

Управление уязвимостями с **Vulns.io Enterprise VM**

23.10.2025



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

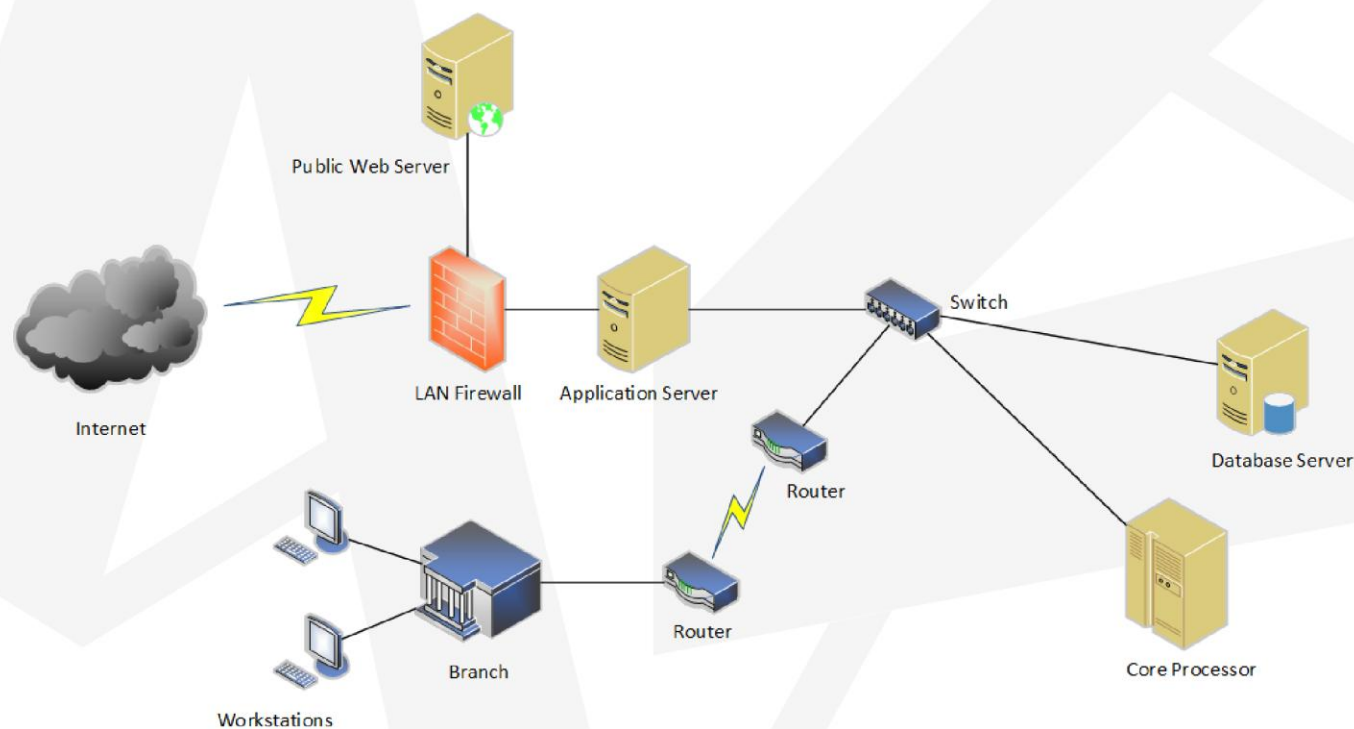
Зачем управлять уязвимостями



Управление уязвимостями – процесс, направленный на повышение защищенности IT-инфраструктуры.

Зачем управлять уязвимостями

Управление уязвимостями – процесс, направленный на повышение защищенности IT-инфраструктуры.

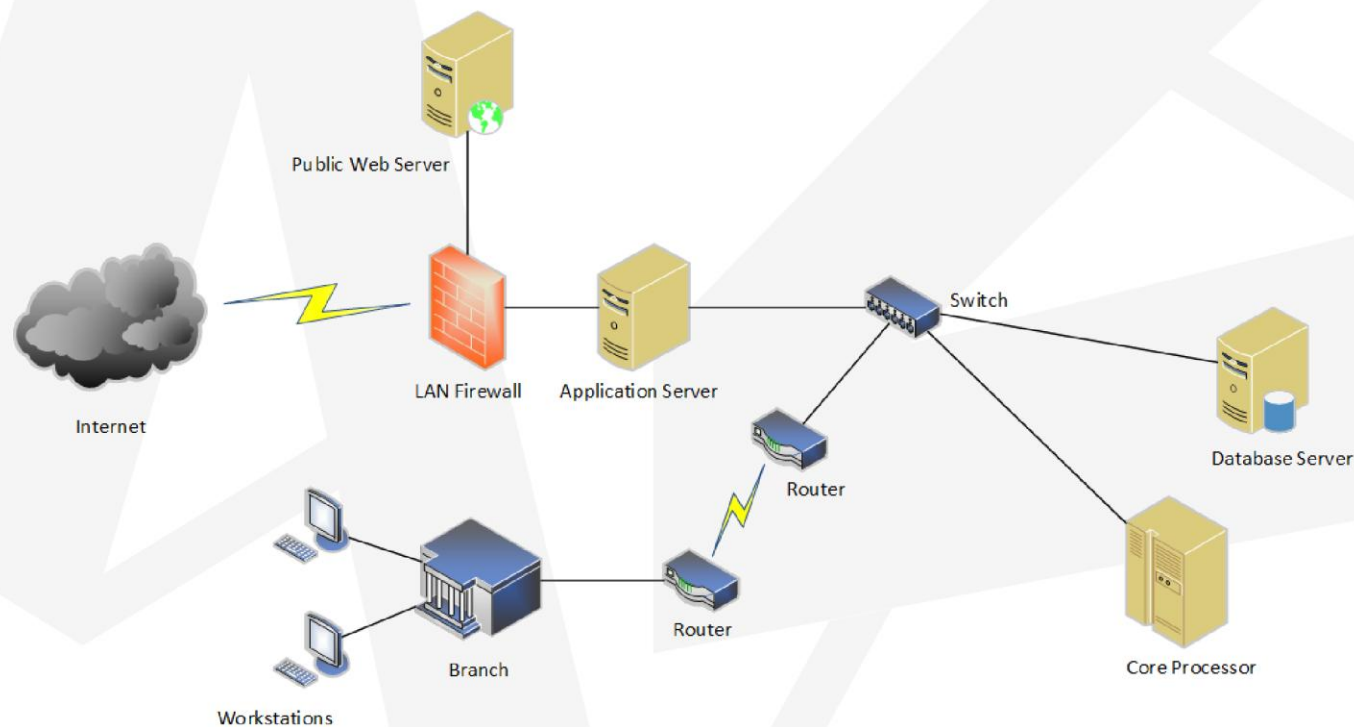


Зачем управлять уязвимостями

Управление уязвимостями – процесс, направленный на повышение защищенности IT-инфраструктуры.



Устраняем «туман войны»
(инвентаризация и аудит)

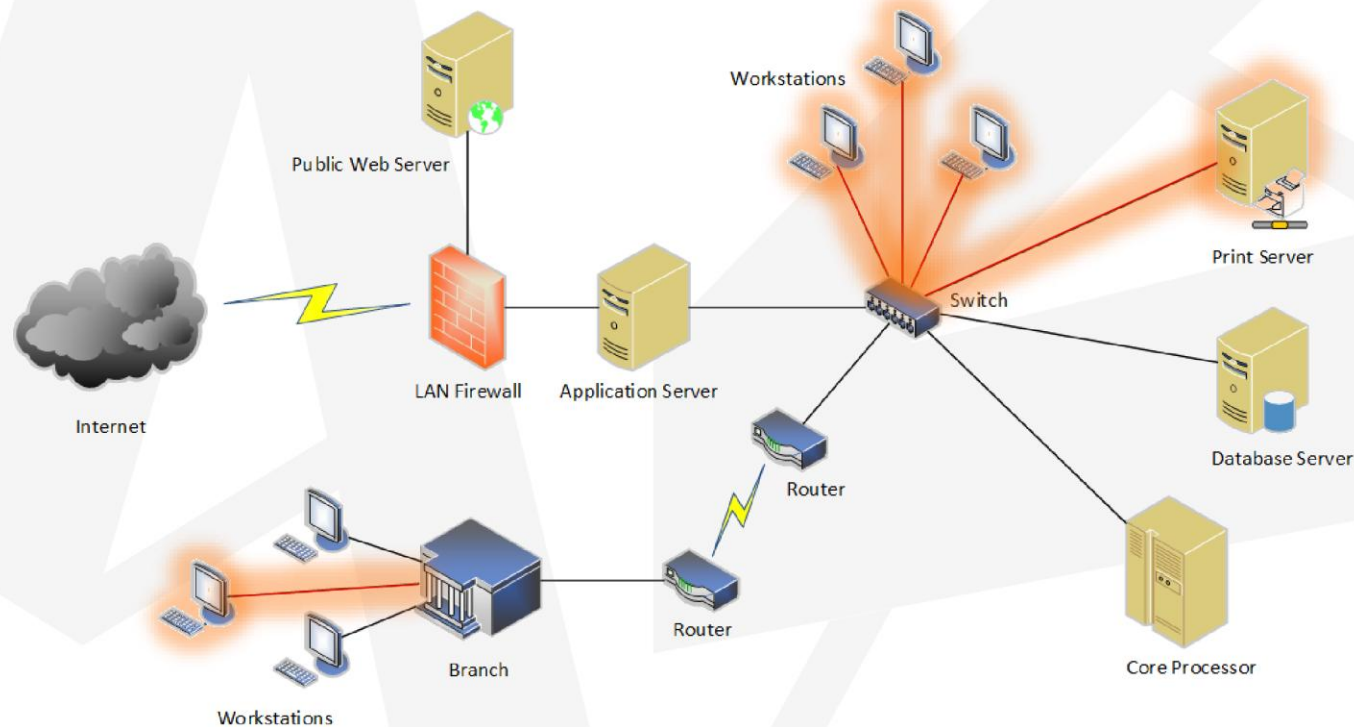


Зачем управлять уязвимостями

Управление уязвимостями – процесс, направленный на повышение защищенности IT-инфраструктуры.



Устраняем «туман войны»
(инвентаризация и аудит)

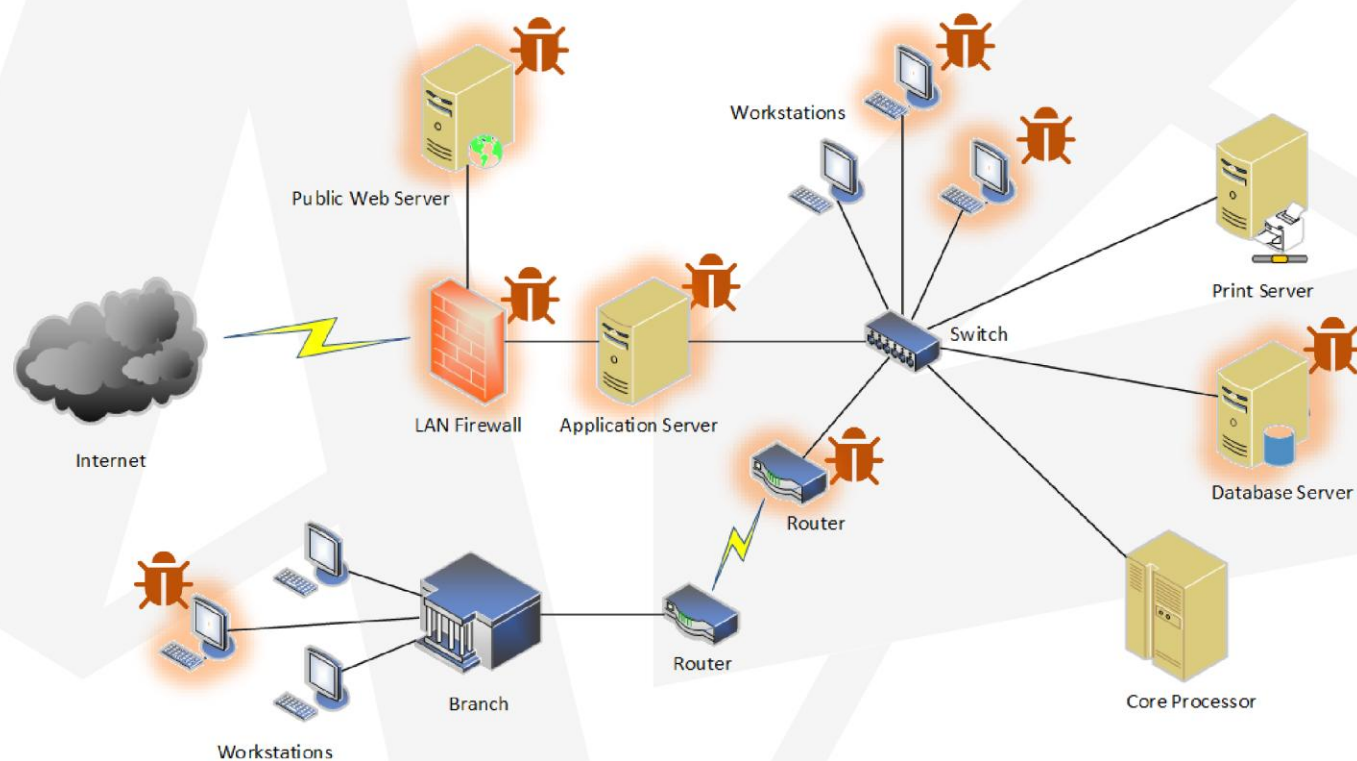


Зачем управлять уязвимостями

Управление уязвимостями – процесс, направленный на повышение защищенности IT-инфраструктуры.



Устраняем «туман войны»
(инвентаризация и аудит)



Зачем управлять уязвимостями

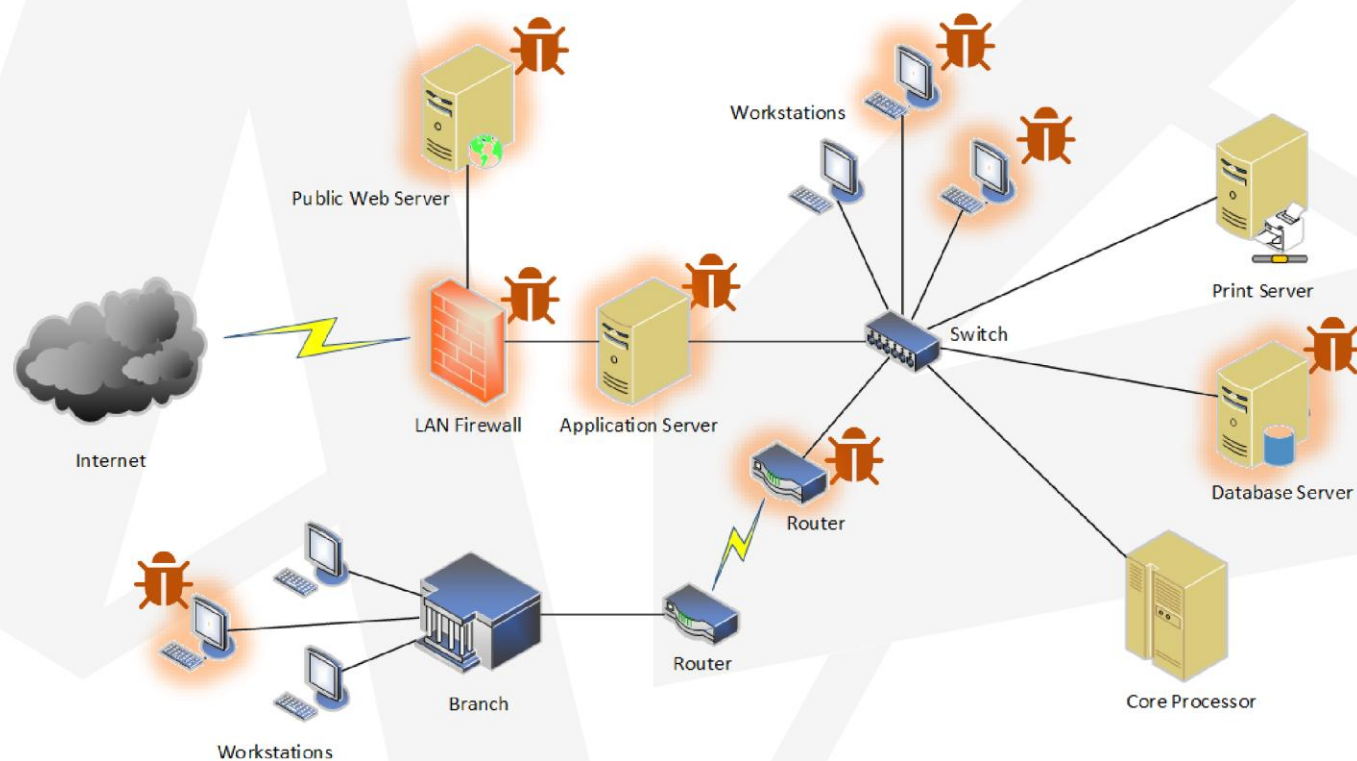
Управление уязвимостями – процесс, направленный на повышение защищенности IT-инфраструктуры.



Устраняем «туман войны»
(инвентаризация и аудит)



Повышаем защищенность
(устраняем уязвимости)



Зачем управлять уязвимостями

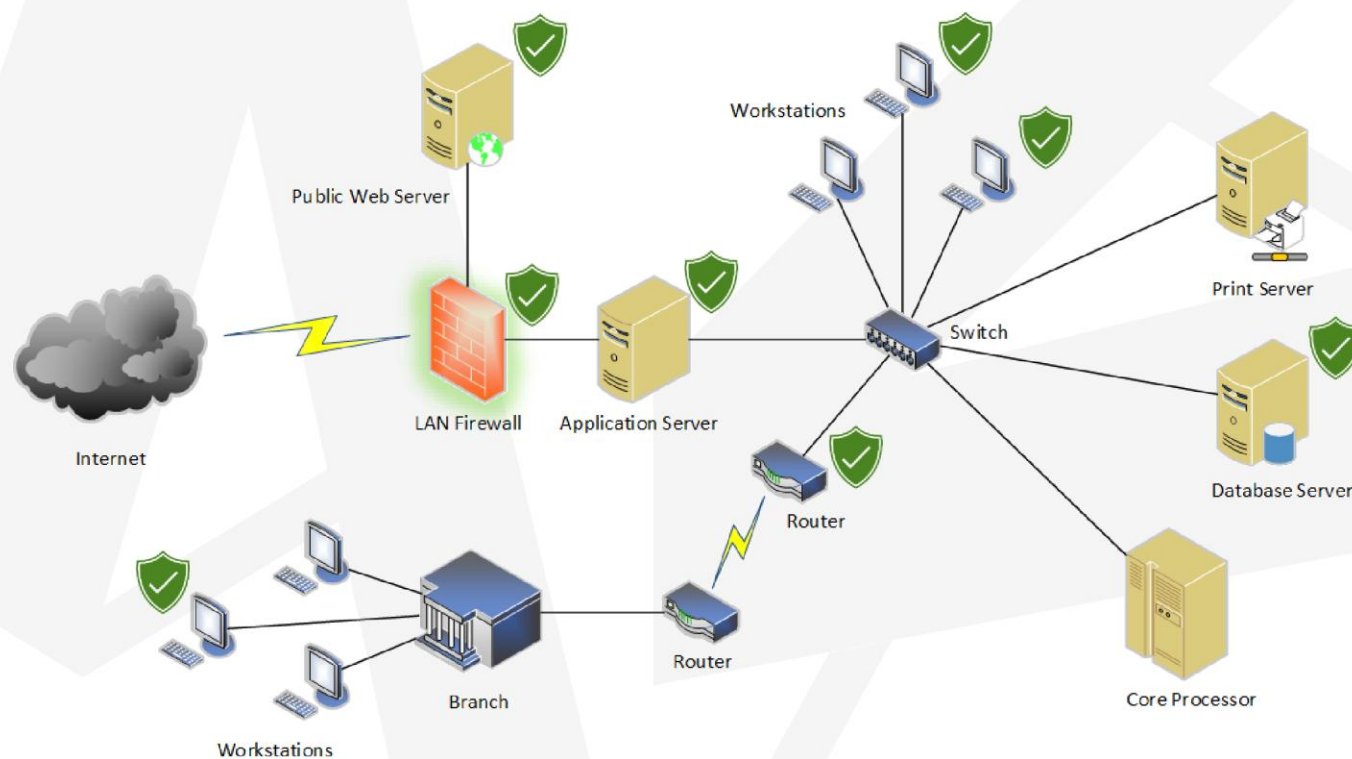
Управление уязвимостями – процесс, направленный на повышение защищенности IT-инфраструктуры.



Устраняем «туман войны»
(инвентаризация и аудит)

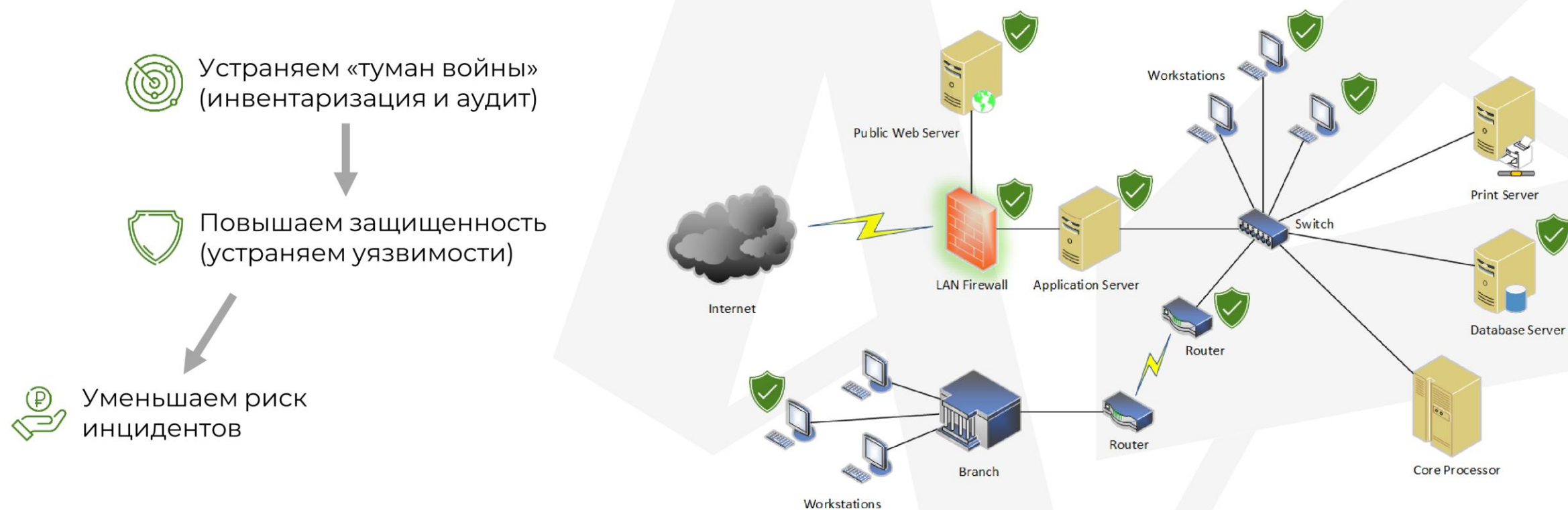


Повышаем защищенность
(устраняем уязвимости)



Зачем управлять уязвимостями

Управление уязвимостями – процесс, направленный на повышение защищенности IT-инфраструктуры.



Зачем управлять уязвимостями

Управление уязвимостями – процесс, направленный на повышение защищенности IT-инфраструктуры.



Как управлять уязвимостями



Руководство по организации процесса управления уязвимостями в органе (организации)

Утвержден ФСТЭК России
17 мая 2023 г.



Детектирование уязвимостей

Уязвимости инфраструктуры

- Периметр: внутри и снаружи
- Изолированные сегменты
- Облака и виртуализация
- CI/CD

Код и приложения

- Статические анализаторы
- Динамические анализаторы
- Фаззинг-анализаторы

Уязвимости конфигураций

- Операционные системы
- Прикладное ПО
- Сетевые устройства

Активные проверки

- Пентесты
- Сигнатуры
- Подбор паролей
- Сканирование web-приложений



Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств

Утвержден ФСТЭК России
30 июня 2025 г.



Зарубежные подходы

- CVSS
- EPSS
- CISA SSVC
- CISA KEV
- CVEShield (CVE Crowd, CVETrends), CMU SSVC
- CVE Prioritizer
- Vulners AI Score
- Zoom VISS
- SSPP



Методика тестирования обновлений безопасности программных, программно-аппаратных средств

Утвержден ФСТЭК России
20 октября 2022 г.



Основные этапы методики

- сверка идентичности;
- проверка подлинности;
- антивирусный контроль;
- поиск опасных конструкций;
- мониторинг активности;
- ручной анализ.

Устранение



Методика тестирования обновлений безопасности программных, программно-аппаратных средств

Утвержден ФСТЭК России
20 октября 2022 г.



Сервис проверки обновлений ФСТЭК

The screenshot displays the Vulns.io service interface for verifying updates. It is divided into two main sections, each showing details for a specific software product.

Top Section (Extron ShareLink Pro):

- Идентификатор обновления:** TC302
- Вендор:** Extron
- ПО:** ShareLink Pro
- Версия тестируемого ПО:** 1.8.12
- Контрольная сумма:** SHA1: F2441570DF86868E4A803E8EC3D8026, SHA-256: 88744725408A68BC7960C22848E8363E310801511EE200E3895E1FC68CCE7E47, ГОСТ R34.11-2012(256): 96F44BFC2B49938DE4AE24DA4189F238C107202410542453898470F47E39CC
- Дата выпуска обновления:** 28.12.2021
- Дата тестирования:** 21.06.2023

Bottom Section (Oracle Java):

- Идентификатор обновления:** TC300
- Вендор:** Eclipse Adoptium
- ПО:** OpenJDK
- Версия тестируемого ПО:** 11.0.19
- Контрольная сумма:** OpenJDK11U-jdk_x86_64_hotspot_11.0.19_7-b1g2, MD5: 54F162F58070E1B50830844A787516, SHA-1: 8509CD7B17C061FE281E7391C326238C28872E49, SHA-256: 5F18F826AE3E28FCC402B73CE72F3260290D048769502E7F81C52CA38A581, ГОСТ R34.11-2012(256): FCF1A1CA14DC654869C8F932AF771B5BC682254D5A8148A1ECF1EFB8184CBE
- Дата выпуска обновления:** 18.04.2023
- Дата тестирования:** 15.06.2023 - 16.06.2023

Results (Результаты): Обновление может быть установлено при определенных ограничениях.

- Дата создания: ноябрь 2022
- Обновлений: **273 → 2171***
- Windows: **259 → 1315**
- Linux: **13 → 736**
- MacOS: **1 → 113**

*Изменение за период 07.2023 – 10.2025

Как управлять уязвимостями?



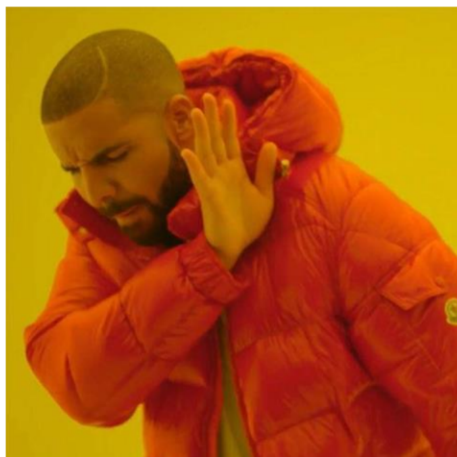
Как управлять уязвимостями?



Вручную

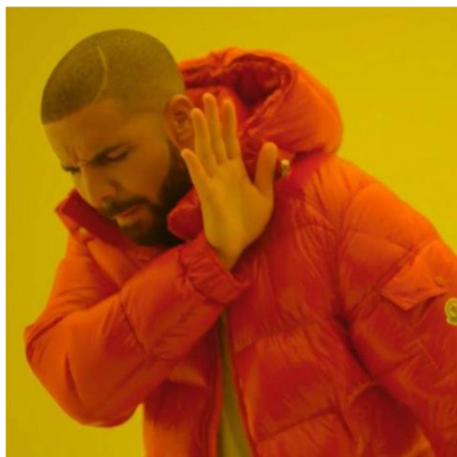
Как управлять уязвимостями?

Вручную



Как управлять уязвимостями?

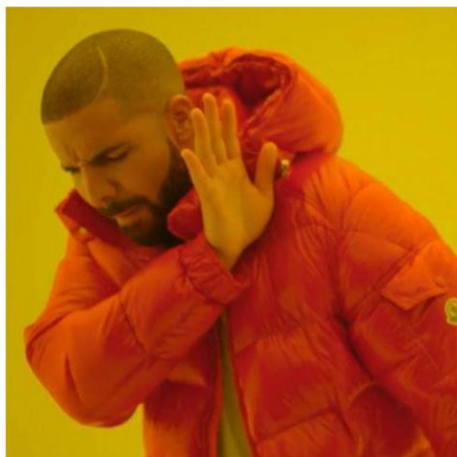
Вручную



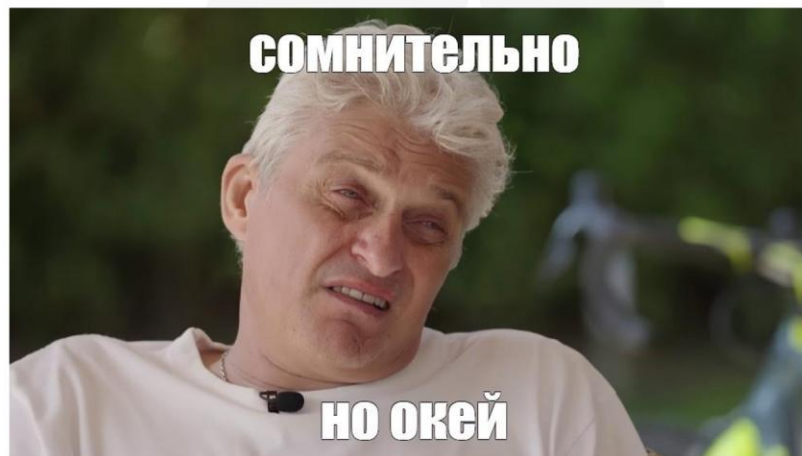
**Open-source или
сканер уязвимостей**

Как управлять уязвимостями?

Вручную

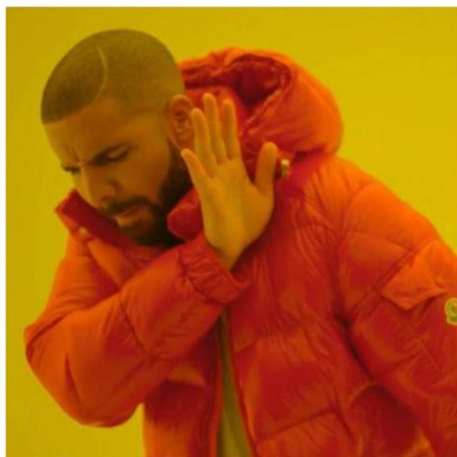


**Open-source или
сканер уязвимостей**

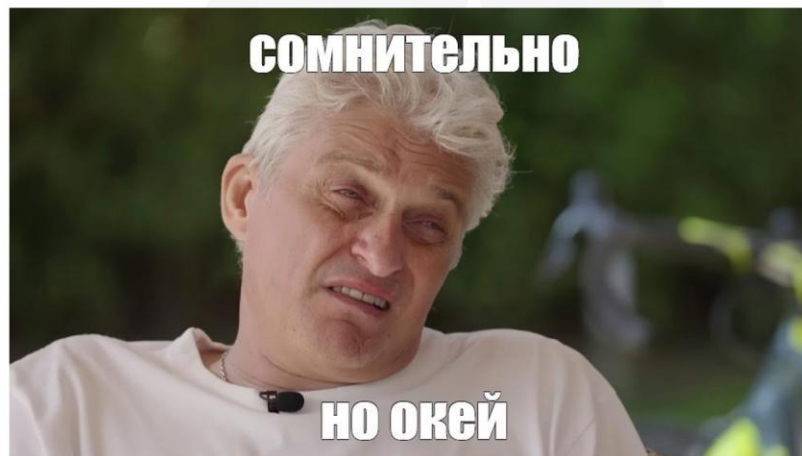


Как управлять уязвимостями?

Вручную



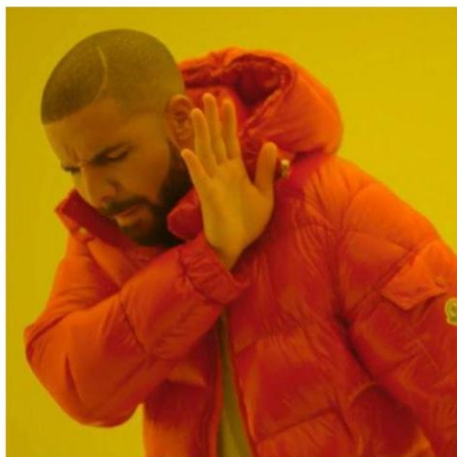
**Open-source или
сканер уязвимостей**



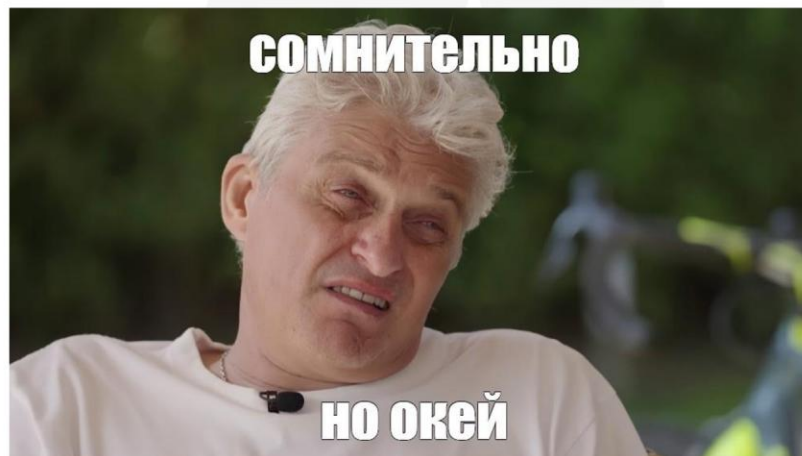
VM-решение

Как управлять уязвимостями?

Вручную



**Open-source или
сканер уязвимостей**



VM-решение



Как выбрать VM-решение

Для работы с продуктом нужны
квалифицированные специалисты

Очень высокая стоимость

Придется внедрять новые бизнес-
процессы

Сложно развернуть продукт

Экосистемы, линейки продуктов –
нужно ли переплачивать

Какой функционал нужен в
первую очередь

Как понять, что продукт
закрывает мои потребности



Что должен уметь VM-инструмент



Что должен уметь VM-инструмент



**Скорость аудита
инфраструктуры**



**Точность определения
уязвимостей**



**Алгоритмы
приоритизации**

Что должен уметь VM-инструмент



**Скорость аудита
инфраструктуры**



**Точность определения
уязвимостей**



**Алгоритмы
приоритизации**



**Устранение
уязвимостей**



Простота работы

Что должен уметь VM-инструмент



**Скорость аудита
инфраструктуры**



**Точность определения
уязвимостей**



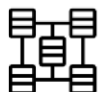
**Алгоритмы
приоритизации**



**Устранение
уязвимостей**



Простота работы



Масштабируемость



Варианты интеграции



**Дополнительный
функционал**



**Возможности
автоматизации**



Стоимость

Что должен уметь VM-инструмент



**Скорость аудита
инфраструктуры**



**Точность определения
уязвимостей**



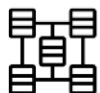
**Алгоритмы
приоритизации**



**Устранение
уязвимостей**



Простота работы



Масштабируемость



Варианты интеграции



**Дополнительный
функционал**



**Возможности
автоматизации**



Стоимость



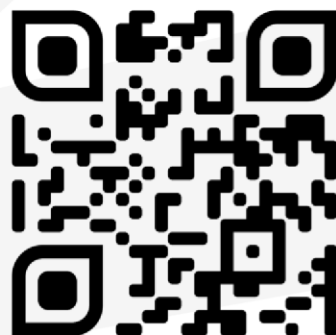
Vulns.io^{VM}

Управление уязвимостями

Сертификат соответствия ТР_{БҮ}:
№BY/112 02.01. ТР027 036.01 02208

Спасибо за внимание!

Андрей Никонов
Руководитель департамента
разработки ПО



 **+7(495) 967 65 19**

 **vulns.io**

 Техническая поддержка:
support@vulns.io

 Офис:
г.Уфа, ул.Пархоменко, 133/1