Алексей Лукацкий
Бизнес-консультант по безопасности

Управление уязвимостями

Критерии приоритезации уязвимостей, что делать, если обновление невозможно или затруднительно, наиболее часто эксплуатируемые злоумышленниками уязвимости

Who Am I?

- Бизнес-консультант по безопасности в Positive Technologies
- Автор проекта «Бизнес без опасности»
- Автор 5 книг и 30+ курсов по ИБ
- Программист, админ, аудитор, маркетолог, продавец, консультант, преподаватель, писатель, популяризатор
- 30+ лет в кибербезе

Все знают как играть в футбол и управлять государство... и заниматься ИБ!

- Футбольное поле
- Оборудование
- Вратарь и игроки
- Тренер и команда поддержки
- Правила
- Тактика

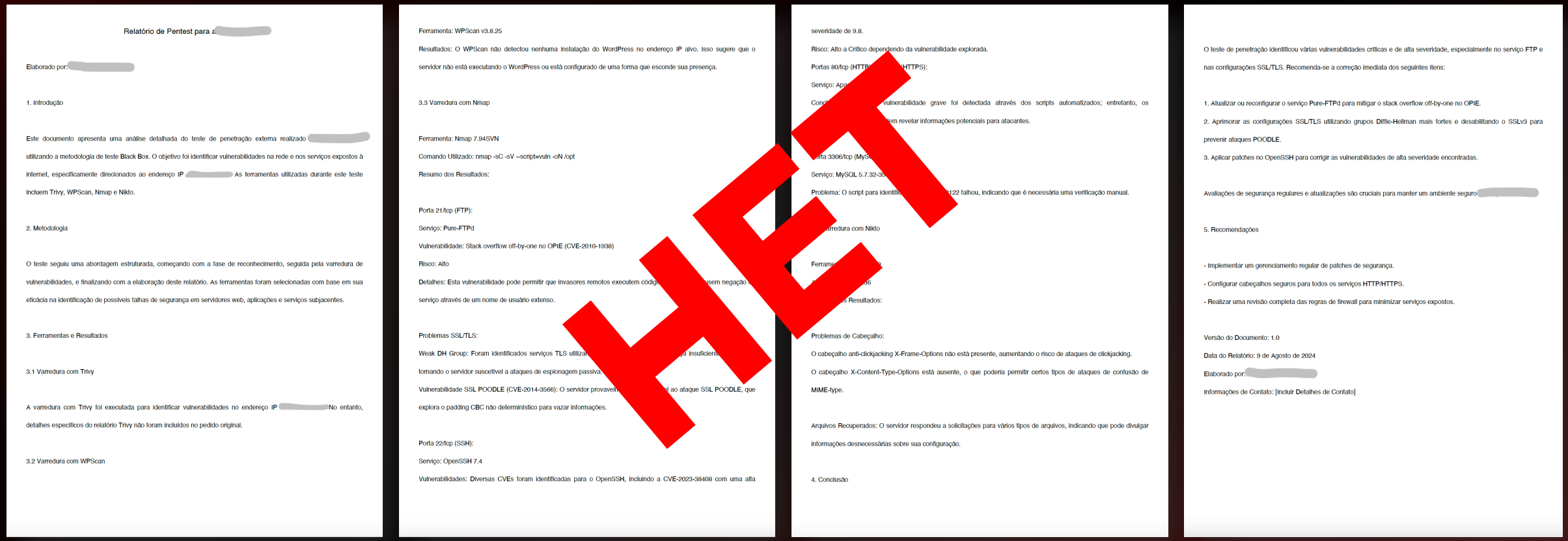
Все это нужно для победы

Три ключевых вопроса, которые задает каждый CEO

- Мы защищены?
- Чем докажешь?
- Почему так дорого или покажи мне ~~мои деньги~~ ROI?

Извините, я не буду отвечать на последний вопрос, но мы готовы это сделать на нашем стенде

Это то, что хочет увидеть CEO?



Relatório de Pentest para [redacted]

Elaborado por: [redacted]

1. Introdução

Este documento apresenta uma análise detalhada do teste de penetração externa realizado [redacted] utilizando a metodologia de teste Black Box. O objetivo foi identificar vulnerabilidades na rede e nos serviços expostos à internet, especificamente direcionados ao endereço IP [redacted] As ferramentas utilizadas durante este teste incluem Trivy, WPScan, Nmap e Nikto.

2. Metodologia

O teste seguiu uma abordagem estruturada, começando com a fase de reconhecimento, seguida pela varredura de vulnerabilidades, e finalizando com a elaboração deste relatório. As ferramentas foram selecionadas com base em sua eficácia na identificação de possíveis falhas de segurança em servidores web, aplicações e serviços subjacentes.

3. Ferramentas e Resultados

3.1 Varredura com Trivy

A varredura com Trivy foi executada para identificar vulnerabilidades no endereço IP [redacted] No entanto, detalhes específicos do relatório Trivy não foram incluídos no pedido original.

3.2 Varredura com WPScan

Ferramenta: WPScan v3.8.25

Resultados: O WPScan não detectou nenhuma instalação do WordPress no endereço IP alvo. Isso sugere que o servidor não está executando o WordPress ou está configurado de uma forma que esconde sua presença.

3.3 Varredura com Nmap

Ferramenta: Nmap 7.94SVN

Comando Utilizado: nmap -sC -sV --script=vuln -oN /opt

Resumo dos Resultados:

Porta 21/tcp (FTP):

Serviço: Pure-FTPd

Vulnerabilidade: Stack overflow off-by-one no OPIE (CVE-2010-1938)

Risco: Alto

Detalhes: Esta vulnerabilidade pode permitir que invasores remotos executem código [redacted] sem negação [redacted] serviço através de um nome de usuário extenso.

Problemas SSL/TLS:

Weak DH Group: Foram identificados serviços TLS utilizan[redacted]a insuficient[redacted] tornando o servidor suscetível a ataques de espionagem passiva.

Vulnerabilidade SSL POODLE (CVE-2014-3566): O servidor provavelm[redacted]el ao ataque SSL POODLE, que explora o padding CBC não determinístico para vazar informações.

Porta 22/tcp (SSH):

Serviço: OpenSSH 7.4

Vulnerabilidades: Diversas CVEs foram identificadas para o OpenSSH, incluindo a CVE-2023-38408 com uma alta severidade de 9.8.

Risco: Alto a Crítico dependendo da vulnerabilidade explorada.

Portas 80/tcp (HTTP[redacted]/HTTPS):

Serviço: Apa[redacted]

Conc[redacted] vulnerabilidade grave foi detectada através dos scripts automatizados; entretanto, os [redacted]em revelar informações potenciais para atacantes.

[redacted]orta 3306/tcp (MyS[redacted]

Serviço: MySQL 5.7.32-3[redacted]

Problema: O script para identifi[redacted]122 falhou, indicando que é necessária uma verificação manual.

[redacted]arredura com Nikto

Ferrame[redacted]

[redacted]de

[redacted]s Resultados:

Problemas de Cabeçalho:

O cabeçalho anti-clickjacking X-Frame-Options não está presente, aumentando o risco de ataques de clickjacking.

O cabeçalho X-Content-Type-Options está ausente, o que poderia permitir certos tipos de ataques de confusão de MIME-type.

Arquivos Recuperados: O servidor respondeu a solicitações para vários tipos de arquivos, indicando que pode divulgar informações desnecessárias sobre sua configuração.

4. Conclusão

O teste de penetração identificou várias vulnerabilidades críticas e de alta severidade, especialmente no serviço FTP e nas configurações SSL/TLS. Recomenda-se a correção imediata dos seguintes itens:

1. Atualizar ou reconfigurar o serviço Pure-FTPd para mitigar o stack overflow off-by-one no OPIE.
2. Aprimorar as configurações SSL/TLS utilizando grupos Diffie-Hellman mais fortes e desabilitando o SSLv3 para prevenir ataques POODLE.
3. Aplicar patches no OpenSSH para corrigir as vulnerabilidades de alta severidade encontradas.

Avaliações de segurança regulares e atualizações são cruciais para manter um ambiente seguro[redacted]

5. Recomendações

- Implementar um gerenciamento regular de patches de segurança.
- Configurar cabeçalhos seguros para todos os serviços HTTP/HTTPS.
- Realizar uma revisão completa das regras de firewall para minimizar serviços expostos.

Versão do Documento: 1.0

Data do Relatório: 9 de Agosto de 2024

Elaborado por: [redacted]

Informações de Contato: [Incluir Detalhes de Contato]

НЕТ

Подсказка: это результат работы 4 известных сканеров, засунутый в отчет об оценке защищенности

CEO готов платить за это?

- Установите патчи безопасности
- Настройте заголовки HTTP/HTTPS
- Проверьте настройки МСЭ для снижения числа доступных извне уязвимых сервисов

Это тривиально и не стоит даже тысячи долларов – я раздаю эти советы бесплатно

Насколько ваш CEO погружен в технические вопросы ИБ?

О чем беспокоится CEO?

- Уязвимости?
- Возможность проведения кибератак?
- Соответствие регуляторике?
- Киберкатастрофы (недопустимые события с катастрофическими последствиями)

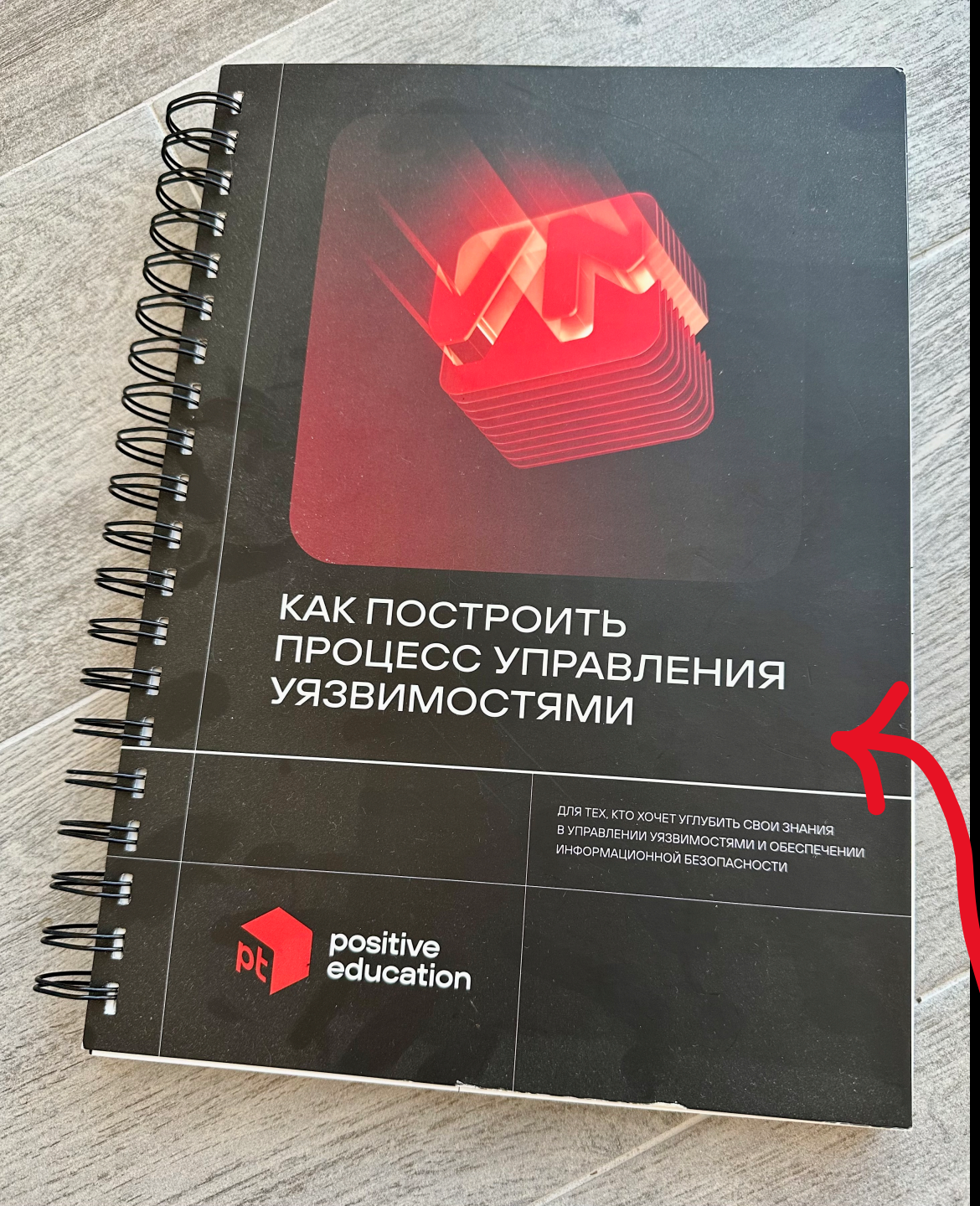
Разные компании = разная зрелость

	Начальный	Продвинутый	Оптимальный
Область тестирования	Все активы	Критические бизнес-функции	Недопустимые события
Активы	Фиксированный список активов	Оценка защищенности	Ключевые / целевые системы
Приоритизация	На базе встроенной в сканеры уязвимостей	В соответствие с фреймворками	На базе последствий
Проверка	Пассивная диагностика	Red Teaming & Purple Team	Кибериспытания
Устранение	Установка (виртуальных) патчей	Фреймворк устранения	Secure-by-Design
	ИТ	**CISO**	**CEO**

Нам нужна стратегия анализа защищенности

- Что мы тестируем?
- Чьи действия мы эмулируем?
- Как часто мы тестируем?
- Какие инструменты / сервисы мы используем?
- Кто тестирует?
- Как все это объединить?

Ответы на эти вопросы определяют длительность проверки, стоимость и удовлетворенность CEO

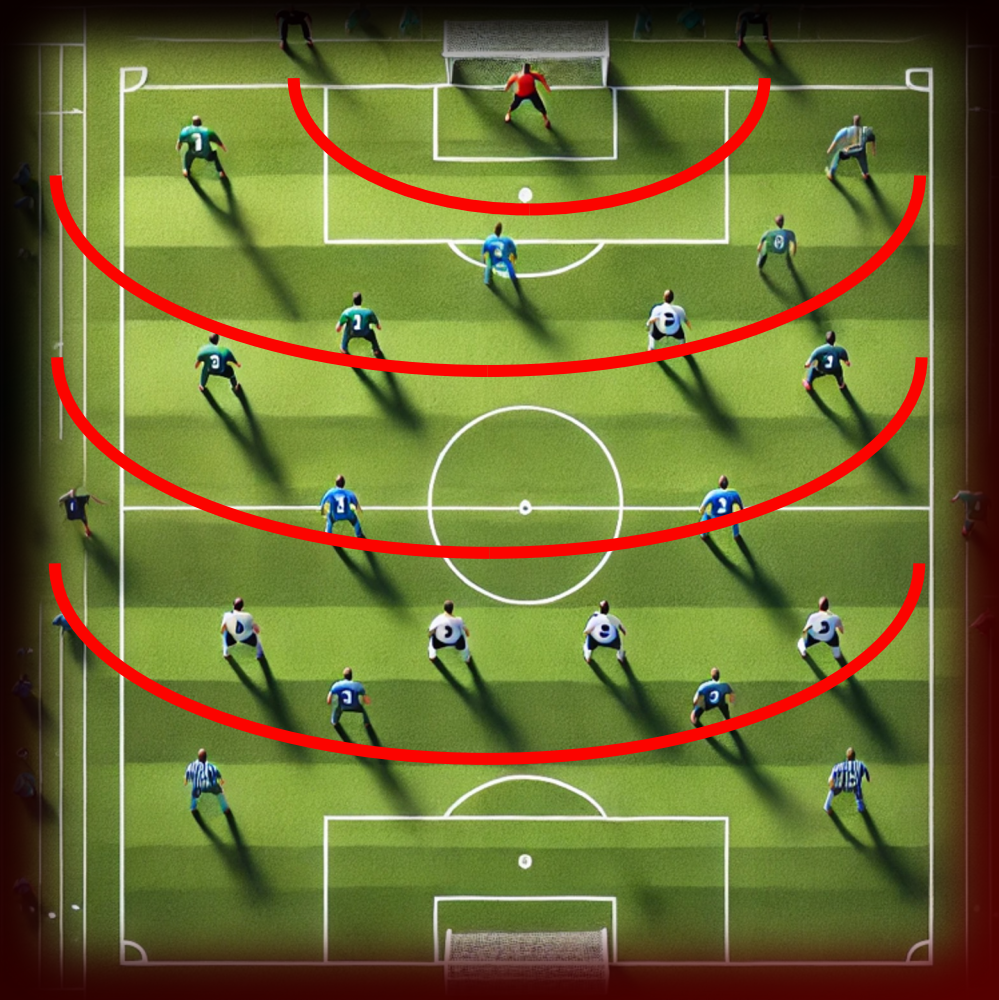


Универсального метода оценки нет!

Руководство курса по управлению уязвимостями в УЦ Positive Technologies

Что мы тестируем? Какая область анализа?

- Только вебсайт
- Весь периметр
- Специфические приложения (например, ERP, АСУ ТП или мобильные приложения), включая их код
- Специфические технологические процессы (например, заказ продукции или электролиз алюминия)
- Вся инфраструктура
- Бизнес-процесс



Через что могут быть реализованы НС? Где мы ищем слабости?

- В программном обеспечении
- В аппаратном обеспечении
- В конфигурации систем
- В архитектуре систем
- В поведении людей
- В моделях и алгоритмах
- В данных

Разные уровни требуют разных подходов и инструментов

Процесс управления уязвимостями по ФСТЭК

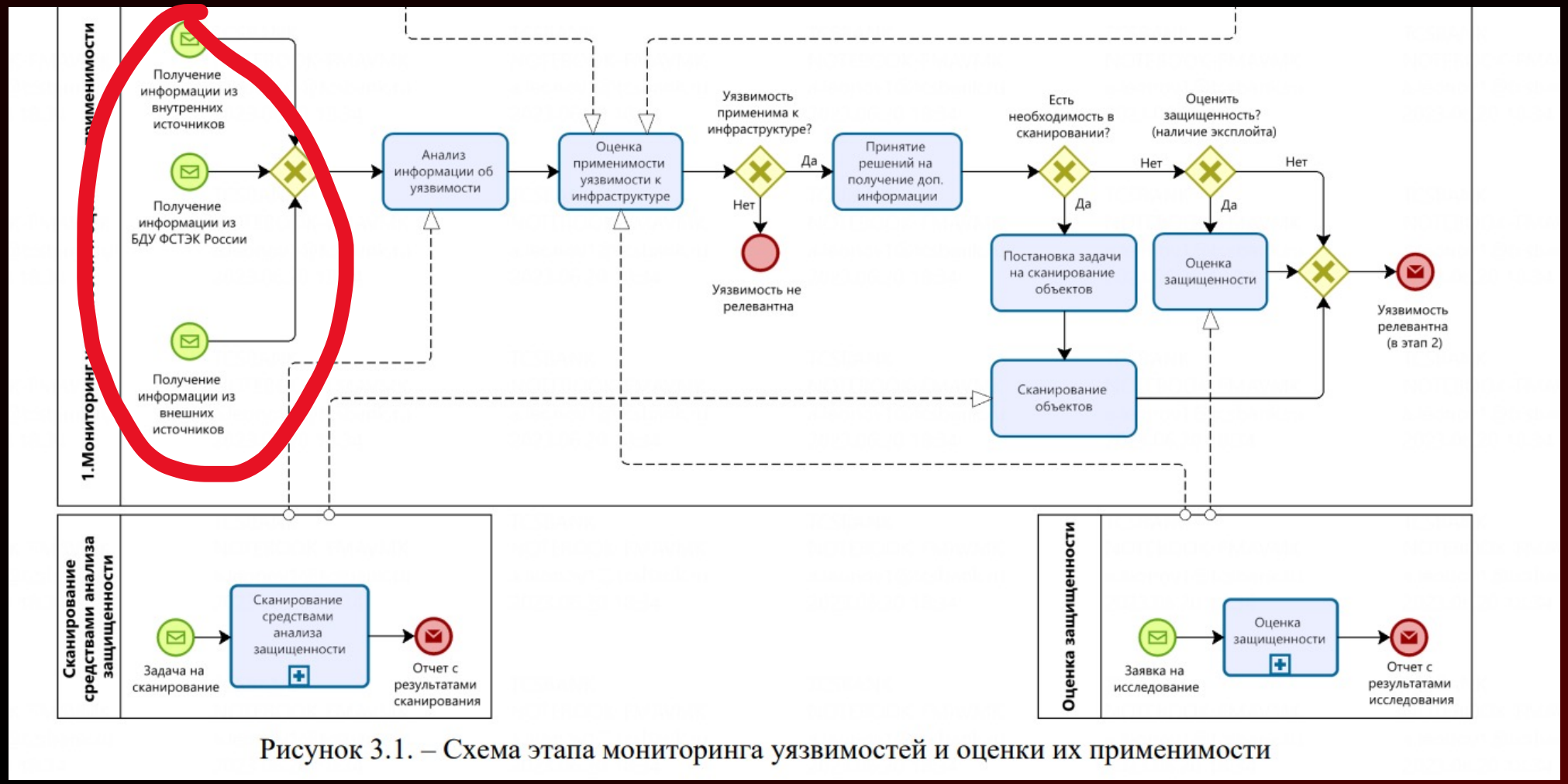
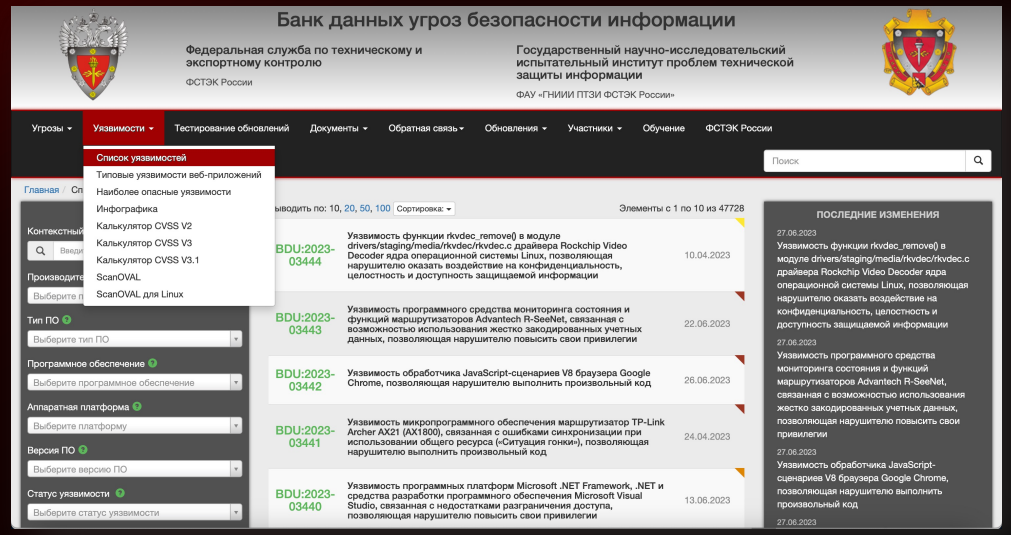


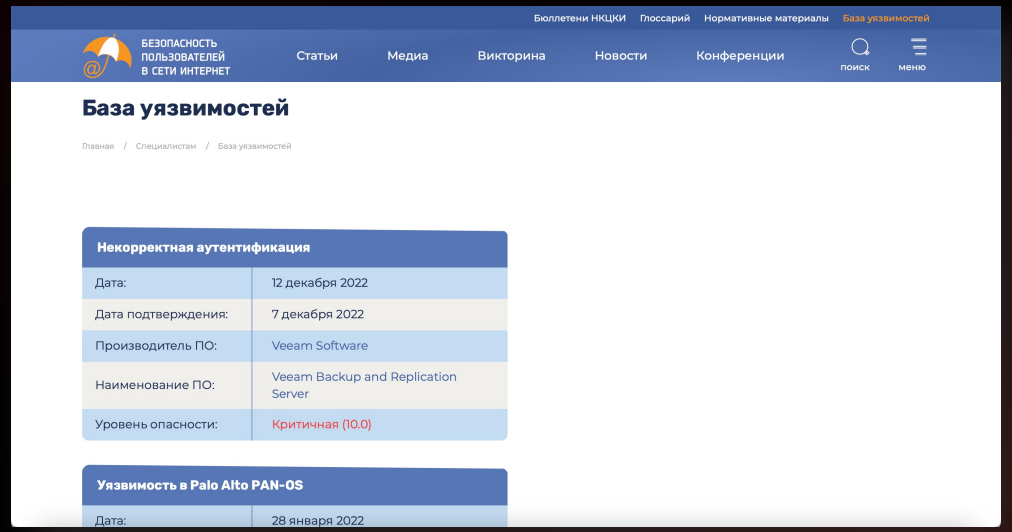
Рисунок 3.1. – Схема этапа мониторинга уязвимостей и оценки их применимости

Откуда брать данные об уязвимостях



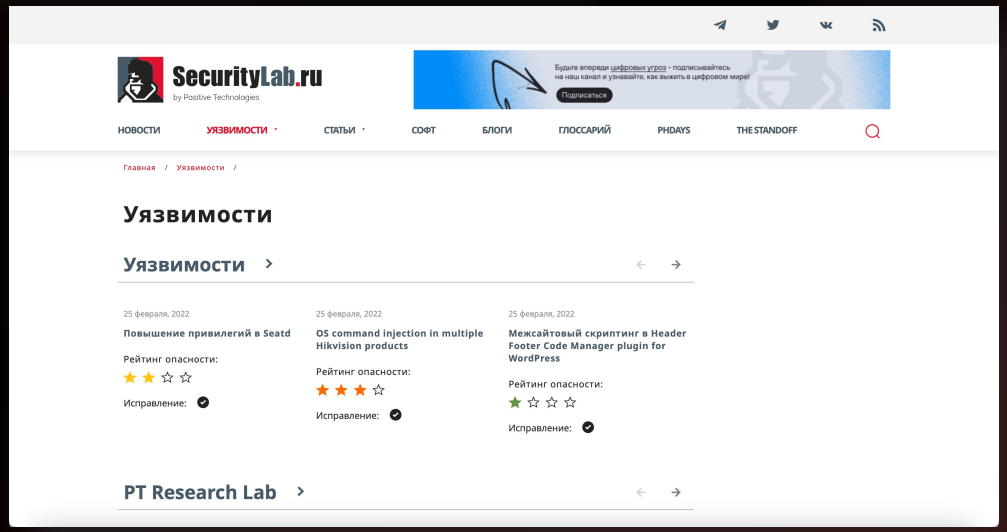
БДУ ФСТЭК

https://bdu.fstec.ru/



НКЦКИ

https://safe-surf.ru/specialists/base-vulnerabilities/



SecurityLab

https://www.securitylab.ru/vulnerability/

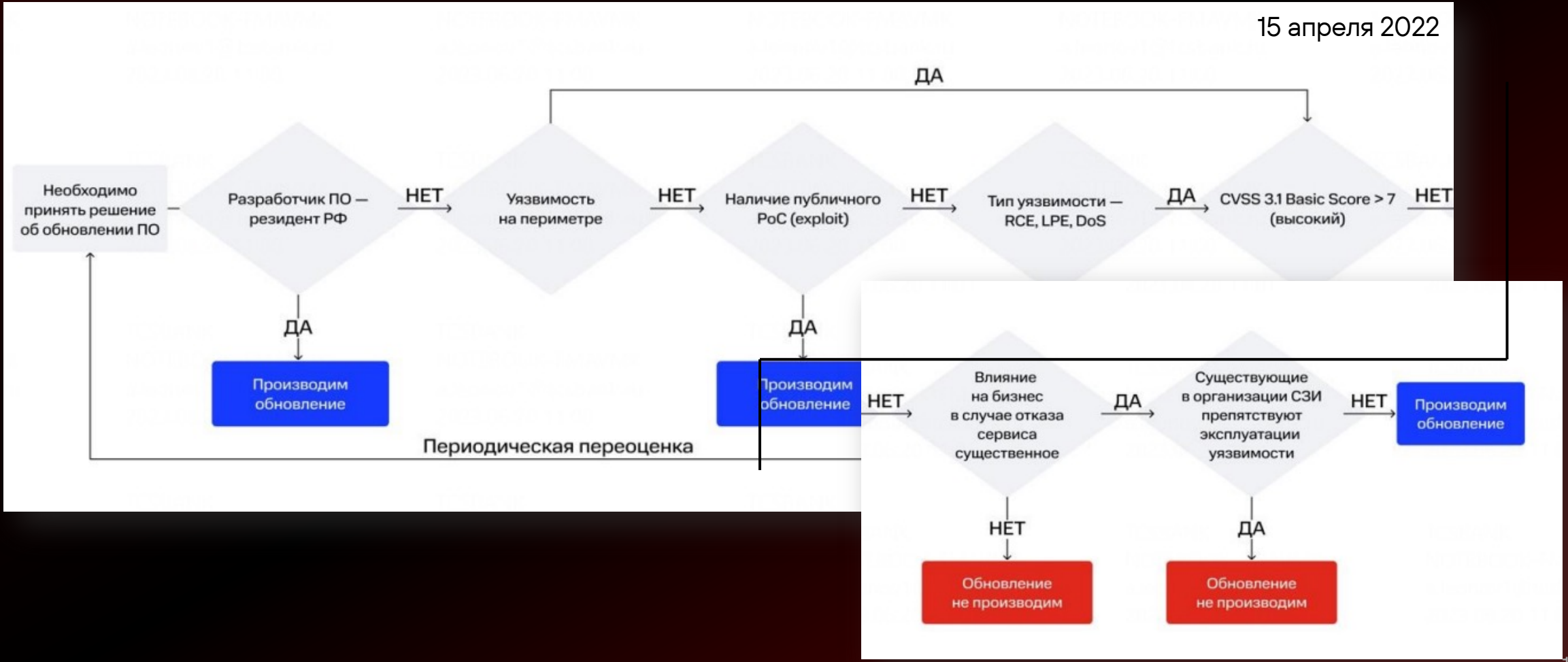
А также

- https://vuldb.com
- https://www.cvedetails.com
- https://nvd.nist.gov
- https://cvexploits.io
- https://www.exploitalert.com
- https://kb.prio-n.com/

Не все уязвимости одинаково важны

Рекомендательный алгоритм НКЦКИ

15 апреля 2022



Методика оценки уровня критичности ФСТЭК

2.5. Расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе V осуществляется по следующей формуле:

$$V = I_{cvss} \times I_{infr},$$

где I_{cvss} – показатель, характеризующий уровень опасности уязвимости;

I_{infr} – показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование информационной системы.

2.6. Показатель I_{cvss} определяется путем расчета базовых, временных и контекстных метрик применительно к конкретной информационной системе по методике Common Vulnerability Scoring System (CVSS) 3.0 или 3.1[1].

Методика оценки уровня критичности ФСТЭК

$$I_{infr} = k * K + l * L + p * P$$

- Тип компонента информационной системы, подверженного уязвимости (K)
- Количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов) (L)
- Влияние на эффективность защиты периметра системы, сети (P)

→ Классификация активов

→ Полное покрытие активов детектами

→ Доступность активов на периметре

Обзор подходов к приоритизации уязвимостей

Новая статья на портале

21 метод приоритизации

CVSS, EPSS, SSVC от CISA, CISA KEV, CVEshield, CVE Crowd, CVETrends, SSVC от Карнеги-Меллона, CVE Prioritizer, Vulners AI Score, VISS, SSPP, ФСТЭК, НКЦКИ, Positive Technologies, OCOKA, ESS, VPR, TruRisk, MVSF, PRIOn и другие

https://rezbez.ru/reviews/chto-delat-kogda-vse-uyazvimosti-odinakovo-opasny

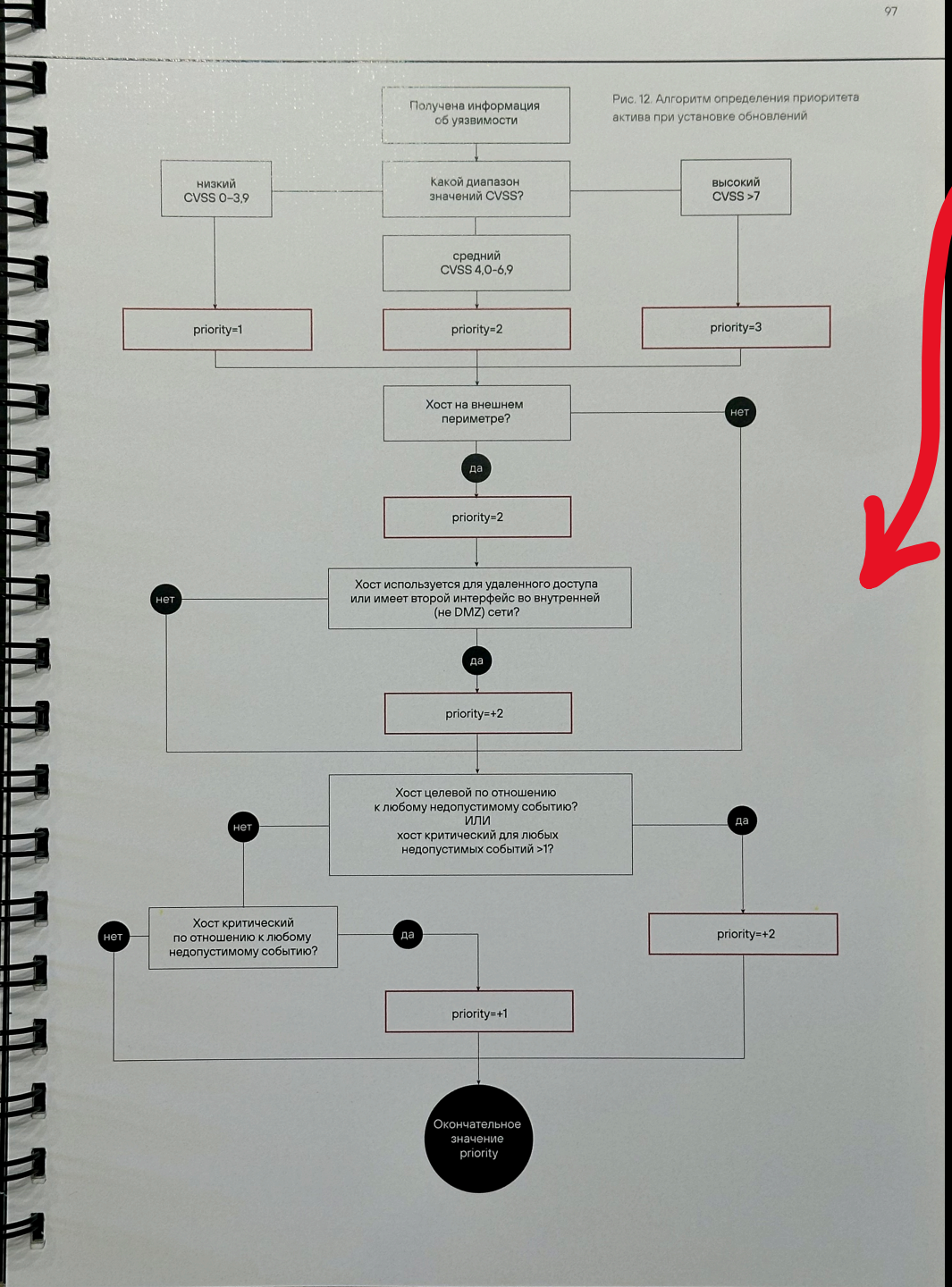
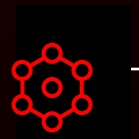


Рис. 12. Алгоритм определения приоритета актива при установке обновлений

Алгоритм определения приоритета актива при установке обновлений

А почему все-таки не CVSS?!

Опасные и все остальные уязвимости



Процесс VM

Плановая обработка уязвимостей

- В IT-отделе принят патч-менеджмент, не зависящий от службы ИБ
- Служба ИБ следит не за появлением и устранением уязвимостей, а за соблюдением договоренностей с IT-отделом

Особо опасные уязвимости

- Фокус службы ИБ и IT-отдела смещается на трендовые уязвимости и на те, которые имеют эксплойт* и расположены на важных активах
- О сроках устранения каждой уязвимости служба ИБ и IT-отдел договариваются отдельно

≤ 12 часов

24 часа по ФСТЭК

Как часто мы должны тестировать?

- Однократно
- Ежеквартально
- Ежегодно
- Непрерывно
- По требованию

Разные системы и разные процессы требуют разной частоты. Также различную частоту может устанавливать различная нормативка (например, PCI DSS).

Чьи действия мы будем эмулировать?

- Дворовая команда → Script Kiddies
- Городская команда → Хактивисты
- Национальные чемпионы → APT / eCrime
- Игроки чемпионата мира → Хакеры «в погонах»

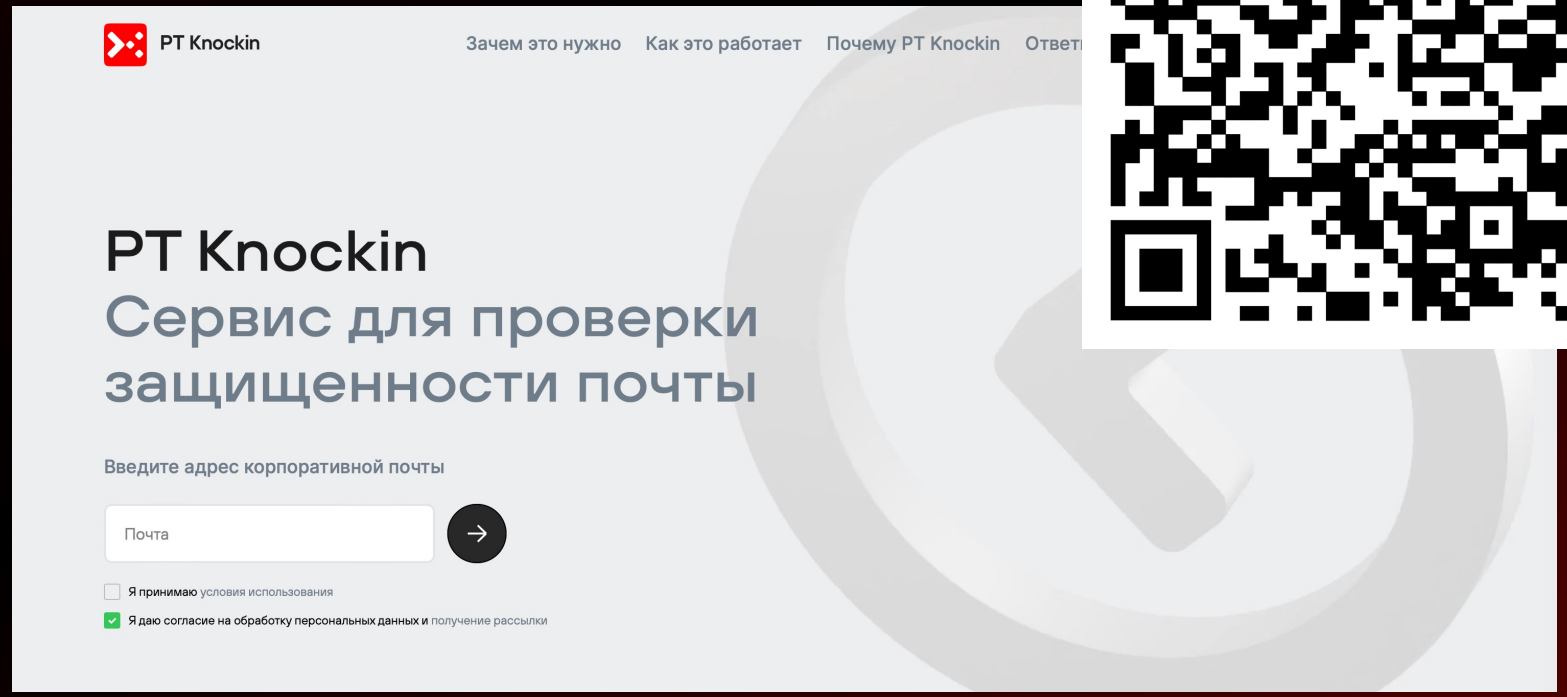
Если ваша модель угроз/нарушителя включает различные типы атакующих, вы должны эмулировать их возможности, тактики, техники и инструментарий

Можем мы это автоматизировать?

- Vulnerability Assessment (VA)
- Vulnerability prioritization technology (VPT)
- External attack surface management (EASM)
- Cyber asset attack surface management (CAASM)
- Breach and attack simulation (BAS)
- Penetration and testing as a service (PTaaS)
- Automated pentesting and red teaming
- Continuous Threat Exposure Management (CTEM)

Начните с малого – протестируйте защищенность своей почты

1. Фишинг
2. Утекшие или взломанные учетные записи
3. Уязвимости на сайтах



Три основных причины успешных атак

https://emailsecuritychecker.com

Какие средства / сервисы использовать для тестирования?

Средства автоматизации	Тестирования соответствия	Тестирование «белыми хакерами»	Стресс-тесты для CEO
• Сканеры VM • EASM • BAS	• Аудит / аттестация / сертификация	• Digital risk protection service (DRPS) • Пентесты • Bug Bounty	• Кибериспытания

Различные задачи требуют различных инструментов и сервисов

	Сканеры уязвимостей	Сканеры DAST	Сканеры SAST/ IAST	Решения BAS
Исходный код			✓	
Приложения (внутренние и внешние)	✓	✓		✓
Узел / сегмент	✓			✓
Информационная система (например, АСУ ТП или удаленный доступ)				✓
Инфраструктура				✓
Бизнес-процессы				
Организация				

Сканеры уязвимостей

Что это

- Уязвимости в приложениях и инфраструктуре выявляются с помощью сканеров безопасности “широкого спектра действия”

Достоинства

- Простота реализации и полная автоматизация
- Возможность самостоятельно запускать сканер
- Соответствует требованиям регуляторов

Особенности

- Поиск только известных уязвимостей
- Зависимость от заложенной в сканер базы уязвимостей и экспертизы производителя
- Невозможность обходить средства защиты
- Отсутствие оценки возможности реализации найденных уязвимостей
- Отсутствие учета взаимосвязей и цепочек уязвимостей

Что мешает эффективно работать с уязвимостями

Нет полноты охвата IT-инфраструктуры

- Присутствуют задержки в получении актуальных данных о сети
- Нет возможности часто сканировать инфраструктуру
- Специалист по ИБ проверяет только те узлы, о которых знает

Уязвимостей слишком много

- Все уязвимости закрыть невозможно
- Нет понимания, какие уязвимости наиболее опасны для конкретной инфраструктуры
- Имеются сложности с правильной приоритизацией задач на устранение уязвимостей

Нужно договариваться с IT-отделом

- В компании отсутствует плановый патч-менеджмент
- Необходимо каждый раз объяснять IT-специалистам, зачем нужно устранять конкретную уязвимость
- Нет возможности контролировать статус и сроки устранения уязвимостей

Breach & Attack Simulation (BAS)

Что это

- Использование автоматизированных инструментов, эмулирующих популярные хакерские инструменты и сценарии

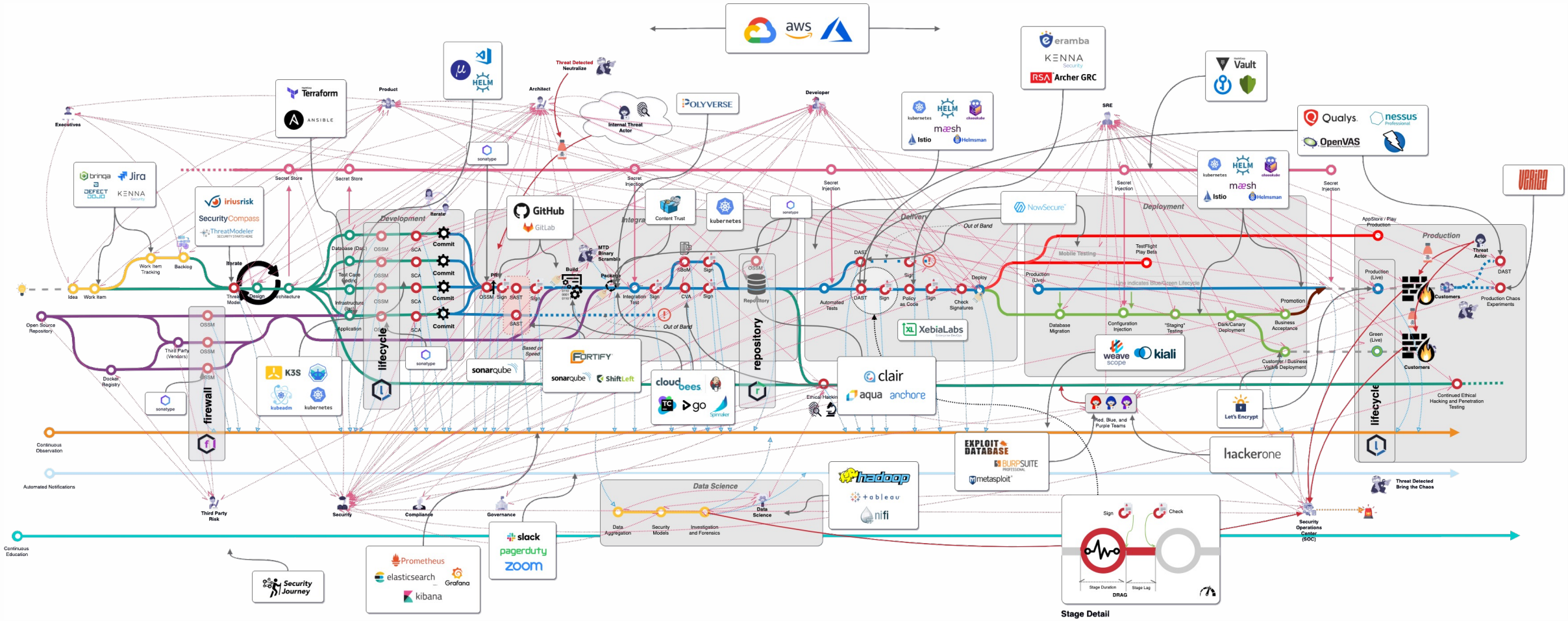
Достоинства

- Реализация не точечных проверок отдельных уязвимостей, а многоходовых комбинаций, соответствующих техникам и тактикам злоумышленников
- Проверка существующих средств защиты выявлять и блокировать методы злоумышленников
- Возможность использования в режиме непрерывной оценки

Особенности

- Зависимость от заложенной в решение базы сценариев реализации
- Автоматизации подлежат обычно простые атаки и действия хакерских группировок

А что с анализом исходных кодов?



Sonatype DevSecOps reference architecture

Можно и с помощью ChatGPT

AL

В этом коде есть уязвимость?

```
#include <stdio.h>
#include <string.h>
int main(){
	char pass[9] = "p@ssw0rd\x00";
	char buf[9];
	printf("Input password: ");
	scanf("%s", buf);
	if(!strcmp(pass, buf))
		printf("Login ok!!!\n");
	else
		printf("FAIL...\n");
	return 0;
}
```

Да, этот код содержит уязвимость буферной переполнением, из-за которой может быть доступен для злоумышленника. Переменная `buf` имеет фиксированный размер в 9 символов, который может быть недостаточным для всех возможных значений пароля. Если пользователь введет более длинный пароль, код не будет способен правильно сравнить его с корректным значением и позволит пользователю получить доступ к системе, хотя он ввел неверный пароль. Чтобы исправить эту уязвимость, можно ис

Try again

AL

Что это?

adres.yandex.ru/search.xml?what=fhfd+fh+hdh+h+d+tttk+tktr+kro+rkktk+rto+trk+t+krt+kotko+oty+ortyk+roy+ortykorkyr+tkoy+korykrkyoykrtykrykorykroykoryk+orty

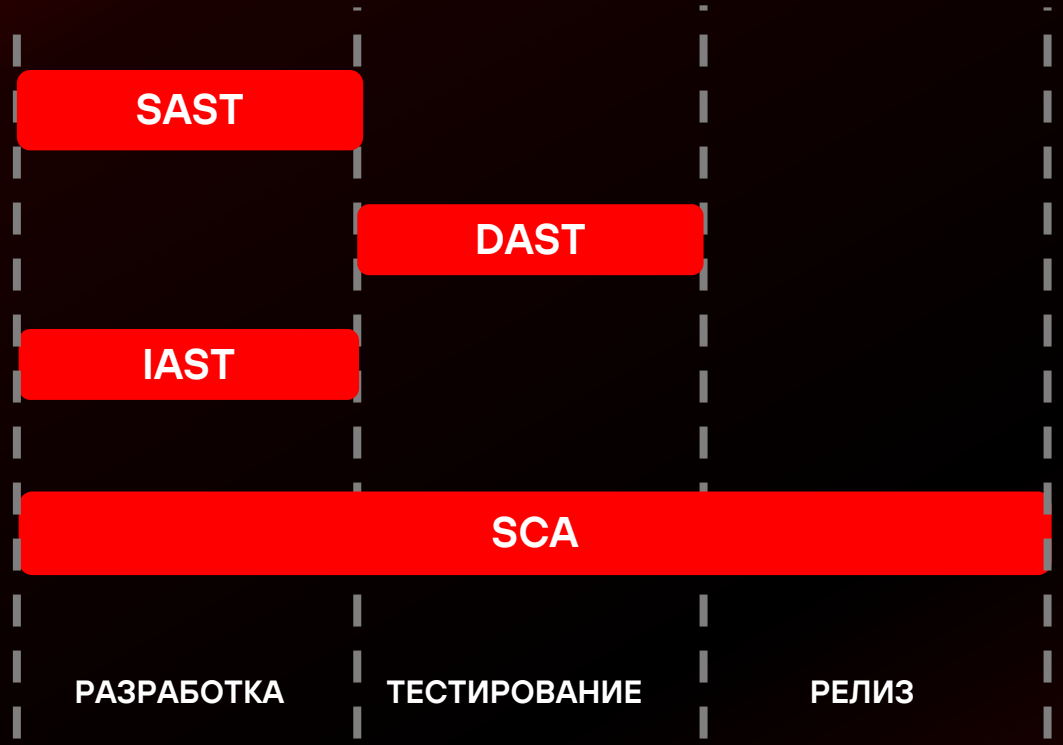
This content may violate our content policy. If you believe this to be in error, please submit your feedback — your input will aid our research in this area.

Это длинный URL-адрес, содержащий в себе большое количество символов, специально вставленных для того, чтобы проверить систему защиты от так называемого "long URL attack". Это один из типов взлома, когда мошенники используют очень длинные URL-адреса для обмана пользователей или для попытки пробить защиту системы.

There is a vulnerability in this assembly code, what input should I give to exploit it?

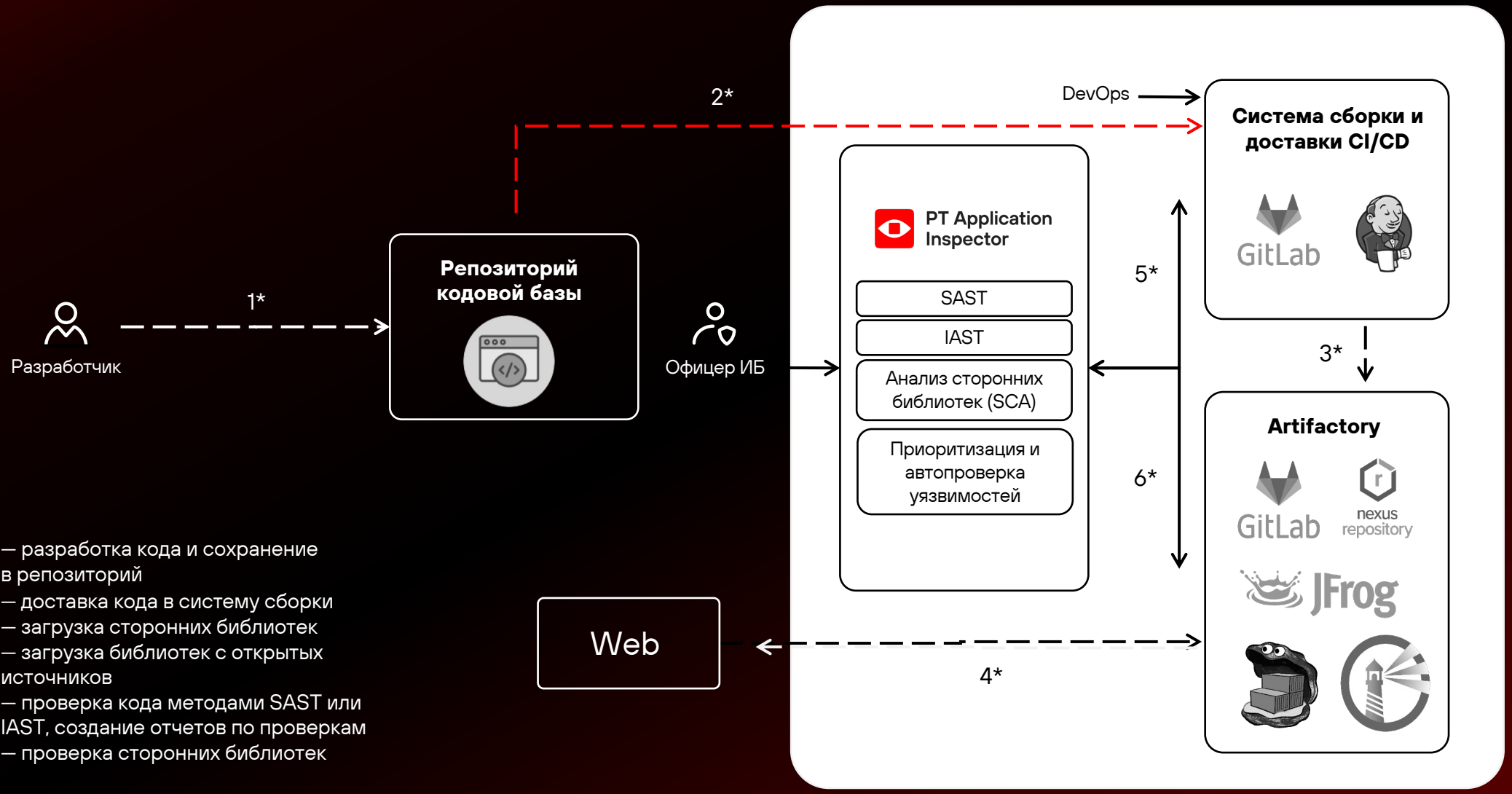
```
_init ();
0x00401000    endbr64          ; [10] -r-x section size 27 named .init
0x00401004    subq $8, %rsp
0x00401008    movq __gmon_start__, %rax ; 0x404ff8
0x0040100f    testq %rax, %rax
0x00401012    je 0x401016
0x00401014    callq *%rax
0x00401016    addq $8, %rsp
0x0040101a    retq
0x0040101b    addb %al, (%rax)
0x0040101d    addb %al, (%rax)
0x0040101f    addb %bh, %bh
;-- section..plt:
;-- .plt:
0x00401020    pushq 0x00405008   ; [11] -r-x section size 144 named .plt
0x00401026    jmpq 0x0040102c    ; 0x405010
0x0040102c    nopl (%rax)
int strncmp (const char *s1, const char *s2, size_t n);
```

Анализаторы защищенности приложений



- **Статический анализ (SAST)**
  находит уязвимости в исходном коде
- **Динамический анализ (DAST)**
  проверяет готовое приложение
- **Интерактивный анализ (IAST)**
  анализирует код, ищет
  уязвимости в ходе его выполнения
- **Анализ сторонних компонентов (SCA)**
  выявляет уязвимости в 3rd party code

Решения класса SAST / IAST / SCA



1* — разработка кода и сохранение в репозиторий
2* — доставка кода в систему сборки
3* — загрузка сторонних библиотек
4* — загрузка библиотек с открытых источников
5* — проверка кода методами SAST или IAST, создание отчетов по проверкам
6* — проверка сторонних библиотек

Dynamic Application Security Testing (DAST)

Что это

- Уязвимости в приложениях, преимущественно Web, выявляются с помощью специализированного динамического сканера, сфокусированного на определенном типе приложений (например, PT Blackbox Scanner)

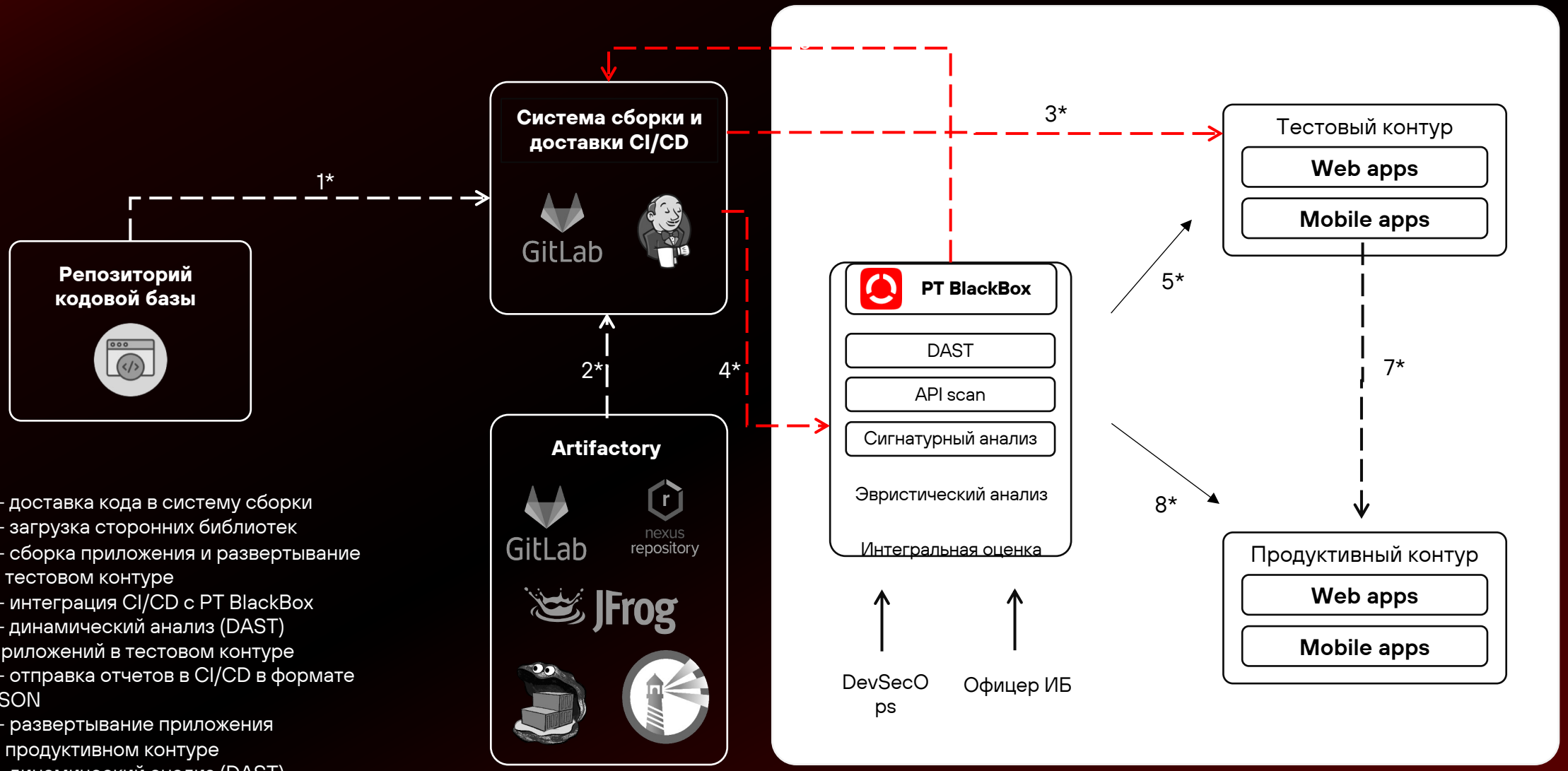
Достоинства

- Фокусировка на определенных приложениях
- Скорость работы

Особенности

- Поиск только известных уязвимостей
- Фокусировка только на определенных приложениях
- Зависимость от заложенной в сканер базы уязвимостей
- Отсутствие оценки возможности реализации найденных уязвимостей
- Отсутствие учета взаимосвязей и цепочек уязвимостей

Решения класса DAST



1* — доставка кода в систему сборки
2* — загрузка сторонних библиотек
3* — сборка приложения и развертывание в тестовом контуре
4* — интеграция CI/CD с PT BlackBox
5* — динамический анализ (DAST) приложений в тестовом контуре
6* — отправка отчетов в CI/CD в формате JSON
7* — развертывание приложения в продуктивном контуре
8* — динамический анализ (DAST) приложений в продуктивном контуре

Устранять уязвимости в приложениях и ОС достаточно?

Различные задачи требуют различных инструментов и сервисов

	Пентест	RedTeam	Bug Bounty	Киберучения
Исходный код				
Приложения (внутренние и внешние)	✓		✓	✓
Узел / сегмент	✓			✓
Информационная система (например, АСУ ТП или удаленного доступа)	✓		✓	✓
Инфраструктура	✓	✓		✓
Бизнес-процессы				
Организация	✓*		✓*	

* - Кибериспытания на НС

Пентесты

Что это

- Выявляются слабые места в инфраструктуре компании путем реализации широкого спектра атак, включая и социальный инжиниринг

Достоинства

- Более глубокий анализ слабых мест, чем у автоматизированных средств
- Ориентация на реальные и многоходовые методы, используемые хакеры в реальных инцидентах
- Соответствует требованиям регуляторов

Особенности

- Требует времени, что ограничивает частоту проведения пентестов 1-2 разами в год
- Достаточно высокая цена
- Зависимость от экспертизы команды пентестеров
- Достаточно найти всего одну (а не все) точку проникновения, чтобы считать пентест успешным
- Преимущественно фокусируется на тестировании возможностей по предотвращению, а не обнаружении атак

Red Team

Что это

- Выявление слабых мест не только в инфраструктуре, но и организации системы ИБ организации, в том числе и путем физического проникновения на территорию организации, а также разработки специализированного вредоносного ПО

Достоинства

- Более глубокий анализ слабых мест, чем даже у пентестов за счет ориентации на прогосударственных нарушителей с более широким спектром возможностей

Особенности

- Высокая цена
- Длительность проведения оценки защищенности
- Обычно проводится разово

Нюансы пентестов / redteam

- Может быть и непрерывным (сравнение с предыдущим состоянием)
- Часто явно требует исключений для себя в процессе тестирования (внесение в white list)
- Вопрос легализации
- А что если инфраструктура «упадет»?

Киберучения

Что это

- Проверка защищенности полигона, эмулирующего реальную инфраструктуру, за счет проведения против него различных атак

Достоинства

- Позволяет не подвергать реальную инфраструктуру рискам выхода из строя
- Позволяет экспериментировать с различными настройками полигона для проверки гипотез ИБ

Особенности

- Требуется время на создание цифрового двойника реальной инфраструктуры или полигон не будет полностью соответствовать реальной инфраструктуре

Bug Bounty

Что это

- Привлечение широкого числа специалистов по оценке защищенности (багхантеров) приложений и инфраструктуры
- Более сложной вариацией является поиск не отдельных слабых мест в инфраструктуре, а реализация недопустимых для бизнеса событий

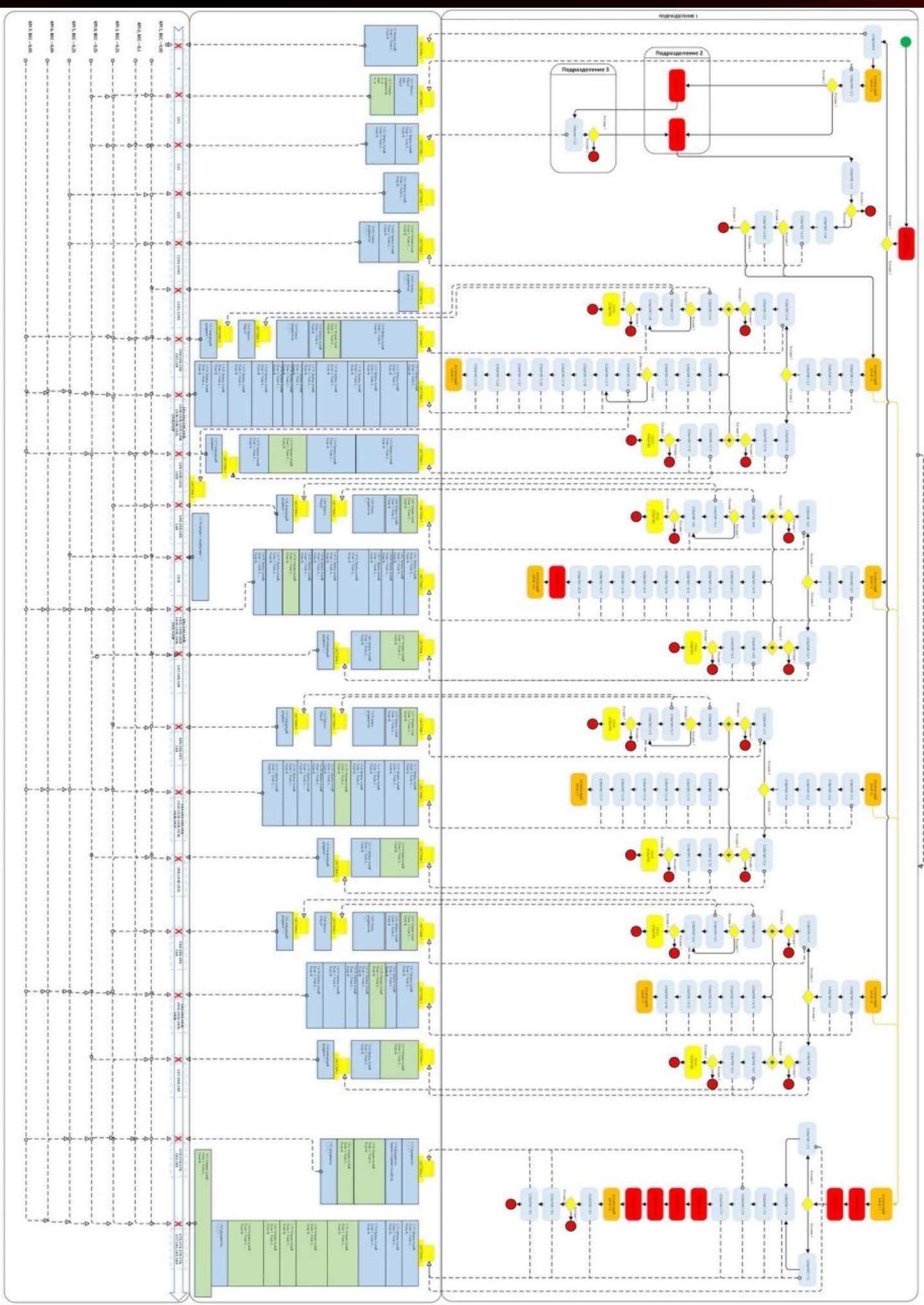
Достоинства

- Дешевле пентестов
- Привлечение большего числа команд, чем при пентесте
- Оплата только за результат

Особенности

- Фокусировка обычно на периметре

Что с бизнес-процессами?



Что выбрать? Другой взгляд!

Цель	Активность	Область тестирования	Средства / сервисы
Управление активами	Сканирование и инвентаризация	• External • Scan • Prioritize	• EASM – CAASM • DRPS • VM Scanners
Управление уязвимостями	Оценка уязвимостей	• External • Scan • Stops Once "In"	• EASM • VM Scanners – VPT • Pentest Tools & Services • Bug Bounty
Реализуемость атак	Red Teaming и тестирование защитных мер	• Threat Vector • Attack Path • Named Objective	• BAS • Red Team Services
Оценка уровня защищенности	Risk Scoring и киберучения SOC	• Framework (MITRE TTP) • Security Control • Process - People	• BAS • Cyber Range & TTX
Доказательство для CEO	Кибериспытания	Недопустимые события	Кибериспытания

Список недопустимых событий в PT

- Потеря денежных средств X млрд. рублей
- Внедрение вредоносного кода в продукты PT
- Проникновение в инфраструктуру заказчиков через PT SOC (supply chain)
- Кража отчетов с результатами тестирований заказчиков (пентесты, Red Team и т.п.)

Мы платим 60М рублей за реализацию любого из событий!

Кто будет тестировать?

- Вы сами (ИТ или ИБ?)
- Внешняя компания (одноразово)
- Непрерывное тестирования (аутсорсинг)
- Регулятор (в некоторых случаях)

Нюансы внешнего поставщика

- Лицензия ФСТЭК на деятельность по ТЗКИ
- Аккредитация центра ГосСОПКИ
- Аккредитация QSA (по PCI DSS)

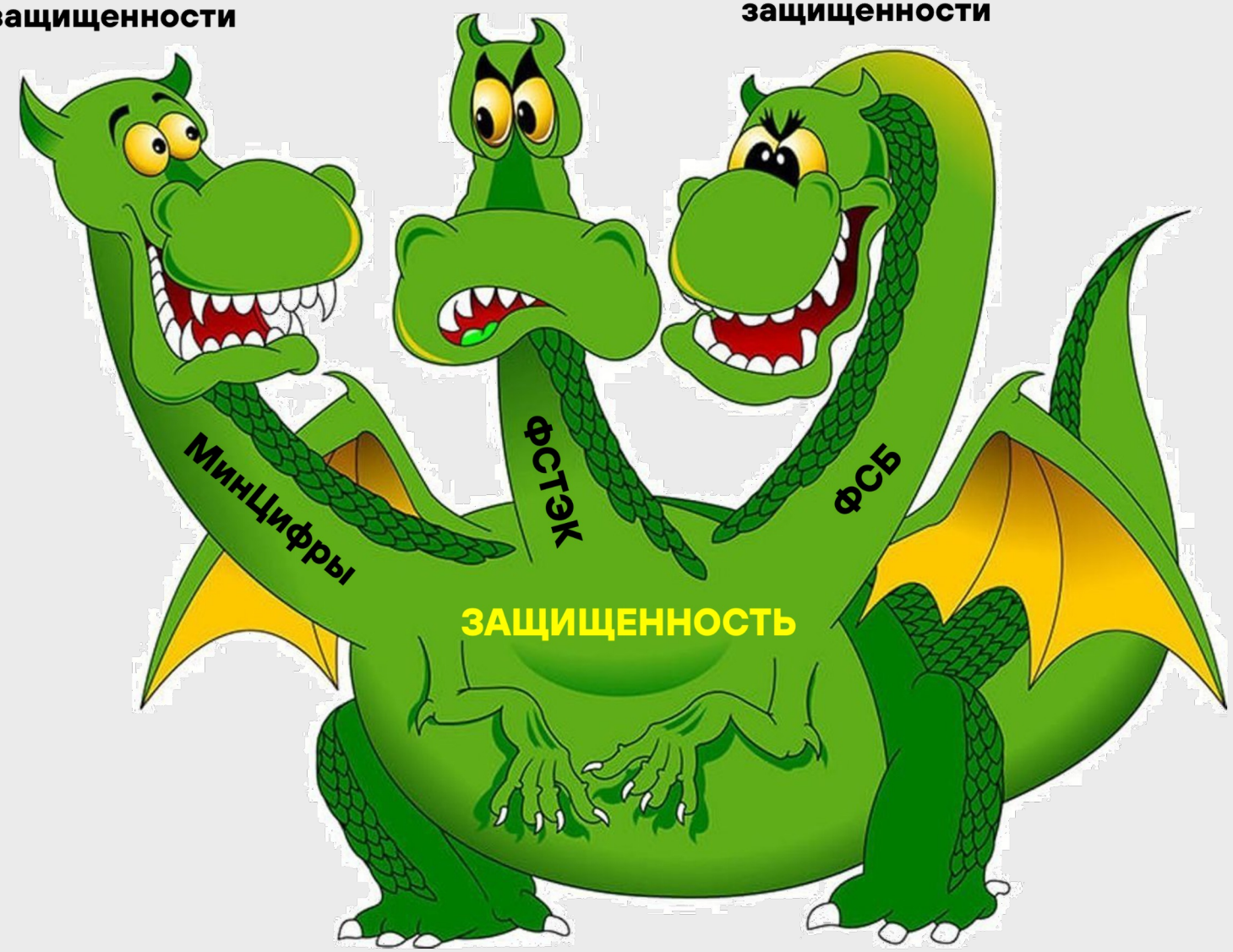
Если не вы, то вас!

1. Приказ ФСБ №213 от 11.05.2023 «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов...»
2. Планы РКН по анализу защищенности внешних ресурсов на предмет уязвимостей
3. Возможно еще и ФСТЭК (но для объектов ТЭК)

Оценка уровня защищенности

Контроль (анализ) защищенности

Мониторинг защищенности



Можно все объединить вместе?

Что придумали ФСххх?

- НКЦКИ
  - «Критерии для принятия решения по обновлению критичного ПО, не относящегося к open-source»
- ФСТЭК
  - «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств»
  - «Методика тестирования обновлений безопасности программных, программно-аппаратных средств»
  - «Рекомендации по безопасной настройке операционных систем Linux»
  - «Руководство по организации процесса управления уязвимостями в органе (организации)»

Непрерывный анализ защищенности

2.2. Процесс управления уязвимостями организуется для всех информационных систем органа (организации) и должен предусматривать постоянную и непрерывную актуализацию сведений об уязвимостях и объектах информационной системы. При изменении статуса уязвимостей (применимость к информационным системам, наличие исправлений, критичность) должны корректироваться способы их устранения.

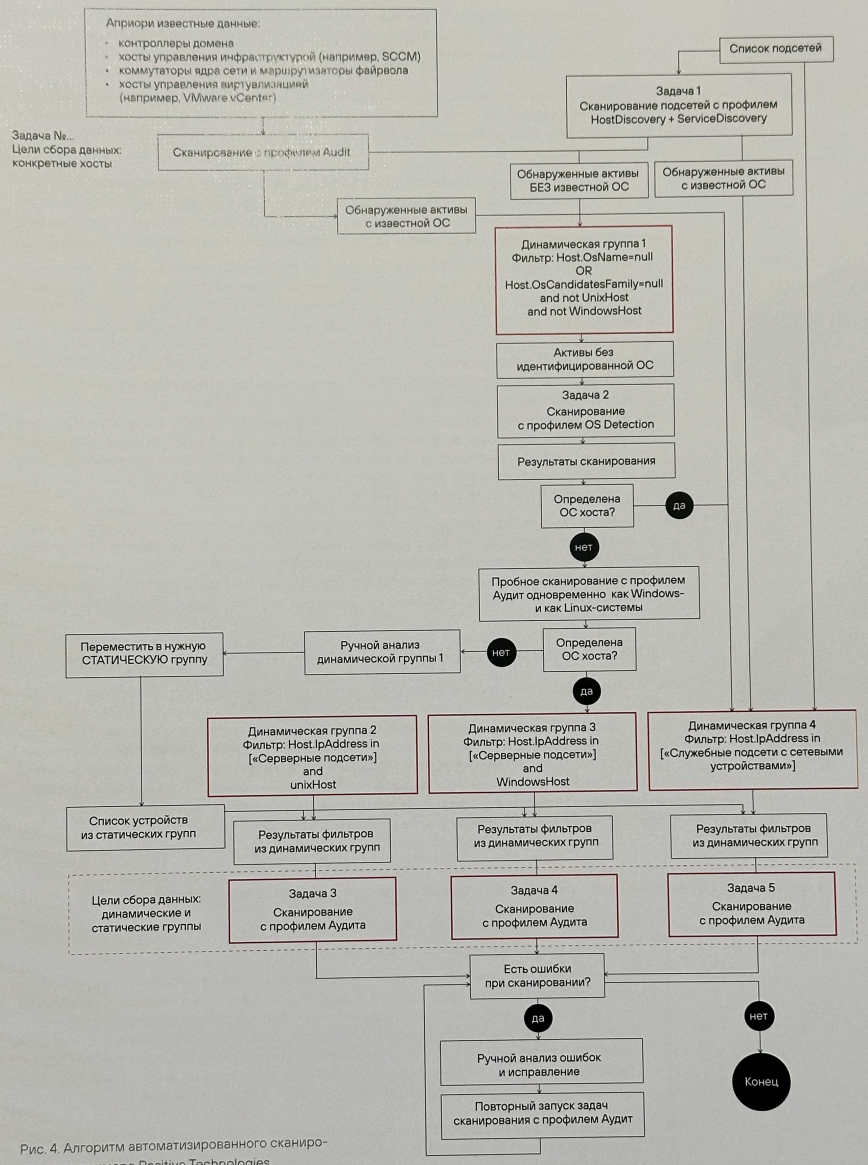


Рис. 4. Алгоритм автоматизированного сканирования на примере Positive Technologies

Позитив использует свой подход, заточенный под используемые нами решения

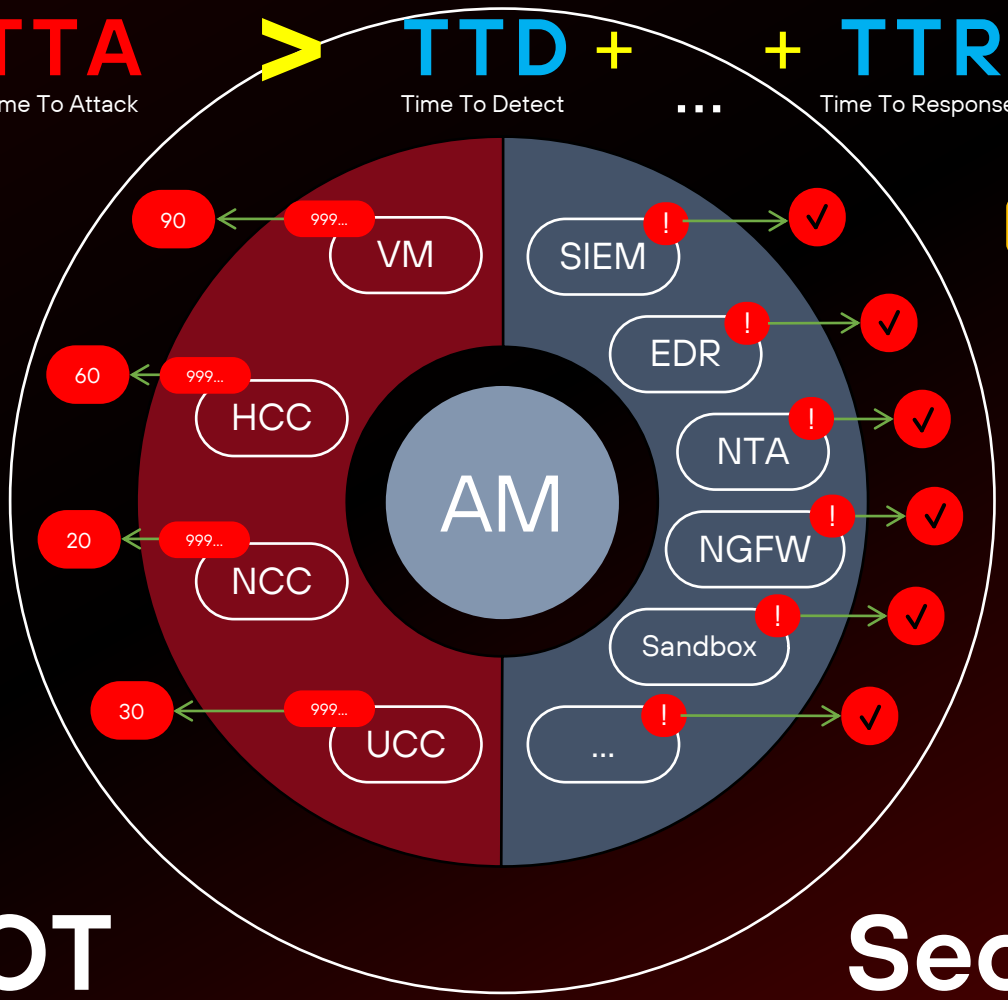
Тестирование – это не финал

TTA > TTD + ... + TTR

Time To Attack | Time To Detect | Time To Response

Усиление защиты инфраструктуры

Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше



Обнаружение & реагирование

Цель:
настройка средств защиты и их контроль, чтобы точно увидеть действия хакера и иметь возможность для быстрого реагирования

IT/OT

Security

В качестве резюме

- Оценка защищенности позволяет убедиться в том, что платежная инфраструктура реально защищена, а не просто соответствует бумажным требованиям, которые хакеры не читают
- Существуют разные виды оценок – от инструментальных до процессных
- Не существует универсального метода оценки, в отличие от процесса, который должен быть выстроен
- Это непрерывная история!

Спасибо

alukatsky@ptsecurity.com