

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

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

Организация цикла управления уязвимостями в корпоративной среде

2025

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

Кто и как находит уязвимости

Организация цикла управления
уязвимостями в корпоративной среде

2025

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



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

Организация цикла управления
уязвимостями в корпоративной среде

2025

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.

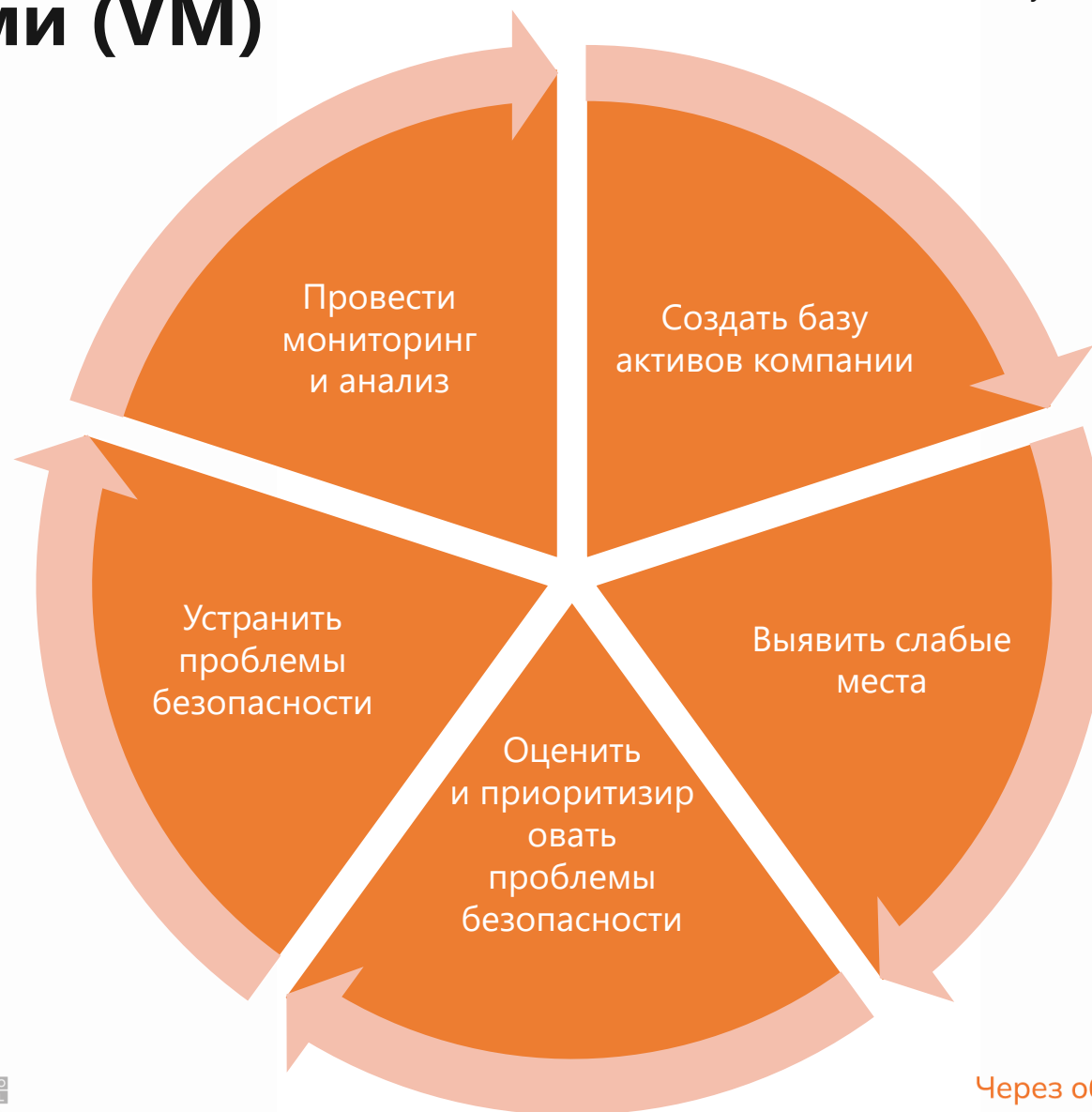
Веб приложения

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)

Организация цикла управления уязвимостями в корпоративной среде

2025



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	Ответственность
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

Организация цикла управления уязвимостями в корпоративной среде

2025

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

Организация цикла управления
уязвимостями в корпоративной среде

2025

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

Организация цикла управления уязвимостями в корпоративной среде

2025

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

Организация цикла управления
уязвимостями в корпоративной среде

2025

**Вендорские
решения**

1

**Сервисы управления
уязвимостями**

2

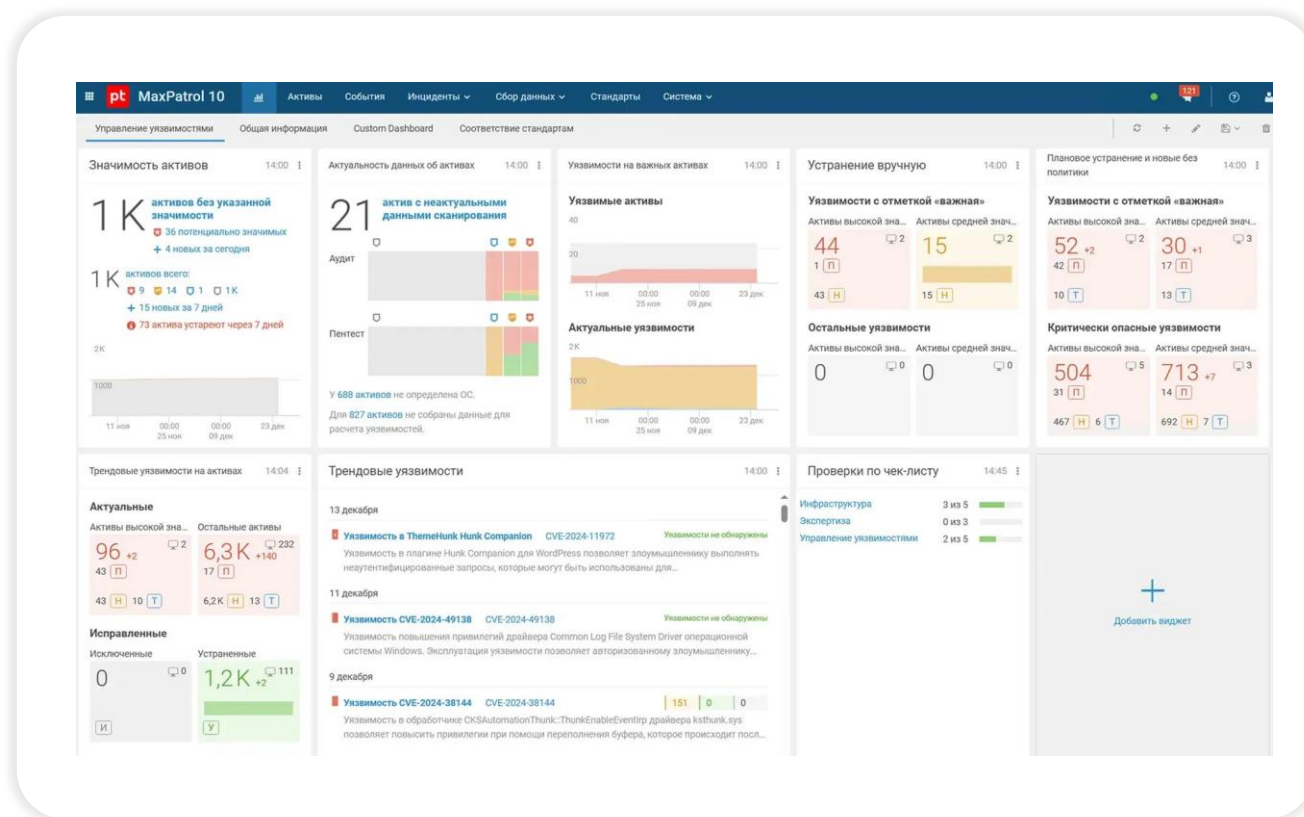
**Open-source
решения**

3

№ 1. Вендорские решения

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

*например, MaxPatrol VM или R-Vision
VM.*



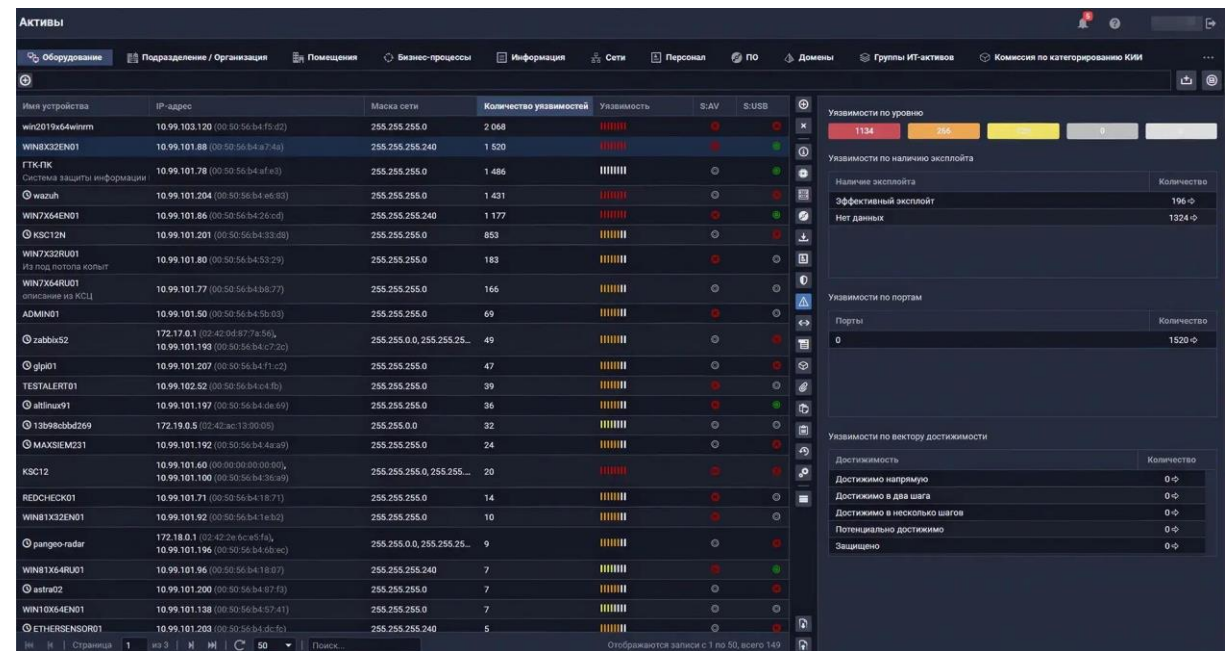
№ 1. Вендорские решения

Организация цикла управления уязвимостями в корпоративной среде

2025

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

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



The screenshot displays the R-Vision VM web interface. The main table lists various assets with columns for name, IP address, subnet mask, number of vulnerabilities, and status indicators for S/AV and S/USB. The right sidebar provides summary statistics and detailed views for vulnerabilities by level, exploitability, and reachability.

Имя устройства	IP-адрес	Маска сети	Количество уязвимостей	Уязвимость	S/AV	S/USB
win2019x64win10	10.99.103.120 (00:50:56:b4:f5:d2)	255.255.255.0	2 068		0	0
WIN8X32EN01	10.99.101.88 (00:50:56:b4:a7:4a)	255.255.255.240	1 520		0	0
ГТК ПК Система защиты информации	10.99.101.78 (00:50:56:b4:af:43)	255.255.255.0	1 486		0	0
Wazuh	10.99.101.204 (00:50:56:b4:e5:83)	255.255.255.0	1 431		0	0
WIN7X64EN01	10.99.101.86 (00:50:56:b4:c2:6d)	255.255.255.240	1 177		0	0
KSC12N	10.99.101.201 (00:50:56:b4:93:08)	255.255.255.0	853		0	0
WIN7X32RU01	10.99.101.80 (00:50:56:b4:53:29)	255.255.255.0	183		0	0
WIN7X64RU01	10.99.101.77 (00:50:56:b4:b6:77)	255.255.255.0	166		0	0
ADMIN01	10.99.101.50 (00:50:56:b4:5b:03)	255.255.255.0	69		0	0
zabbix2	172.17.0.1 (02:42:ac:11:00:00), 10.99.101.193 (00:50:56:b4:c7:2c)	255.255.0.0, 255.255.25.0	49		0	0
glpi01	10.99.101.207 (00:50:56:b4:f1:c2)	255.255.255.0	47		0	0
TESTALERT01	10.99.102.52 (00:50:56:b4:c4:b3)	255.255.255.0	39		0	0
alllinux91	10.99.101.197 (00:50:56:b4:de:69)	255.255.255.0	36		0	0
13b98cbb4269	172.17.0.5 (02:42:ac:11:00:00)	255.255.0.0	32		0	0
MAXSEM231	10.99.101.192 (00:50:56:b4:4a:a9)	255.255.255.0	24		0	0
KSC12	10.99.101.60 (00:00:00:00:00:00), 10.99.101.100 (00:50:56:b4:36:a9)	255.255.255.0, 255.255.25.0	20		0	0
REDCHECK01	10.99.101.71 (00:50:56:b4:18:71)	255.255.255.0	14		0	0
WIN81X32EN01	10.99.101.92 (00:50:56:b4:1e:b2)	255.255.255.0	10		0	0
rangeo-radar	172.18.0.1 (02:42:ac:11:00:00), 10.99.101.196 (00:50:56:b4:66:ec)	255.255.0.0, 255.255.25.0	9		0	0
WIN81X64RU01	10.99.101.96 (00:50:56:b4:18:07)	255.255.255.240	7		0	0
astra02	10.99.101.200 (00:50:56:b4:07:b3)	255.255.255.0	7		0	0
WIN10X64EN01	10.99.101.138 (00:50:56:b4:57:41)	255.255.255.0	7		0	0
ETHERSENSOR01	10.99.101.203 (00:50:56:b4:d4:fc)	255.255.255.240	5		0	0

Summary statistics on the right:

- Уязвимости по уровню: 1134 (High), 264 (Medium), 9 (Low), 0 (Info)
- Уязвимости по наличию эксплойта: 196 (Effective), 1324 (None)
- Уязвимости по портам: 1520 (Ports)
- Уязвимости по вектору достижимости: 0 (Direct), 0 (Two steps), 0 (Multiple steps), 0 (Potentially reachable), 0 (Protected)

№ 2. Сервисы управления уязвимостями

Организация цикла управления уязвимостями в корпоративной среде

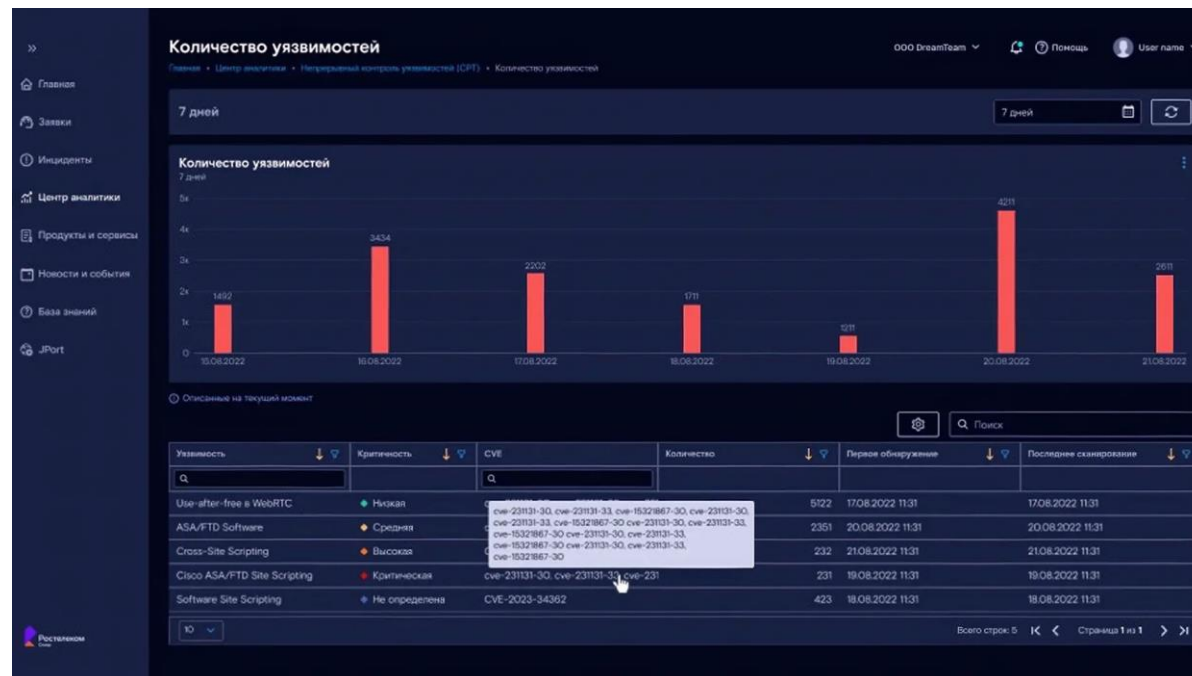
2025

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

Организация цикла управления уязвимостями в корпоративной среде

2025

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.

Уязвимости												
Новые 2 В работе 3 На проверке 1 Устранено 3 Отклонено 1												
+ ДОБАВИТЬ УЯЗВИМОСТЬ СКАЧАТЬ ОТЧЕТ												
Сайт	IP-адрес	Имя серв...	Порт сер...	Протокол...	Имя	Приоритет	Уровень у...	CVSS	CVE	Создано	Обновлено	Обновлен...
☐ http://dns.google.com	8.8.8.8	http	80	tcp	SQL Dump Files Disclosed via Web Server	Важная	Medium	5		08.04.2022 16:31	13.11.2023 16:43	11.10.2023 16:52
☐ https://dev-test.bi.zone	1.2.3.4	https	443	tcp	Local File Read	Важная	High	7.5		08.04.2022 16:27	27.12.2022 18:53	08.04.2022 17:06
☐ -	100.200.100.200	https	433	tcp	TLS Version 1.0 Protocol Detection	Важная	Medium	6.5		08.04.2022 16:01	27.12.2022 18:53	08.04.2022 17:07

Open-source решения

Организация цикла управления
уязвимостями в корпоративной среде

2025

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

agentless-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.



OpenVAS
Open Vulnerability Assessment Scanner



- + 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

Задавайте вопросы

 **Антон Носков**



Пентестер: этичный
хакинг и анализ систем
безопасности



Подписывайтесь
на наш Телеграм канал