Комплаенс-контроль с результатом

MaxPatrol HCC и MaxPatrol VM 2.0

О чем расскажем сегодня?

- Как защитить инфраструктуру от самых опасных уязвимостей
- Почему необходимо быстро получать информацию о трендовых уязвимостях
- Как проверить инфраструктуру на соответствие важным требованиям
- Основные стандарты для безопасности Linux-систем
- Оценка уровня критичности уязвимостей по методике ФСТЭК

Количество новых уязвимостей растет с каждым годом — NVD

>18 000 уязвимостей	>20 000 уязвимостей	>25 000 уязвимостей	?
2020г.	2021г.	2022г.	2023г.

По информации из базы данных National Vulnerability Database

Количество новых уязвимостей растет с каждым годом — БДУ ФСТЭК

>5900 уязвимостей	>6400 уязвимостей	>7500 уязвимостей	>3200 уязвимостей
2020г.	2021г.	2022г.	На 18 июня 2023г.

Всего **более 47 500 уязвимостей,** по данным на 18 июня 2023 года

По информации из БДУ ФСТЭК

Результаты пилотных проектов MaxPatrol VM

Более 850 трендовых уязвимостей на каждом проекте

их нужно устранить как можно скорее

В среднем 42 трендовых уязвимости

на активах высокой значимости

В среднем 30 166 уязвимостей

обнаруживалось на 1 проекте

До 3% уязвимостей являются крайне опасными, при этом могут не иметь максимальной оценки по CVSS

По результатам пилотных проектов, которые проводились в 2021 году

Почему важно быстро устранять опасные уязвимости

24

часа

время на устранение наиболее опасных уязвимостей согласно рекомендациям ФСТЭК

56%

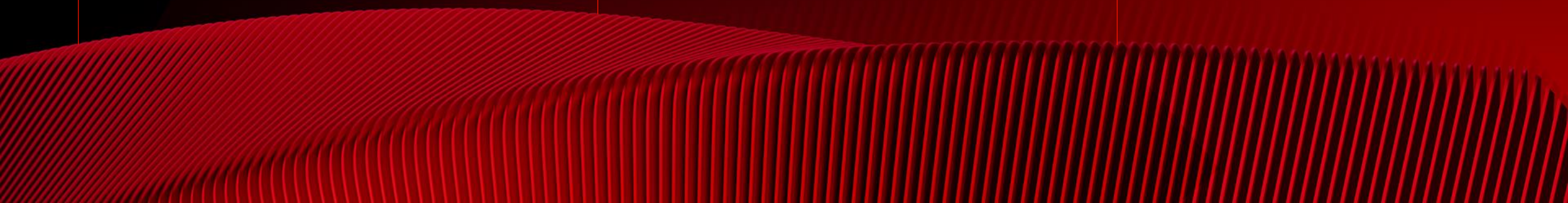
уязвимостей

в 2022 году эксплуатировались уже в течение семи дней после публичного раскрытия

24

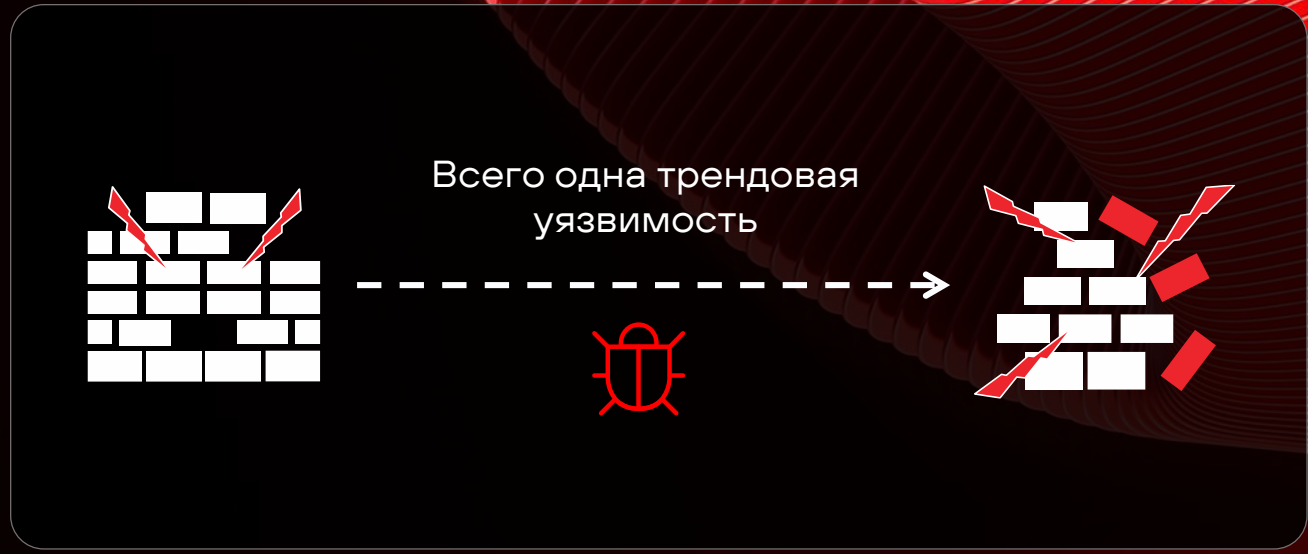
часа

среднее время до появления эксплойта



Трендовые уязвимости

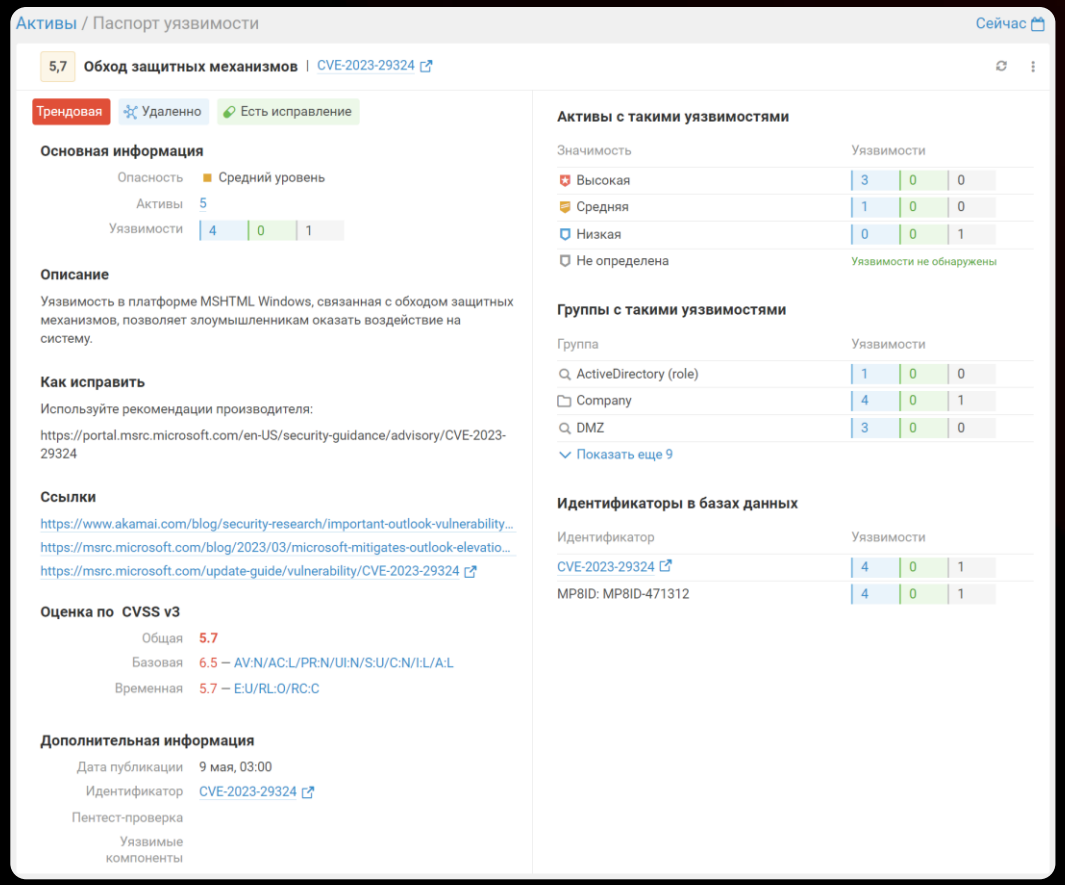
Уязвимости, которые представляют наибольшую опасность для организации или активно эксплуатируются злоумышленниками, либо уязвимости нулевого дня, для которых есть подтвержденные механизмы эксплуатации

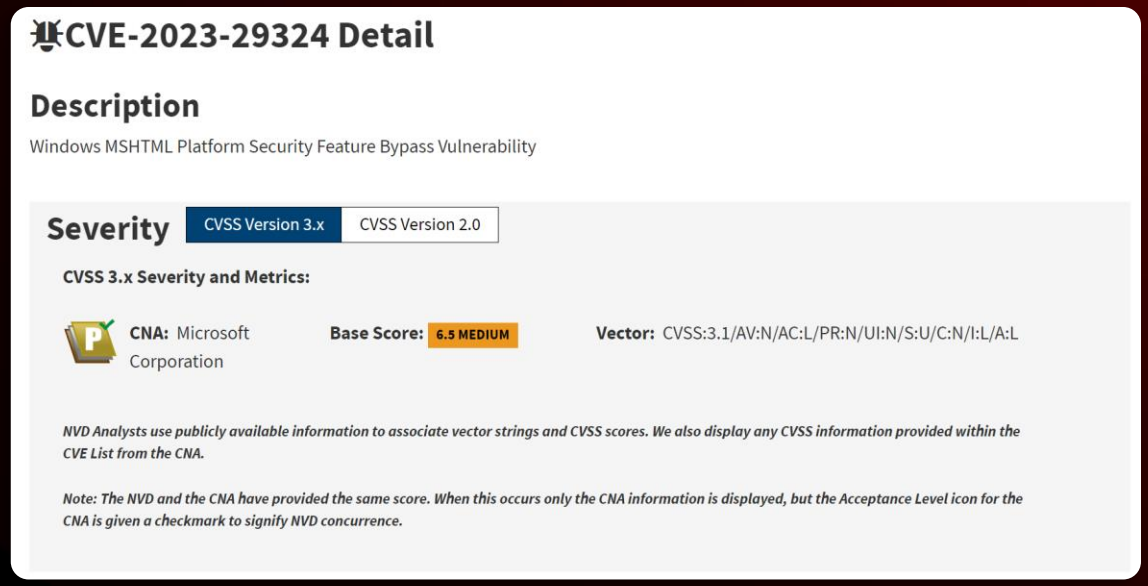


Рекомендации

Нужно обрабатывать и устранять трендовые уязвимости в первую очередь, не дожидаясь плановых сроков обновления

Трендовые уязвимости ≠ высокая оценка по CVSS





Трендовые уязвимости

Опыт и знания специалистов Positive Technologies

- Пентесты
- Исследование угроз
- Расследование инцидентов ИБ

Positive Technologies Knowledge Base

- Способы выявления и устранения уязвимостей
- Бюллетени безопасности

MaxPatrol VM

- Выявление уязвимостей
- Выделение трендовых уязвимостей
- Рекомендации по их устранению

Информация о трендовых уязвимостях доставляется в MaxPatrol VM 2.0 в течение 12 часов

Positive Technologies

Заказчик

Уязвимость 1
Уязвимость 2
Уязвимость 3
Уязвимость ...

Expert (person)
Осуществляет выпуск пакетов, содержащие паспорта уязвимостей

PT Knowledge Base

vm_content

PT Knowledge Base

vm_content → MP VM

Artifactory

vm.adobe
vm.alt_linux
vm.cisco.cisco_asc
vm.astra_linux
...

<= 4 часа

<= 12 часов

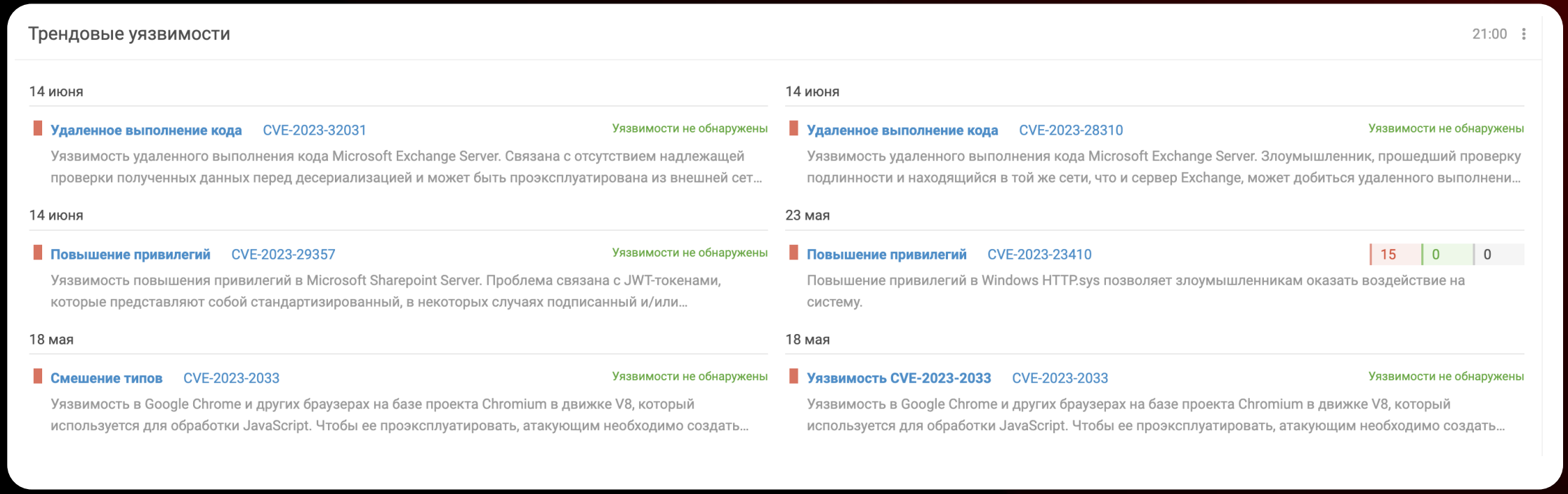
Уязвимость 1
Уязвимость 2
Уязвимость 3
Уязвимость ...

Expert (person)
Осуществляет выпуск пакетов, содержащие паспорта уязвимостей

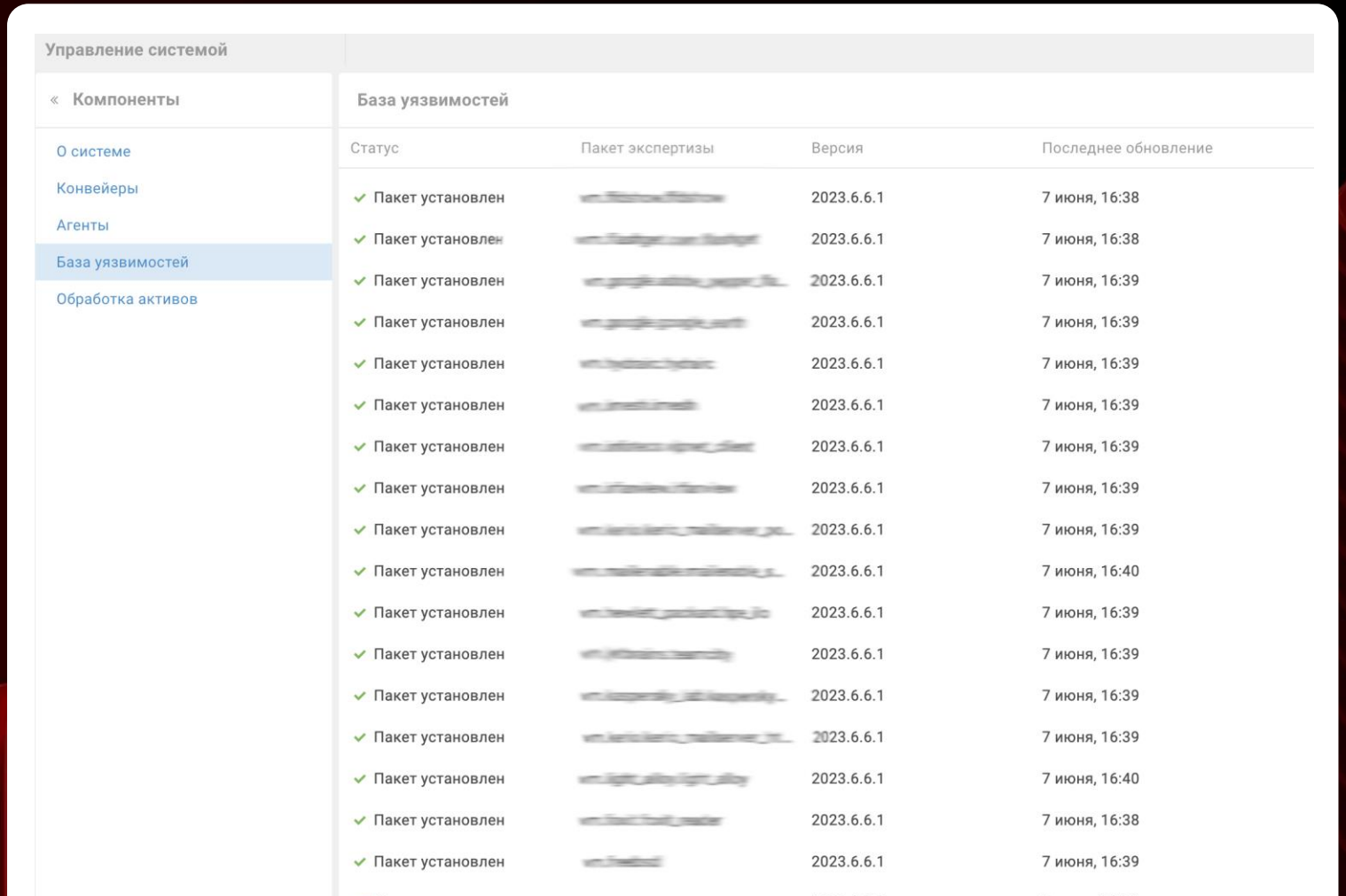
MP VM

<= 2 часа

Дашборд с трендовыми уязвимостями



Обновление базы уязвимостей



MaxPatrol HCC (Host Compliance Control)

Управление уязвимостями
и комплаенс — необходимые условия
результативной кибербезопасности

Как российские компании подходят к комплаенс-контролю

Действующие лица

IT-специалист

Руководитель
отдела ИБ

Ответственный
за комплаенс

Построение комплаенса. Вариант 1

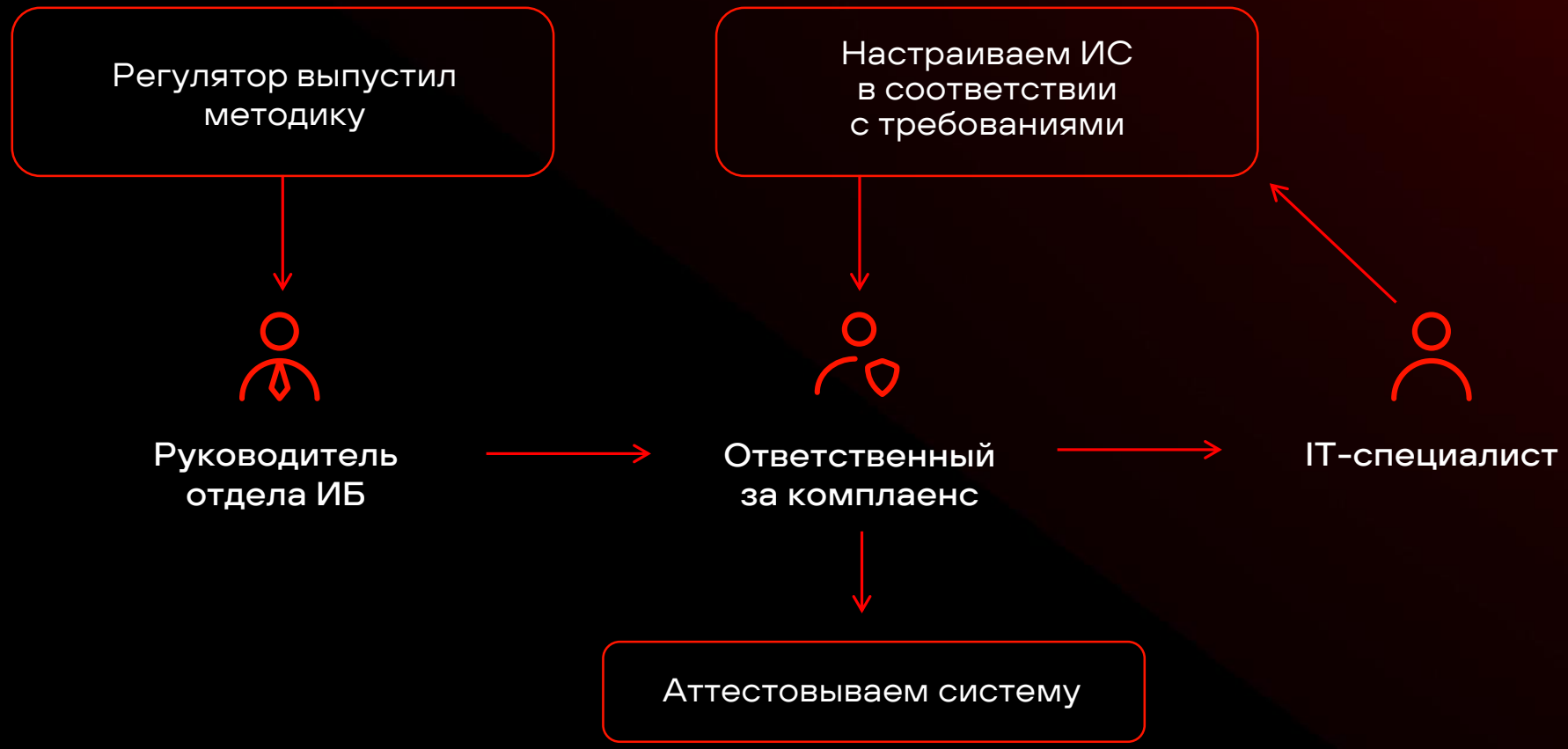
Руководитель
отдела ИБ

IT-специалист

Ничего не делаем
и руководствуемся
здравым смыслом

Ответственный
за комплаенс

Построение комплаенса. Вариант 2



Построение комплаенса. Вариант 3

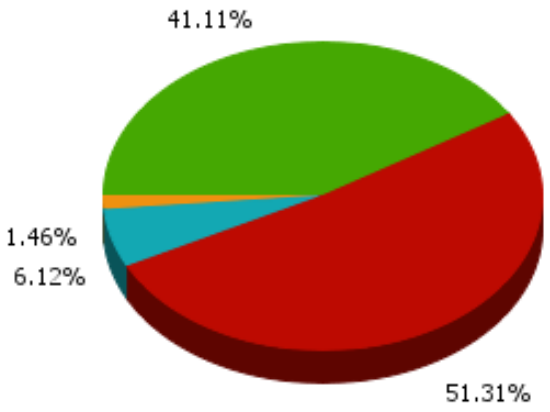
Почему сложно соответствовать международным стандартам?

CIS — Microsoft Windows 2012 R2

Подробные данные по узлам

192.168.56.2

IP-адрес	192.168.56.2
NetBIOS	MAXPATROL8
FQDN	maxpatrol8.ptdemo.local
Имя из задачи	192.168.56.2



Статус	Количество проверок	Доля проверок
Не проверялось	0	0,00%
Соответствует	141	41,11%
Не соответствует	176	51,31%
Неприменимо	21	6,12%
Не определено	5	1,46%
Итого:	343	100%

- Общий подход (масштабный стандарт) годится не для всех
- Компания не может соответствовать всем стандартам

Много требований. Рабочие станции

Более 500 требований для Windows и Microsoft Office, количество узлов — более тысячи

500 * 1000 = 500 000

Много требований. Серверы

В зависимости от ОС и установленного серверного ПО — от 100 до 700 требований на узел, количество узлов — несколько сотен

400 * 100 = **40 000**

Много требований. Сетевое оборудование

В зависимости от ОС и установленного серверного ПО — от 100 до 700 требований на узел, количество узлов — несколько сотен

50 * 100 = 5000

Много требований

Кто-нибудь в реальной жизни сможет соответствовать таким стандартам на 100%?

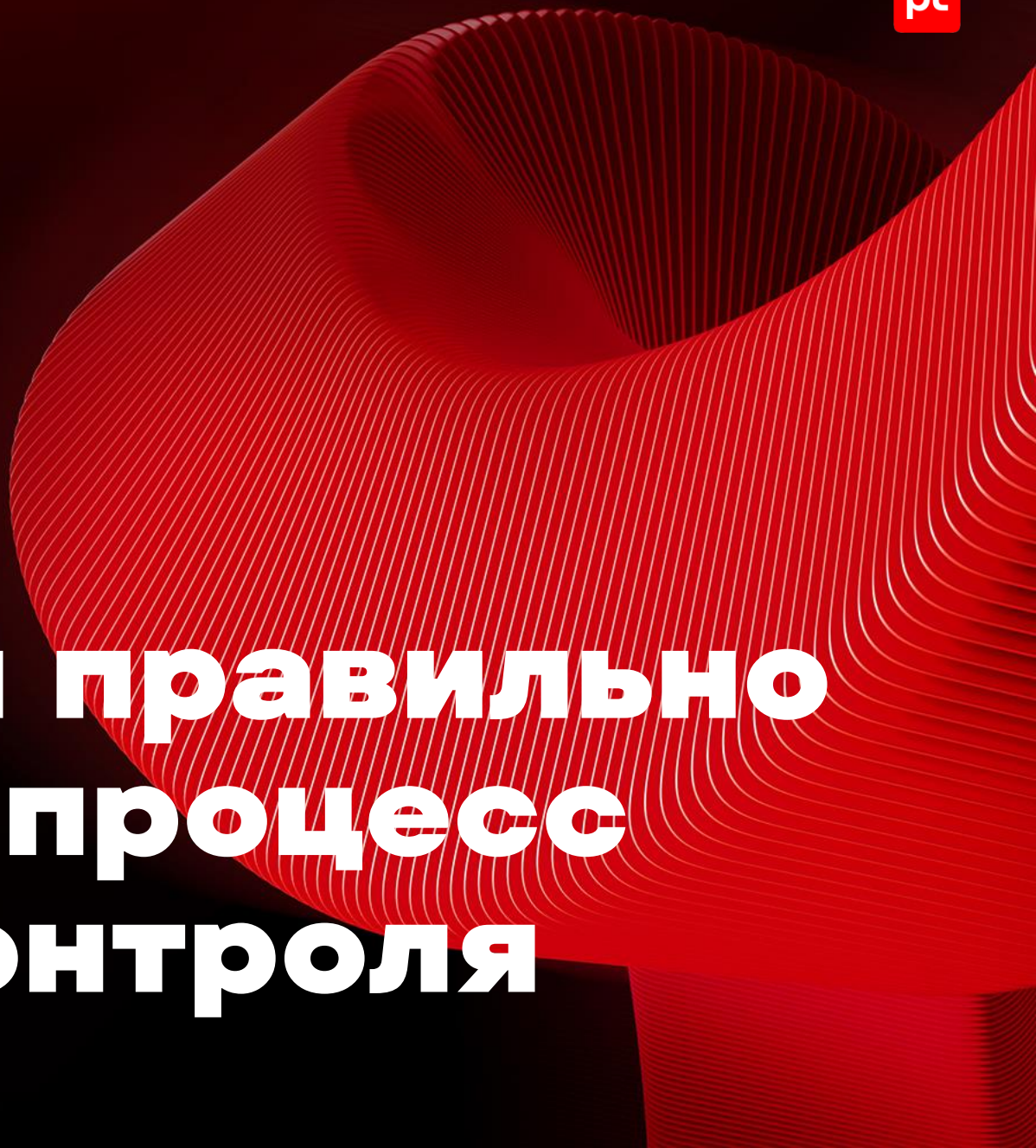
Зачем нужны стандарты, которые нельзя выполнить?

Что не так с требованиями

Сложно понять, какие из требований стандартов имеют отношение к практической безопасности и помогают защититься от взлома, не нарушая при этом работу инфраструктуры

Чтобы разобраться в этом, необходимо детально знать систему, для которой написан бенчмарк

Как мы видим правильно построенный процесс комплаенс-контроля



Внедрение стандартов

Регулярный контроль соответствия стандартам

Преимущества стандартов PT Essentials

- Готовая экспертиза
- Поддержка распространенного ПО и отечественных ОС
- Приоритизация обнаруженных рисков
- Конкретные рекомендации по устранению рисков

Список стандартов PT Essentials

- PT Essential — Windows Desktop
- PT Essential — Windows Server
- PT Essential — Microsoft SQL Server
- PT Essential — Generic Linux
- PT Essential — Oracle Database
- PT Essential — VMware ESXi
- PT Essential — VMware vCenter
- PT Essential — Microsoft Exchange
- PT Essential — RHEL-based Linux

- PT Essential — HP UX
- PT Essential — IBM AIX
- PT Essential — Linux Kernel
- PT Essential — Docker
- PT Essential — Cisco IOS
- PT Essential — Cisco IOS XE
- PT Essential — Cisco ASA
- PT Essential — Cisco Nexus

MaxPatrol HCC — новый модуль комплаенс-контроля

1

Проверка инфраструктуры на соответствие готовым стандартам и требованиям

2

Приоритизация обнаруженных рисков

3

Контроль выполнения требований с помощью динамических дашбордов

4

Назначение политик и эффективный контроль за сроками устранения несоответствий

«Три кита» MaxPatrol HCC

Активы

Инвентаризация
информационных активов

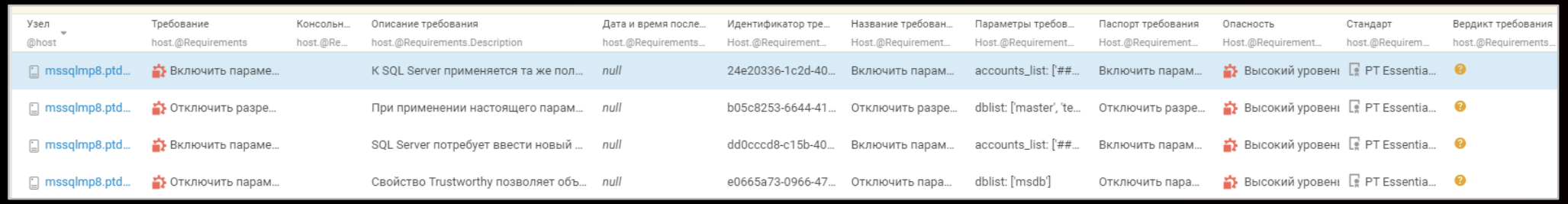
Стандарты

Оценка защищенности

Политики

Контроль за соблюдением
требований политик
и стандартов безопасности

Как работает MaxPatrol HCC



Узел @host	Требование host.@Requirements	Консольн… host.@Re…	Описание требования host.@Requirements.Description	Дата и время после… host.@Requirements…	Идентификатор тре… Host.@Requirement…	Название требован… Host.@Requirement…	Параметры требов… Host.@Requirement…	Паспорт требования Host.@Requirement…	Опасность Host.@Requirement…	Стандарт host.@Requirem…	Вердикт требования host.@Requirements…
mssqlmp8.ptd…	Включить параме…		К SQL Server применяется та же пол…	*null*	24e20336-1c2d-40…	Включить парам…	accounts_list: ['##…	Включить парам…	Высокий уровен	PT Essentia…	
mssqlmp8.ptd…	Отключить разре…		При применении настоящего парам…	*null*	b05c8253-6644-41…	Отключить разре…	dblist: ['master', 'te…	Отключить разре…	Высокий уровен	PT Essentia…	
mssqlmp8.ptd…	Включить параме…		SQL Server потребует ввести новый …	*null*	dd0cccd8-c15b-40…	Включить парам…	accounts_list: ['##…	Включить парам…	Высокий уровен	PT Essentia…	
mssqlmp8.ptd…	Отключить парам…		Свойство Trustworthy позволяет объ…	*null*	e0665a73-0966-47…	Отключить пара…	dblist: ['msdb']	Отключить пара…	Высокий уровен	PT Essentia…	

Сбор данных об активах инфраструктуры → Назначение активам стандартов для оценки соответствия им → Расчет требований на основе собранных данных об активах → Управление циклом устранения несоответствий требованиям

О ядре Linux

Ядро Linux — основа семейства операционных систем GNU/Linux и Android. Разрабатывается под открытой лицензией GPL 2.0.

На Linux-системах работают:

100% суперкомпьютеров из рейтинга Top500

90% публичных ресурсов

62% рынка встраиваемых устройств

77% веб-серверов

>3 млрд активных Android-устройств

Скорость развития кодовой базы ядра Linux

Более 30 миллионов строк кода

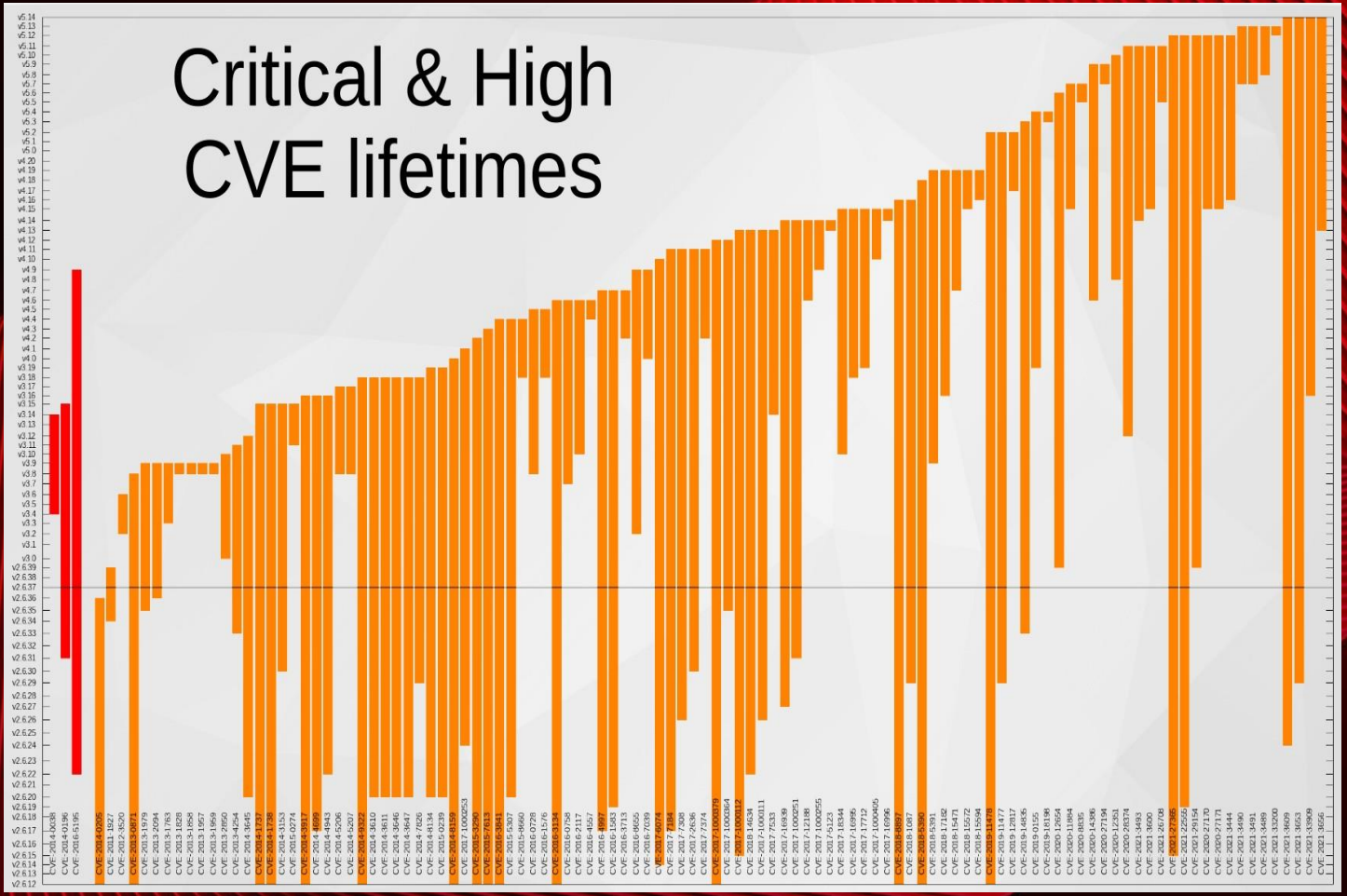
Средняя скорость merge — около 10 патчей в час

8900 строк добавляется, 2500 удаляется и **2100** изменяются каждый день

Каждый год в развитии участвуют более 4000 разработчиков

У сообщества есть санитайзеры, фаззер syzkaller, инструменты статического анализа, но... уязвимости появляются быстрее, чем исправляются

Среднее время жизни ядерных уязвимостей — 5,5 лет



Проект самозащиты ядра Linux

Kernel Self Protection Project

Целью проекта является устранение классов уязвимостей и методов их эксплуатации в ядре Linux

- Чтобы повысить безопасность ядра, нужно больше чем исправление ошибок
- Ядро Linux должно безопасно отрабатывать в ошибочной ситуации
- Идеи grsecurity и PaX — во многом источник вдохновения проекта Kernel Self Protection Project

Как настраиваются средства защиты ядра Linux

Три вида параметров ядра Linux

1

Параметры сборки

(Kconfig)

2

Параметры загрузки

(kernel cmdline)

3

Динамические параметры

(sysctl)

При эксплуатации дистрибутива GNU/Linux со штатным ядром возможно изменить только параметры загрузки и динамические параметры

Как разобраться во множестве настроек безопасности

Drawn by Daniel Reeve, made by weta

Ключевые понятия безопасности операционных систем:

- Классы уязвимостей
- Техники эксплуатации уязвимостей
- Механизмы выявления ошибок
- Технологии защиты:
  - входящие в mainline
  - поставляемые отдельно (в том число коммерческие)
  - требующие аппаратной поддержки

Все они имеют сложные взаимосвязи. Было бы полезно иметь их визуальное представление

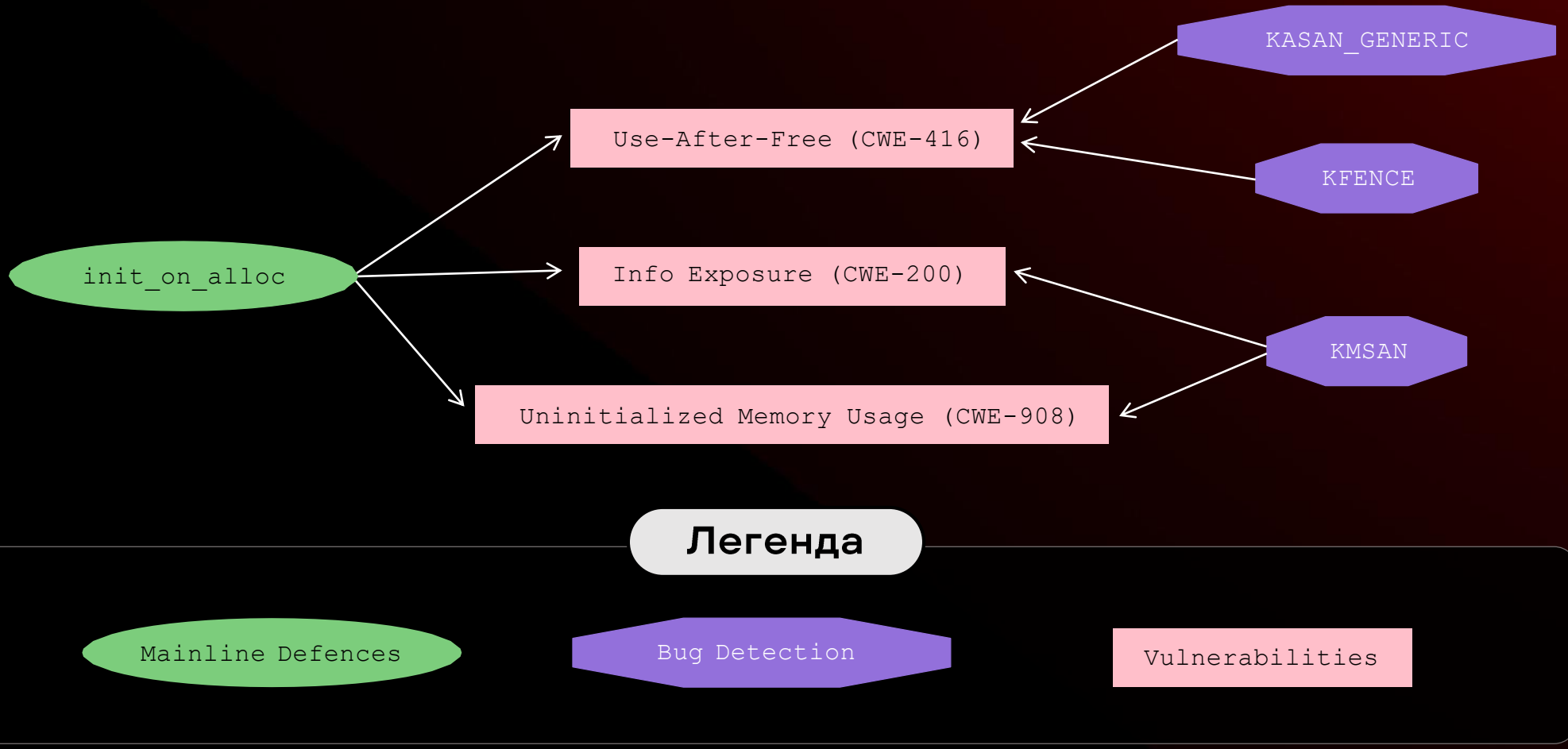
Карта защиты ядра Linux

Карта не затрагивает способы уменьшения поверхности атаки

Карта и дополнительная документация к ней доступны по ссылке

Linux Kernel Defence Map

Пример из карты: механизм init_on_alloc



Стандарт PT Essential – Linux Kernel

Наша многолетняя экспертиза по безопасности ядра Linux теперь в MaxPatrol HCC

- Наш набор рекомендаций по безопасной настройке ядра Linux вошел в методический документ ФСТЭК России от 25 декабря 2022 года
- Более 20 ключевых параметров ядра, корректная настройка которых существенно усложняет задачу атакующего

Методический документ ФСТЭК России от 25 декабря 2022 года

MaxPatrol HCC (Host Compliance Control)

Экспертиза Positive Technologies

Возможности

MaxPatrol VM

База знаний об уязвимостях

Построение процесса управления уязвимостями

- Обнаружение и приоритизация уязвимостей
- Контроль выявления и устранения уязвимостей

+

MaxPatrol HCC

Пакеты стандартов

Построение процесса комплаенс-контроля

- Использование экспертных стандартов
- Возможность создавать свои критерии проверки

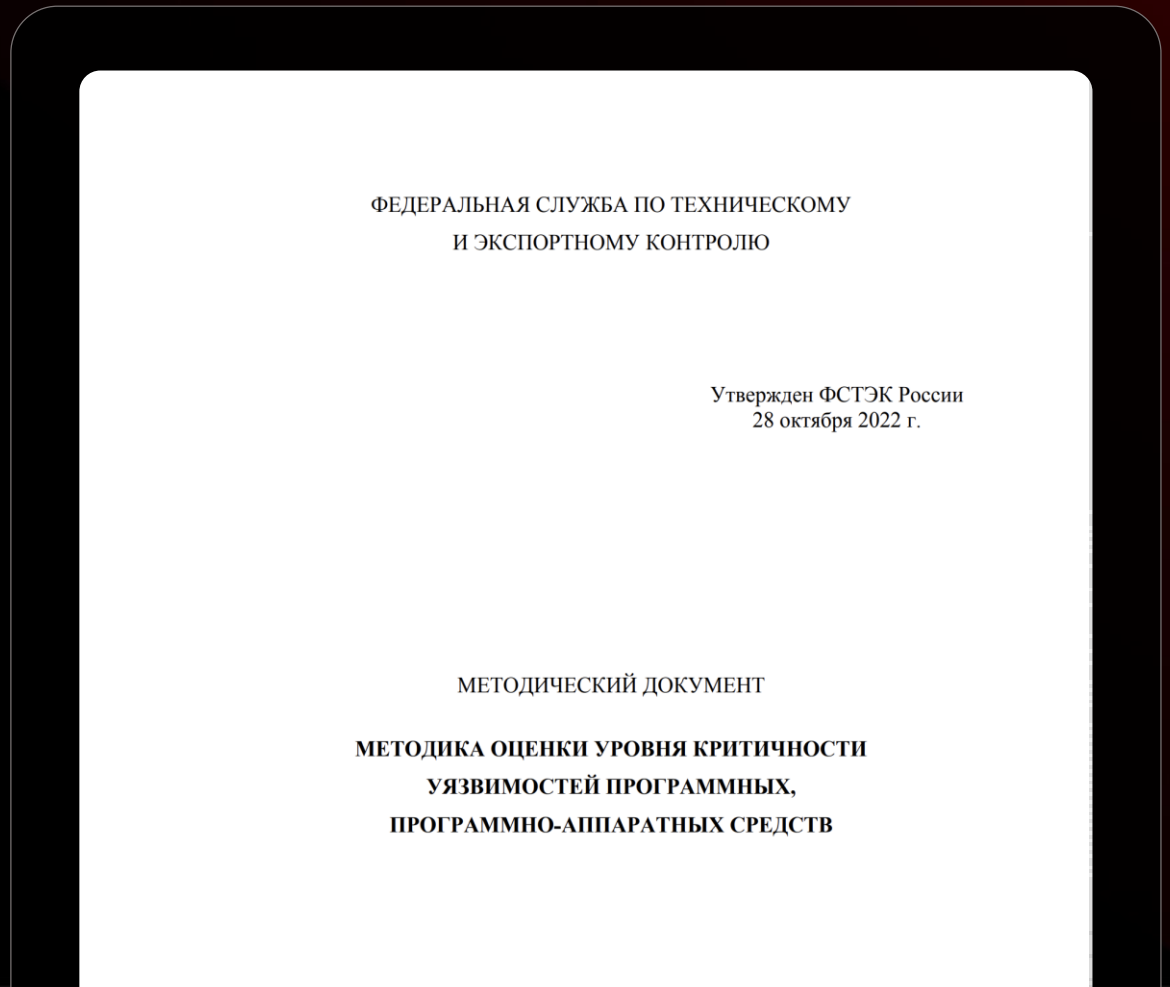
Основа

SECURITY ASSET MANAGEMENT

- Сбор полной информации об инфраструктуре
- Автоматическое определение активов, непрерывная актуализация данных, учет изменений

И кое-что еще...

Оценка уровня критичности уязвимостей по методике ФСТЭК



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
28 октября 2022 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА ОЦЕНКИ УРОВНЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

Оценка уровня критичности уязвимостей по методике ФСТЭК

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

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].

Ссылки

https://www.mozilla.org/en-US/security/advisories/mfsa2019-07/#CVE-2019-9799

Оценка по CVSS v3

Общая	6.5
Базовая	7.5 – AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Временная	6.5 – E:U/RL:O/RC:C

2.7. Показатель I_{infr} определяется по следующей формуле:

$$I_{infr} = k * K + l * L + p * P, \text{ где}$$

K – показатель, характеризующий тип компонента информационной системы, подверженного уязвимости;

L – показатель, характеризующий количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов);

P – показатель, характеризующий влияние уязвимого компонента на защищенность периметра информационной системы;

k, l, p – весовые коэффициенты показателей.

№ п/п	Суммарное количество баллов уязвимости	Оценка уровня критичности уязвимости
1	$7,0 \le V \le 10,0$	Критичный
2	$4,5 \le V < 7,0$	Высокий
3	$1,5 \le V < 4,5$	Средний
4	$V < 1,5$	Низкий

Оценка уровня критичности уязвимостей по методике ФСТЭК

	ПОКАЗАТЕЛЬ	ВЕС	ЗНАЧЕНИЕ	ОЦЕНКА	ИТОГ (k ∗ Ki, l ∗ Lj, p ∗ Pm)
1	Тип компонента информационной системы, подверженного уязвимости (K)	0,4	Уязвимости подвержены компоненты информационной системы, обеспечивающие реализацию критически важных процессов (бизнес-процессов), функций, полномочий	1	0,4
			Уязвимости подвержены серверы	0,8	0,32
			Уязвимости подвержено телекоммуникационное оборудование, система управления сетью передачи данных	0,8	0,32
			Уязвимости подвержены автоматизированные рабочие места	0,5	0,20
			Уязвимости подвержены другие компоненты	0,5	0,20
2	Количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телеком-муникационного оборудования, средств защиты информации и других компонентов) (L)	0,2	Более 70% от общего числа компонентов в информационной системе	1	0,2
			50–70% от общего числа компонентов в информационной системе	0,8	0,16
			10–50% от общего числа компонентов в информационной системе	0,6	0,12
			Менее 10% от общего числа компонентов в информационной системе	0,5	0,10
3	Влияние на эффективность защиты периметра системы, сети (P)	0,4	Уязвимое программное, программно-аппаратное средство доступно из интернета	1	0,4
			Уязвимое программное, программно-аппаратное средство недоступно из интернета	0,5	0,2

Записаться на демонстрацию MaxPatrol VM с модулем MaxPatrol HCC


Спасибо!