академия softline

Организация цикла управления уязвимостями в корпоративной среде

Антон Носков
Руководитель отдела кибербезопасности и телекоммуникационных систем, ЯГТУ. Преподаватель направления «Информационная безопасность» Академии Softline

Через обучение - к успеху!
Знания работают на вас

Угрозы уязвимости и риски

Обнаружение угроз

Потенциальная опасность для ресурсов, таких как данные или сеть

Уязвимость и поверхность атаки

- **Слабое место в системе или ее проекте, которое может быть использовано угрозой.**
- **Поверхность атаки определяет различные точки, в которых хакер может проникнуть в систему и получить доступ к данным (пример — операционная система без исправлений безопасности)**

Эксплойт

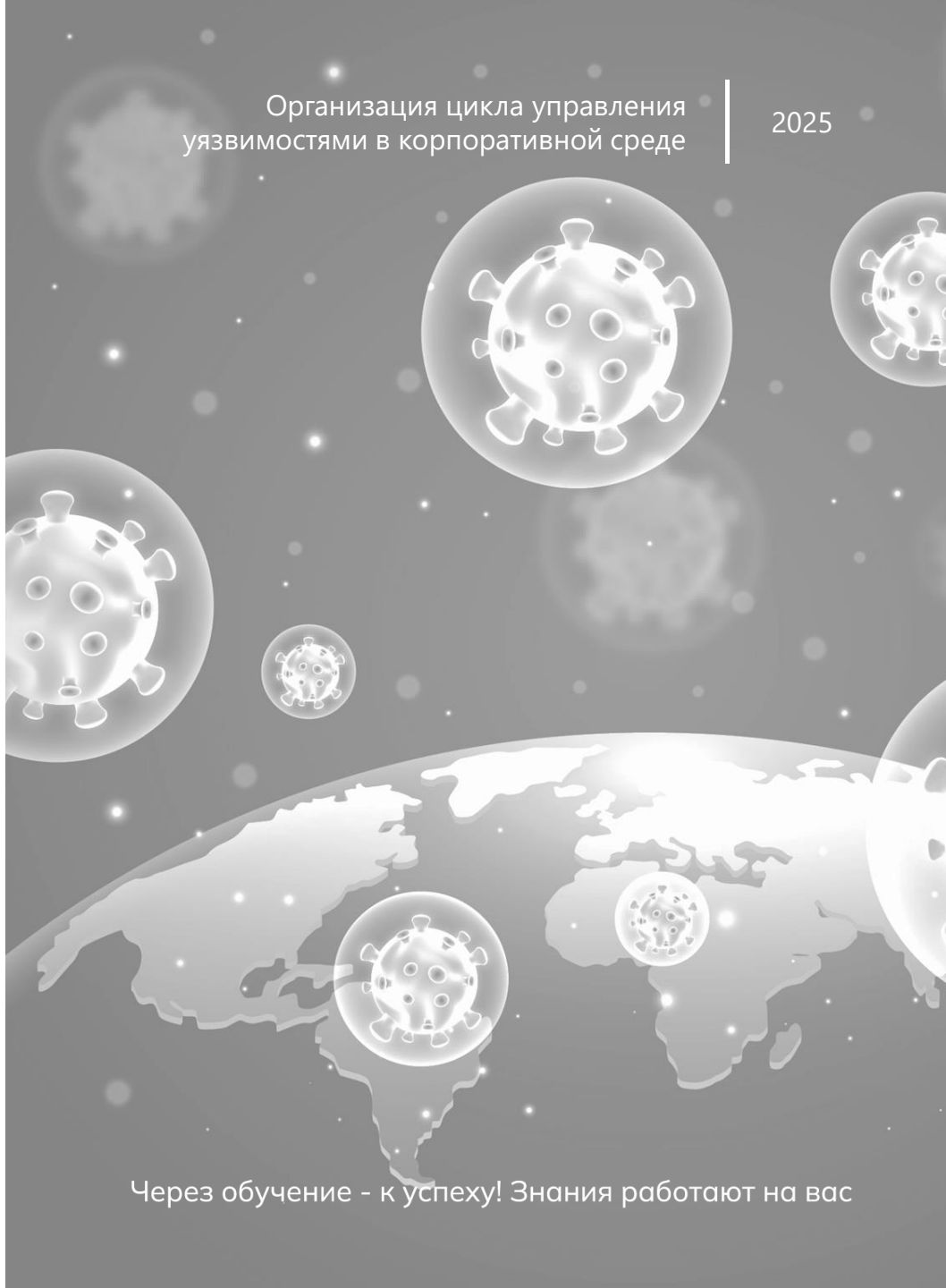
- Механизм для использования уязвимости в целях взлома ресурса.
- Удаленный - работает по сети.
- Локальный - хакер имеет пользовательский или административный доступ к конечной системе

Риски

Вероятность того, что угроза воспользуется уязвимостью ресурса и приведет к нежелательным последствиям

Какие категории уязвимостей существуют

- **Программные**
- **Сетевые**
- **Конфигурационные**
- **Аппаратные**
- **Связанные с процессами или политикой безопасности**



Кто и как находит уязвимости

Кто занимается поиском уязвимостей?

- Специалисты по кибербезопасности
- Компании по информационной безопасности
- Разработчики программного обеспечения
- Независимые эксперты
- Пользователи (случайные обнаружения)

Методы поиска уязвимостей:

- Ручной анализ исходного кода
- Тестирование на проникновение
- Мониторинг подозрительной активности
- Использование специализированных сканеров

Дополнительно:

- Пользователи могут случайно обнаружить уязвимости и сообщить о них разработчикам

Угрозы уязвимости и риски

Международная база данных уязвимостей:

Уязвимости в системах часто получают названия, такие как Meltdown или Spectre, о которых мы уже упоминали. Однако большинство из них специалисты обозначают уникальными идентификаторами и заносят в специализированные базы данных. Одной из наиболее известных таких баз является National Vulnerability Database (NVD), которая использует систему идентификации Common Vulnerabilities and Exposures (CVE).

Российская база данных уязвимостей:

В России существует собственная база данных, адаптированная к отечественным стандартам, - Банк данных угроз безопасности информации (БДУ ФСТЭК). Для описания проблем российского оборудования или программного обеспечения БДУ применяет собственные идентификаторы, в то время как для описания уязвимостей зарубежного оборудования или ПО используются идентификаторы CVE.

Трендовые уязвимости 2025 года

Windows

Уязвимости CVE-2024-38014 и CVE-2024-38217 позволяют злоумышленникам локально повысить привилегии до уровня SYSTEM, обойдя защиту Mark of the Web. Это даёт им возможность маскировать вредоносные файлы под безопасные.

VMware vCenter

Уязвимость CVE-2024-38812 также даёт несанкционированным пользователям возможность удалённого выполнения кода. Благодаря этому они могут получить контроль над сервером.

Veeam Backup & Replication

Уязвимость CVE-2024-40711 даёт атакующим возможность удалённо выполнять код без аутентификации. Это ставит под угрозу сервер, что может привести к полной компрометации инфраструктуры.

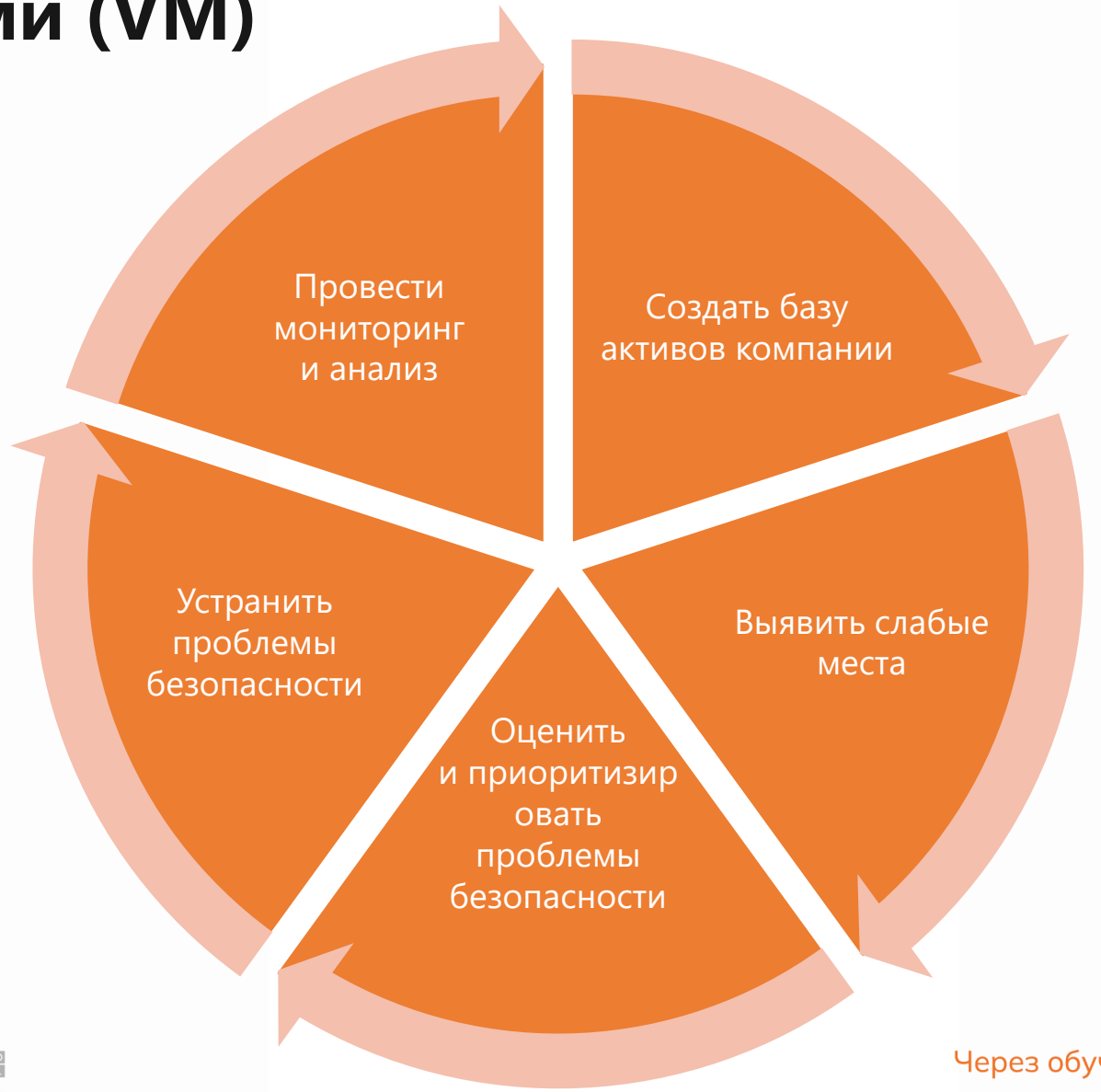
Процессоры

Уязвимости GhostRace и RFDS, затрагивающие архитектуры Intel, AMD и ARM, позволяют хакерам извлекать конфиденциальные данные через спекулятивные атаки.

Веб приложения

Идентификаторы CVE-2024-37383 и CVE-2024-8275 описывают недостатки в Roundcube Webmail и плагине The Events Calendar для WordPress. Эти уязвимости открывают доступ к базе данных, позволяя взломщикам выполнять JavaScript-код, что угрожает безопасности учётных записей пользователей.

Как организовать управление уязвимостями (VM)



Классифицируя активы, специалисты определяют, какие из них важнее.

Например, серверы с клиентскими данными - это важные активы, за которыми нужно следить чаще, а тестовые серверы менее важны, поэтому их можно контролировать реже.

ID актива	Название актива	Тип	Критичность	Ответсвенность
001	База данных клиентов	Сервер	Критический	Иван Иванов
002	Не защищена от атак на ИИ-системы	Сервер	Высокий	Петр Петров
003	Система обработки платежей	Приложение	Критический	Ольга Смирнова
004	Рабочая страница разработки	Рабочая страница	Средний	Анна Васильева
ID актива	Название актива	Тип	Критичность	Ответственный

Итоги этапа оценки и приоритизации может выглядеть так:

Уязвимость	CVSS Балл	Контекстная значимость	Принятое решение
Удалённое выполнение кода на веб-сервере	9.5	Высокая (доступен из внешней сети, обрабатывает личные данные)	Немедленное устранение: обновление безопасности в течение 24 часов
SQL-инъекция в базе данных финансовой системы	8.2	Высокая (содержит конфиденциальную финансовую информацию)	Устранение в течение недели: минимизация рисков для базы данных
Проблема безопасности XSS на внутреннем портале	5.4	Средняя (внутренний доступ, некритичный актив)	Мониторинг и отложенное устранение в следующем плановом обновлении
Отказ в обслуживании на сервере отчётности	4.0	Низкая (сервер используется для нерегулярных отчётов)	Принятие риска: устранение запланировано на конец квартала

Устранение проблем безопасности

Команда ИБ передаёт ИТ-специалистам приоритизированный список рисков: *какие устранить немедленно, какие принять, где нужны временные меры.*

ИТ-специалисты поэтапно внедряют патчи, тестируя их на менее критичных системах перед основным внедрением.

Усиление безопасности включает ограничение прав доступа, отключение неиспользуемых портов и двухфакторную аутентификацию.

Если обнаружена критическая уязвимость, например, Log4j, ИБ уведомляет ИТ.
ИТ тестируют патч в безопасной среде, затем внедряют ночью и проверяют сервер. Для защиты временно усиливают мониторинг и ограничивают доступ.
Если патч невозможен, изолируют уязвимые серверы, ограничивают доступ и усиливают мониторинг до выпуска обновления.

Оценка и отчётность

Финальный этап

команда ИБ оценивает работу ИТ-специалистов, анализирует их технические отчёты, мониторит остаточные риски, составляет рекомендации по усилению безопасности

Как управление уязвимостями помогает ИТ и ИБ работать вместе

Проблема без VM

Отдел информационной безопасности (ИБ) выявляет множество потенциальных угроз и передает их отделу информационных технологий (ИТ) без приоритезации. ИТ-специалисты решают задачи по мере поступления, не имея четкого представления о том, какие из угроз наиболее критичны. В результате они могут упустить опасные уязвимости, подвергая систему риску.

Как помогает VM:

VM помогает ИТ и ИБ лучше понимать друг друга и действовать согласованно. Благодаря этой системе, ИТ-специалисты могут определить, какие угрозы требуют немедленного внимания, и сосредоточиться на них, не тратя время на менее значимые задачи.

Результат:

Отделы не просто обмениваются задачами, а работают над общей целью — защитой компании, при этом каждый выполняет свою роль. Появляются четкие правила, зоны ответственности и KPI для оценки результатов и внесения улучшений.

Какие нормативные акты и стандарты обязаны выполнять российские компании

ГОСТ Р 56545-2015, ГОСТ Р 56546-2015

Эти стандарты описывают, как классифицировать риски безопасности, оценивать их и устранять.

Приказ ФСТЭК России № 17

Этот приказ требует от компаний, работающих с персональными данными, регулярно проверять защищённость данных и ограничивать доступ к ним.

Федеральный закон № 152-ФЗ «О персональных данных».

Этот закон обязывает компании защищать персональные данные от утечек, несанкционированного доступа, кибератак, других угроз.

Как VM помогает выполнять требования закона и взаимодействовать с регуляторами

Как система VM помогает соответствовать требованиям ФСТЭК

Организации, обрабатывающие персональные данные, должны информировать ФСТЭК о выявленных угрозах безопасности и о принятых мерах по их устранению. Система VM позволяет компании соответствовать требованиям ФСТЭК, обеспечивая точное ведение документации и упрощая отчётность.

Поддержание безопасности и отчётности с помощью VM

VM помогает специалистам ИТ-отдела оперативно выявлять и устранять риски, предотвращая несанкционированный доступ к корпоративным данным. При этом компания постоянно обновляет список обнаруженных и устранённых уязвимостей, что позволяет в любой момент продемонстрировать проверяющим органам последовательность действий по повышению безопасности информационных систем.

Как автоматизировать VM

Вендорские решения

1

Сервисы управления уязвимостями

2

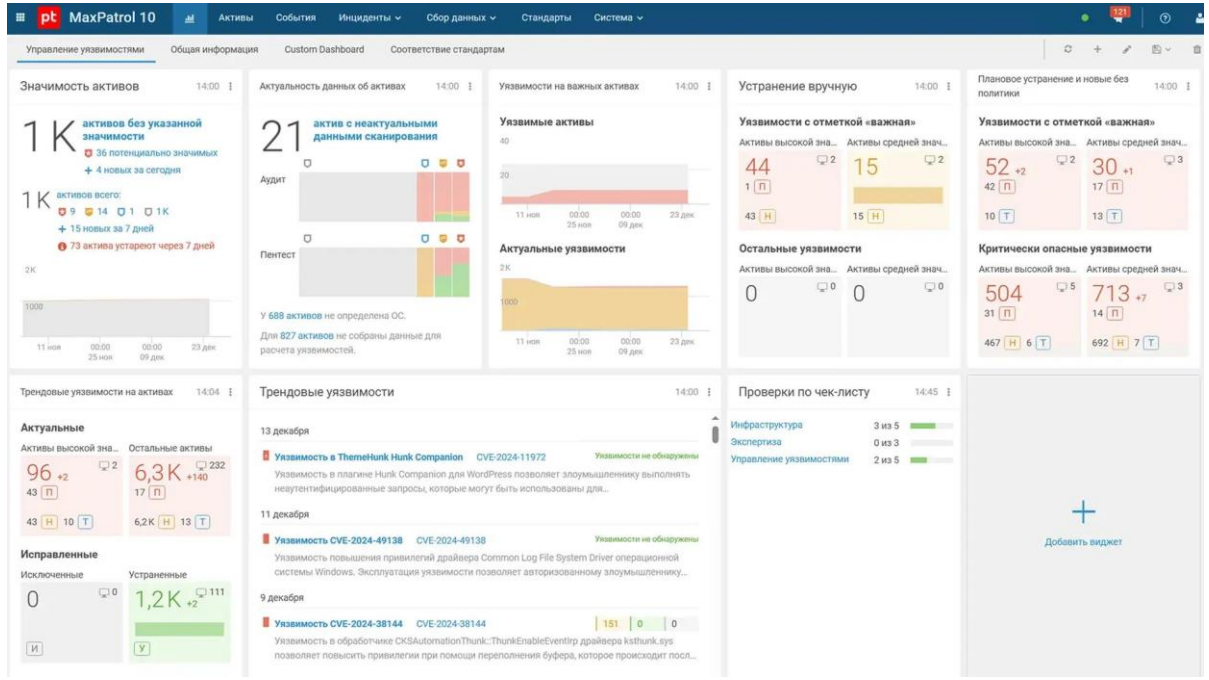
Open-source решения

3

№ 1. Вендорские решения

На рынке уже есть отечественные решения, которые адаптированы для комплексной защиты,

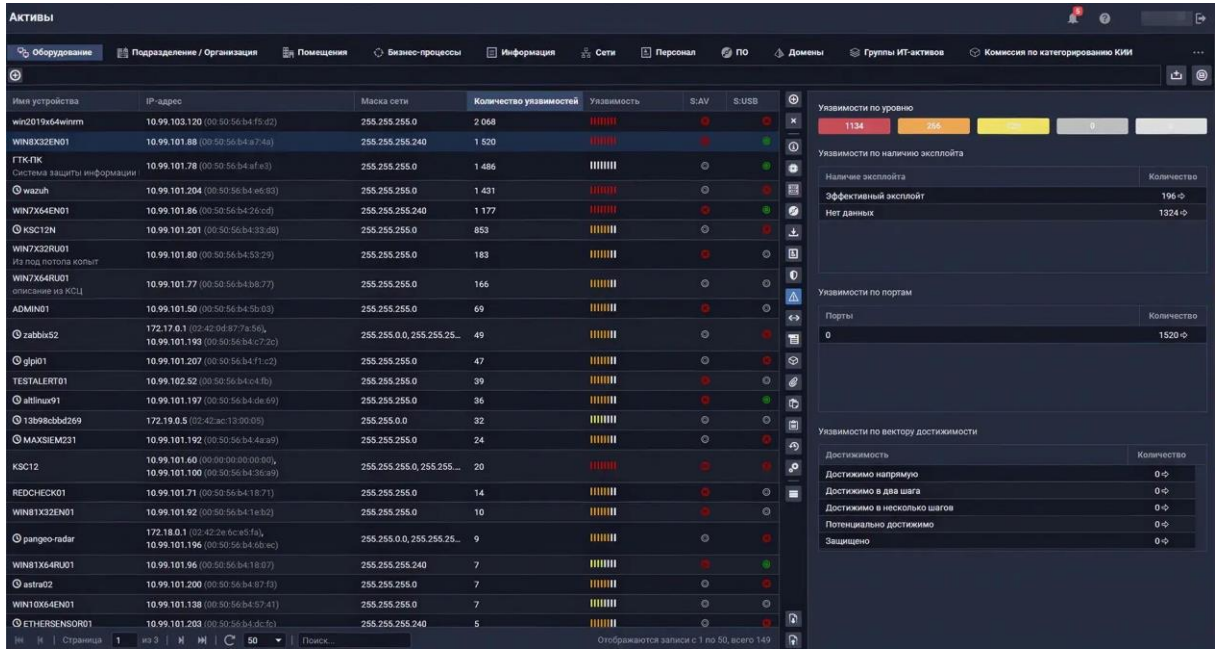
например, MaxPatrol VM или R-Vision VM.



№ 1. Вендорские решения

R-Vision VM от компании R-Vision-
это платформа для автоматизации VM.

Особенность платформы -гибкие настройки сканирования, которые можно адаптировать под нужды конкретной компании

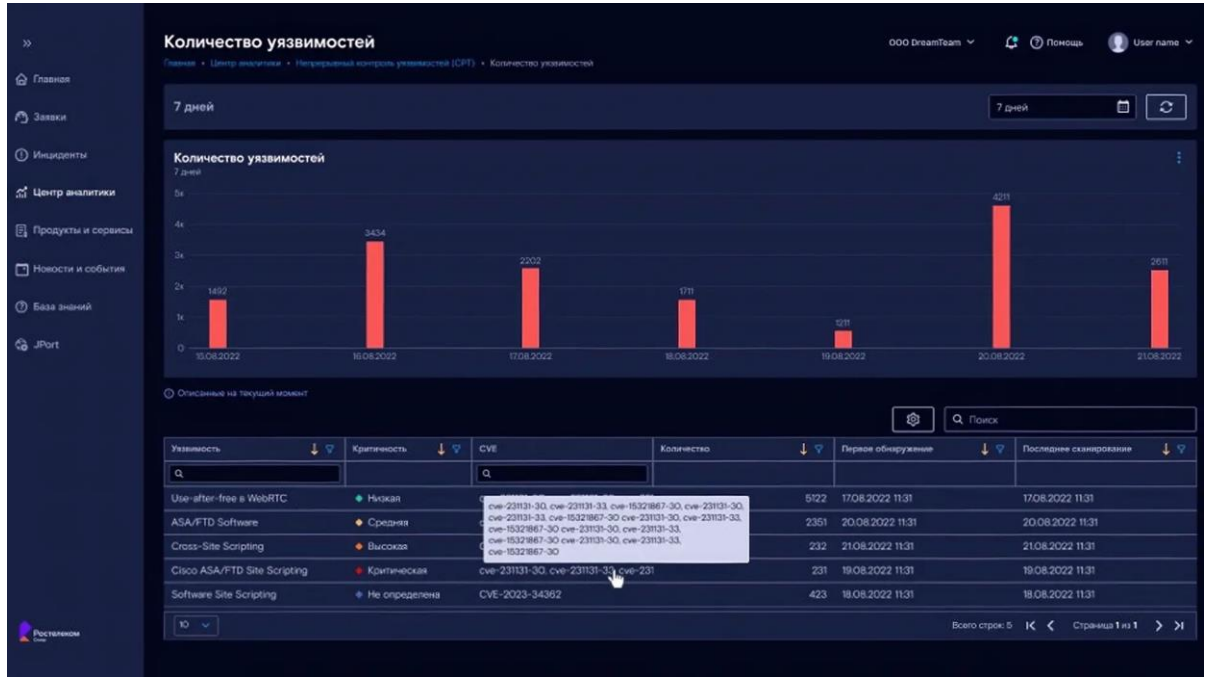


№ 2. Сервисы управления уязвимостями

Solar CPT от ГК Солар - это централизованный сервис для VM и работы с конфигурациями.

Он ориентирован на сети компаний и госорганизаций.

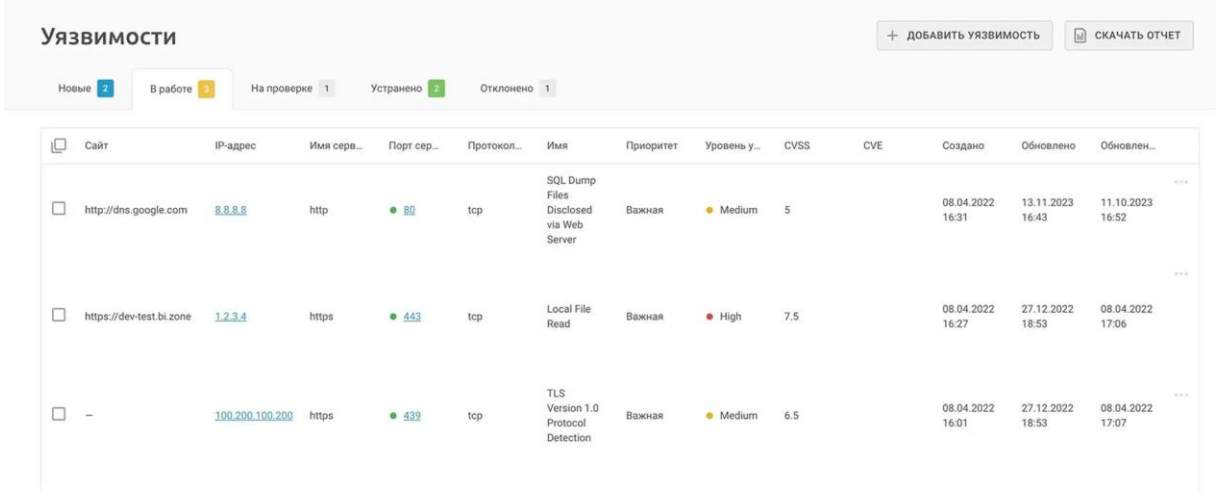
Solar CPT выполняет постоянное тестирование на проникновение, поддерживает активный и пассивный мониторинг, проверяет протоколы FTP и SMB, оценивает уязвимости устройств и серверов.



№ 2. Сервисы управления уязвимостями

BI.ZONE от компании Continuous Penetration Testing (CPT) - это сервис для непрерывного тестирования безопасности в режиме реального времени, с фокусом на уязвимости в IT-системах.

Он обеспечивает активное и пассивное сканирование, анализируя популярные протоколы, такие как FTP и HTTP.



Open-source решения

OpenVAS (Greenbone Vulnerability Management, GVM)

мощная платформа для сканирования уязвимостей, включает инструменты для поиска, анализа и управления обнаруженными проблемами

DefectDojo

система управления уязвимостями и тестированием безопасности (Vulnerability Management and Security Orchestration Platform), поддерживает интеграцию с другими сканерами и трекинг исправлений

Vlus

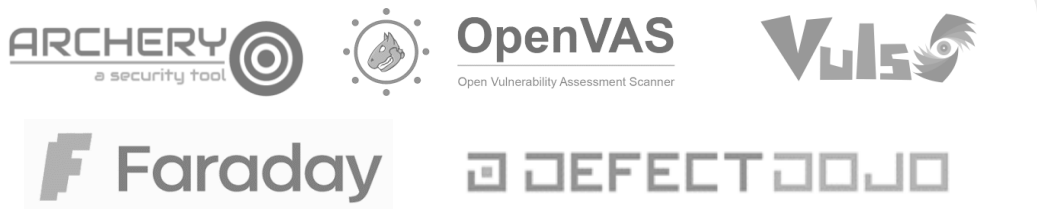
агентless-сканер уязвимостей на Linux, умеет искать уязвимости по CVE и сравнивать версии установленных пакетов, предоставляет отчеты в различных форматах (HTML, JSON

ArcherySec

платформа для управления уязвимостями с поддержкой автоматического запуска сканеров и отслеживания статусов исправлений, есть интеграции с OpenVAS, ZAP и другими инструментами.

Faraday

платформа для управления процессами тестирования на проникновение и уязвимостей, поддерживает импорт результатов разнообразных сканеров.



Ресурсы

- Руководство ФСТЭК России по управлению уязвимостями
- Рекомендации НКЦКИ
- Книга Джона Эриксона «Hacking: The Art of Exploitation»
- Книга Андре Магнуссона «Practical Vulnerability Management: A Strategic Approach to Managing Cyber Risk»
- **Профессиональная переподготовка «Пентестер: этичный хакинг и анализ систем безопасности»**

Подробнее о программе
«Пентестер: этичный хакинг и анализ систем безопасности»

Старт 9 декабря

академия softline

Задавайте вопросы

Антон Носков

Пентестер: этичный хакинг и анализ систем безопасности

Подписывайтесь на наш Телеграм канал