

Повестка

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



tenable[®]

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

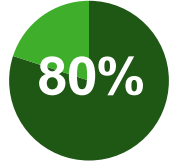
Выявление активов и анализ
уязвимостей в облаках,
контейнерах, АСУ ТП и ИТ-средах

Довольные заказчики

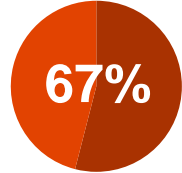
50% из Fortune 500

25% Global 2000

Fortune 10



Fortune 100



Прочие





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.

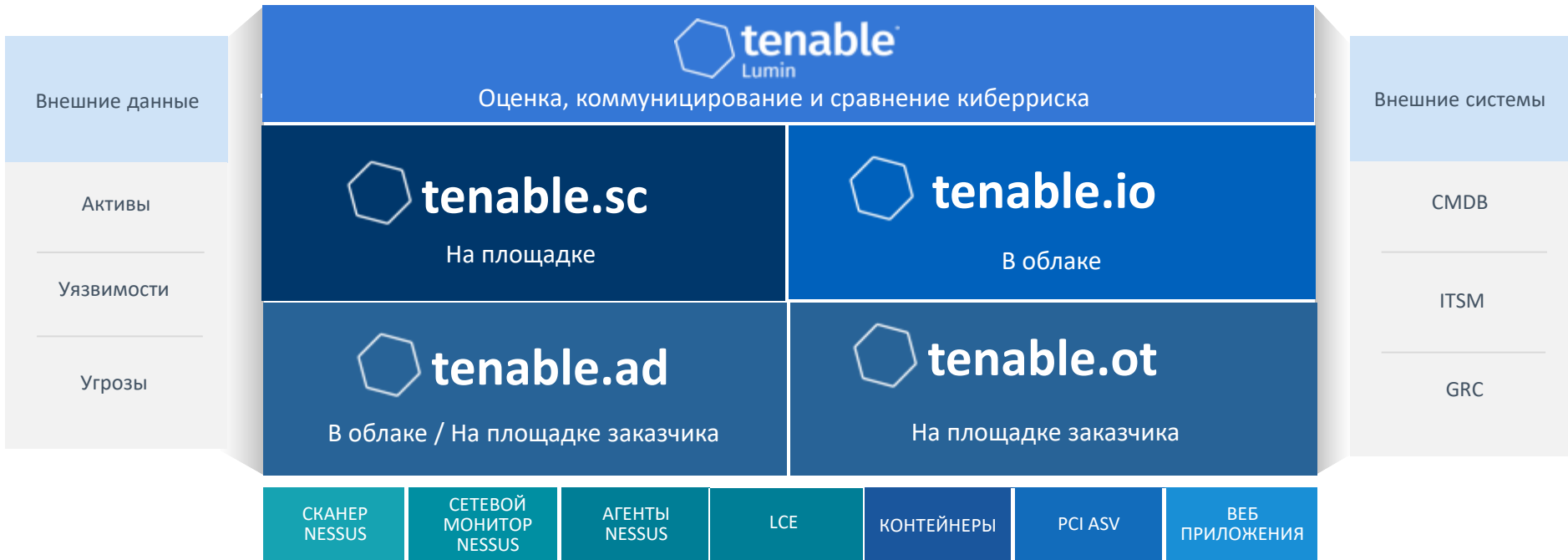
24 часа

Медианное время на выпуск
новых проверок

64.000+

Покрытие CVE (лидирующий
показатель)

Платформа киберриска Tenable



Полное отслеживание всех активов



Приоритизация и гибкая отчетность



Гибкость внедрения

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.”

THE FORRESTER WAVE™

Vulnerability Risk Management

Q4 2019





Tenable.sc

Управление уязвимостями
на основе уровня риска

Процесс управления уязвимостями с Tenable.sc

Выявление

Оценка

Приоритизация

Исправле
ние

Оценка

Изучите вашу
бизнес-среду

Внедрите
Tenable.sc и
сенсоры

Найдите и
классифицируйте
активы

Оцените все
активы на
уязвимости

Проведите аудит
конфигураций

Приоритизируйте
уязвимости и
активы

Определите
наиболее
эффективные
действия

Исправьте,
компенсируйте
или примите
приоритетные
уязвимости

Измеряйте KPI

Оценивайте и
оптимизируйте

Архитектура Tenable.sc



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

Обширная и открытая база проверок



Plugins

Settings ▾

Newest

Updated

Search

Nessus Families

WAS Families

NNM Families

LCE Families

About Plugin Families

Nessus Release Notes

Plugins / Newest

Newest Plugins

All

Nessus

Web Application Scanning

Nessus Network Monitor

Log Correlation Engine

« Previous

Page 1 of 1221 • 161039 total

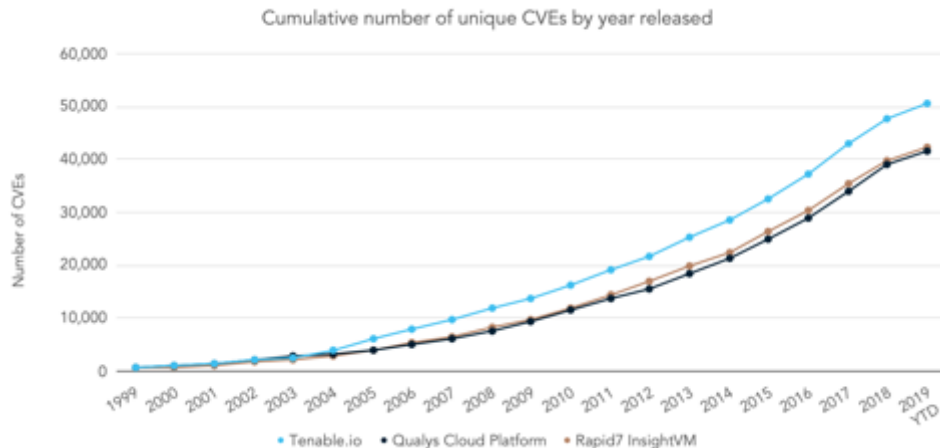
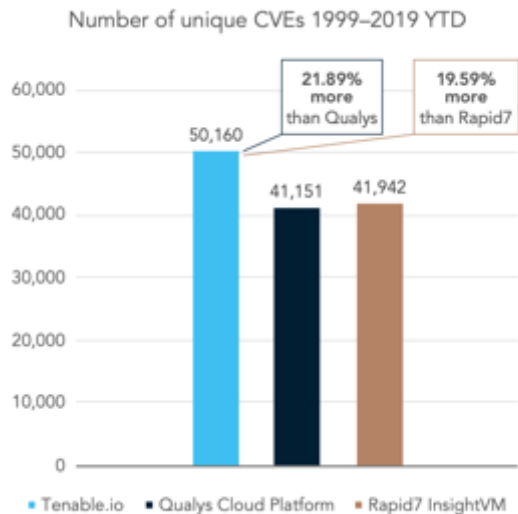
Next »

ID	Name	Product	Family	Published	Severity
151678	Scientific Linux Security Update : firefox on SL7.x i688/x86_64 (2021:2741)	Nessus	Scientific Linux Local Security Checks	7/15/2021	HIGH
151677	Debian DLA-2709-1 : firefox-esr - LTS security update	Nessus	Debian Local Security Checks	7/15/2021	HIGH
151675	RHEL 7 : nettle (RHSA-2021:2758)	Nessus	Red Hat Local Security Checks	7/15/2021	HIGH
151674	CentOS 7 : firefox(CESA-2021:2741)	Nessus	CentOS Local Security Checks	7/15/2021	HIGH
151673	Google Chrome < 91.0.4472.184 Multiple Vulnerabilities	Nessus	MacOS X Local Security Checks	7/15/2021	CRITICAL

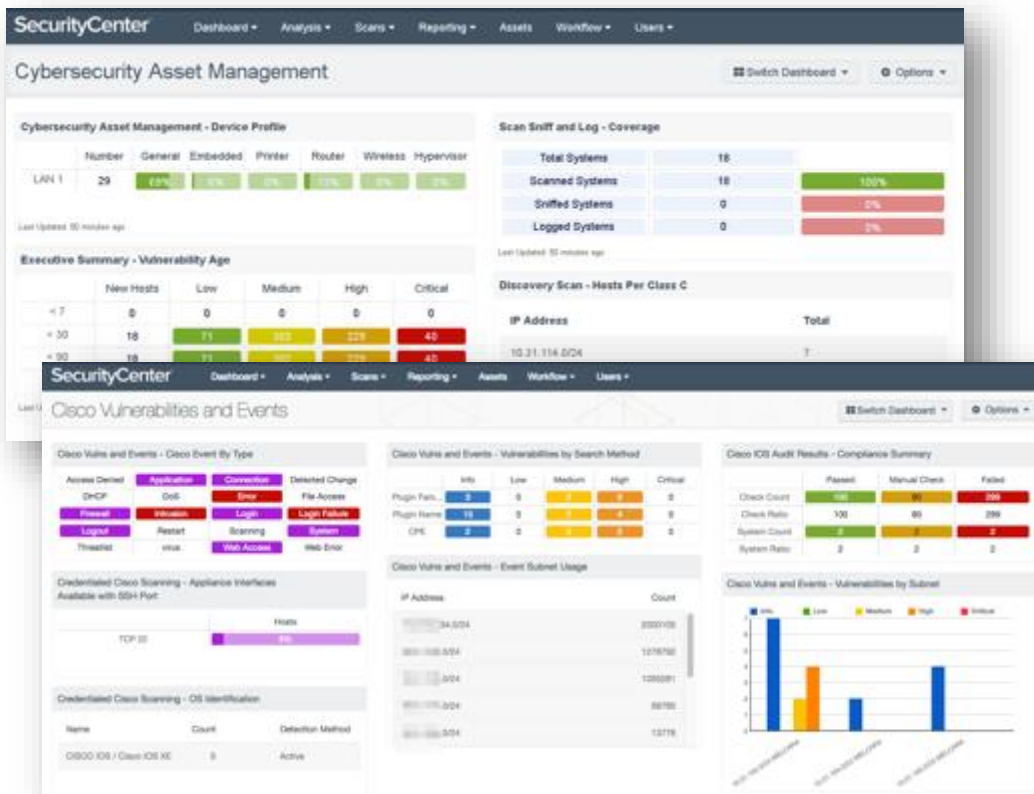
<https://www.tenable.com/plugins>

Лидирующее покрытие по CVE

На 16 июля 2021 года Tenable выявляет 64023 CVE IDs

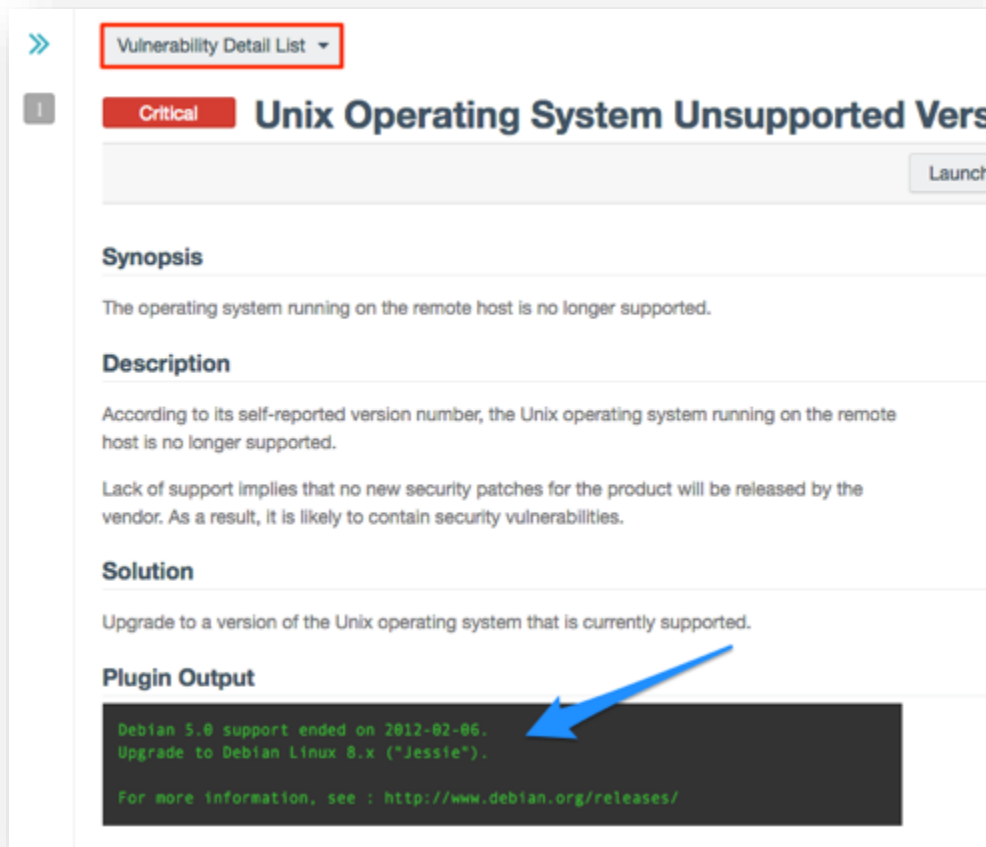


Современный, быстрый и удобный веб-интерфейс



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



>> Vulnerability Detail List ▾

Critical **Unix Operating System Unsupported Vers** Launch

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

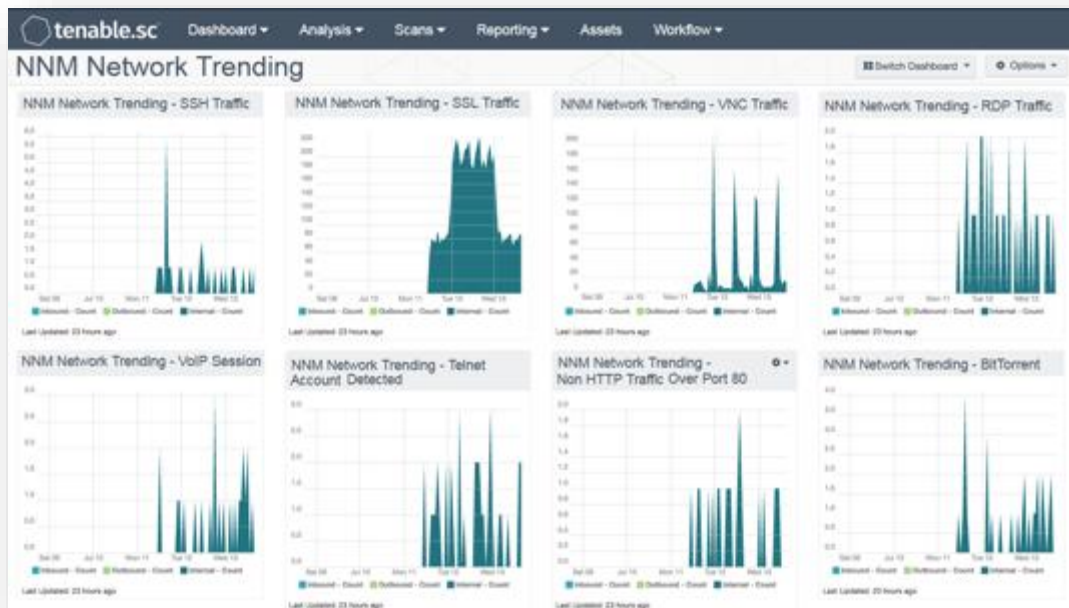
Upgrade to a version of the Unix operating system that is currently supported.

Plugin Output

```
Debian 5.0 support ended on 2012-02-06.  
Upgrade to Debian Linux 8.x ("Jessie").  
  
For more information, see : http://www.debian.org/releases/
```

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

General

Name* 1 - Системы Linux на улице Правды без

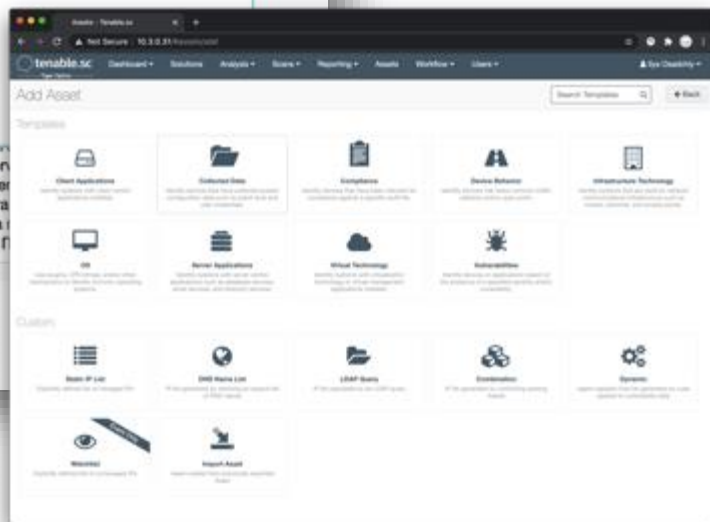
Description

Tag

Combination* (NOT "Botnet Activity" AND ("Подсеть на улице Правды" AND "Linux Hosts"))

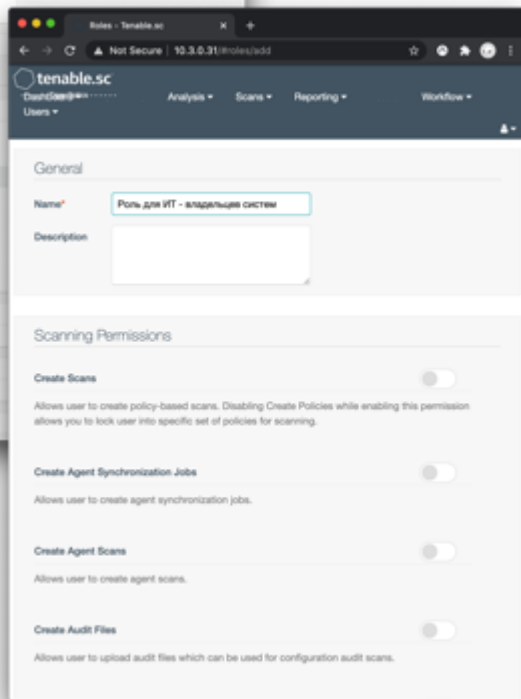
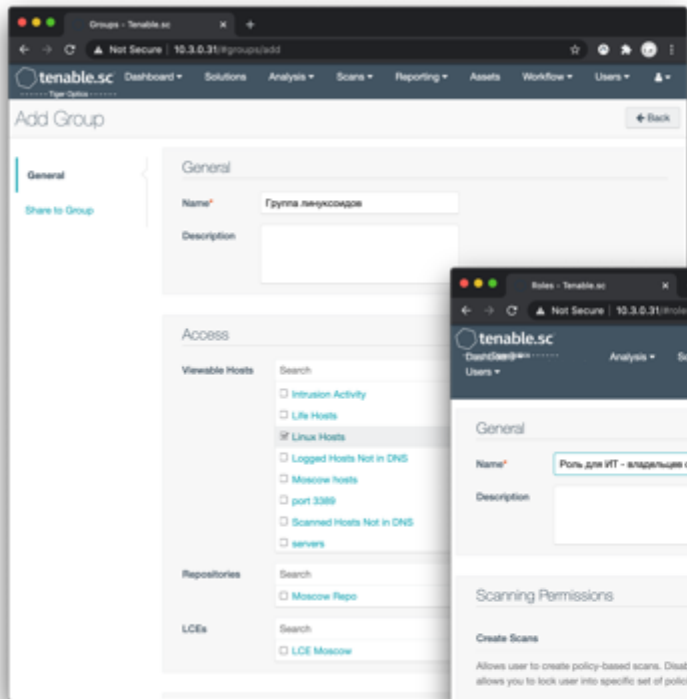
VMWare ESX Hyper
Voice or Mobile Client
Windows Hosts (Или
Видели порт 22 за
Подсеть на улице

Submit Cancel



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)

Fix CentOS 7 : kernel (CESA-2020:3220)

6 Hosts Affected | 41 Vulnerabilities | 7.4 VPR | 9.8 CVSS v3

Vulnerabilities Included

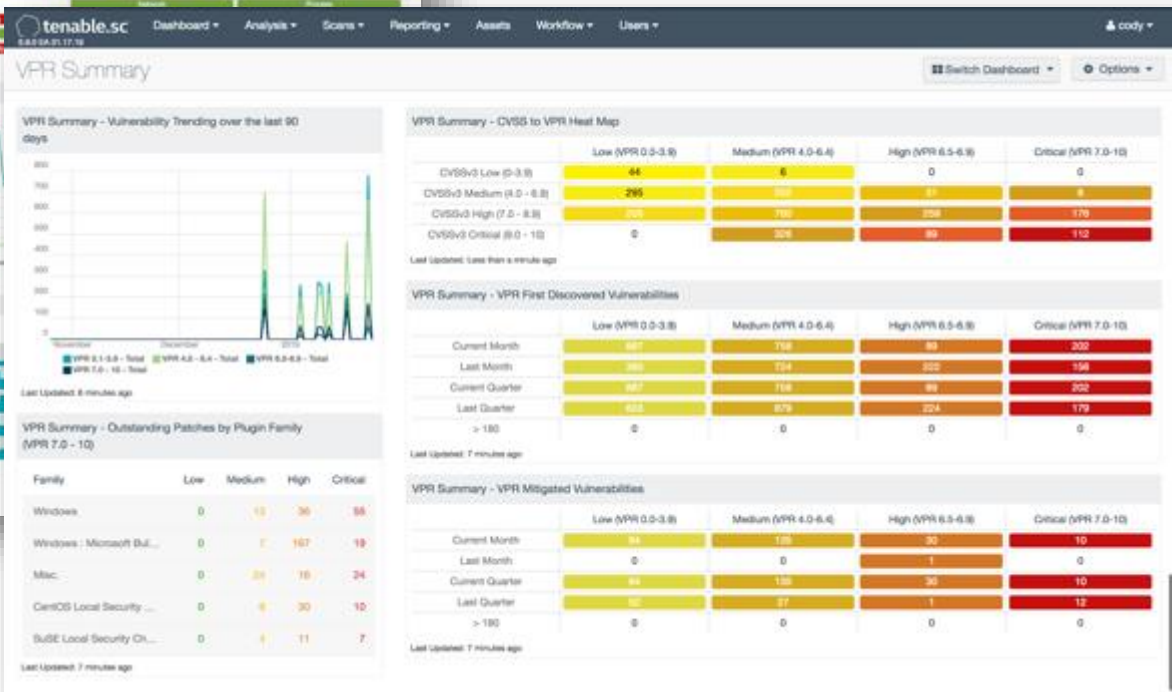
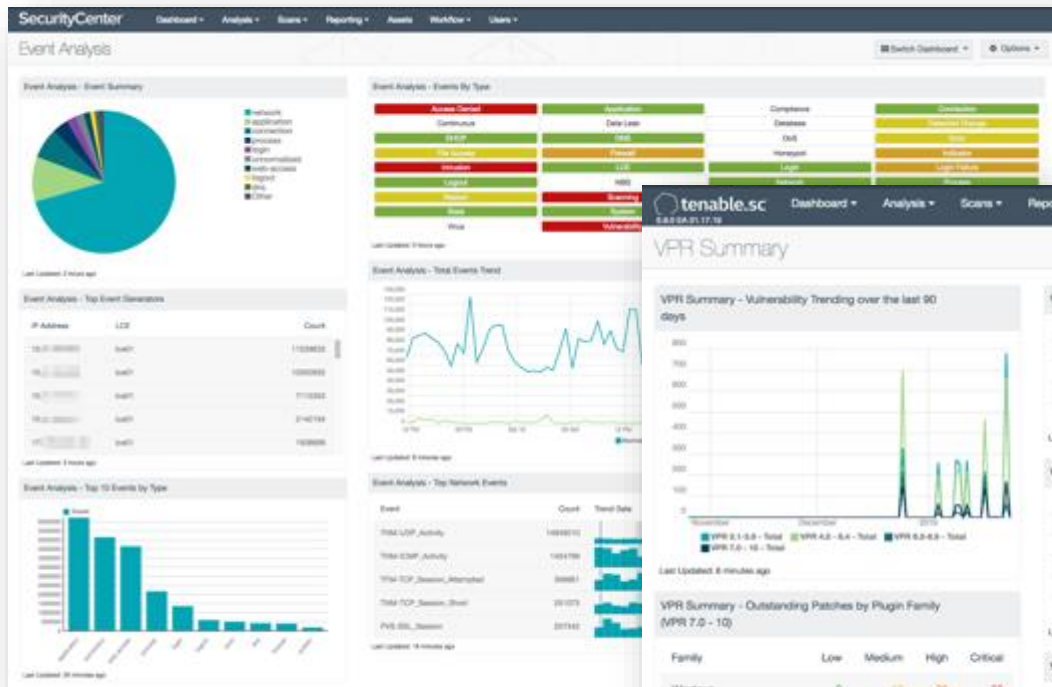
Plugin	Hosts Affected	VPR	CVSS v3
134267	4	7.4	9.8
129538	3	7.4	7.8
135316	4	7.3	8.3
131571	3	7.3	7.8
129020	3	7.3	8.3
131032	3	7.1	6.5
138235	5	6.7	8.8
134802	4	6.7	8.8
131033	3	6.7	7.8
130128	3	6.7	8.8
137763	6	5.2	5.3

Hosts Affected

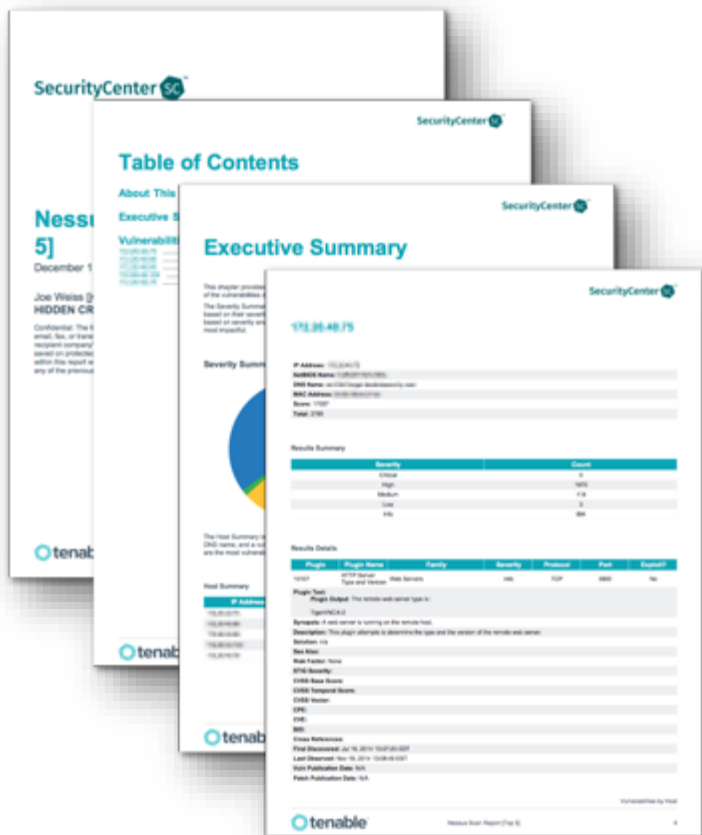
IP Address	NetBIOS	DNS	OS CPE
192.168.0.19			
192.168.0.31		scvx.tgr.local	
192.168.0.32		localhost.localdomain	cpe:/o:centos:centos:7:update8
192.168.0.33			cpe:/o:centos:centos:7:update7
192.168.0.34			cpe:/o:centos:centos:7:update7
192.168.0.36			cpe:/o:centos:centos:7:update8

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



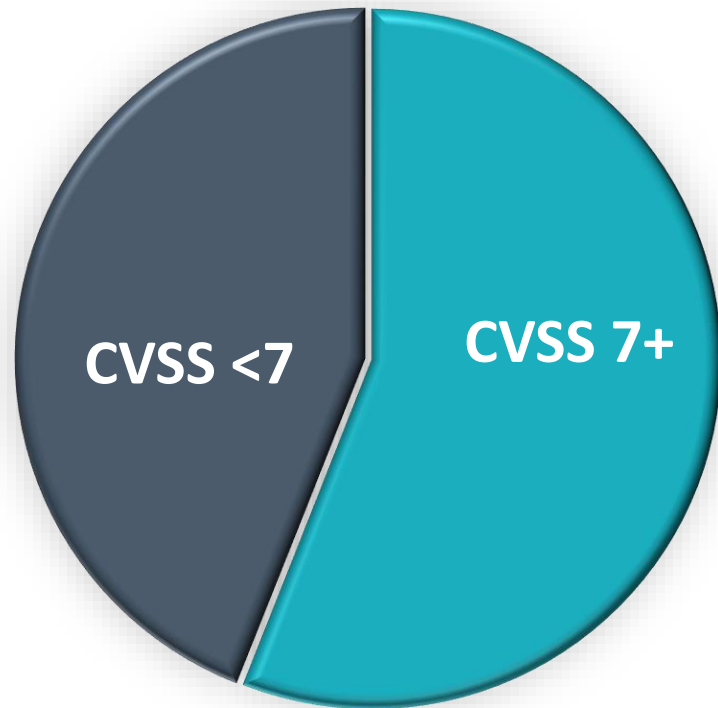
Отчеты для ИТ-админов, безопасников, менеджеров



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

Киберразведка

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

Оценка уязвимости

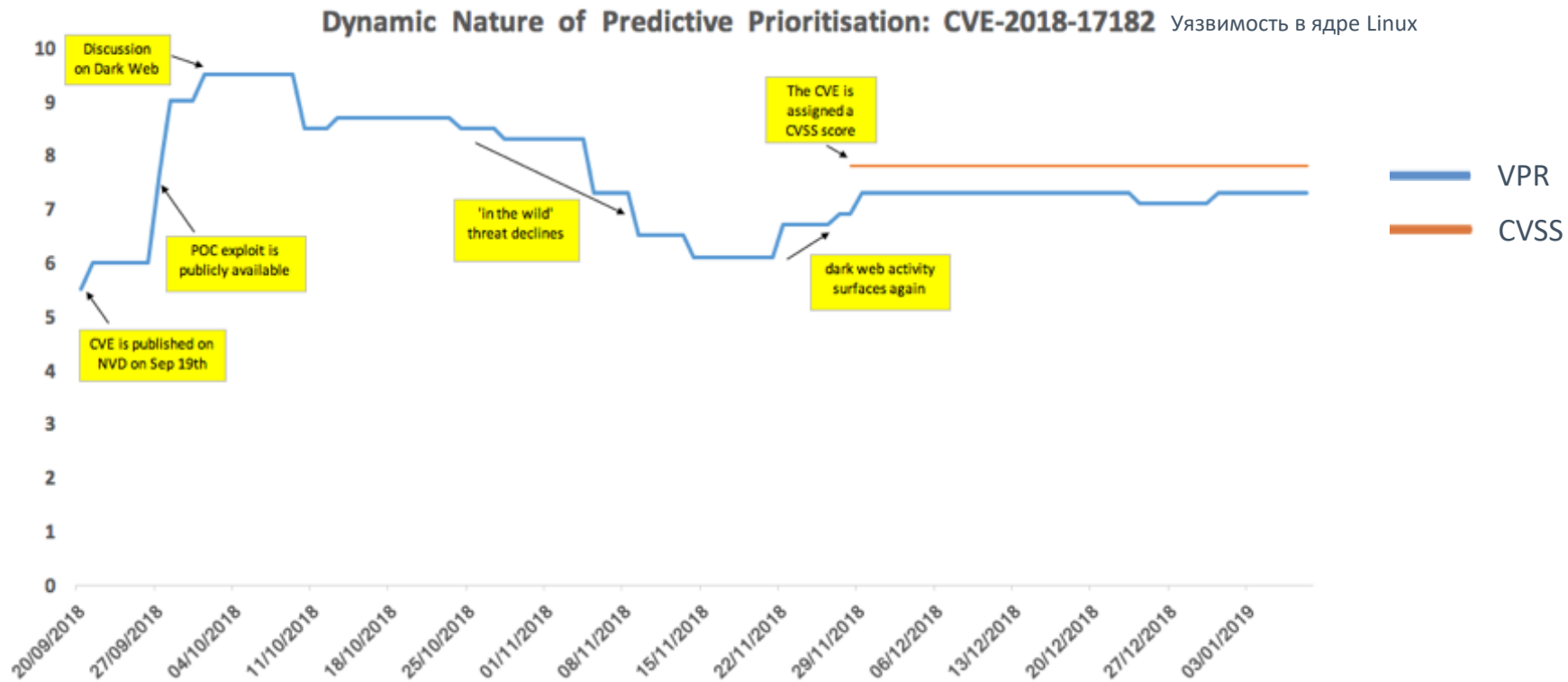
Критичность, легкость эксплуатации и вектора атаки уязвимости

VPR
Управление
уязвимостями
на основе риска

97%

Уменьшение числа уязвимостей к устранению с равным снижением уровня риска

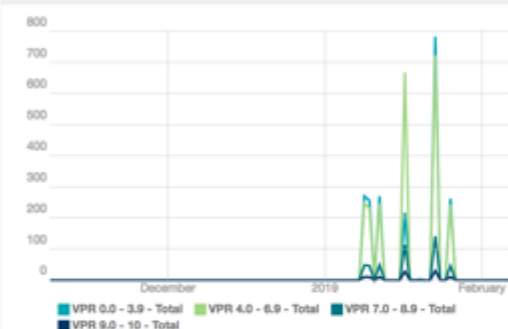
Пример силы VPR – за 70 дней до CVSS



Аналитика VPR построена в Tenable.sc

VPR Summary

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