Vulns.io VM
Управление уязвимостями

фродекс

Особенности национального управления уязвимостями

itsec ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ РОССИИ

Июнь 2024

Этапы процесса управления уязвимостями

Vulns.io™

Руководство
по организации процесса управления уязвимостями в органе (организации)

Утвержден ФСТЭК России
17 мая 2023 г.

Ссылка:

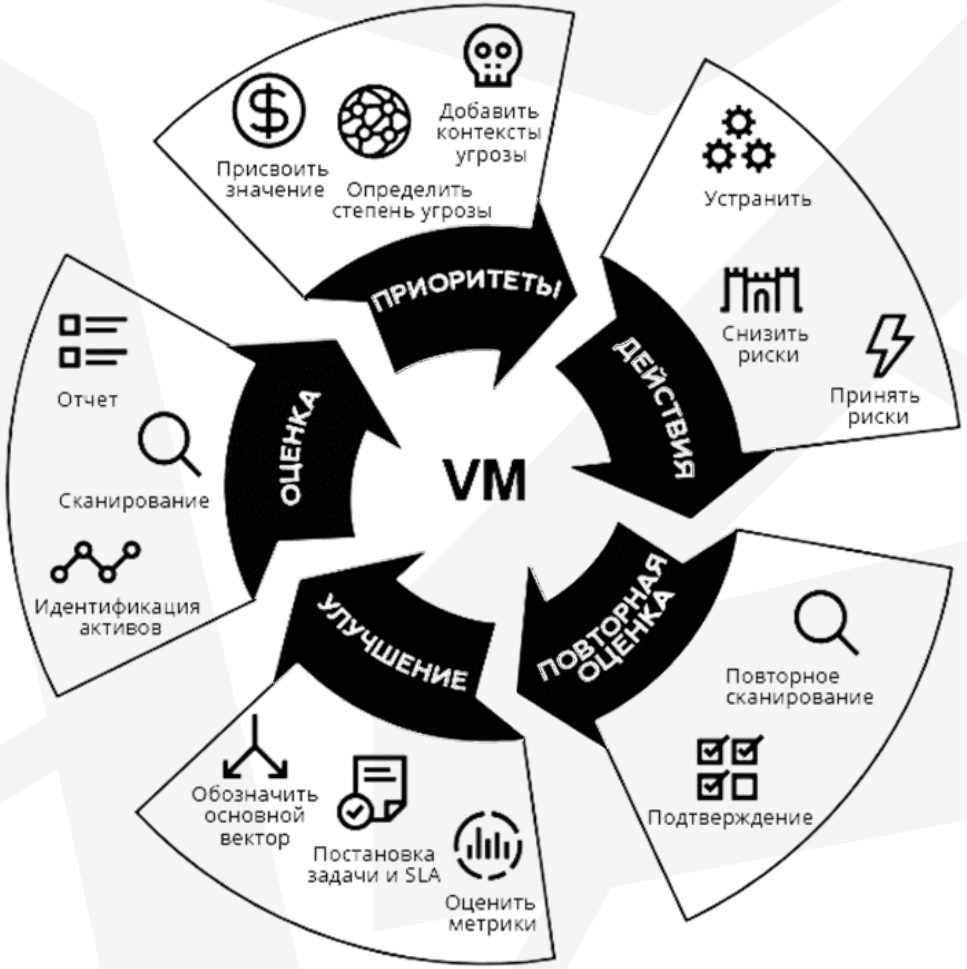
Этапы работ по управлению уязвимостями (ФСТЭК)
25.12.2022

Этапы процесса управления уязвимостями

Vulns.io™

Этапы работ по управлению уязвимостями (ФСТЭК)

25.12.2022



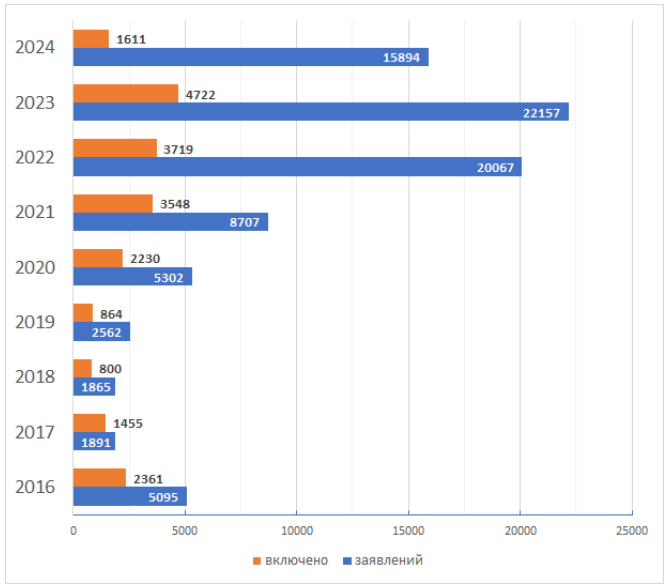
The Vulnerability Management Cycle (Gartner)

25.10.2019

Оценка защищенности инфраструктуры

Vulns.io VM

Отечественное ПО



РЕЕСТР РОССИЙСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

21 310

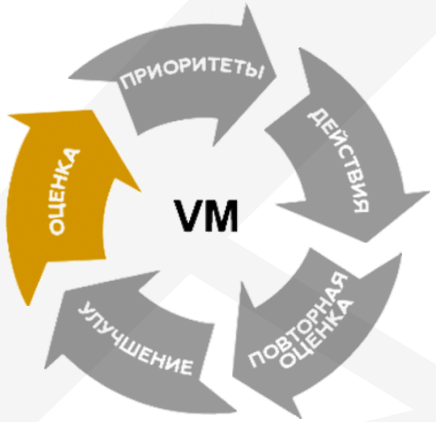
Включено ПО в Реестр

7 977

Правообладателей

Отечественные уязвимости

БДУ ФСТЭК



ASTRA LINUX

РЕДОС

alt linux ALT LINUX TEAM

ROSA

ОСНОВА

KASPERSKY lab

UB Linux

WEBSOFT

СТРЕЛЕЦ ОПЕРАЦИОННАЯ СИСТЕМА ОБЩЕГО НАЗНАЧЕНИЯ

ELTEX

ФССП России GosLinux

РУБИНТЕХ технологии информационной безопасности

АВРОРА

МСВСфера

AlterOS

Отечественный VM

Qualys

~~RAPID7~~

tenable

CANCELED

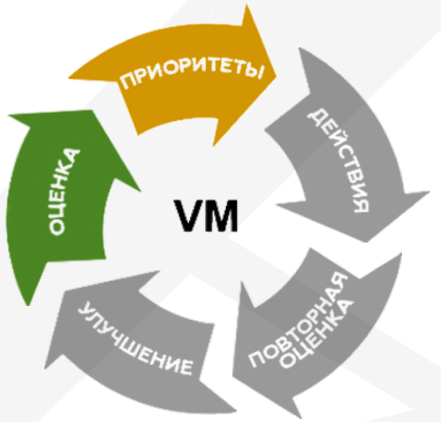
Vulns.io VM

Управление уязвимостями

Приоритизация уязвимостей

Vulns.io™

Отечественная методика приоритизации



Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств

Утвержден ФСТЭК России
28 октября 2022 г.

Ссылка:

Приоритизация уязвимостей

Vulns.io VM

Отечественная методика приоритизации

Результат аудита ИС

CVE

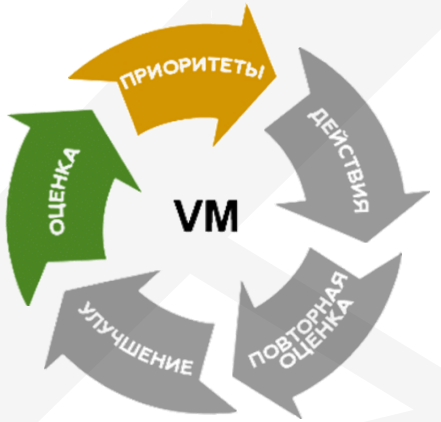
CVSS 3.1

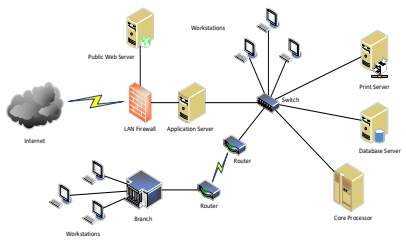
- Базовые метрики
- Временные метрики
- Контекстные метрики

I_{cvss}

ГОССОПКА

НКЦКИ





Сведения о составе и архитектуре ИС

Тип компонента

$k \cdot K$

Кол-во уязвимых компонент

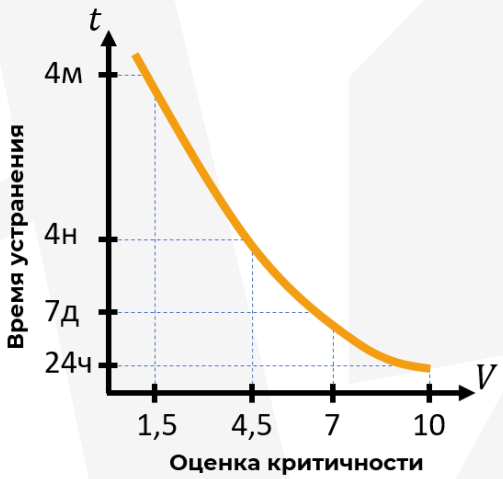
$l \cdot L$

Влияние на защиту периметра

$p \cdot P$

I_{infr}

V



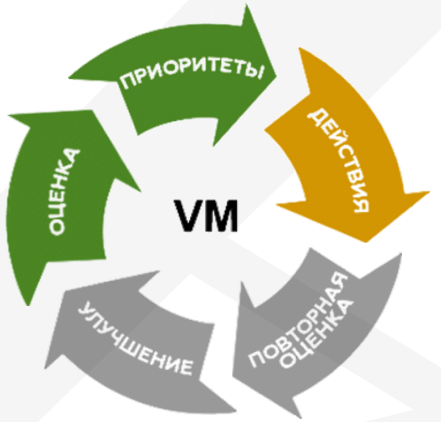
Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств

Утвержден ФСТЭК России
28 октября 2022 г.

Устранение уязвимостей

Vulns.io™

Отечественная методика проверки обновлений



Методика тестирования обновлений безопасности программных, программно-аппаратных средств

Утвержден ФСТЭК России
20 октября 2022 г.

Ссылка:

Устранение уязвимостей

Vulns.io VM

Отечественная методика проверки обновлений

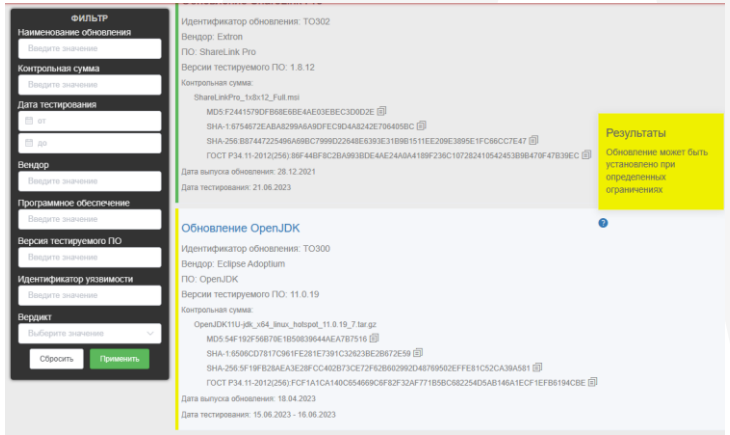
- сверка идентичности;
- проверка подлинности;
- антивирусный контроль;
- поиск опасных конструкций;
- мониторинг активности;
- ручной анализ.

Методика тестирования обновлений безопасности программных, программно-аппаратных средств

Утвержден ФСТЭК России
20 октября 2022 г.

Отечественный сервис проверки обновлений*

- Дата создания: ноябрь 2022
- Обновлений: **1151**
- Microsoft: **836**
- Linux: **264**
- MacOS: **45**
- Unix, etc: **6**



* Ссылка: bdu.fstec.ru/software-section/updates

Повышение уровня защищенности

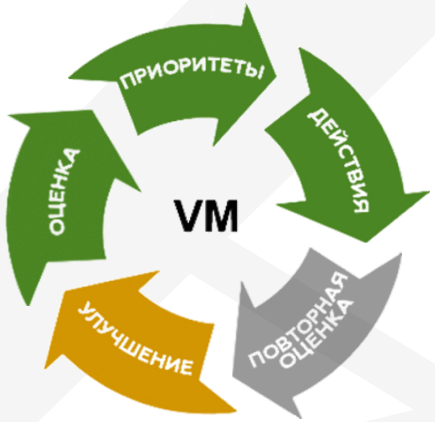
Vulns.io™

Отечественная методика проверки конфигураций

Рекомендации по безопасной настройке операционных систем Linux

Утвержден ФСТЭК России
25 декабря 2022 г.

Ссылка:

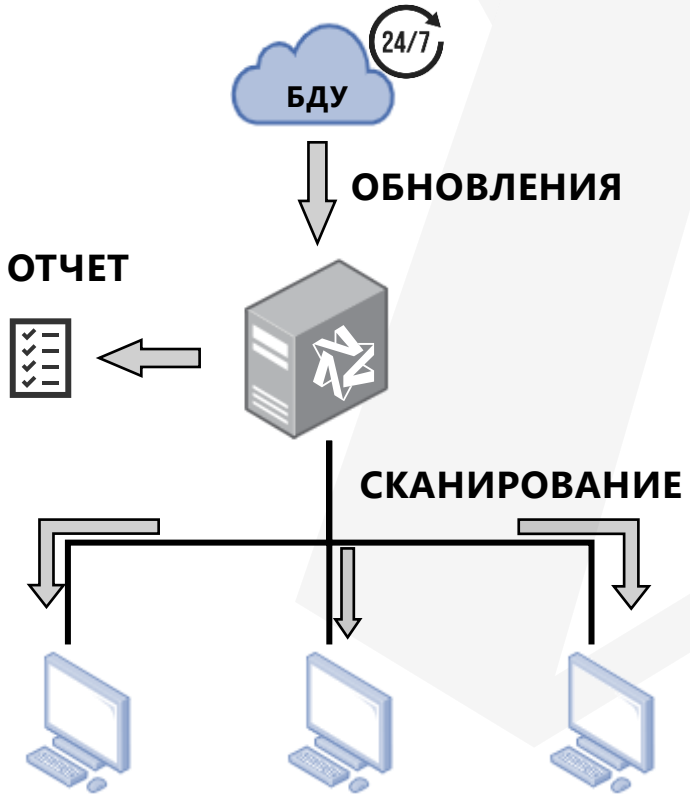


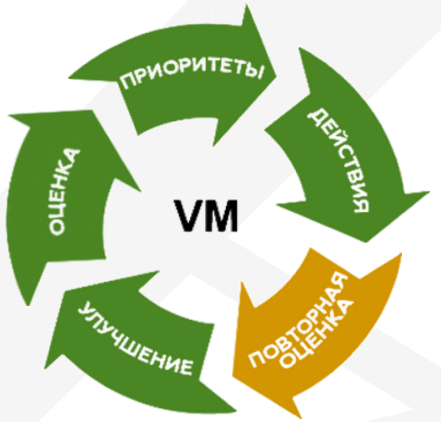
- настройка авторизации;
- ограничение привилегий;
- настройка прав доступа;
- настройка механизмов защиты ядра;
- уменьшение периметра атаки ядра;
- настройка СЗ пользовательского пространства со стороны ядра.

Контроль уровня защищенности

Vulns.io VM

По мере обнародования новых уязвимостей



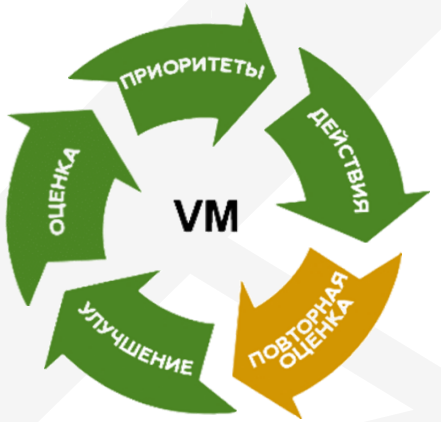


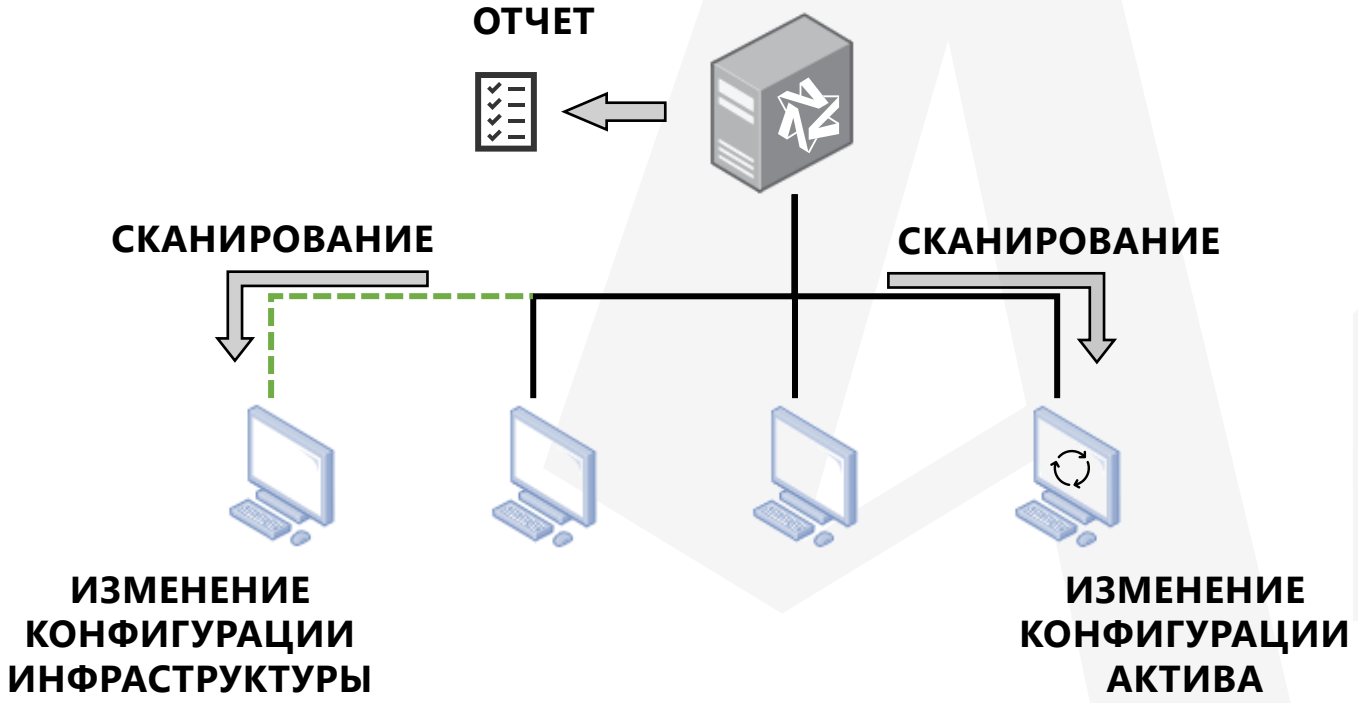
Контроль уровня защищенности

Vulns.io VM

По мере обнародования новых уязвимостей

По факту изменения конфигурации



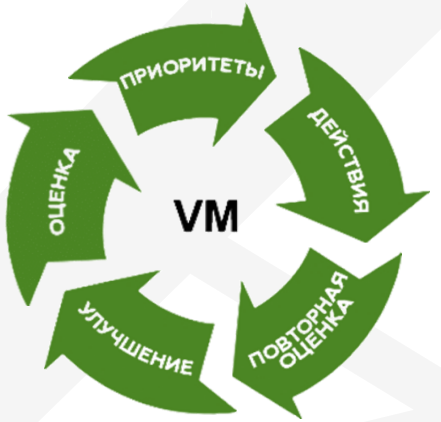


Контроль уровня защищенности

Vulns.io VM

По мере обнародования новых уязвимостей

По факту изменения конфигурации



Цель:
Знать про все уязвимости в инфраструктуре

Задача инструмента VM:
как можно быстрее отображать изменения уровня защищенности инфраструктуры

К чему стремиться

Vulns.io™

Вести собственный рейтинг актуальных и опасных уязвимостей

Наращивать базу проверенных обновлений

Публиковать данные об уязвимостях российского ПО

Работать с актуальными данными

Вырабатывать методики для российских ОС

Vulns.io VM

Управление уязвимостями

Андрей Никонов
Главный инженер-программист
ООО «Фродекс»

a.nikonov@frodex.ru

t.me/mordron

frodex.ru

Техническая поддержка:
support@frodex.ru

Офис:
г.Уфа, ул.Пархоменко, 133/1

Спасибо за внимание!