с конфигурацией

Методы OSINT:

Поиск учетных данных сотрудников в открытом доступе

Атака на цепочку поставок

Поверхность атак SSC

ПО используемое поставщиком:

Системное и прикладное ПО

Библиотеки ПО:

Сторонние библиотеки и пакеты

Код:

Исходный код производимый поставщиком

Конфигурации:

Пароли, ключи API, URLs

Базы данных:

Информация о поставщике

Персональные данные сотрудников

Процессы:

Обновления, резервного копирования,
проверки сертификатов

Люди:

Допущенные к инфраструктуре

Что делать? Как защищаться?

- Внедрить процесс безопасной разработки программного обеспечения
- Мониторинг сети на подозрительную активность
- Мониторинг каждой конечной точки: серверы, персональные компьютеры
- Своевременное обновление ПО
- Резервное копирование





Безопасная разработка

Безопасная разработка

Безопасная разработка
(SSDLC - Secure Software Development Lifecycle) —

это **процесс** создания **программного обеспечения** с учетом аспектов информационной **безопасности** с самого начала жизненного цикла **разработки** до завершения эксплуатации

Предотвращает

- случайное внедрение уязвимостей
- несанкционированный доступ

Обеспечивает

- устойчивость к внедрению вредоносных программ

Безопасная разработка

Принципы

Работоспособность и полезность

1

Безопасность

- возможность защиты от внешних угроз и атак
- сохранение работоспособности после их отражения и устранения последствий

2

Надежность

- предсказуемое, безопасное и корректное поведение в случае некорректных входных данных

3

Конфиденциальность

- безопасная и корректная работа с конфиденциальной информацией

4

Целостность и корректность бизнеса

- сопровождение программы
- контроль прозрачности, законности, корректности работы пользователя

5

Преимущества SSDLC

Повышение безопасности приложений

безопасность должна обеспечиваться и соблюдаться на каждом этапе жизненного цикла продукта

Сокращение Time-to-market

большинство ошибок обнаруживается в момент появления, что уменьшает время на их устранение
Shift left – раньше нашел, раньше исправил

Улучшение качества продуктов

проработка требований безопасности и вариантов реагирования на уязвимости происходит на этапе проектирования



Преимущества SSDLC



Внедрение культуры безопасности

обучения сотрудников практикам безопасной разработки



Выстраивание коммуникации и унификация подходов

взаимодействие разработчиков, тестировщиков,
администраторов и безопасников, унификация инструментов
и методов

Безопасная разработка

Классический жизненный цикл ПО



Анализ требований – «Какие проблемы требуют решений?»

Планирование – «Что мы хотим сделать?»

Дизайн – «Как мы добьемся наших целей?»

Разработка ПО – регулирует процесс создания продукта

Тестирование – регулирует обеспечение качественной работы продукта

Развертывание – регулирует использование финального продукта

⚠ **Анализ безопасности разрабатываемого продукта не предусмотрен**

Безопасная разработка

«Думайте о безопасности на всех этапах жизненного цикла разработки ПО, с самого начала»



Risk Assessment – анализ угроз, формирование требований безопасности, соответствие регуляторным требованиям

Threat Modeling & Design Review – проектирование выполняется с учетом анализа угроз

Static Analysis – статический анализ кода (SAST) и зависимостей на наличие уязвимостей (SCA)

Security Testing – тестирование отказоустойчивости и динамический анализ приложения DAST

Secure Configuration – оценка уровня безопасности приложения

Методологии безопасной разработки

1. **DSOMM** (DevSecOps Maturity Model) –
2. **BSIMM** (Building Security In Maturity Model)-
3. **OWASP SAMM** (Software Assurance Maturity Model) -
4. **Microsoft SDL** (Security Development Lifecycle)–
5. **NIST SP 800-64** – (Security Considerations in the System Development Life Cycle)
6. **ГОСТ 56939 – 2016** «Разработка безопасного программного обеспечения»
7. **ГОСТ 58412-2019** «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения»

Requirement. Risk Assessment

Risk Assessment – анализ угроз, формирование требований безопасности

- Идентификации и аутентификации
- Защита от несанкционированного доступа к информации
- Процесс регистрации событий и ошибок
- Контроль качества данных, поступающих в систему
- Применение надежных алгоритмов шифрования
- Управление секретами, хранение ключей
- Безопасность инфраструктуры
- Модель угроз



Выполняется до первой строчки
кода

Requirement. Risk Assessment / Реальный проект

Архитектурные требования безопасности

1	Все сетевое взаимодействие должно осуществляться по защищенным каналам связи (https и т.д.)
2	При публикации сайта в сеть интернет, сайт должен быть опубликован через корпоративный сервис защиты web-трафика (WAF, anti-ddos, anti-bot)
3	Функционал подключения captcha для форм аутентификации и обратной связи
4	Код разрабатываемого сайта должен проходить проверку исходного кода на отсутствие уязвимостей (SAST)
5	Загружаемые на сайт файлы должны проверяться с помощью корпоративных СЗИ, запрещена загрузка файлов форматов: .exe .ini .apk .bat .bin .cgi .cmd .cmd .cpp .js .jse .gadget .gtp .hta .jar .msi .msu .paf.exe .pif .ps1 .pwz .scr .thm .vb .vbe .vbs .wsf
6	На форме загрузке файлов должна выполняться проверка MIME-типов загружаемых файлов
7	Административная консоль сайта должна быть доступна только из локальной сети компании. Запрещается публиковать административные интерфейсы в сеть интернет
8	API сайта должно требовать обязательной аутентификации
9	БД с учетными записями от личного кабинета сайта должна размещаться на отдельном сервере
10....	Сервер с БД учетных записей должен быть зашифрован
...51	Аутентификационные данные, которые использует сервис должны храниться в корпоративном сервисе Secresy. Не допускается хардкод аутентификационные данных в конфигурационных файлах или переменных окружения

Модель угроз

Модель угроз –

детальный анализ потенциальных угроз и уязвимостей, последствия от возможных атак

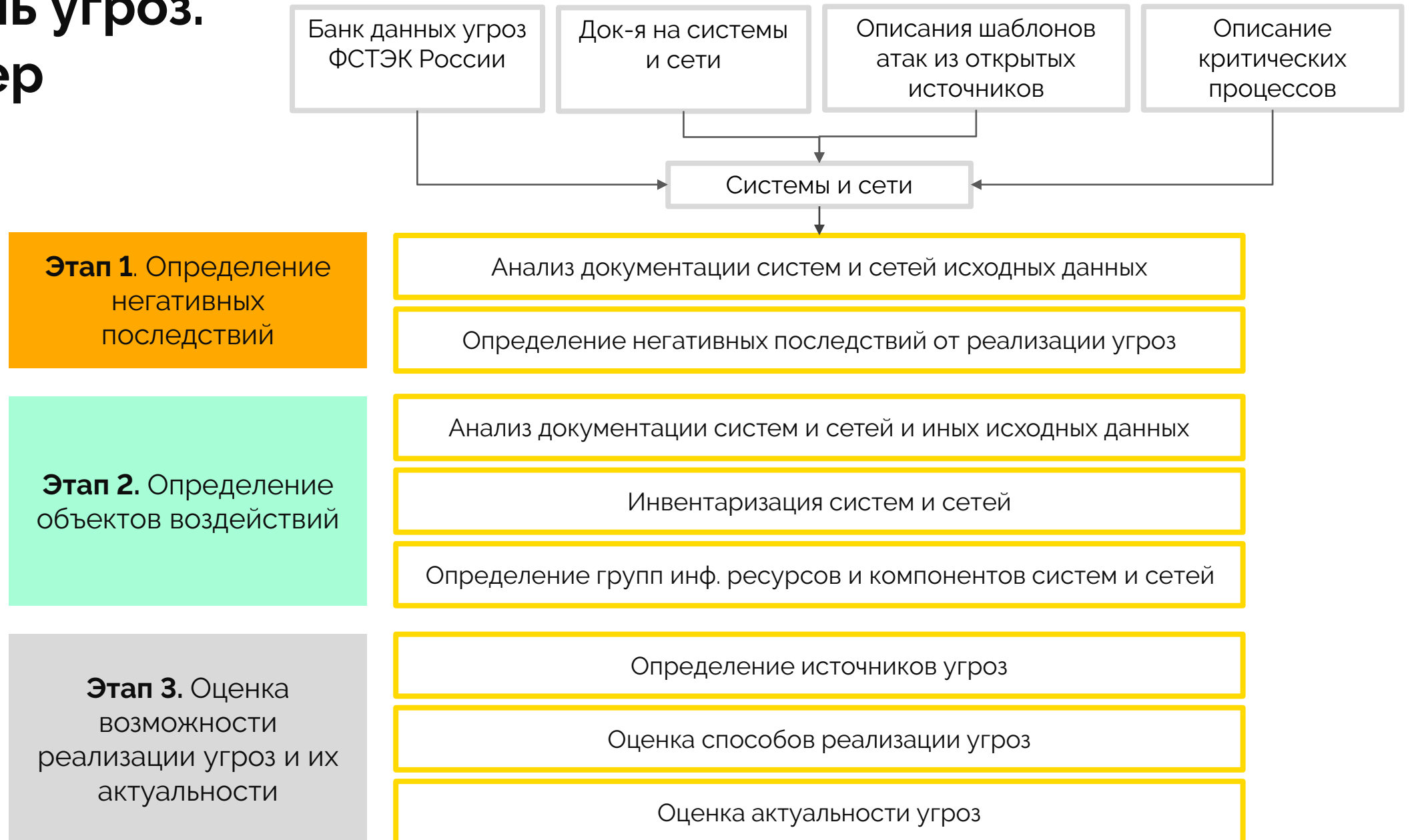
Процесс моделирования

включает:

- идентификацию активов
- определение потенциальных злоумышленников и их целей
- выявление слабых мест в системе
- описание возможных векторов атак
- оценка потенциального ущерба от их реализации

Модель угроз.

Пример



Secrets Management

Секреты – привилегированные учетные данные, не принадлежащие человеку, чаще всего те, которые используются системами и приложениями для аутентификации или в качестве входных данных для криптографического алгоритма.

Управление секретами – процесс организации, управления и защиты секретов ИТ-инфраструктуры

- позволяет безопасно хранить, передавать и проверять секреты
- позволяет защитить секреты от несанкционированного доступа и обеспечивает надлежащее функционирование систем

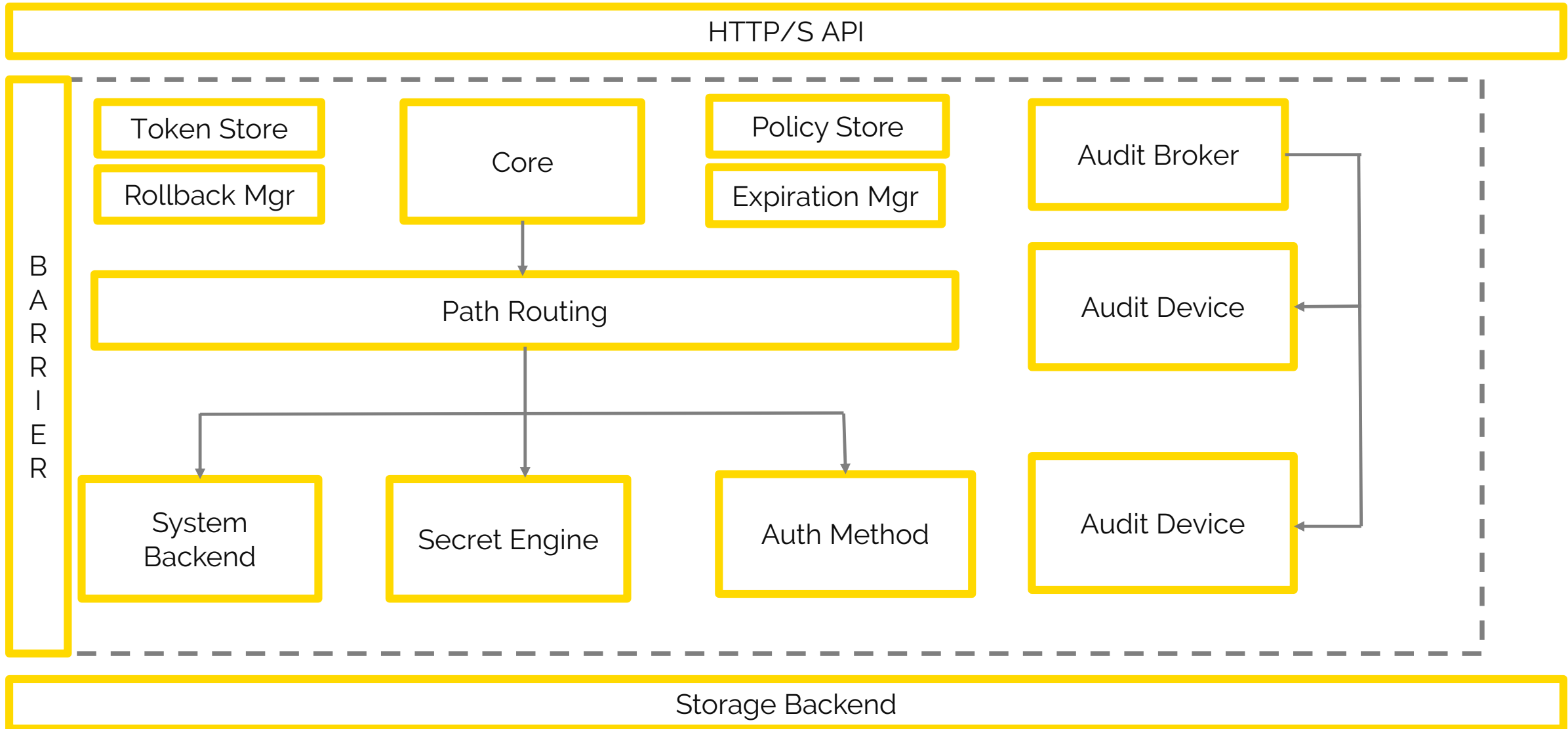
Менеджер секретов – безопасная система хранения и единственный источник достоверных данных для привилегированных учетных данных, ключей API и другой особо конфиденциальной информации, используемой в ИТ-инфраструктурах

Secrets Management

Hashicorp Vault – инструмент для хранения секретов, де-факто стандарт для Kubernetes

- **Безопасное хранение секретов** - хранятся в виде ключ-значение, то есть мы можем создать некий секрет, положить туда любой набор этих пар — и всё будет безопасно храниться
- **Хранение динамических секретов** - Vault сам управляет динамическими секретами с определённым сроком жизни, их не придётся постоянно менять их вручную
- **Шифрование данных** – позволяет сгенерировать так называемый Transit Key, хранить его внутри самого Hashicorp Vault, и сделать не экспортируемым. То есть из Vault секретный ключ для шифрования получить будет нельзя

Secrets Management / Архитектура Hashicorp Vault



Secrets Management

Core – работает с запросами, в Core запрос маршрутизируется с помощью Path

Routing – перенаправить запрос на соответствующий backend

System Backend – отвечает за системные функции Vault

Secret Engine – хранение секретов и шифрование. Два разных Secret engine нельзя активировать по одному Path

Auth Method – аутентификация пользователей Vault

Token Store – выдаёт свои токены доступа для взаимодействия пользователя с Vault

Policy Store - хранения политик, которые позволяют разграничивать доступ к различным частям внутри Vault

- Path – путь по которому назначаются права
- Capabilities – наборы прав на определенный путь

Design Review

Проектирование системы выполняется с учетом Risk Assessment

Простыми словами – это интеграция безопасности в будущий проект наравне с функциональными требованиями

- Потенциальные риски учтены
- Сформулированы требования безопасности
- Расходы на безопасность включены в бюджет, запланированы трудозатраты

 Выполняется до первой строчки кода

Security Development

Этап **Development** предполагает:


- Использование инструментов статического анализ исходного кода SAST
- Использование инструментов анализа компонентов на наличие уязвимостей SCA
- Использование инструментов для обнаружения в исходном коде секретов: пароли, токены, ключи API

 Выполняется от первой строчки кода до выката в ПРОД

Security Development

Статический анализ (SAST) – исследование исходного кода программы без ее фактического выполнения

Анализ компонентов (SCA) – сканирование и анализ сторонних компонентов и компонентов open-source на наличие известных уязвимостей

 **Цель** – обнаружение потенциальных ошибок, уязвимостей, нарушение стиля кодирования и других ошибок которые могут привести к багам и снижению производительности программы

Development. Static Analysis

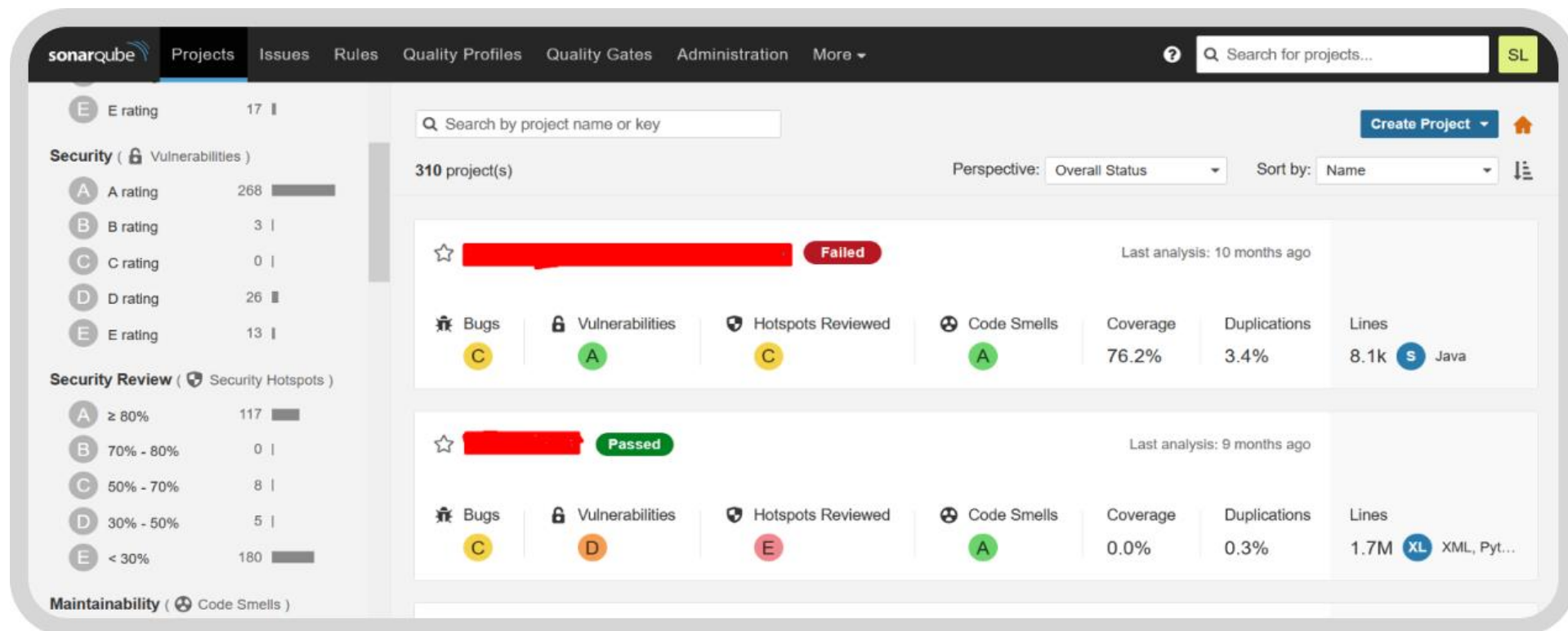
Примеры инструментов SAST

Sonar Qube

Open-source инструмент, поддержка более 20 языков программирования

Оценка качества кода в реальном времени

Интеграция CI/CD



Development. Static Analysis

Примеры инструментов SAST

Trivy

Open-source инструмент для поиска уязвимостей, неправильных настроек, секретов, в контейнерах, Kubernetes, репозиториях кода, облачных средах

Интеграция CI/CD



Development. Static Analysis

Примеры инструментов SAST

GitLeaks

Поиск секретов в коде, при обнаружении секрета сборка блокируется

!

#GitLeaks - Поиск секретов

Добавлен конфиг с паролями

в GitLeaks-samples-for-test

↗

 Сохранено

Сводка Artifactory Artifactory

Запрос на вытягивание кем вич ()

Репозитории 3

GitLeaks-samples-for-test , +1

Дополнительные сведения см. в карточке источников

Время начала и затраченное время

Сейчас

19 с

Соответствующие

Рабочих элементов: 0

1 опубликовано; 2 использовано

Предупреждения 1

!

 Обнаружены секреты в исходном коде, однако, репозиторий gitleaks-samples-for-test в исключении, сборка не блокируется

Принятие решения

Задания

Имя	Состояние	Длительность
<div>!</div> GitLeaks: Поиск секретов	Предупрежден...	<div></div> 14 с

Забутые пароли и токены. Последствия

30.01.2024

Mercedes-Benz признала, что оставила в сети закрытый токен к GitHub Enterprise Server Mercedes



В результате утечки стали доступны:

- конфиденциальные репозитории, содержащие огромное количество интеллектуальной собственности компании
- строки для подключения к базам данных,
- ключи доступа к облаку, чертежи, проектную документацию,
- пароли SSO, ключи API и другую важную внутреннюю информацию

Development. Static Analysis

Примеры инструментов SCA

Dependency
Track

Проект OWASP для компонентного анализа и снижения рисков в цепочке поставок

Vulnerability	Title	Severity	Analyzer	Published	CWE	CVSSv2	CVSSv3	Project Name	Component	Version	Analysis	Suppressed	Attributed C
NVD CVE-2023-37920	-	Critical	OSS Index	26 Jul 2023	CWE-345	-	9.8	VP_another_test_cdxgen-master 1719	certifi	2023.5.7	-		26 Apr 2024
NVD CVE-2023-37920	-	Critical	OSS Index	26 Jul 2023	CWE-345	-	9.8	VP_another_test_cdxgen-master 1718	certifi	2023.5.7	-		26 Apr 2024
NVD CVE-2023-37920	-	Critical	OSS Index	26 Jul 2023	CWE-345	-	9.8	node-php_custom_imagesdocker 0	certifi	2022.12.7	-		7 Mar 2024
NVD CVE-2023-37920	-	Critical	OSS Index	26 Jul 2023	CWE-345	-	9.8	node-php_custom_imagesdocker 0	certifi	2021.10.8	-		7 Mar 2024
NVD CVE-2023-37920	-	Critical	OSS Index	26 Jul 2023	CWE-345	-	9.8	node-php_custom_imagesdocker 0	certifi	2021.10.8	-		7 Mar 2024
NVD CVE-2023-37920	-	Critical	OSS Index	26 Jul 2023	CWE-345	-	9.8	VP_API_tests_cdxgen-master_6 1516	certifi	2023.5.7	-		26 Feb 2024
NVD CVE-2023-37920	-	Critical	OSS Index	26 Jul 2023	CWE-345	-	9.8	VP_Internal_D_cdxgen-master_4 1447	certifi	2023.5.7	-		6 Feb 2024

Security Testing

Динамический анализ приложения (DAST) – тестирование безопасности приложения во время его работы. Не привязан к языкам программирования

Этап **Security Testing** предполагает применение инструментов динамического анализа **DAST**

- Имитация хакерских атак
- Тестирование функций безопасности
- Тестирование на проникновение
- Тестирование отказоустойчивости, fuzz testing – ввод случайных, заведомо неверных данных с целью вызвать сбой системы

Security Testing

Примеры инструментов DAST

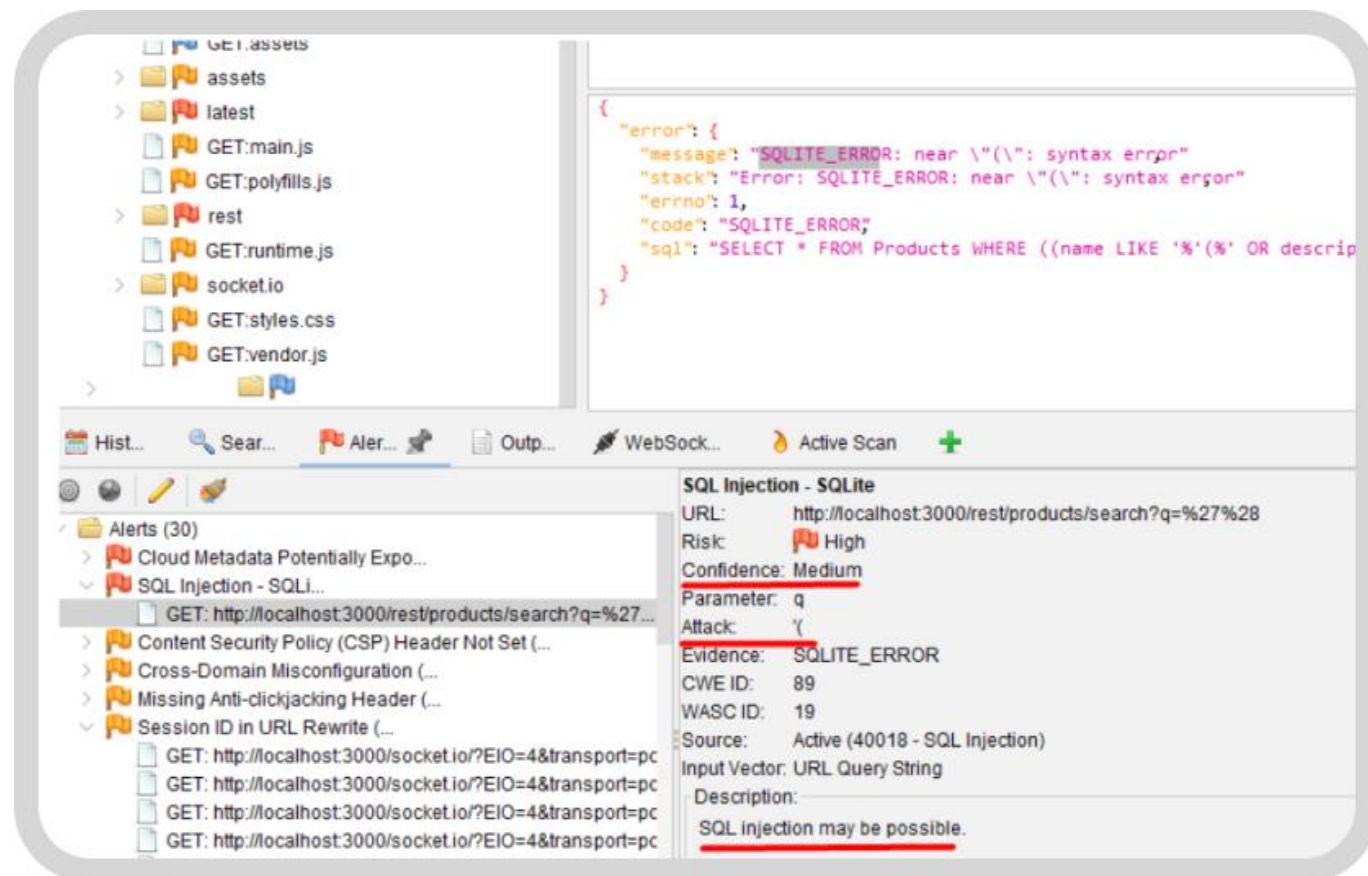
OWASP ZAP

Open-source инструмент динамического анализа. Проект OWASP

Имитация атак злоумышленника

Fuzz – тестирования


Имитация атаки SQLi



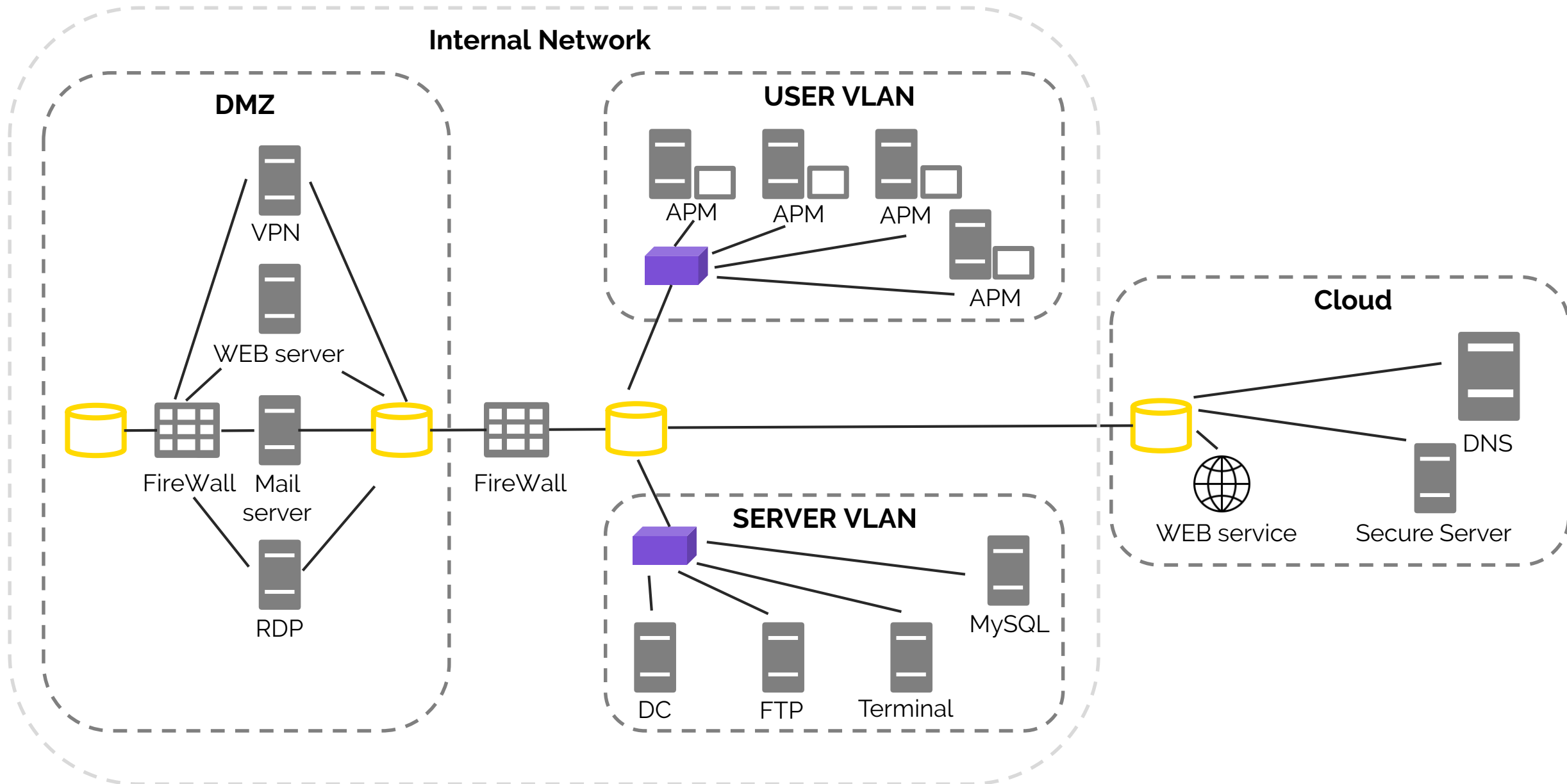
Secure Configuration

Secure Configuration – проверка приложения на соответствие установленным требованиям информационной безопасности:

- Тест-кейсы для проверки соответствия требованиям ИБ
- Определить, какие требования выполнены, а какие нет
- Тест-кейсы проверки механизмов безопасности; авторизация, идентификация, криптография..
- Исправление ошибок и уязвимостей
- Провести повторное тестирование
- Внешние аудиты безопасности приложения

 **Проводится перед релизом в продуктовую среду**

Защита инфраструктуры разработки



Защита инфраструктуры

Сетевая безопасность –

меры, направленные на защиту подключенных сетей и инфраструктуры несанкционированного доступа, утечки информации, вредоносных программ, DDoS и других угроз которые могут привести к нежелательным последствиям

Основные методы СБ:

- Разграничение доступа
- аутентификация и авторизация
- сегментация сети и виртуальные частные сети
- применение инструментов защиты от утечек (DLP)
- применение инструментов обнаружения и предотвращения вторжений (IPS/IDS)
- использование брандмауэров
- использование протоколов шифрования
- мониторинг безопасности
- антивирусная защита

Защита инфраструктуры. Сегментация сети

Сегментация сети – разделение инфраструктуры на изолированные зоны с различными уровнями доверия

- Контроль доступа между зонами
- Предотвращение несанкционированного доступа
- Ограничение зоны поражения в случае инцидента

Типовые сегменты сети:

- внутренняя сеть (INT) для хранения конфиденциальных данных
- внешняя сеть (EXT) для публичного доступа
- демилитаризованная зона (DMZ) для размещения общедоступных сервисов

Защита инфраструктуры. Мониторинг безопасности

SIEM – класс программных продуктов для сбора и анализа информации о событиях безопасности в сети и приложениях

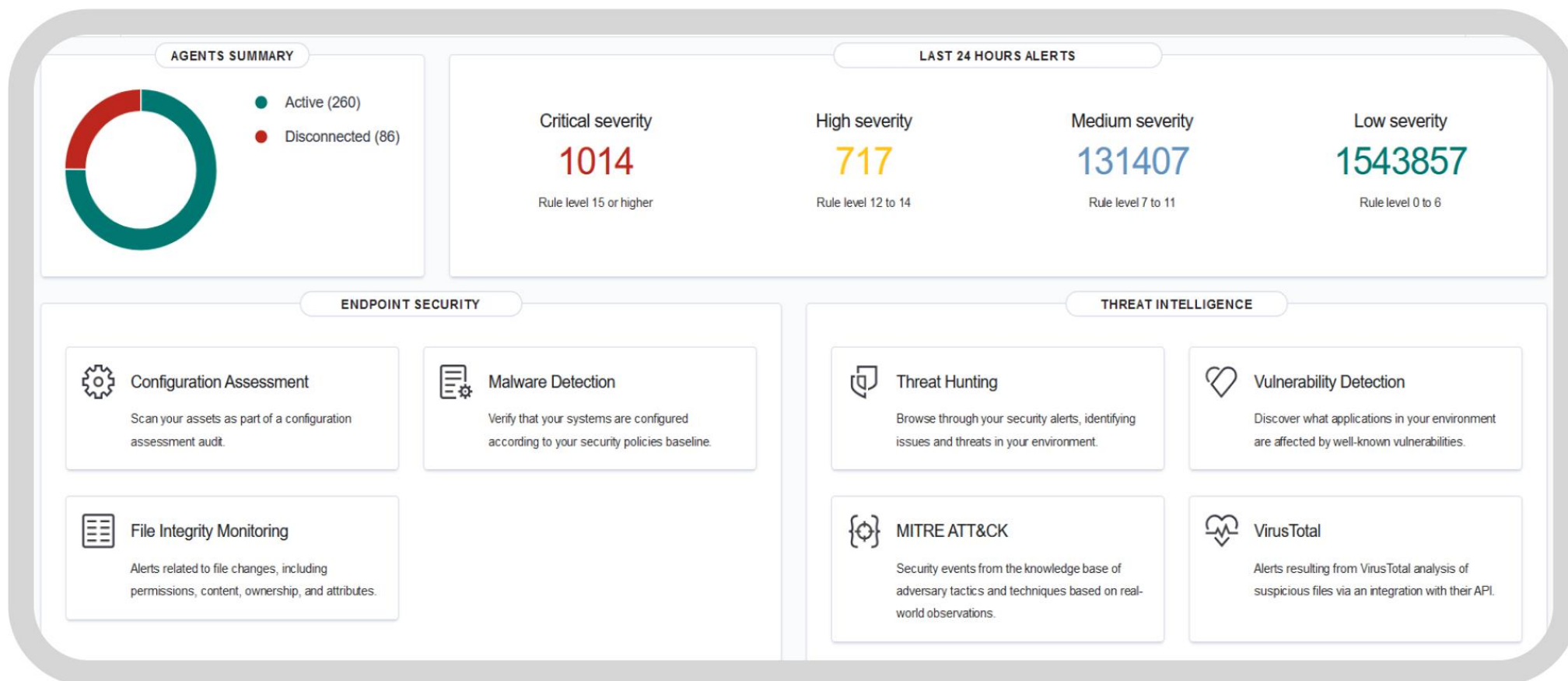
Источники информации для SIEM-решений:

- антивирусные программы;
- системы авторизации и аутентификации;
- межсетевые экраны, брандмауэры;
- журналы сетевого оборудования, серверов и рабочих станций;
- контроллеры домена
- системы обнаружения и предотвращения вторжений IDS/IPS
- Решения для контроля активов и инвентаризации

Защита инфраструктуры. Мониторинг безопасности

SIEM Wazuh

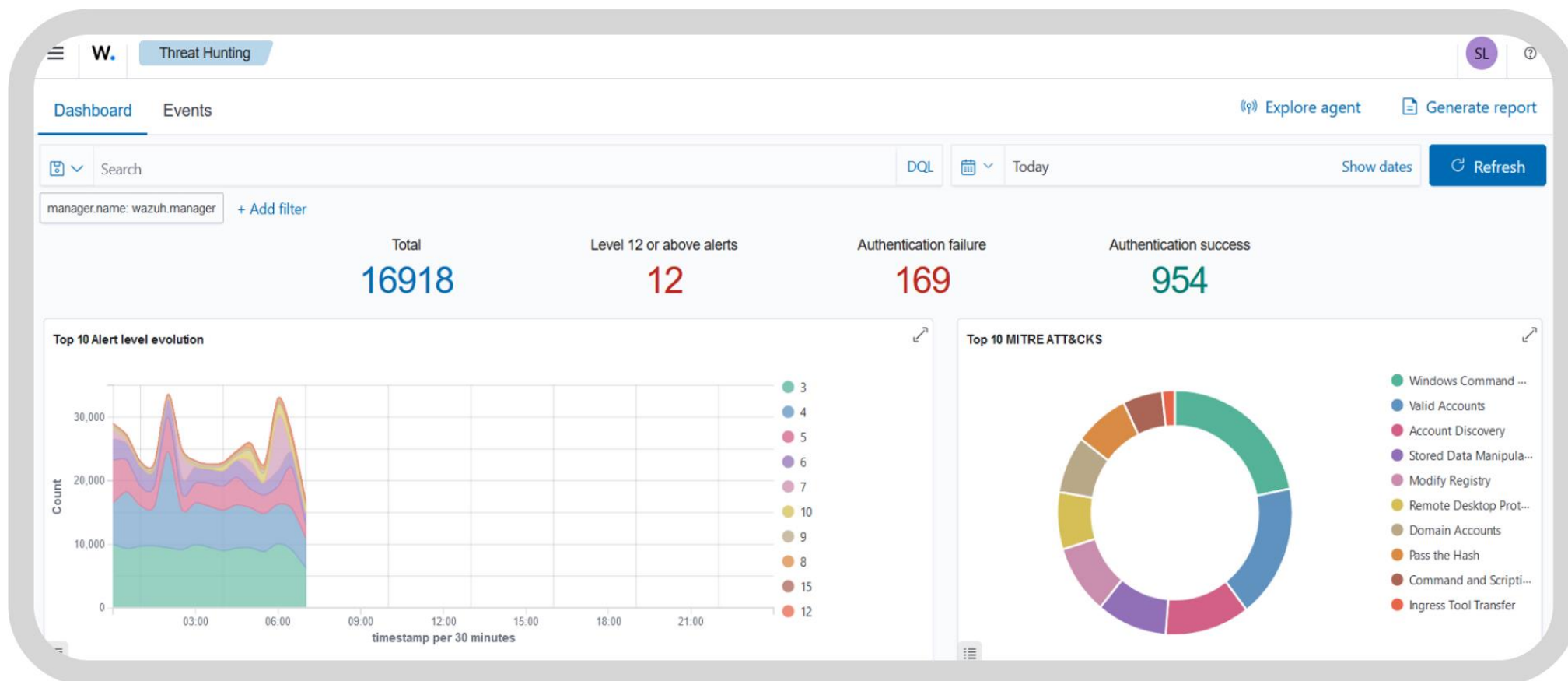
Open-source система мониторинга событий ИБ. Основные модули



Защита инфраструктуры. Мониторинг безопасности

SIEM Wazuh

Модуль Threat Hunting



Защита инфраструктуры. Мониторинг безопасности

SIEM Wazuh

Инцидент ИБ. Детектирование вредоносного IP-адреса

manager.name: wazuh.manager

GeoLocation.country_name: is one of United States, Iraq, Belgium, Germany, France, Kazakhstan, Sweden, Czechia, Kyrgyzstan X

+ Add filter

> Nov 28, 2024 @ 09:03:24.780

Successful Remote 6

92657

United States

104.28.239.219

Logon Detected -

User:\ -

NTLM authenticati

on, possible pas

s-the-hash attack

- Possible RDP co

104.28.239.219

Malicious IP

21 queries left for the week. ?

Upgrade to get more quota

Crowd Confidence: High

Location: Leipzig, Germany

First Seen: over 1 year ago

Last Seen: 3 days ago

Background Noise ?

Noisy

Known For:

HTTP Bruteforce

HTTP Scan

HTTP Exploit

MITRE Techniques:

Brute Force

Gather Victim Identity Information

Active Scanning

Exploit Public-Facing Application

IP Range

Range: 104.16.0.0/12

Very aggressive

Reverse DNS

Unknown

Top Classifications

CrowdSec Community Blocklist

View all

Предупрежден – значит вооружен

Базы данных и справочники
уязвимостей и недостатков
программного обеспечения



Common Weakness Enumeration

A community-developed list of SW & HW weaknesses that can become vulnerabilities

Проекты OWASP


OWASP

SSC — software supply chain attacks

OWASP – самый известный, открытый проект по безопасности мобильных и веб-приложений

Цели OWASP:

- Помощь в создании, разработке, поддержке приложений которым можно доверять.
- Повышение осведомленности о безопасности приложений путем определения наиболее критичных рисков

 Все проекты, инструменты, стандарты, образовательные программы и документы абсолютно бесплатны

Проекты OWASP

OWASP

Стандарты и руководства

[OWASP TOP-10](#) , топ рисков безопасности WEB приложений: описание, риски, как избежать

[OWASP TOP 10 API Security](#) - топ рисков безопасности API: описание, риски, как избежать

[OWASP TOP-10 Cloud Native](#) - безопасность облаков: описание, риски, как избежать

[OWASP Kubernetes TOP 10](#) - топ рисков безопасности kubernetes: описание, риски, как избежать

[OWASP DevSecOps Guideline](#) - путеводитель по безопасной разработке

[OWASP ASVS](#) - Стандарт, требования к безопасности web-приложений

[OWASP WSTG](#) - Руководство по тестированию безопасности веб-приложений и веб-сервисов

[OWASP MASVS](#) – Стандарт безопасности мобильных приложений

[OWASP MASTG](#) – Руководство по тестированию безопасности мобильных приложений

[OWASP CHEAT SHEET](#) - **шпаргалки** по безопасности приложений (web, mobile) для архитекторов и разработчиков

Базы данных угроз и уязвимостей

1. **CVE (Common Vulnerabilities and Exposures)** – структурированная база общеизвестных уязвимостей:
 - содержит подробное описание уязвимости, ее воздействие, критичность, способы устранения уязвимости или смягчению последствий ее воздействия
2. **CWE (Common Weakness Enumeration)** – структурированная база общеизвестных недостатков и дефектов аппаратного и программного обеспечения которые могут привести к уязвимости
 - по каждому дефекту дается подробное описание, примеры воздействия, способы устранения
 - используется в качестве базового стандарта для идентификации, предупреждения и смягчения последствий

Базы данных угроз и уязвимостей

3. [БДУ ФСТЭК](#) - структурированная база общеизвестных уязвимостей.

Ориентирована на использование в государственном секторе и субъектах критической информационной инфраструктуры

4. [Exploit Database](#) – структурированная база сценариев эксплуатации уязвимостей (exploits) и примеров эксплуатации уязвимостей (Proof of Concept)

5. [MITRE ATT&CK](#) – ориентирована на описание техник и тактик используемых злоумышленниками, а не конкретных уязвимостей.

- помогает понимать методы атак и разрабатывать стратегии обнаружения и предотвращения

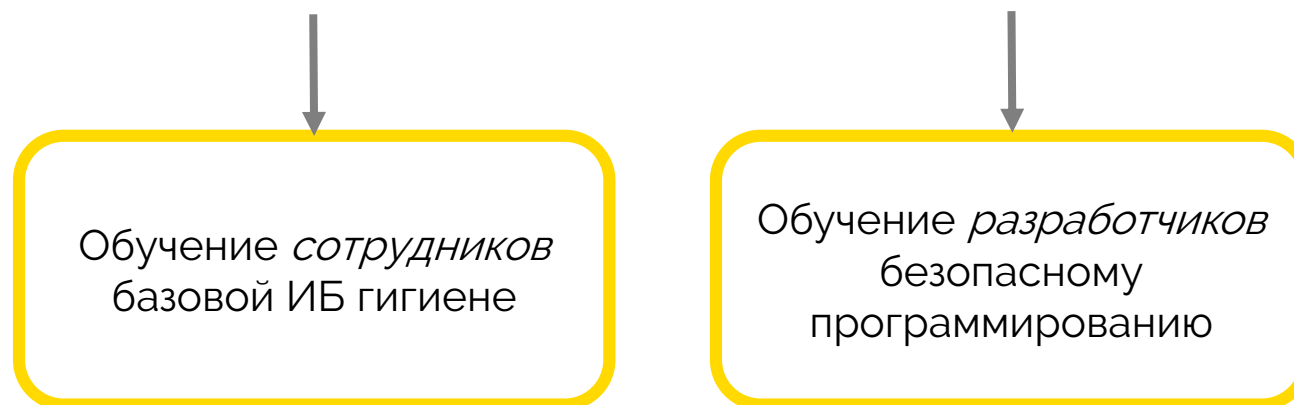


**Обучение
сотрудников.
Культура
безопасности**

Культура безопасности в компании

Обучение сотрудников - **неотъемлемая часть процесса безопасной разработки**

Обязательно для всех сотрудников и входит в онбординг для новичков



Культура безопасности – сотрудники **знают, понимают и разделяют** правила информационной безопасности

Культура безопасности в компании

Базовая ИБ гигиена

Цель

1. Снижение рисков внутренних нарушений ИБ
2. Общая осведомленность о безопасности в организации

Тематика

1. Ландшафт угроз ИБ
2. Безопасная передача данных
3. Хранение паролей
4. Фишинг
5. Работа с чувствительной информацией

! Обязательно для всех сотрудников и входит в онбординг для новичков

Культура безопасности в компании

Обучение разработчиков

Цель

1. Сокращение уязвимостей на этапе написания кода
2. Понимание своей ответственности за написание кода

Тематика

1. Принципы безопасной разработки
2. Трендовые уязвимости
3. Методы тестирования безопасности
4. Вредоносные атаки



Разработка ПО для субъектов КИИ

Разработка ПО для КИИ

Критическая информационная инфраструктура (КИИ) –

это системы и сети, которые имеют жизненно важное значение для функционирования целых отраслей экономики и страны в целом. Защита КИИ от кибератак является защитой национальных интересов.

Правовое регулирование защиты КИИ осуществляется в рамках **ФЗ № 187** «О безопасности критической информационной инфраструктуры Российской Федерации»

За исполнением требований **ФЗ № 187** отвечают **ФСТЭК и ФСБ**

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ФСБ – Федеральная служба безопасности



Разработка ПО для КИИ

Для разработки ПО для КИИ необходимы лицензии:

- **ФСТЭК** – дает право на деятельность по защите информации не составляющей государственную тайну без использования криптографии и шифрования
- **ФСБ** – дает право на деятельность по защите информации не составляющей государственную тайну с использованием криптографии и шифрования

Разработка ПО для КИИ

Субъекты ККИ

Гос. органы

Гос. учреждения

Юридические лица

ИП

Которым принадлежат

Которые обеспечивают взаимодействие

Объекты ККИ

Информационные
системы

Информационно-
телекоммуникационные
системы

Автоматизированные
системы управления

Работающие в областях

Промышленность

Горно-добывающая

Металлургическая

Химическая

Оборонная

Ракетно-космическая

Энергетика

Атомная энергетика

ТЭК

Банки

Финансовая сфера

Связь

Транспорт

Здравоохранение

Наука

Разработка ПО для КИИ

Значимость объектов КИИ

Не значимый

не требуется дополнительных мер по обеспечению информационной безопасности

Значимый (ЗОКИИ)

объект критической информационной инфраструктуры, которому присвоена одна из **трех категорий** значимости

категория значимости **зависит от вреда**, который может быть нанесен при несанкционированном вмешательстве или повреждении объекта КИИ

Разработка ПО для КИИ

Как это касается разработчиков промышленного ПО?

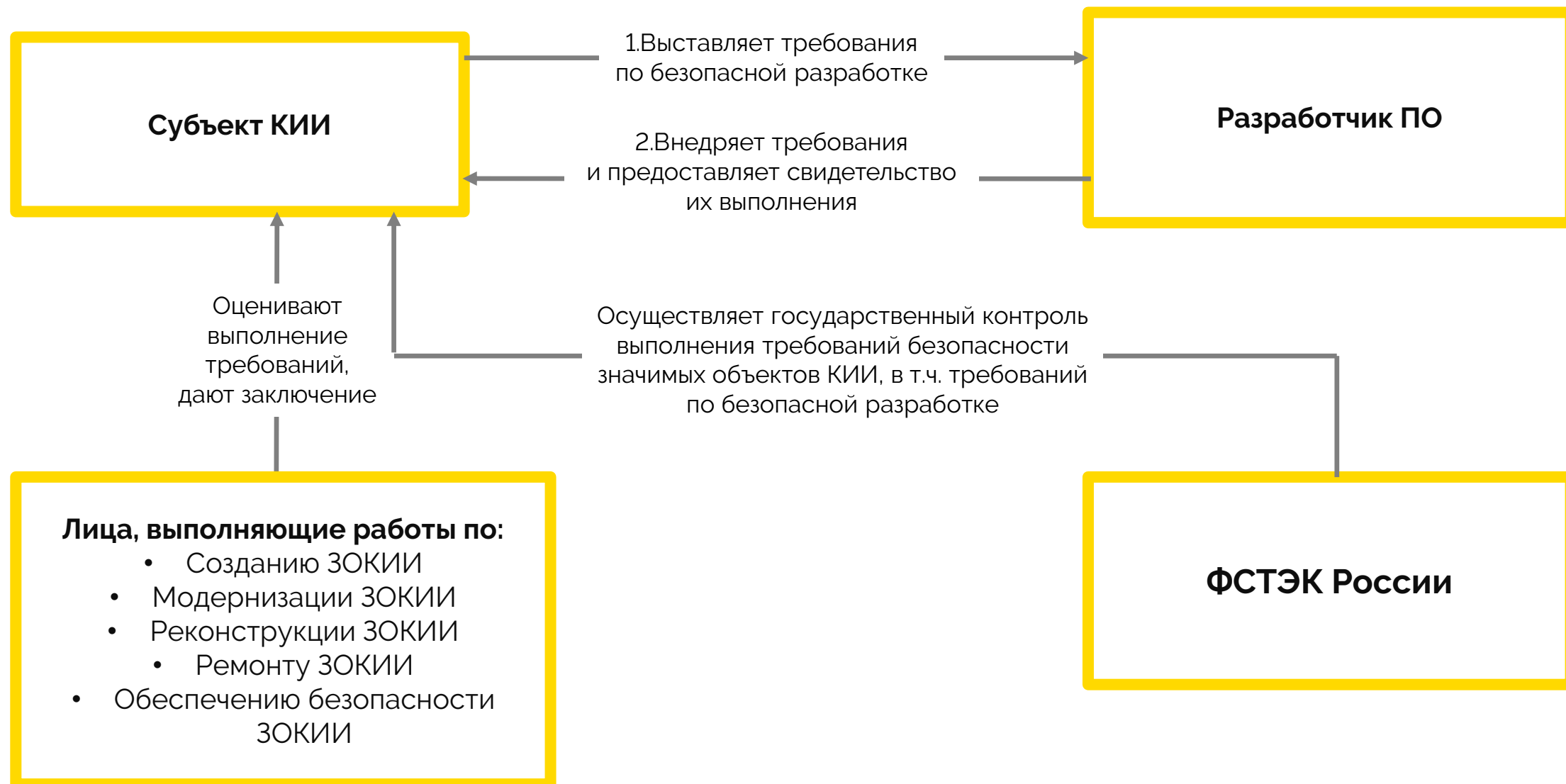
Мы не являемся
субъектами КИИ

Дело в том, что:

Системы, которые мы разрабатываем, работают
в компаниях субъектах КИИ

- **Заказчик** – выставляет требования ИБ
- **Мы** – выполняем
- **ФСТЭК** – контролирует выполнение

Разработка ПО для КИИ



Разработка ПО для КИИ vs SSDLC

ПО для КИИ

- Руководство по безопасной разработке
- Требования к испытанию ПО
- Анализ угроз безопасности информации в ПО
- Проведение статического анализа кода
- Фаззинг-тестирование ПО
- Динамический анализ ПО
- Информирование о найденных уязвимостях, их устранении
- Обучение и повышение компетенций

SSDLC

- Регламент безопасной разработки
- Анализ угроз ИБ
- Статический анализ кода
- Фаззинг тестирование ПО
- Динамический анализ ПО
- Устранение уязвимостей
- Тестирование безопасности
- Обучение и повышение компетенций



ИсПДн

**Безопасность персональных
данных при их обработке
в информационных
системах обработки
персональных данных**

Безопасность ПДн. Правовое регулирование

Защита ПДн при автоматизированной обработке



Безопасность ПДн

Персональные данные (ПДн) –

любая информация, относящаяся к **прямо** или **косвенно определенному** или **определяемому** физическому лицу (субъекту ПДн)

Безопасность Пдн. Категории

- **Пдн, разрешенные** субъектом Пдн для распространения
- **Специальные** – сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни
- **Биометрические** – сведения о физиологических и биологических особенностях человека, которые позволяют установить его личность, например фото, голос
- **Иные** – данные, которые не относятся к общедоступным, специальным или биометрическим. Например зарплата, периоды отпусков, больничных – корпоративные данные

Не Пдн	Пдн
mchr12@gmail.com	Имя: Иванов Петр, email: mchr12@gmail.com
15% сотрудников пойдут в отпуск в июле	Иванов Петр взял отпуск в июле

Безопасность ПДн

Обработка ПДн - любые действия с ними, в том числе сбор, анализ, передача, предоставление доступа к базе данных ПДн, изменение и удаление

Хранение ПДн - сохранение ПДн у себя в базах данных или другом месте

Оператор ПДн – юридическое или физическое лицо организующее или обрабатывающее ПДн, определяющие цель, состав ПДн.

Оператором может стать любой бизнес, у которого есть сотрудники, клиентская база или сайт где собираются email, телефон для регистрации

Безопасность ПДн

Информационная система ПДн (ИСПД) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств



Примеры
ИсПДн



Безопасность ПДн

Правовое регулирование защиты ПДн:

ФЗ 152 «О персональных данных»

ФЗ 149 «Об информации, информационных технологиях и о защите информации»

Оператор ПДн обязан:

- Хранить данные на серверах расположенных в РФ
- Принимать меры по защите информации
- Ограничивать доступ к информации, если такая обязанность установлена федеральными законами

Информационная безопасность ПДн – защищенность ПДн и обрабатывающей инфраструктуры от случайных или намеренных воздействий, результатом которым будет нанесение ущерба информации, ее владельцам или инфраструктуре.

Безопасность ПДн. Состав ИСПДн



Безопасность ПДн. Средства защиты ИСПДн



Безопасность ПДн

Определение уровня защиты ИсПДн (УЗ)

Исходные данные

Категория ПДн

- Пдн, разрешенные субъектом Пдн для распространения
- Биометрические
- Специальные
- Иные

Объем ПДн

- Количество субъектов ПДн

Отношение между оператором и субъектом ПДн

- Сотрудник оператора
- Не сотрудник оператора

Актуальные угрозы безопасности ПДн

Актуальные угрозы



Угрозы 1 типа

если для ИсПДн актуальны угрозы связанные с НДВ в системном ПО



Угрозы 2 типа

если для ИсПДн актуальны угрозы связанные с НДВ в прикладном ПО



Угрозы 3 типа

если для ИсПДн актуальны угрозы не связанные с системным и прикладным ПО

Безопасность ПДн

Уровни защищенности

УЗ № 1

- ИсПДн для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к **значительным негативным** последствиям для субъектов персональных данных (жизнь, здоровье)

УЗ № 2

- ИсПДн для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных

УЗ № 3

- незначительные негативным последствиям для субъектов персональных данных

УЗ № 4

- не приводит к негативным последствиям для субъектов персональных данных

! От уровня защищенности зависит выбор средств защиты ИсПДн



Безопасность ПДн

Категория ПДн	Специальные			Биометрия	Иные			Общедоступные		
Сотрудники	нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов	> 100 тыс.	< 100 тыс.			> 100 тыс.	< 100 тыс.		> 100 тыс.	< 100 тыс.	
Тип актуальных угроз	УЗ 1	УЗ 1	УЗ 1	УЗ 1	УЗ 1	УЗ 2	УЗ 2	УЗ 2	УЗ 2	УЗ 2
	УЗ 1	УЗ 2	УЗ 2	УЗ 2	УЗ 2	УЗ 3	УЗ 3	УЗ 2	УЗ 3	УЗ 3
	УЗ 2	УЗ 3	УЗ 3	УЗ 3	УЗ 3	УЗ 4	УЗ 4	УЗ 4	УЗ 4	УЗ 4

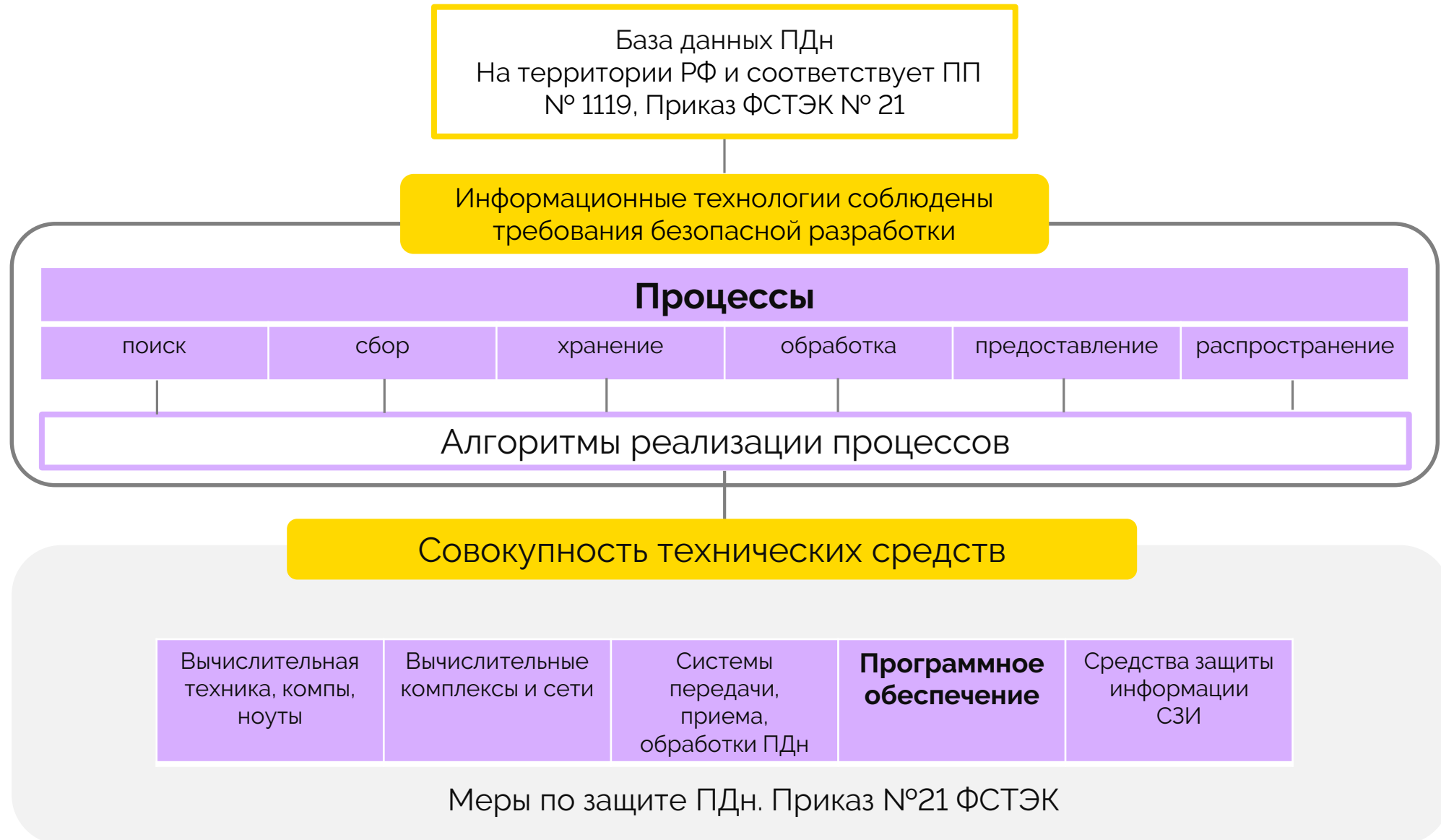
***Общедоступные – разрешенные субъектом ПДн для распространения**

Разработка ИСПДн

Базовый состав мер для безопасности ПДн. Приказ ФСТЭК №21

- идентификация и аутентификация субъектов доступа и объектов доступа
- управление доступом субъектов доступа к объектам доступа
- ограничение программной среды
- защита машинных носителей информации с ПДн
- регистрация событий безопасности
- антивирусная защита
- обнаружение (предотвращение) вторжений
- контроль (анализ) защищенности персональных данных
- обеспечение целостности ИСПДн
- обеспечение доступности персональных данных
- защита среды виртуализации
- защита технических средств
- защита информационной системы, ее средств, систем связи и передачи данных
- выявление инцидентов ИБ и реагирование на них
- управление конфигурацией **информационной системы** и **системы защиты** персональных данных

Безопасность ПДн. Разработка ИСПДн



Вопросы?



N*

**Спасибо
за внимание**

ФИТ Лекция N°5. 25'