Повестка

- О компании Tenable
- Продукты Tenable, их особенности
- Как Tenable.sc позволяет автоматизировать процесс управления уязвимостями
- Демонстрация решения
- Ответы на вопросы

Tenable.sc

Корпоративное управление уязвимостями

Илья Батетников, Тайгер Оптикс
Email: sales@tiger-optics.ru

Более 27.000 организаций, в том числе 250+ в России и СНГ, доверяют Tenable анализ уязвимостей

СОЗДАТЕЛЬ NESSUS

Более 2.000.000 скачиваний по всему миру

20 ЛЕТ ЛИДЕРСТВА

Лидер по числу выявлению 0-day среди VM-вендоров, лидер в исследовании Forrester, лидер по покрытию CVE

ИНОВАЦИИ

Выявление активов и анализ уязвимостей в облаках, контейнерах, АСУ ТП и ИТ-средах

Довольные заказчики

50% из Fortune 500 **25% Global 2000**

Fortune 10

Chevron

Walmart

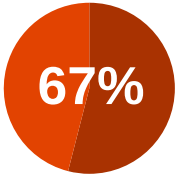
at&t

ExxonMobil

VALERO

PHILLIPS 66

Fortune 100



McKESSON
Empowering Healthcare

CardinalHealth

BEST BUY

Microsoft

THE HOME DEPOT

CISCO

TARGET

ORACLE

COSTCO WHOLESALE

Google

Прочие

ING

amazon.com

SIEMENS

Morgan Stanley

QUALCOMM

Spotify

BARCLAYS

NIKE

PayPal

KAYAK

Dropbox

vmware

xerox

Johnson&Johnson

adidas

NBA

tenable | RESEARCH

Одна из лучших команд исследований

5-20 мин

Средняя длительность сканирования хоста

30%

Инвестиции в R&D и инновации

100+

0-day обнаружено в 2019 году

161.000+

Готовых проверок на уязвимости, нарушения и пр.

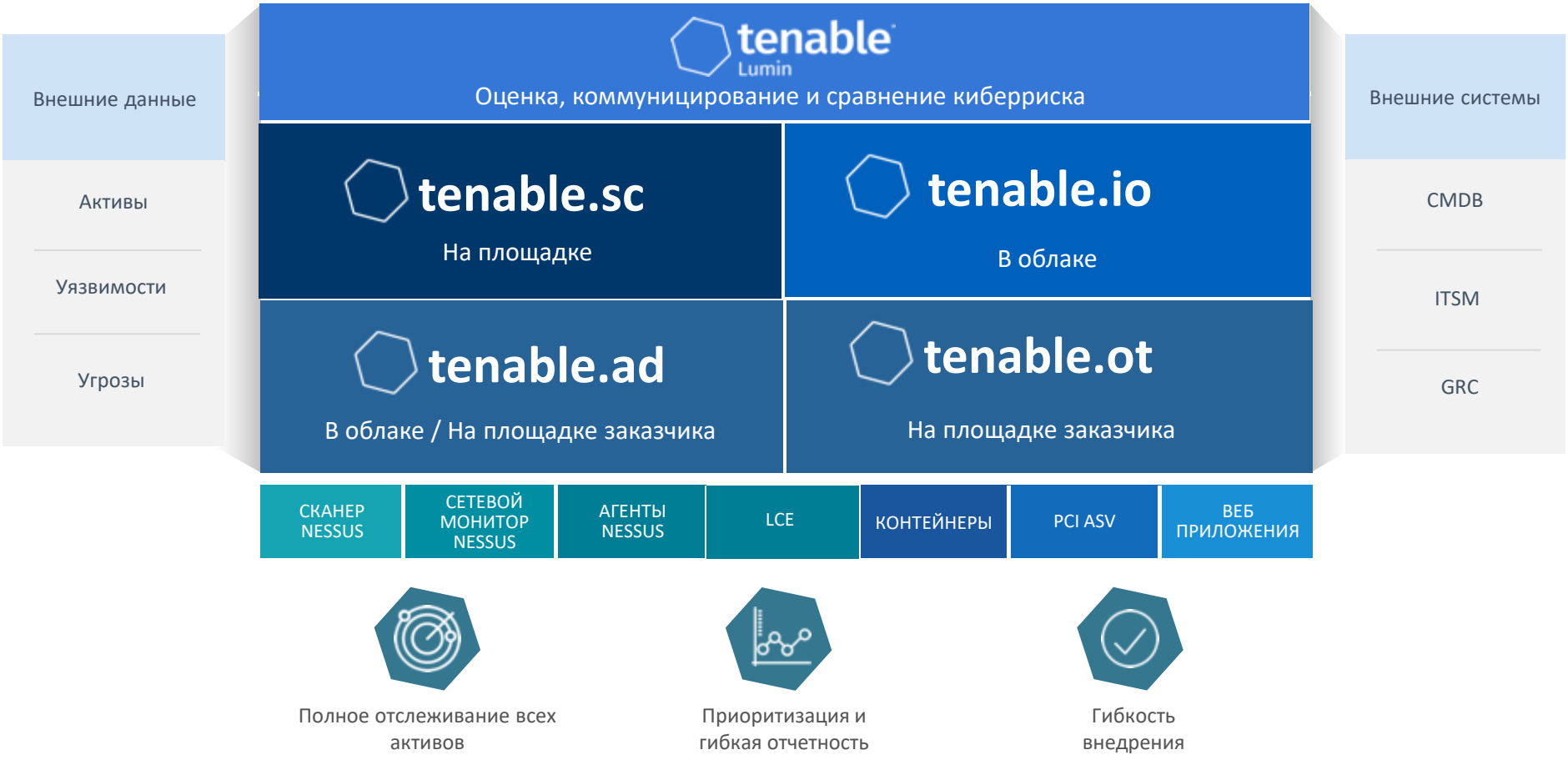
24 часа

Медианное время на выпуск новых проверок

64.000+

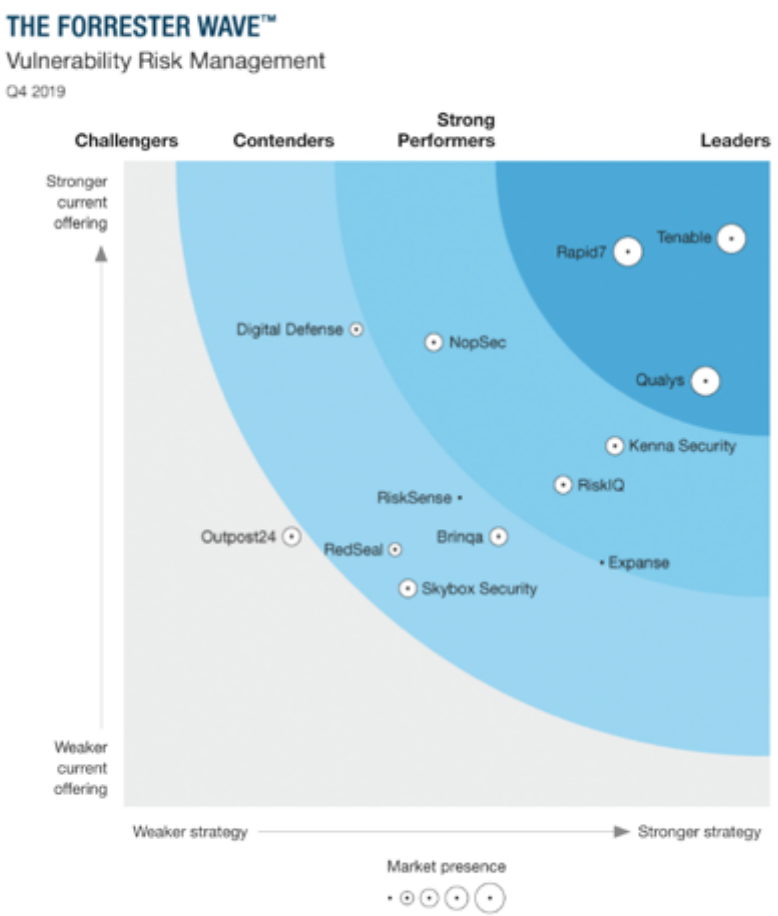
Покрытие CVE (лидирующий показатель)

Платформа киберриска Tenable



FORRESTER®

“Tenable следует своему видению по созданию **единой платформы управления уязвимостями.** Одна из сильных сторон Tenable заключается в **трансляции данных в бизнес-термины** для приоритизации риска.”



Tenable.sc

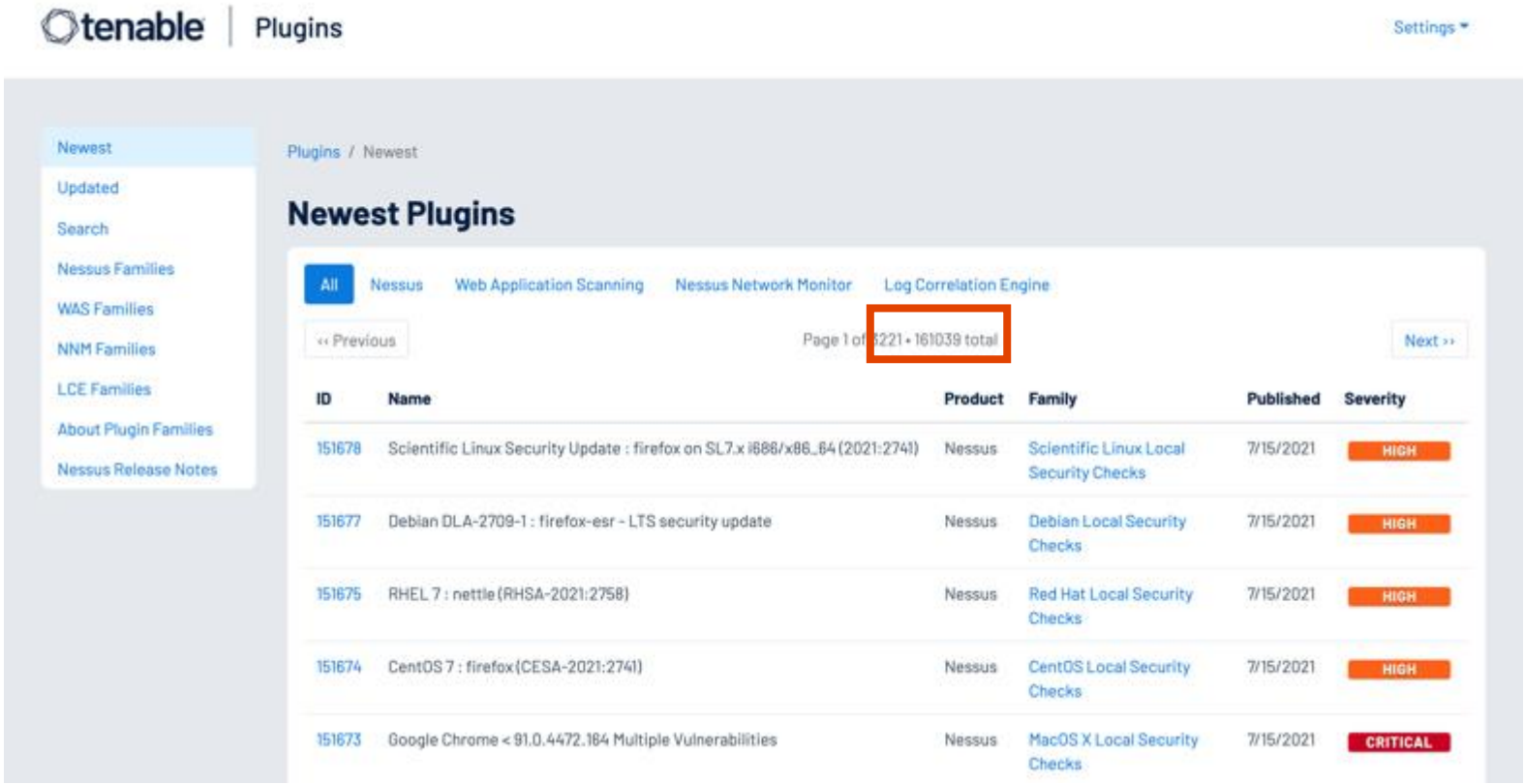
Управление уязвимостями на основе уровня риска

Процесс управления уязвимостями с Tenable.sc

Архитектура Tenable.sc

Лицензирование по IP-адресам. Сканеры бесплатны и не требуют покупки лицензии.

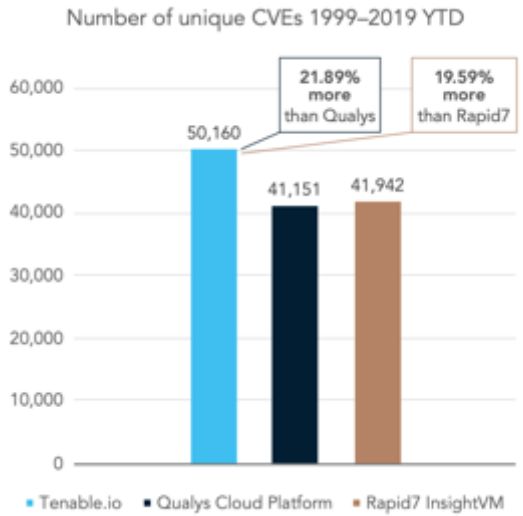
Обширная и открытая база проверок

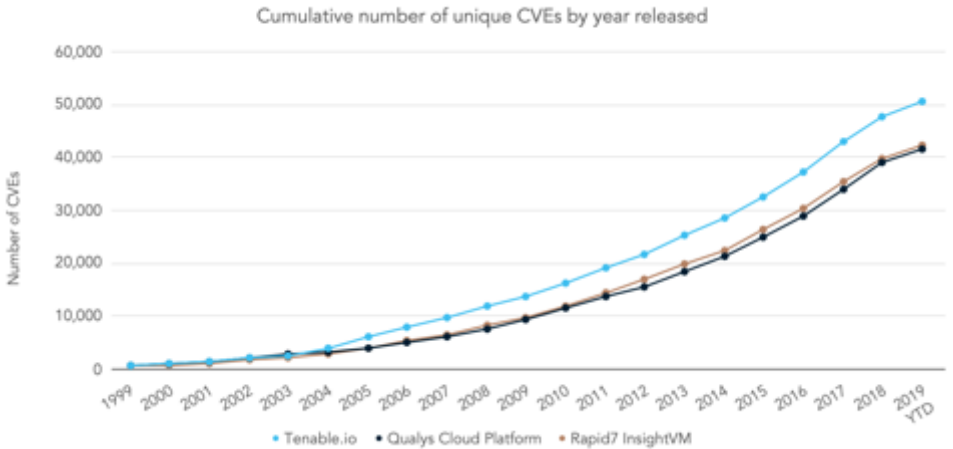


https://www.tenable.com/plugins

Лидирующее покрытие по CVE

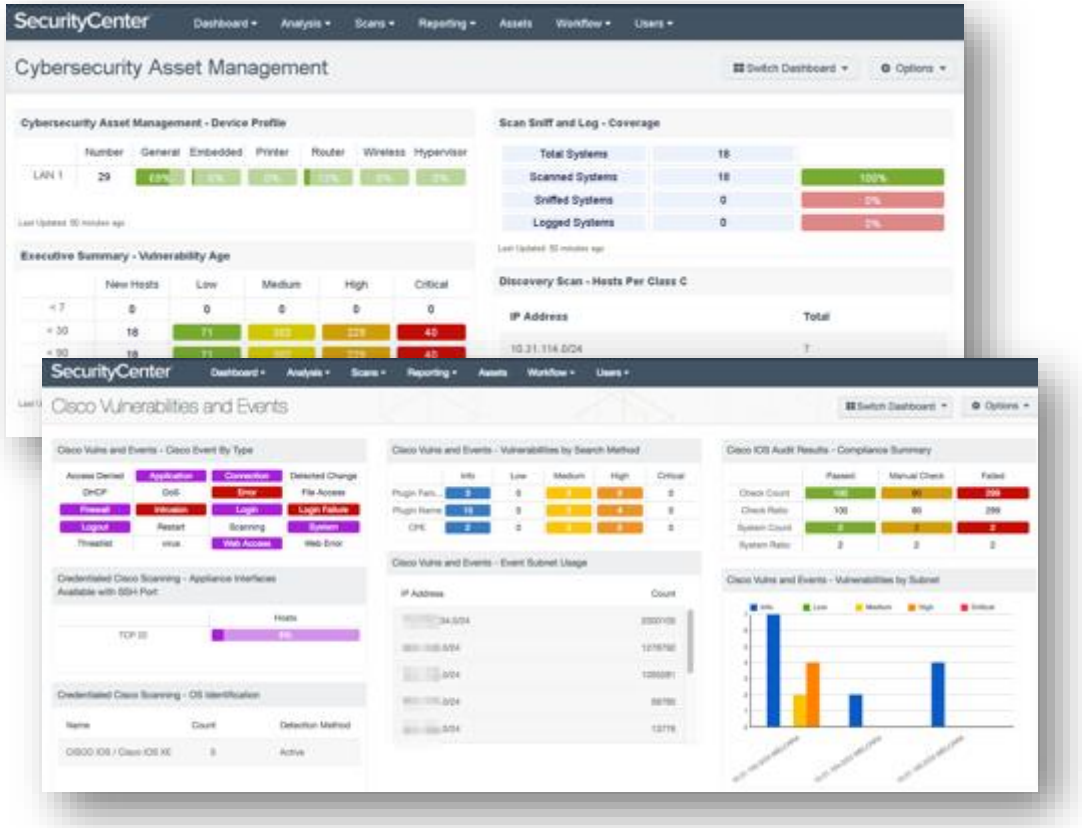
На 16 июля 2021 года Tenable выявляет 64023CVE IDs





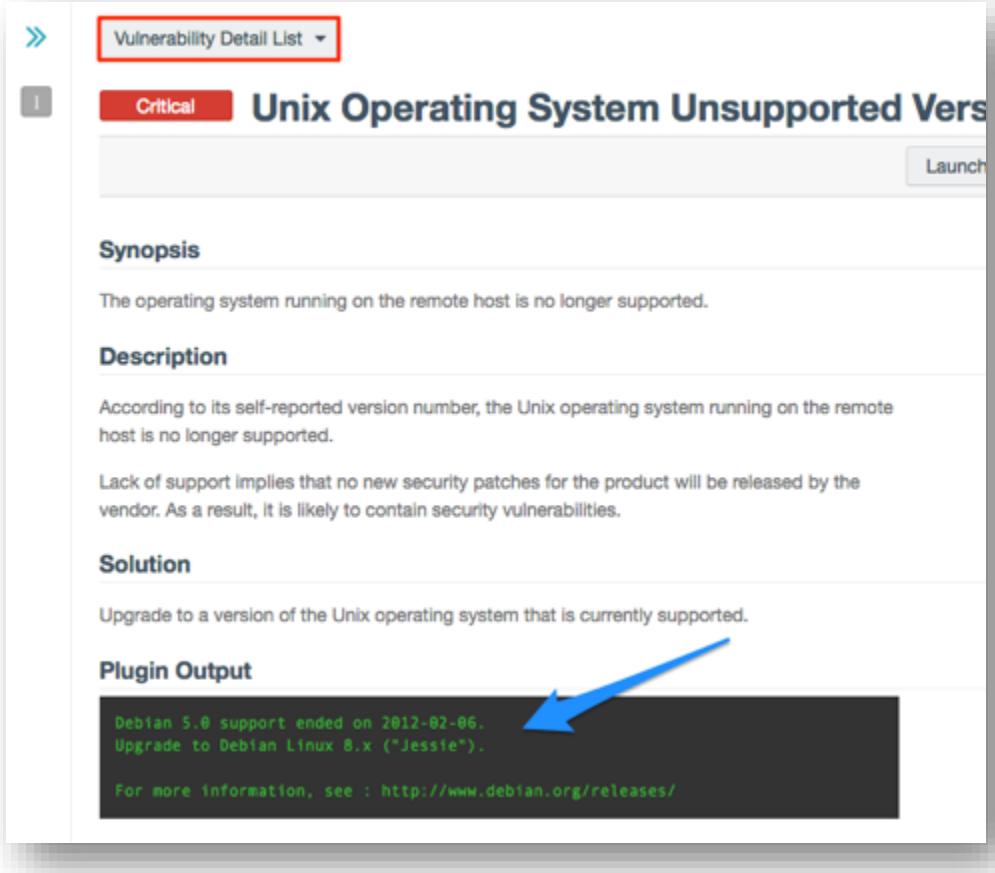
Источник: https://welcome.tiger-optics.ru/сравнение-сканеров-уязвимостей-qualys-rapid7-tenable

Современный, быстрый и удобный веб-интерфейс



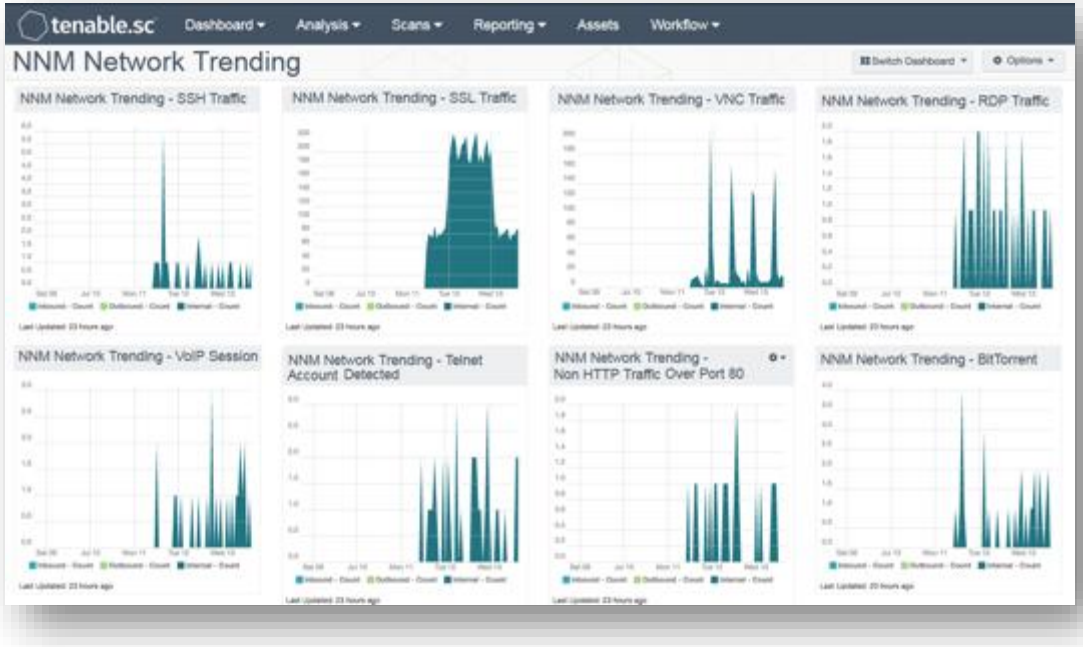
1. Централизованный веб-интерфейс управления всеми задачами сканирования
2. Многопользовательский режим с возможностью гибкой настройки доступа
3. Более 100 готовых дашбордов и конструкторы для мониторинга всех аспектов управления уязвимостями
4. Технологии Web 2.0, поддержка планшетов и смартфонов

Доказательность результатов сканирования



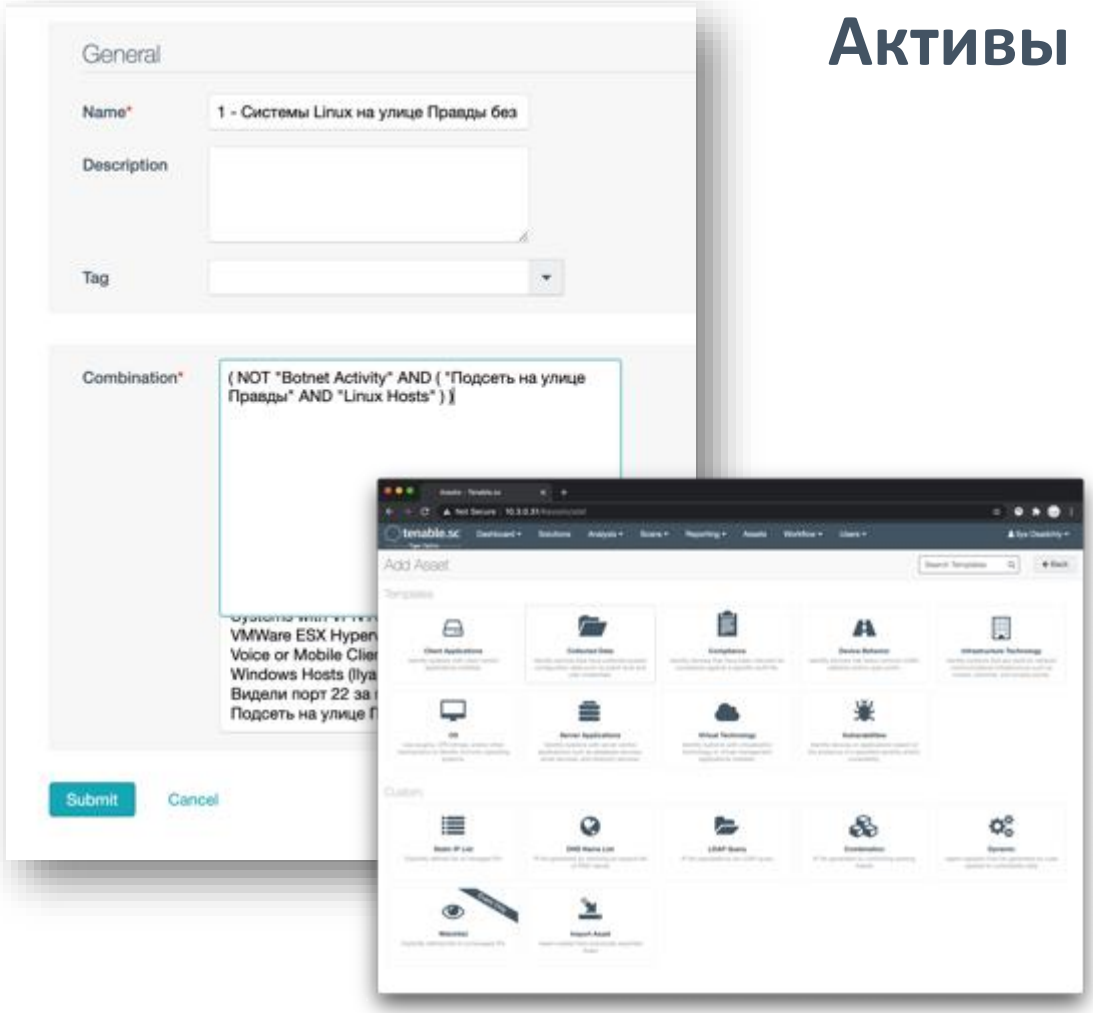
1. Каждая уязвимость сопровождается доказательством (выводом командной строки), где указано, на основании чего определена уязвимость
2. Отображается детальная статистика по уязвимости
3. Предоставляются ссылки на подробные описания и патчи для устранения

Моментальное выявление хостов и уязвимостей



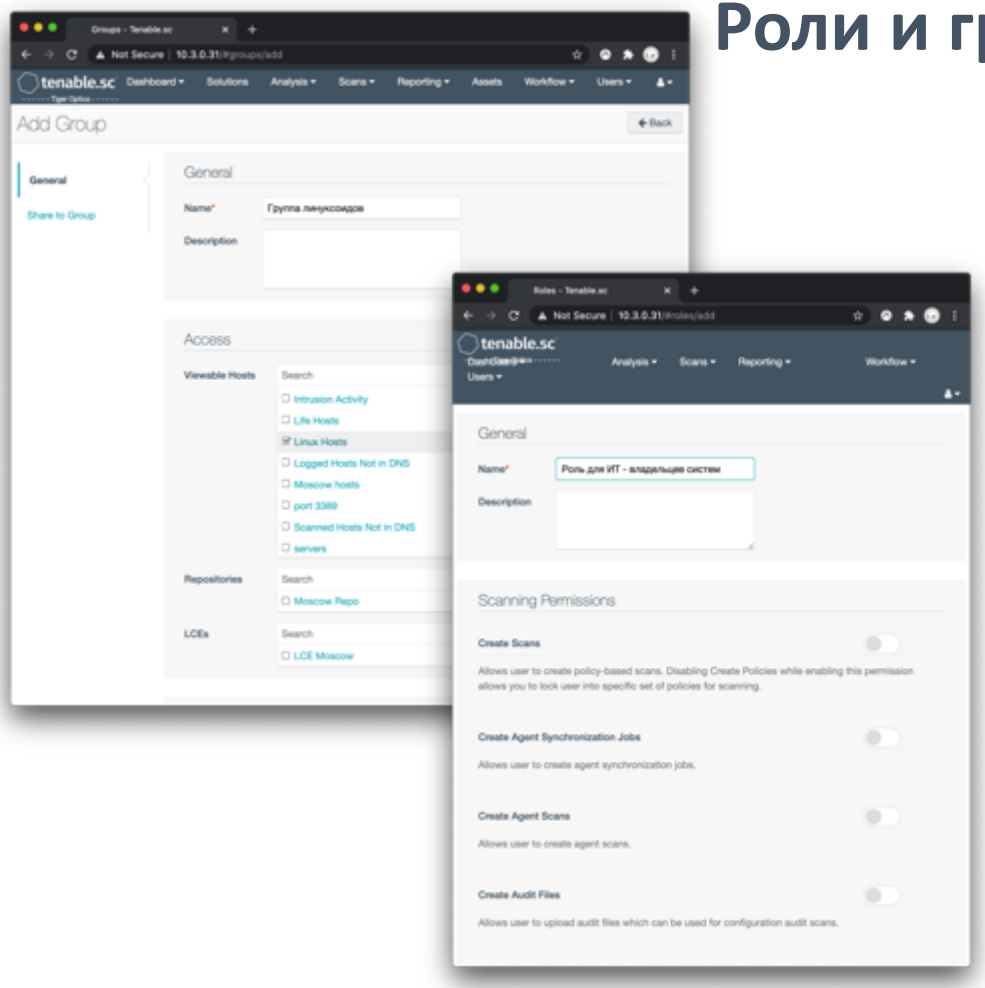
1. **Пассивный сканер** слушает трафик и выявляет новые и активные хосты, а также уязвимости на них
2. Незаменимо для гостевых сегментов и систем, для которых недоступны УЗ и нельзя поставить агент
3. Полезно для любых критичных сегментов для улучшения понимания обстановки с уязвимостями и ускорения детекта

Активы



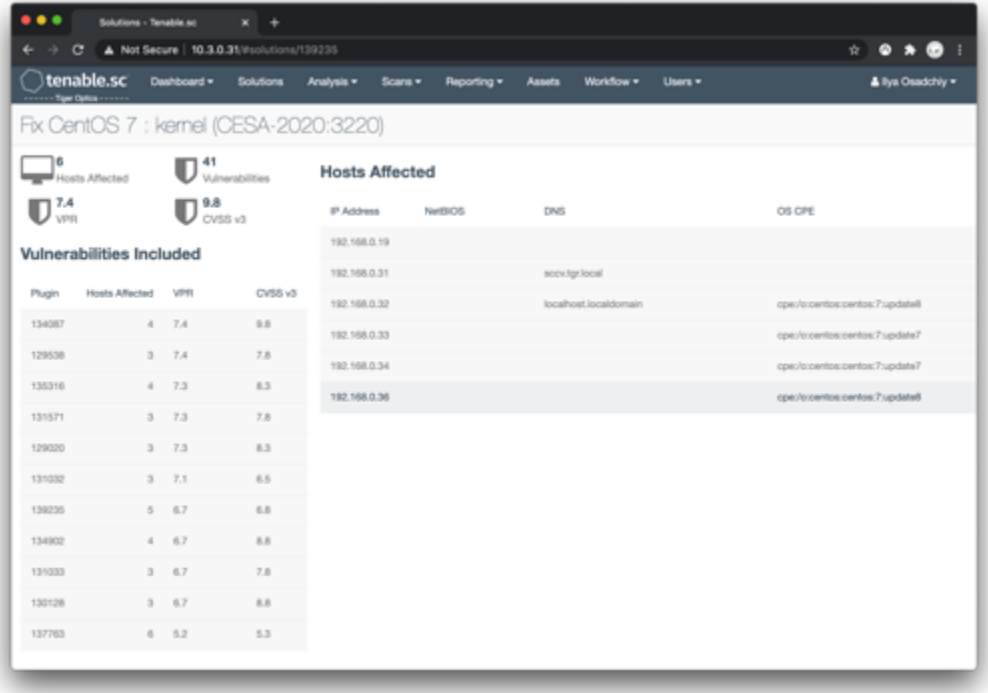
1. Произвольная группировка хостов по статическим и динамическим признакам
2. IP, подсеть, ОС, когда увидели хост в первый раз, наличие определенной уязвимости, наличие эксплойта, количество и возраст уязвимостей, открытые порты и пр.
3. Пример актива: **«Системы Linux в Москве на улице Правды без ботнетов»**
4. Используются для назначения задач, фильтрации результатов, построения отчетов и дашбордов и пр.

Роли и группы



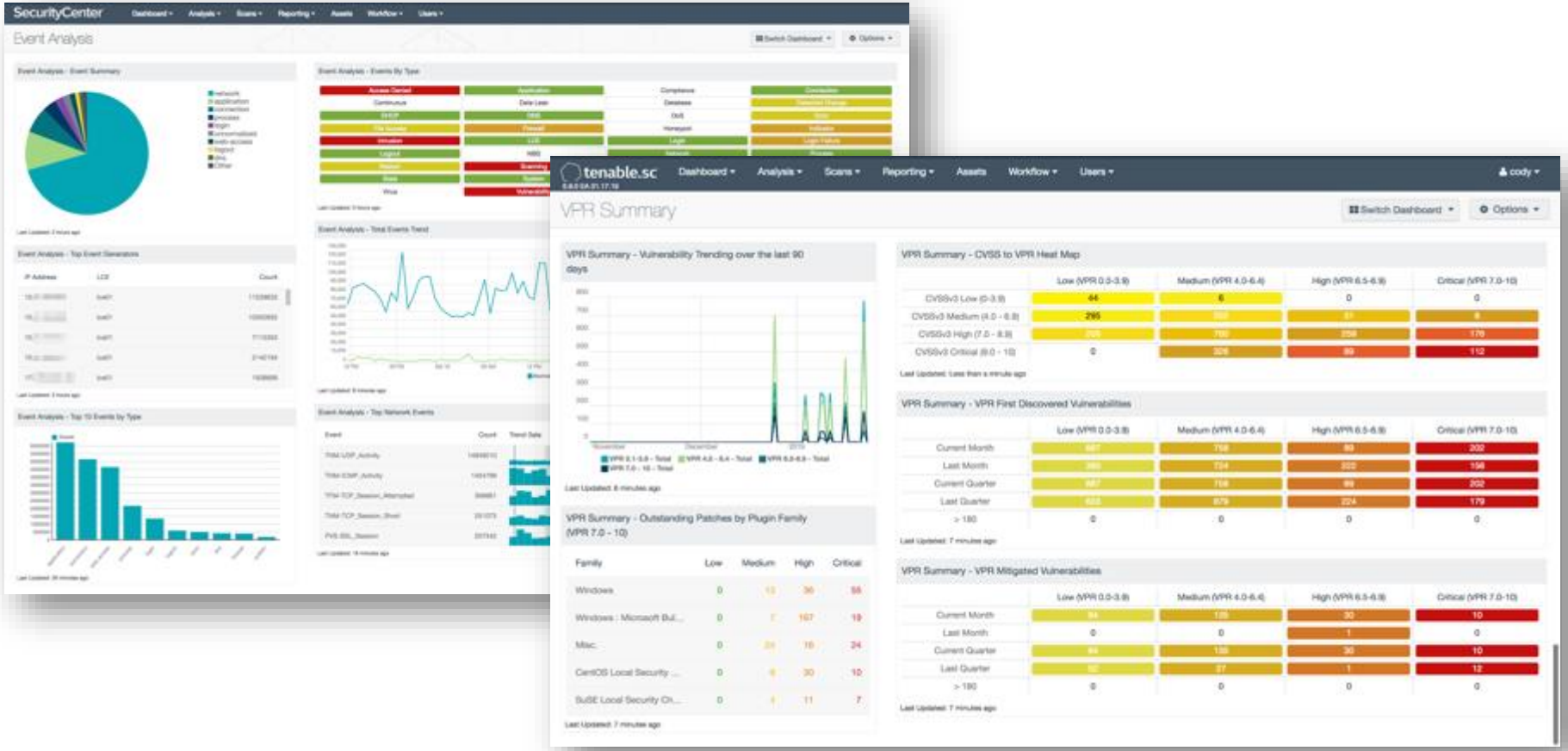
1. Роли – что пользователь может делать в системе
   - На выбор 21 действие
2. Группы – с какими данными он может это делать
   - Хосты, УЗ, дашборды, сканирования…
3. Давайте доступ в систему ИТ, владельцам систем, руководству, аудиторам и пр., каждый может делать и видеть только то, что вы разрешите

Решения (Solutions)

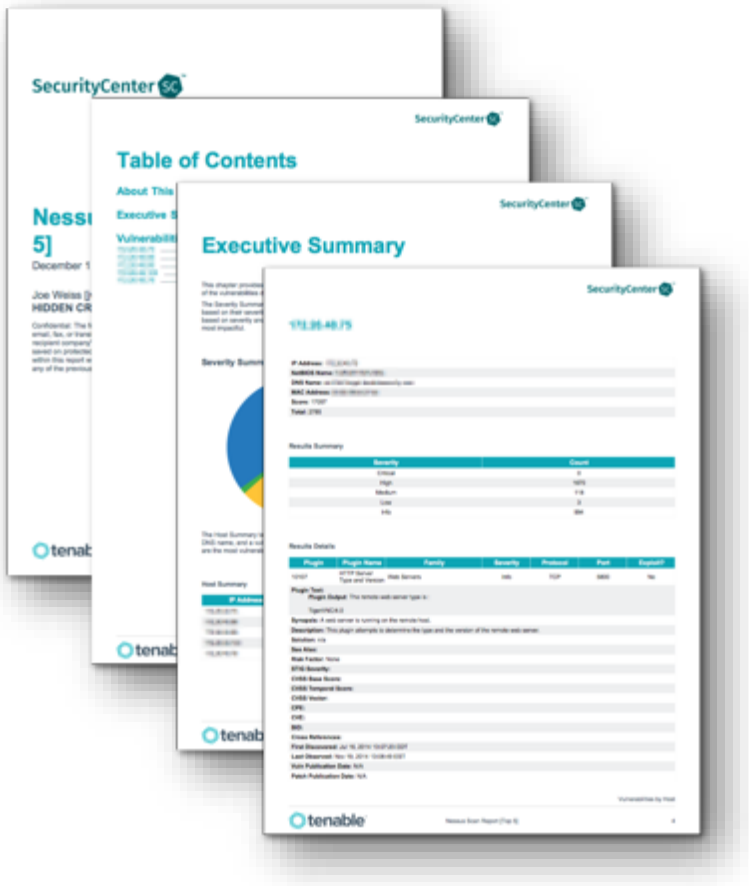


1. Рекомендации по группам хостов, которые приводят к наибольшему снижению уровня риска
2. Анализ всей сети или отдельных групп хостов (на основе Активов)

Дашборды для специалистов и менеджмента



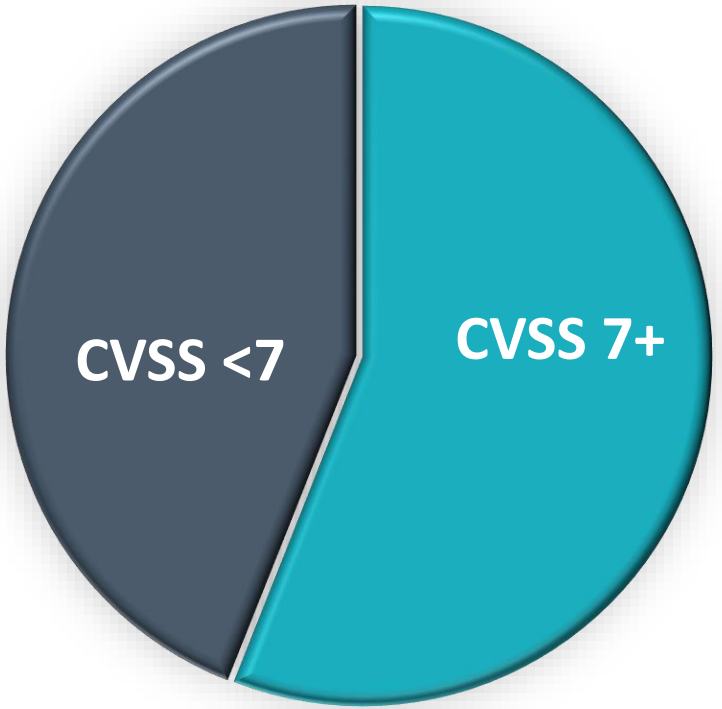
Отчеты для ИТ-администраторов, безопасников, менеджеров



1. Более 100 предустановленных отчетов для топ-менеджмента, линейных руководителей и специалистов
2. Возможность гибко корректировать любой из уже имеющихся шаблонов
3. Создание собственных шаблонов отчетов в форматах HTML, CSV, PDF, Nessus XML и через API
4. Возможности гибкой выгрузки результатов сканирования с применением фильтров
5. Отправка отчетов на e-mail или в папку сразу по завершению сканирования

Проблема с CVSS

- Для 56% всех уязвимостей серьезность Высокая или Критичная
- CVSS не учитывает риск
- Специалисты тратят существенную часть времени, чтобы решать нерелевантные проблемы



Источник: Отчет по уязвимостям, Tenable Research

Рейтинг VPR. Находим иглу в стоге сена

Наработки Tenable

Аналитика по более чем 109.000 уязвимостей позволяет дифференцировать реальный и теоретический риск уязвимостей

Кибербразведка

Ежедневное выявление уязвимостей, которые наиболее активно эксплуатируются как нацеленными, так и обычными хакерами

Оценка уязвимости

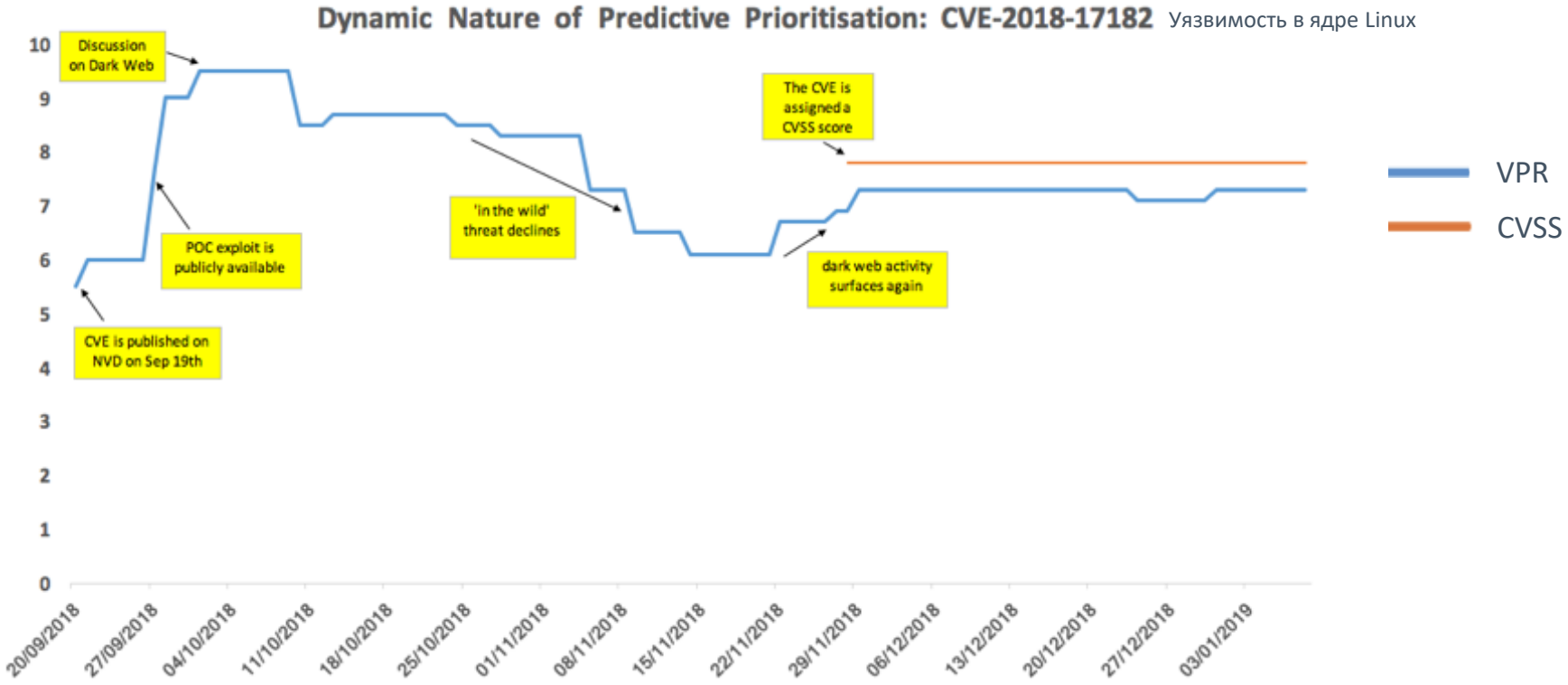
Критичность, легкость эксплуатации и вектора атаки уязвимости

VPR
Управление уязвимостями на основе риска

97%

Уменьшение числа уязвимостей к устранению с равным снижением уровня риска

Пример силы VPR – за 70 дней до CVSS



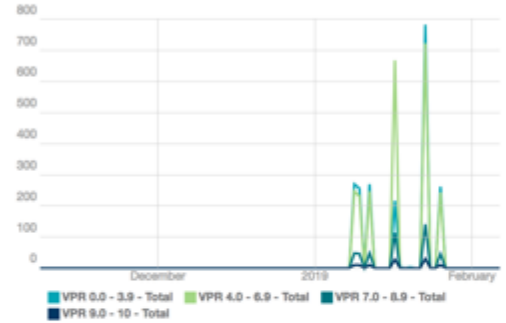
Аналитика VPR встроена в Tenable.sc

tenable.sc Dashboard Analysis Scans Reporting Assets Workflow Users

VPR Summary

Switch Dashboard Options

VPR Summary - Vulnerability Trending over the last 90 days



Last Updated: 2 minutes ago

VPR Summary - Highlighted Patches (VPR 7.0 - 10)

Solution	Risk ...	H...	T...	Vulnerability...
Upgrade to Adobe Flash	13.96%	67	468	17.11%
Apply MS17-013: Security Update	13.13%	212	299	10.93%
Apply Microsoft Security Advisory	12.41%	211	275	10.05%
Apply MS16-142: Cumulative	10.26%	165	344	12.57%

VPR Summary - CVSS to VPR Heat Map

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.9)	High (VPR 7.0-8.9)	Critical (VPR 9.0-10)
CVSSv3 Low (0-3.9)	67	142	0	0
CVSSv3 Medium (4.0 - 6.9)	615	310	7	1
CVSSv3 High (7.0 - 8.9)	511	5262	338	322
CVSSv3 Critical (9.0 - 10)	14	970	170	94

Last Updated: 2 minutes ago

VPR Summary - First Discovered Vulnerabilities

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.9)	High (VPR 7.0-8.9)	Critical (VPR 9.0-10)
Current Month	0	0	0	0
Last Month	7497	14526	1773	574
Current Quarter	7497	14526	1773	574
Last Quarter	603	1103	146	33
> 180 Days	0	0	0	0

Last Updated: 2 minutes ago

VPR Summary - Mitigated Vulnerabilities

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.9)	High (VPR 7.0-8.9)	Critical (VPR 9.0-10)
Current Month	0	0	0	0
Last Month	95	166	9	2
Current Quarter	95	166	9	2
Last Quarter	52	28	11	1
> 180 Days	0	0	0	0

Last Updated: Less than a minute ago

Демонстрация

Спасибо!

Вопросы и консультация
Email: marketing@dialognauka.ru