Empowering Security Teams

Аношко Володимир

vanoshko@nwu.com.ua

О КОМПАНИИ BEYOND SECURITY

- Beyond Security, штаб-квартира в США, Сан-Хосе, Калифорния
- Центр исследований и разработок, Израиль
- Поддержка и офисы продаж по всему миру
- Владелец ресурса SecuriTeam один из 5 лучших порталов глобальной безопасности
- Разрабатывает автоматизированные средства защиты от уязвимостей для обнаружения любых типов известных или НЕИЗВЕСТНЫХ уязвимостей, включая сеть, приложение, веб-приложения, исходный код.

WORLDWIDE CUSTOMERS

GLOBAL COVERAGE

International Offices: San Jose, California, with R&D Headquarters in Israel

10 local branches covering 72 countries through certified partners

Support: 24X7 follow the Sun

Инструменты для каждого этапа, SDLC + DevOps PATHWAY TO PRODUCTION

SSD Securiteam Secure Disclosure

in 2018 published over 100 advisories and CVEs

PRODUCTION
Automated Scanning, Compliance + Risk Management

besecure

- Убедитесь, что ваша сеть действительно безопасна. Используется MSP, SOCs, ИТ-менеджерами и менеджерами по безопасности,
- Тесты сети и пользовательских веб-приложений
- Автоматически и постоянно сканирует обнаруженные системы и уязвимости
- Анализ поведения с точностью (менее 0,01% ложных срабатываний),
- Карта сети и интегрированные пошаговые процессы восстановления

Bug bounty program for any discovered proven false positives!

DAST: Blackbox Testing, Fuzzing,
Build security and quality in your SDLC

bestorm

- IoT, Critical Infrastructure, Automotive, Lab Certification, R&D / QA testing, Mobile, API, Wifi, BT,…
- Динамически оценивать программное обеспечение, аппаратное обеспечение и проприетарные протоколы для UNknown flaws.
- DevOps: Защитите свои продукты перед релизом
- Создайте свой собственный проприетарный протокол тестирования, или используйте модуль самообучения beSTORM
- Возможность изменения глубины тестирования, исходя из вашего уникального подхода.

SAST: App and Code Testing
Build security and quality in your SDLC

besource

- Статический анализ, тестирование кода и исправление для разработчиков программного обеспечения.
- DevOps: Безопасность кода и приложений на этапе разработки
- Уменьшение количества циклов QA на этапе разработки
- Поделитесь проектом разработки с членами вашей команды

PCI Security Standards Council APPROVED SCANNING VENDOR

GDPR The General Data Protection Regulation

ISASecure®

ISO 27001 Certified

OWASP Open Web Application Security Project

beyond SECURITY

ЧТО ТАКОЕ ОЦЕНКА УЯЗВИМОСТИ

- Определите все активные узлы в вашей сети.
- Необходимые тестирования на уровне сети, сервера, базы данных и приложений
- Откройте для себя и классифицируйте все известные уязвимости в сети.

Если бы каждая сеть была защищена от уязвимостей, многие утечки данных можно было бы предотвратить

Automated Vulnerbility Scanning, Compliancy and Risk Management

beSECURE

Advantages

- Сеть и веб-приложения в одном инструменте
- Тестируйте любой хост который “говорит”на IP: firewalls, routers, wireless routers, printers, switches, workstations, servers, ...
- Полностью автоматизирован – настройка и запуск за считаные минуты
- Определите недостатки безопасности и уязвимостей на уровнях 2-7
- Простая интеграция.
- Функция консолидированной отчетности, для простых и кратких отчетов.

Your Benefits

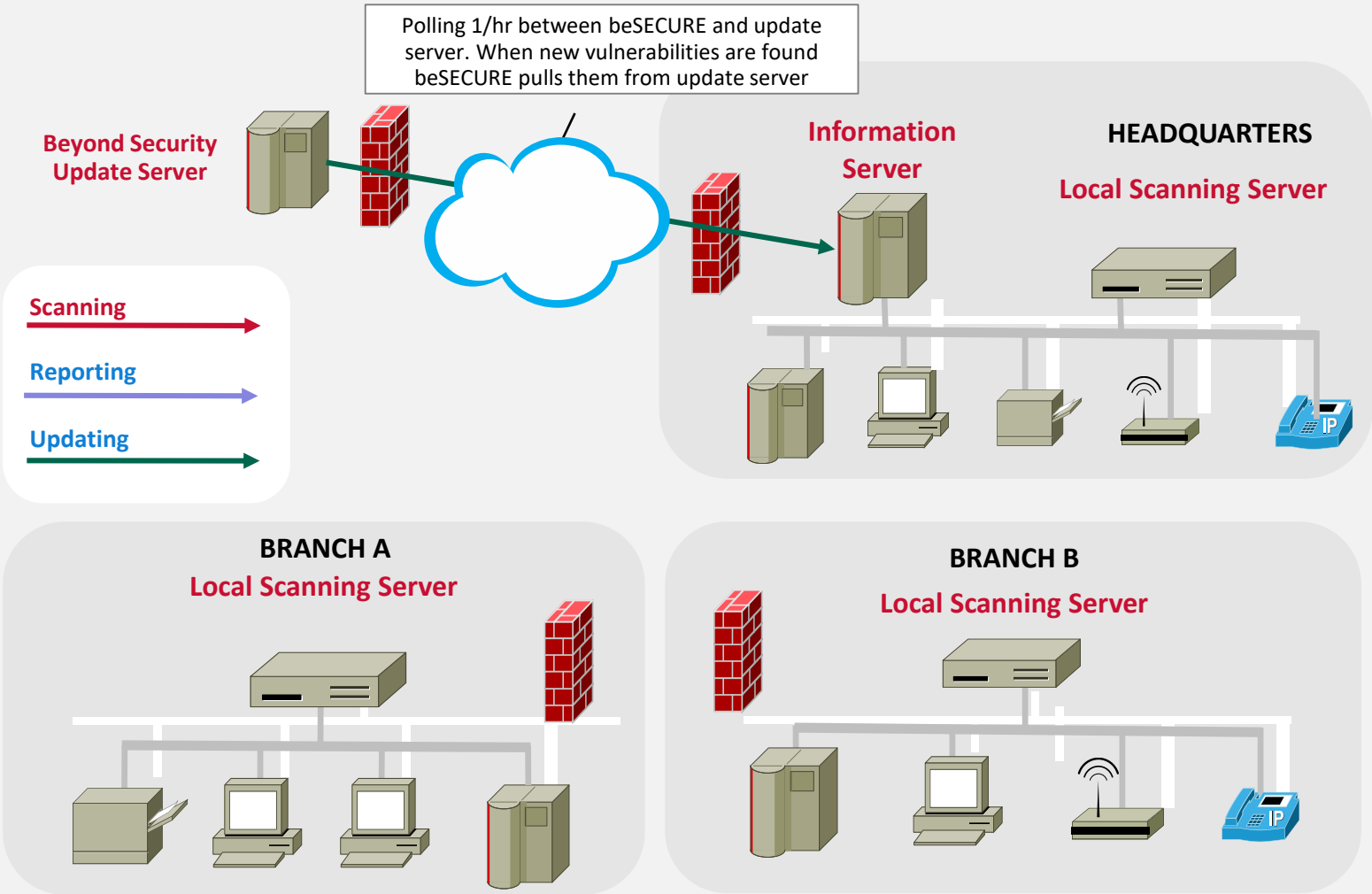
- Знайте что вы в безопасности, без сюрпризов!
- Экономьте время соблюдая правила безопасности (SDP/PCI - ASV certified, ISO2700x, AIS/CIS сертификация соответствия , NEN7510, HIPPA,GLBA, SB 1386, SOX, OWASP, GDPR and more..)
- Он-лайн отчеты, мгновенно предоставьте любой отчет, необходимый для ваших встреч
- Выбирайте любой отчет по дате/пользователю/системе/, в соответствии со списком приоритетных задач.
- Защищает ваши сетевые активы, сохраняет непрерывность бизнеса.

beSECURE Модель развертывания Option - 1

On-Premise Starter Kit for BOTH Internet facing and Internal systems

- 1 x Appliance IS Сервер управления информацией для отчетности (manages the LSS)
- 1 x Appliance LSS: Локальный сервер сканирования (2500 IP's / domains per day)
- Интеграция с вашей системой тикетов, SIEM и внутренними процессами (через API)
- Обучение и полная техническая поддержка
- Может предоставлять ежеквартальные отчеты PCI
- Настраиваемые отчеты под ваши нужны(цвета, бренд, информативность).
- Модуль тестирования клиентских веб-приложений со встроенным сканером
- Раздел отчета и заметок, где инженеры могут оставлять рекомендации для своих клиентов

beSECURE
NEW UPDATING



beSECURE Модель развертывания Option - 2.

Cloud Hosted (AWS) Starter Kit - For Internet facing systems,

- Нет оборудования и потребности в установке решения
- 1 x Appliance LSS: Локальный сервер сканирования (2500 IP's / domains per day)
- Интеграция с вашей системой тикетов, SIEM и внутренними процессами (через API)
- Обучение и полная техническая поддержка
- Может предоставлять ежеквартальные отчеты PCI
- Настраиваемые отчеты под ваши нужны(цвета, бренд, информативность).
- Модуль тестирования клиентских веб-приложений со встроенным сканером
- Раздел отчета и заметок, где инженеры могут оставлять рекомендации для своих клиентов

beyond SECURITY

MSP/SOC/NOC – DISTRIBUTED NETWORKS

Full Mulit-Tentant Deployment for MSPs and Enterprise scale networks

Резюме предложений о MSP

- Два модели использования –Локальная и Облачная(AWS)
- Сканирование L2-L7 web-application testing module
- Полный спектр автоматизированных отчетов, в том числе: анализ тенденций, дифференциальные отчеты, настраиваемые отчеты…
- Полная техническая поддержка с назначенным инженером
- Соответствие отчетности (ISO, CIS, PCI*, ect)
- Дополнительная печать безопасности для вашего клиента
- Ваш собственный языковой интерфейс
- Внутренний Аудит

beSECURE, BETTER THAN PENT TESTING?

- Нет необходимости в привлечении сторонних консультантов, что бы проверить ваши сайты и вашу сеть.
- Масштабируется просто и легко
- Регулярное и текущее сканирование: ежедневно, еженедельно, ежемесячно. Вы решаете, основываясь на ваших требованиях а не на консультационной оценке.
- Онлайн отчеты и информация в любой момент, когда вам нужно предоставить либо проверить ваш статус безопасности.
- Затраты меньше, чем ежегодный penetration testing.

УПРАВЛЕНИЕ РИСКАМИ, ОТОБРАЖЕНИЕ И ОЦЕНКА

Location	Host(s)	Scan Date	Total	High	Medium	Score	Trend	Compliant
NTTC HQ (Demo)	551 (551)	Sep 19, 2017	3056 (1777)	328 (87)	1003 (395)	81.79 (90.01)	▼ 8.23	
Accounting Servers	11 (11)	Mar 03, 2014	14 (13)	0 (0)	14 (11)	89.07 (91.00)	▼ 1.93	
Commenters	62 (62)	Apr 19, 2016	127 (507)	5 (5)	67 (48)	87.66 (90.17)	▼ 2.51	
Corporate Servers	16 (16)	Jul 03, 2016	27 (40)	1 (0)	11 (12)	98.97 (90.92)	▲ 8.05	
Corporate Web Site	2 (2)	Jun 15, 2016	9 (8)	0 (0)	1 (0)	90.13 (100.00)	▼ 9.87	
Mail Servers	53 (53)	Jun 12, 2015	19 (248)	4 (1)	15 (52)	56.70 (75.39)	▼ 18.69	
Test	1 (1)	Sep 18, 2017	0 (0)	0 (0)	0 (0)	100.00 (100.00)	= 0	
Web Portals	2 (2)	Nov 05, 2015	21 (39)	9 (9)	12 (12)	50.03 (50.03)	= 0	
Web Servers	18 (18)	Jun 08, 2014	147 (130)	21 (19)	62 (27)	92.82 (87.65)	▲ 5.17	
NTTC Accounting (Demo)	93 (93)	Sep 19, 2017	389 (353)	22 (28)	121 (95)	88.86 (93.65)	▼ 4.79	
Bad Hosts	18 (18)	Mar 03, 2014	187 (0)	2 (0)	42 (0)	76.78 (100.00)	▼ 23.22	
Dictionary Servers	64 (64)	May 18, 2016	202 (353)	20 (28)	79 (95)	89.80 (80.95)	▲ 8.85	
Internal network scan	11 (11)	Sep 19, 2017	0 (0)	0 (0)	0 (0)	99.99 (99.99)	= 0	
NTTC Development (Demo)	189 (189)	Aug 25, 2017	2009 (18)	248 (0)	601 (6)	72.32 (99.21)	▼ 26.89	
File Servers	18 (18)	Aug 25, 2017	90 (18)	21 (0)	36 (6)	80.22 (96.84)	▼ 16.62	
Food Processors	55 (55)	Oct 21, 2014	652 (0)	66 (0)	192 (0)	63.28 (100.00)	▼ 36.72	
NTT Deep	97 (97)	Feb 23, 2015	1249 (0)	161 (0)	355 (0)	53.76 (100.00)	▼ 46.24	
Suspicious	19 (19)	Apr 14, 2016	18 (0)	0 (0)	18 (0)	92.03 (100.00)	▼ 7.97	
NTTC R&D (Demo)	104 (104)	Sep 07, 2015	294 (391)	18 (25)	99 (132)	83.18 (86.83)	▼ 3.65	

Общая оценка организации и уровень риска

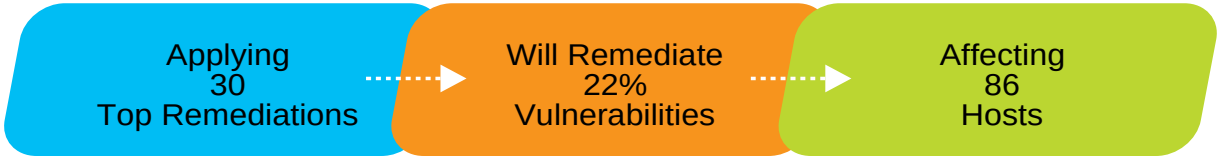
Самый низкий бал системы, наибольшая степень риска.

beSECURE Отчет о восстановлении

Ваш собственный рассчитанный список задач уязвимости с легкими для исправления направлениями

Как вы решаете, что исправить в первую очередь, когда у вас мало времени?

Просто начните сверху и двигайтесь вниз!

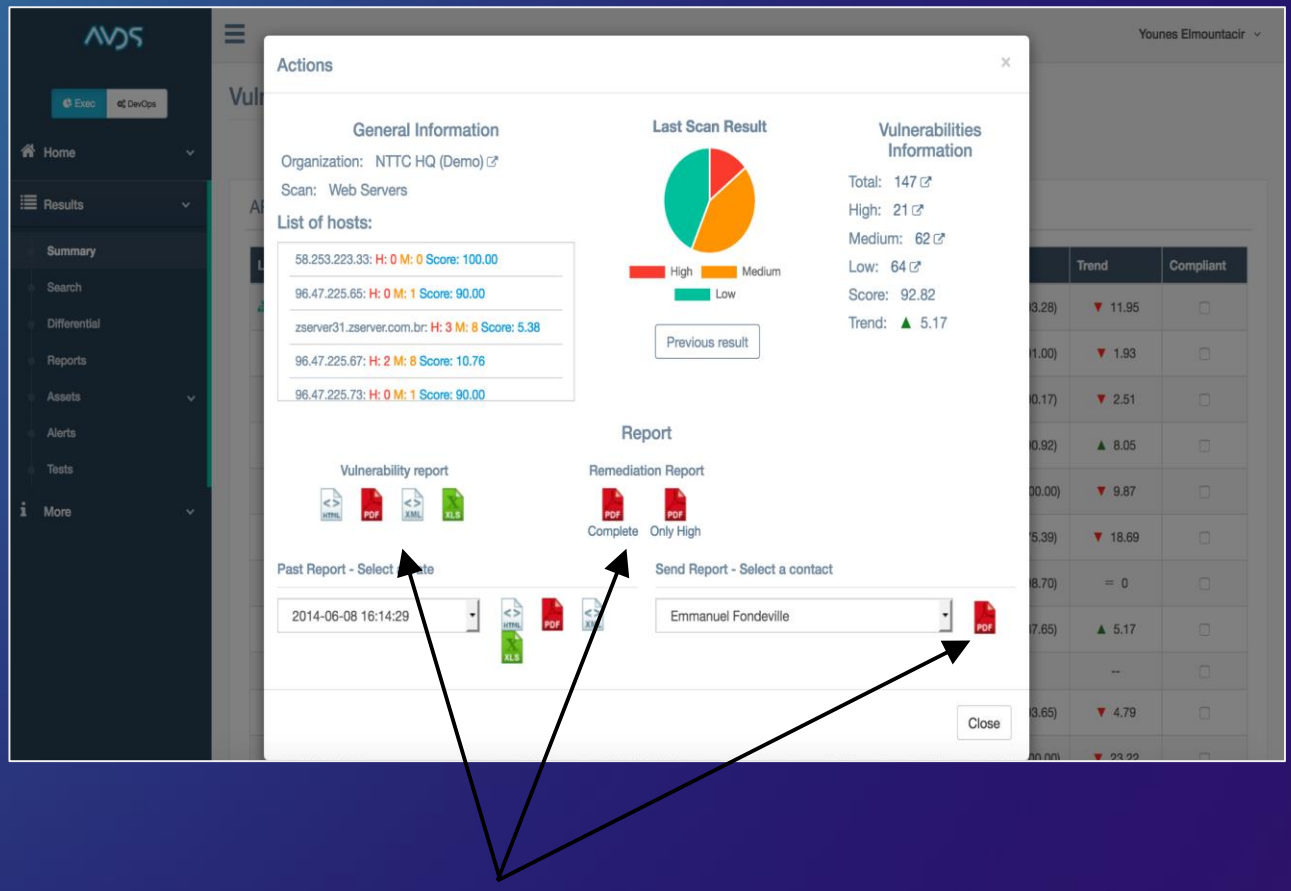


Remediations	Remediated Vulns	Affected Assets	Risk
PHP Unsupported Version Detection	50	50	20000
PHP CGI Query String Code Execution	30	30	7200
PHP Running Version Prior to 5.3.11	30	30	7200
PHP Running Version Prior to 5.3.2 / 5.2.13	15	15	1800
PHP Running Version Prior to 5.2.15	14	14	1568
PHP Running Version Prior to 5.3.13	14	14	1568
PHP Running Version Prior to 5.3.15	14	14	1568
PHP Running Version Prior to 5.3.14	14	14	1568
PHP Running Version Prior to 5.3.22	14	14	1568
PHP Running Version Prior to 5.3.26	14	14	1568
MySQL Unsupported Version Detection	12	12	1152
Obsolete Web Server Software Detection	6	6	288
OpenSSL Running Version Prior to 1.0.1o (POODLE)	9	5	360
Oracle DBMS_SCHEDULER Vulnerability	4	4	128
Multiple Vulnerabilities in Oracle Database Server (40 Issues)	4	4	128
OpenSSL Running Version Prior to 1.0.1i	4	4	128
OpenSSH J-PAKE Public Parameter Validation Shared Secret Authentication Bypass	4	4	128
Oracle TNSLSNR Insecurity	4	4	128
Oracle LINK Buffer Overflow	4	4	128
Buffer Overflow in the Oracle Executeable of Oracle Server	4	4	128
OpenSSH Privilege Separation Monitor Weakness	3	3	72

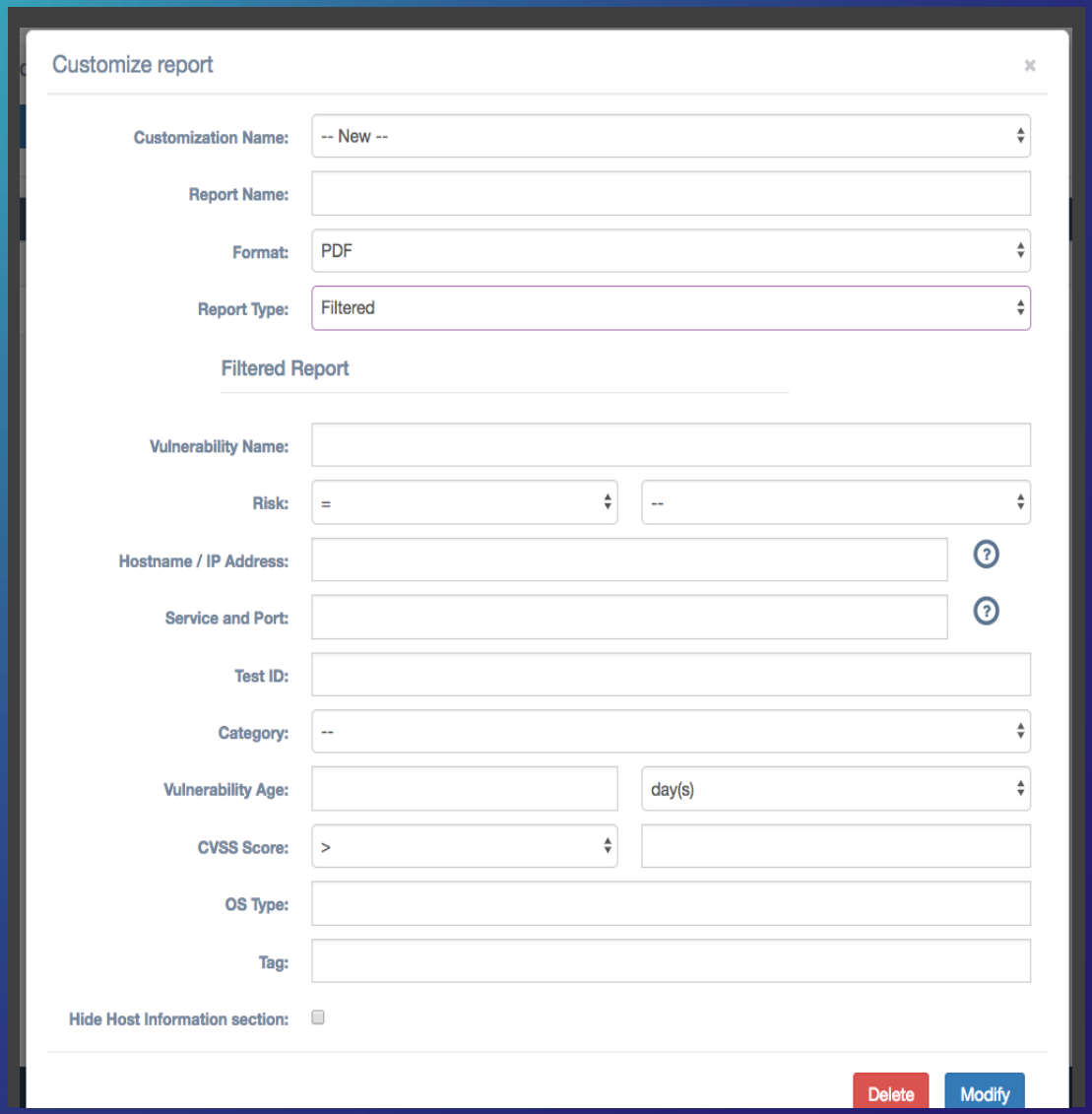
beSECURE Индивидуальные отчеты

Выберите любой тип отчета, который вам нужен: по дате, в соответствии со списком приоритетных задач, пользователем/группой, системами и т. д.

Также включает отчеты ISO, CIS, PCI, SOX и OWASP Top 10

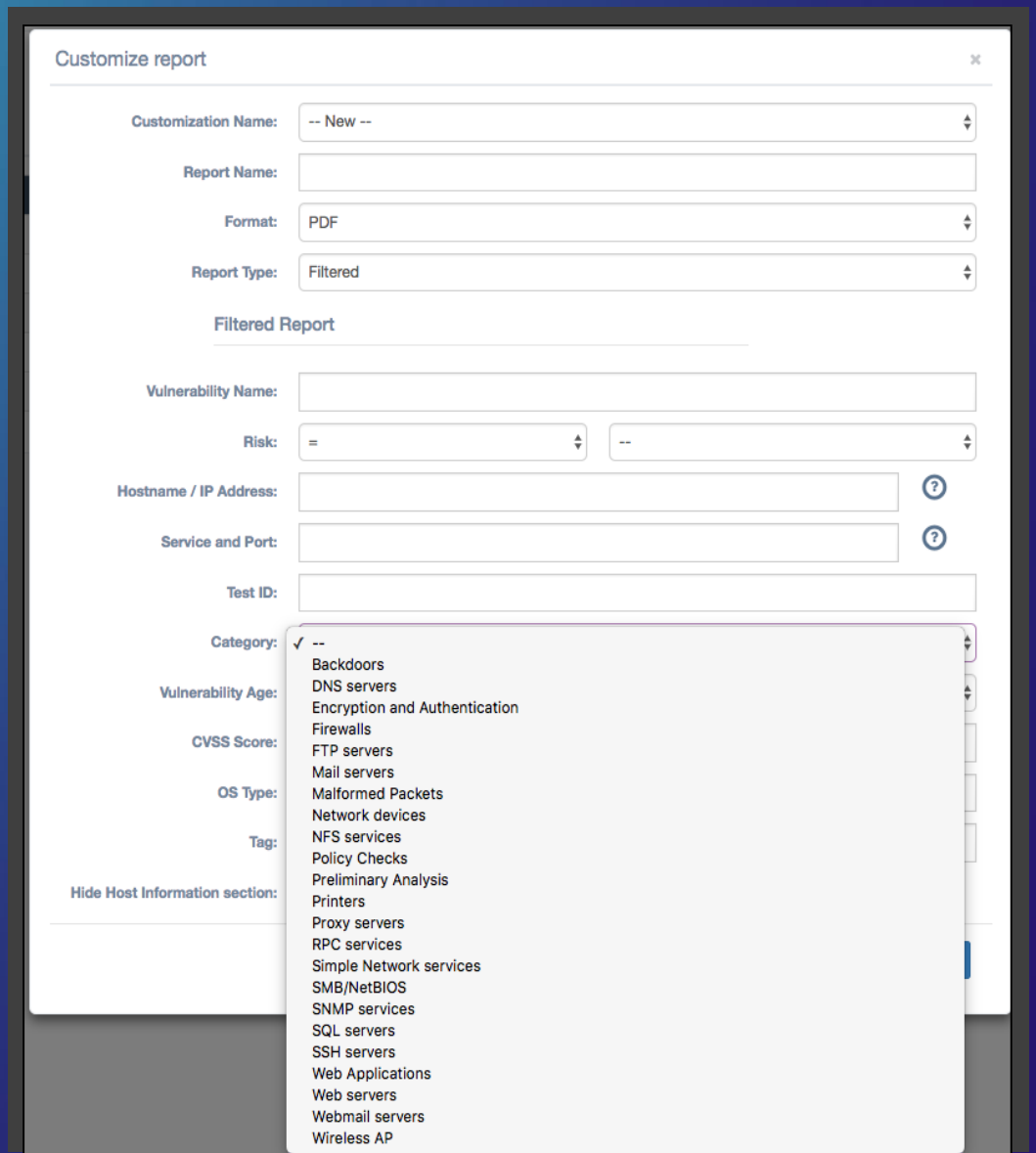


beSECURE Индивидуальный генератор отчетов



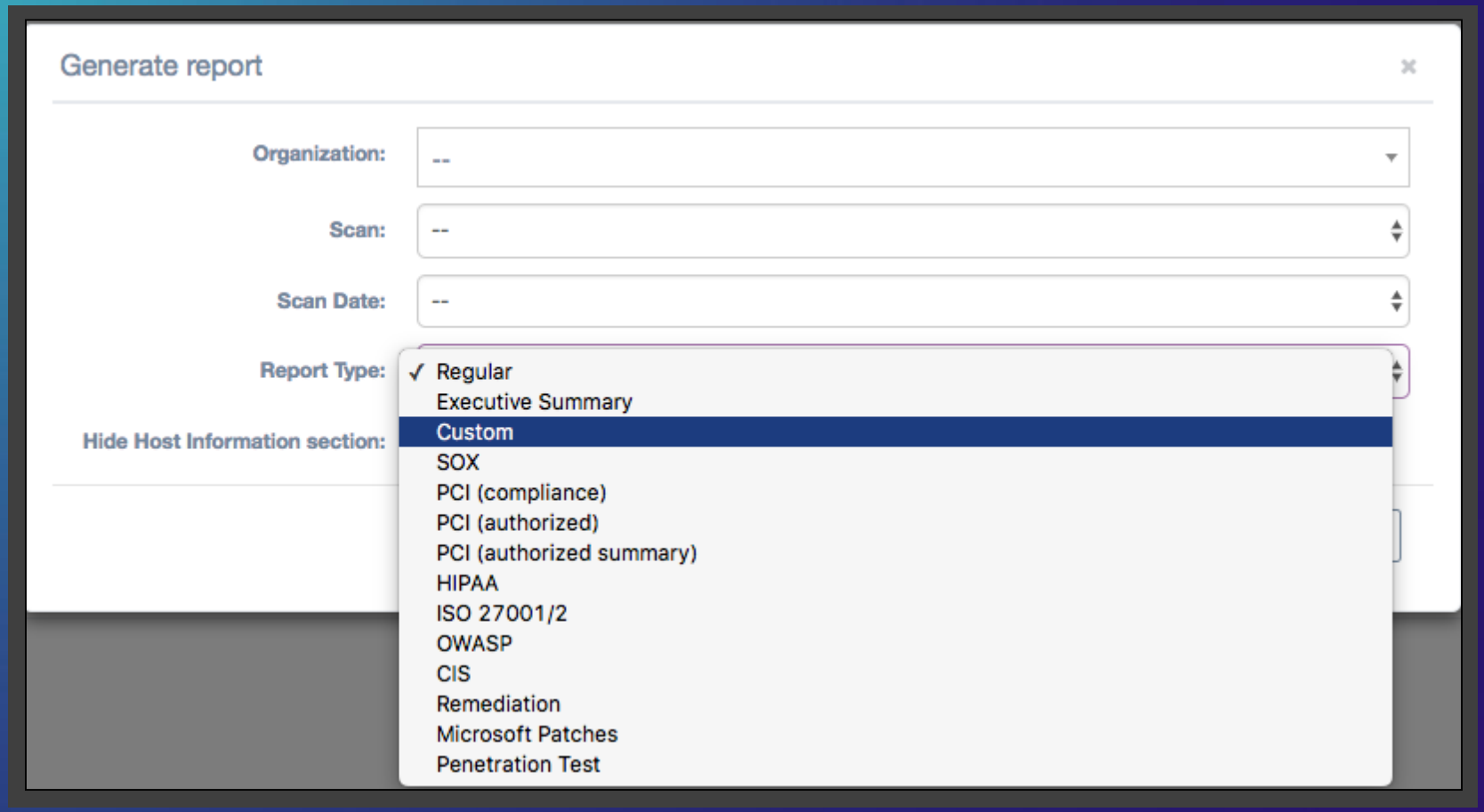
- Определите и создайте любой требуемый тип отчета.
- Автоматически отправлять ответственной группе после завершения сканирования
- Пример: команда Sap получает отчеты по SAP и приложениям, менеджмент, инженеры, веб-разработка, все получают конкретные отчеты, которые им нужны.

beSECURE Customized Report Generator



Генератор отчетов о соответствии

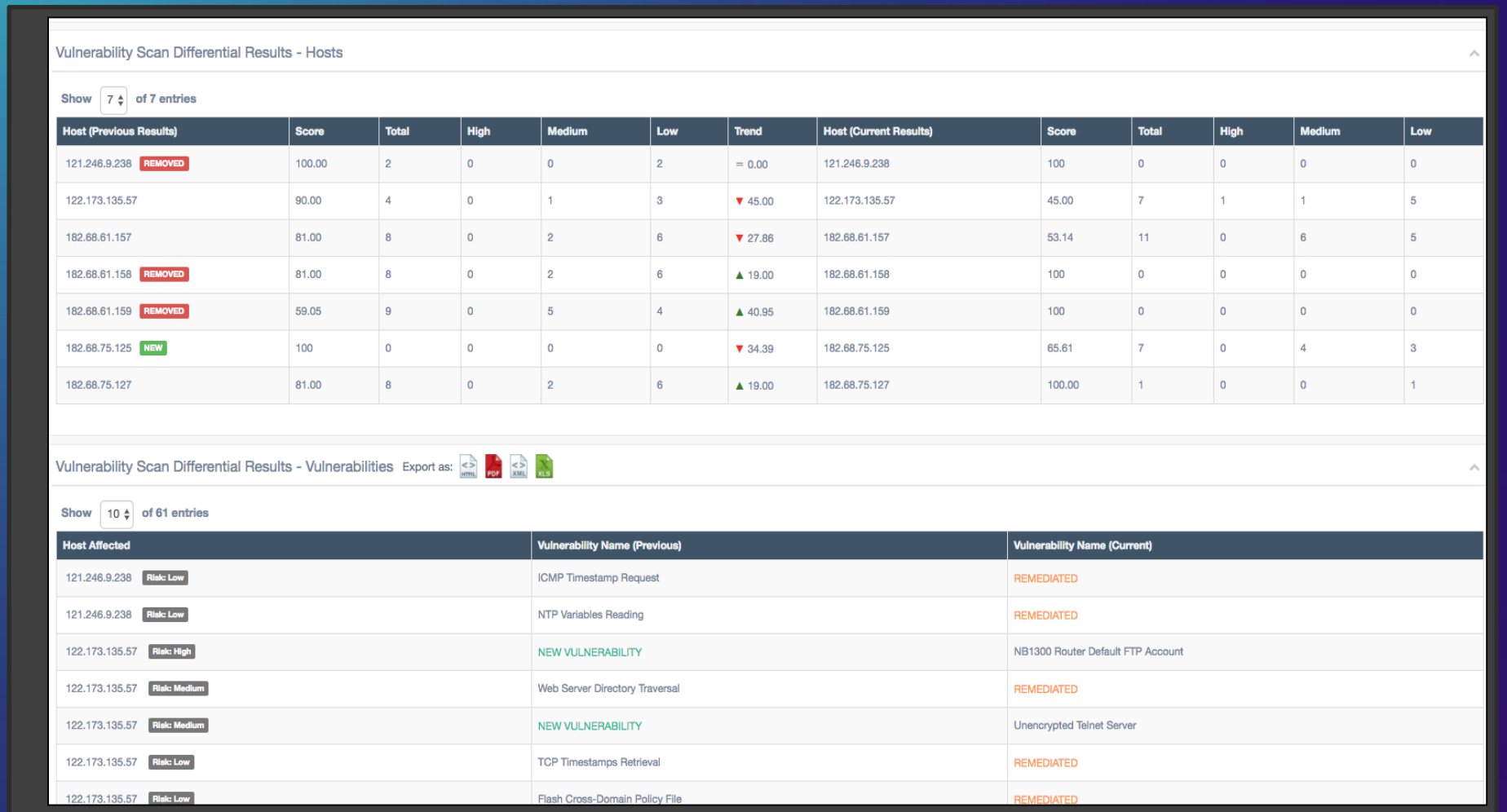
Просто щелкните раскрывающееся меню и выберите требуемый отчет о соответствии.



beSECURE Дифференциальные отчеты

Проверьте свой прогресс, выберите любые 2 даты и сравните результаты сканирования. Гарантирует, что вы не утонете в информационной перегрузке. Например, запустите ежемесячный базовый отчет и еженедельные дифференциальные отчеты, чтобы видеть только новые данные отчета.

Такие как: Новые системы, Новые уязвимости с прошлой недели по эту неделю, Исправлено: уязвимости, исправленные с прошлой недели по эту неделю. Устойчивые уязвимости, которые все еще существуют. Не исправлено



Vulnerability Scan Differential Results - Hosts

Show 7 of 7 entries

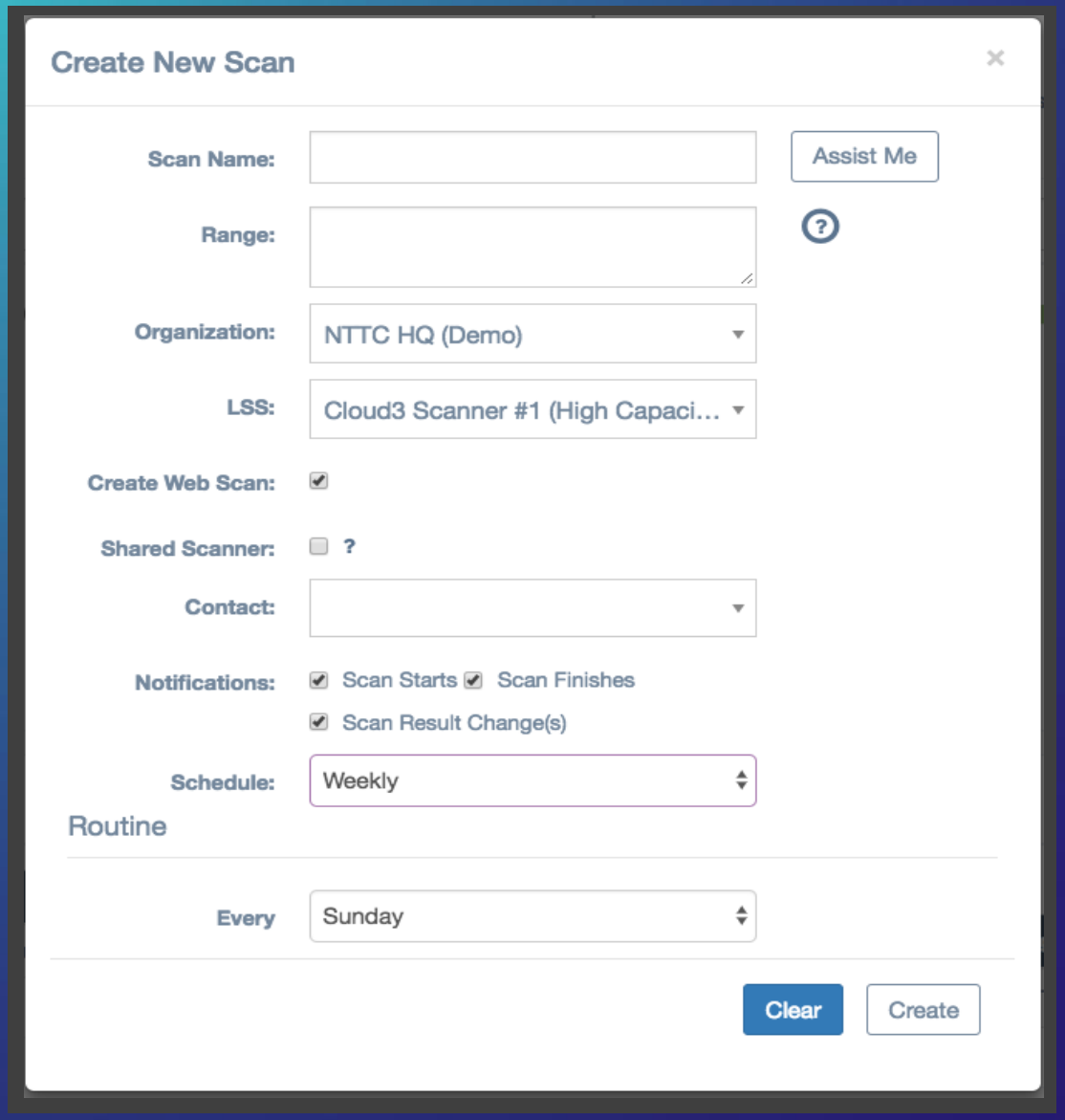
Host (Previous Results)	Score	Total	High	Medium	Low	Trend	Host (Current Results)	Score	Total	High	Medium	Low
121.246.9.238 REMOVED	100.00	2	0	0	2	= 0.00	121.246.9.238	100	0	0	0	0
122.173.135.57	90.00	4	0	1	3	▼ 45.00	122.173.135.57	45.00	7	1	1	5
182.68.61.157	81.00	8	0	2	6	▼ 27.86	182.68.61.157	53.14	11	0	6	5
182.68.61.158 REMOVED	81.00	8	0	2	6	▲ 19.00	182.68.61.158	100	0	0	0	0
182.68.61.159 REMOVED	59.05	9	0	5	4	▲ 40.95	182.68.61.159	100	0	0	0	0
182.68.75.125 NEW	100	0	0	0	0	▼ 34.39	182.68.75.125	65.61	7	0	4	3
182.68.75.127	81.00	8	0	2	6	▲ 19.00	182.68.75.127	100.00	1	0	0	1

Vulnerability Scan Differential Results - Vulnerabilities Export as:

Show 10 of 61 entries

Host Affected	Vulnerability Name (Previous)	Vulnerability Name (Current)
121.246.9.238 Risk: Low	ICMP Timestamp Request	REMEDIATED
121.246.9.238 Risk: Low	NTP Variables Reading	REMEDIATED
122.173.135.57 Risk: High	NEW VULNERABILITY	NB1300 Router Default FTP Account
122.173.135.57 Risk: Medium	Web Server Directory Traversal	REMEDIATED
122.173.135.57 Risk: Medium	NEW VULNERABILITY	Unencrypted Telnet Server
122.173.135.57 Risk: Low	TCP Timestamps Retrieval	REMEDIATED
122.173.135.57 Risk: Low	Flash Cross-Domain Policy File	REMEDIATED

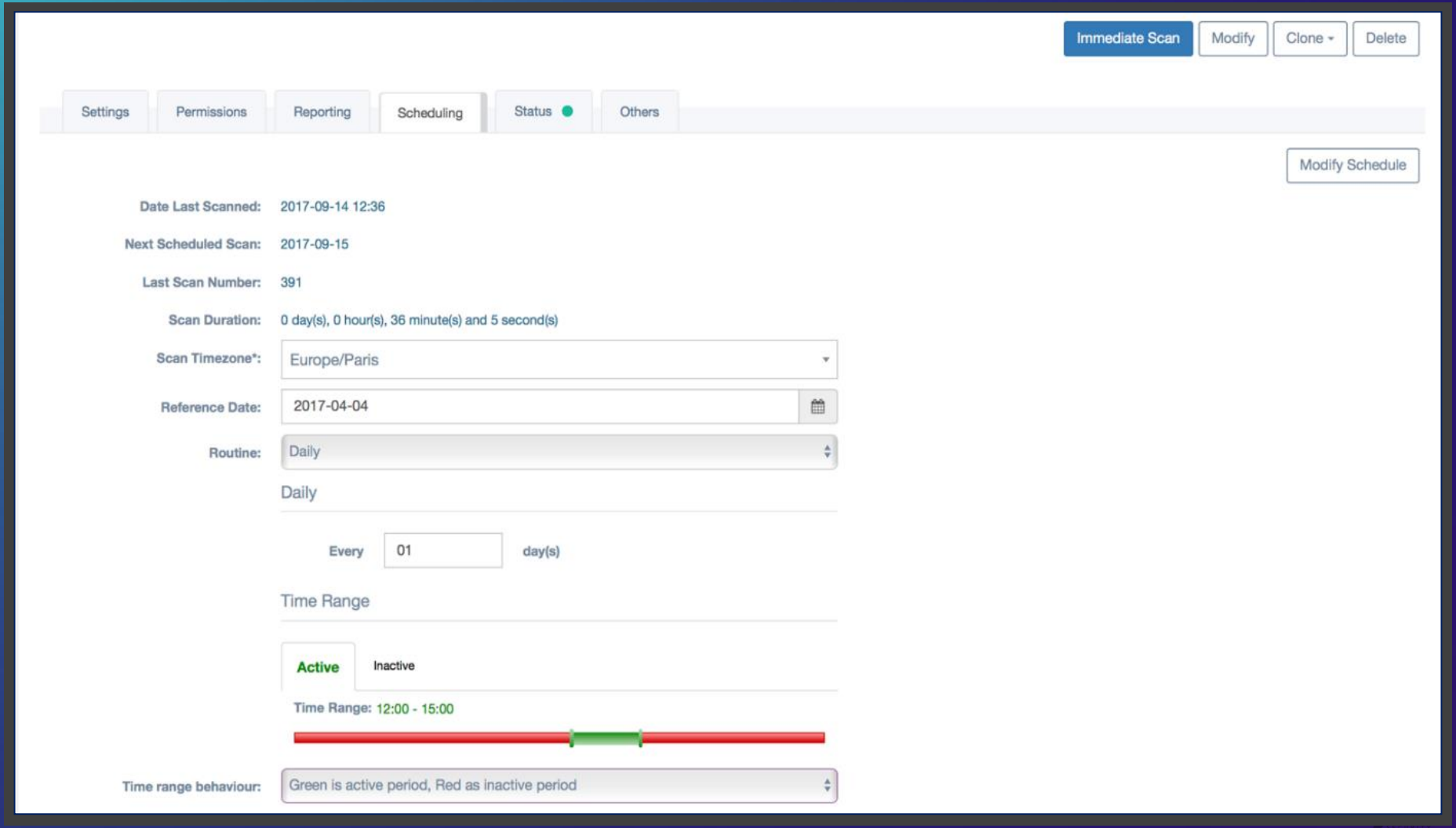
Quick Scan



Функция быстрого сканирования позволяет создавать и планировать сканирование за секунды.

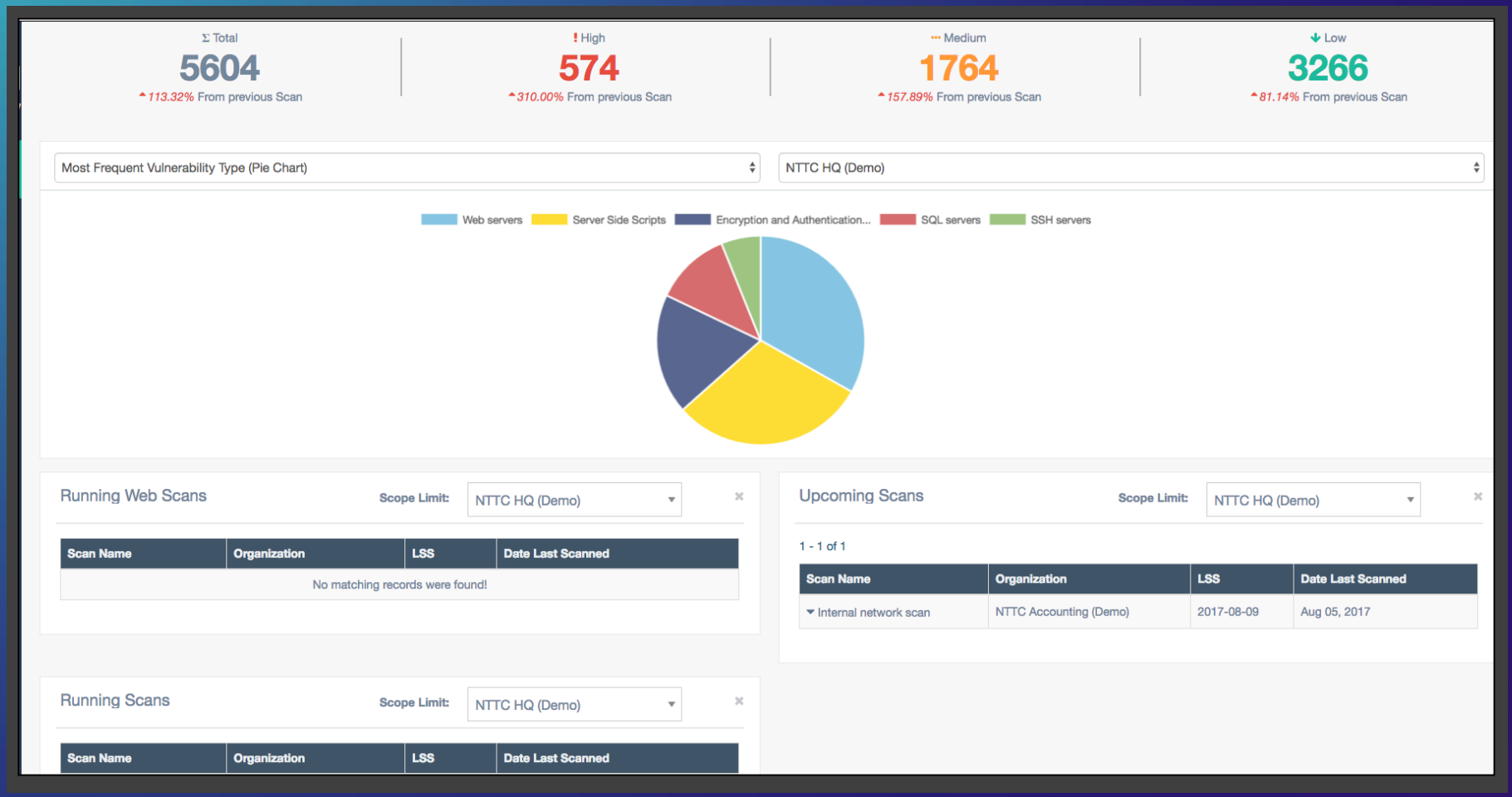
Планирование сканирования

Установите собственное окно сканирования, автоматическую паузу и продолжите
Сканирование по запросу и по расписанию

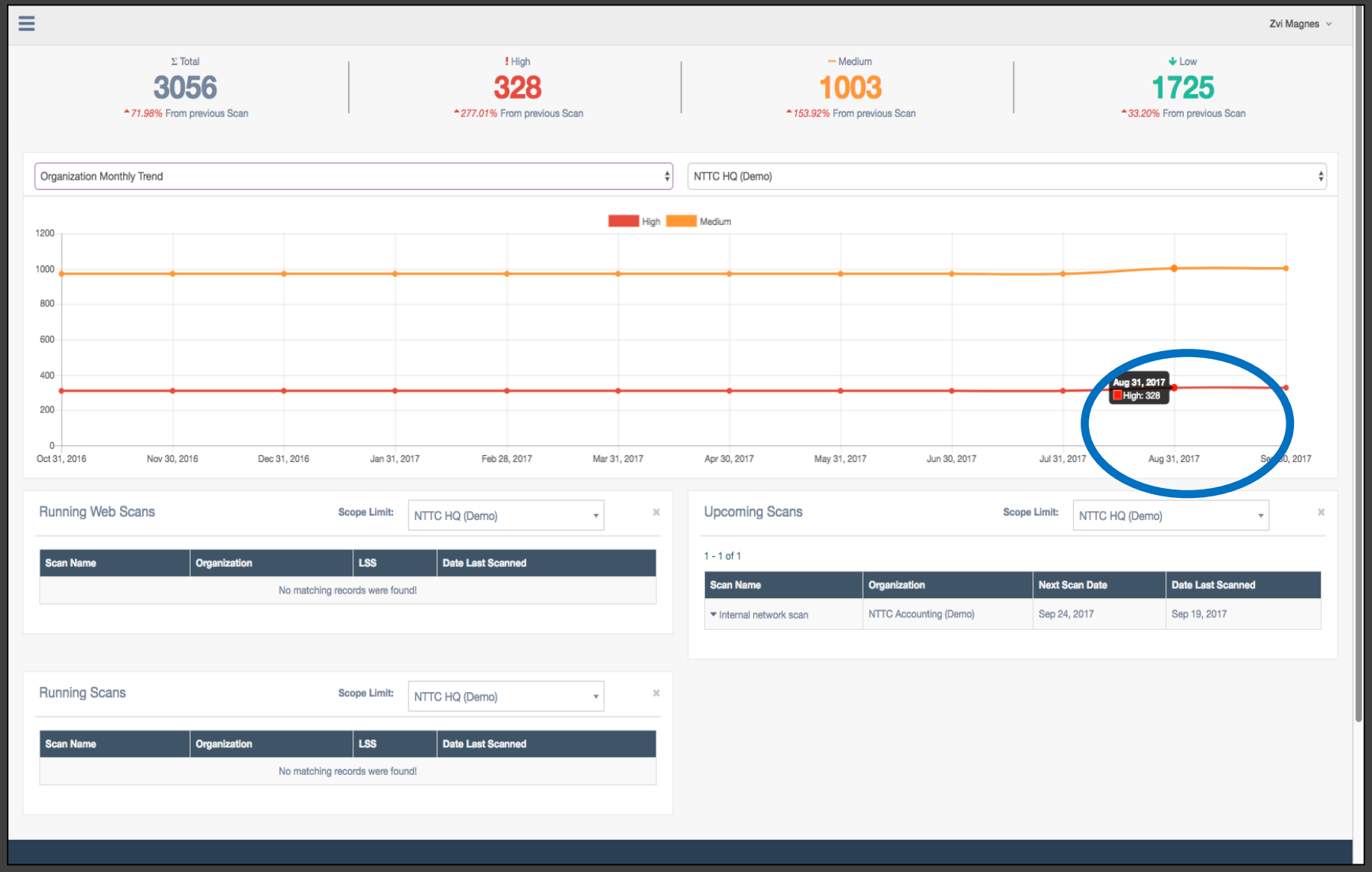


Ваша персональная панель мониторинга

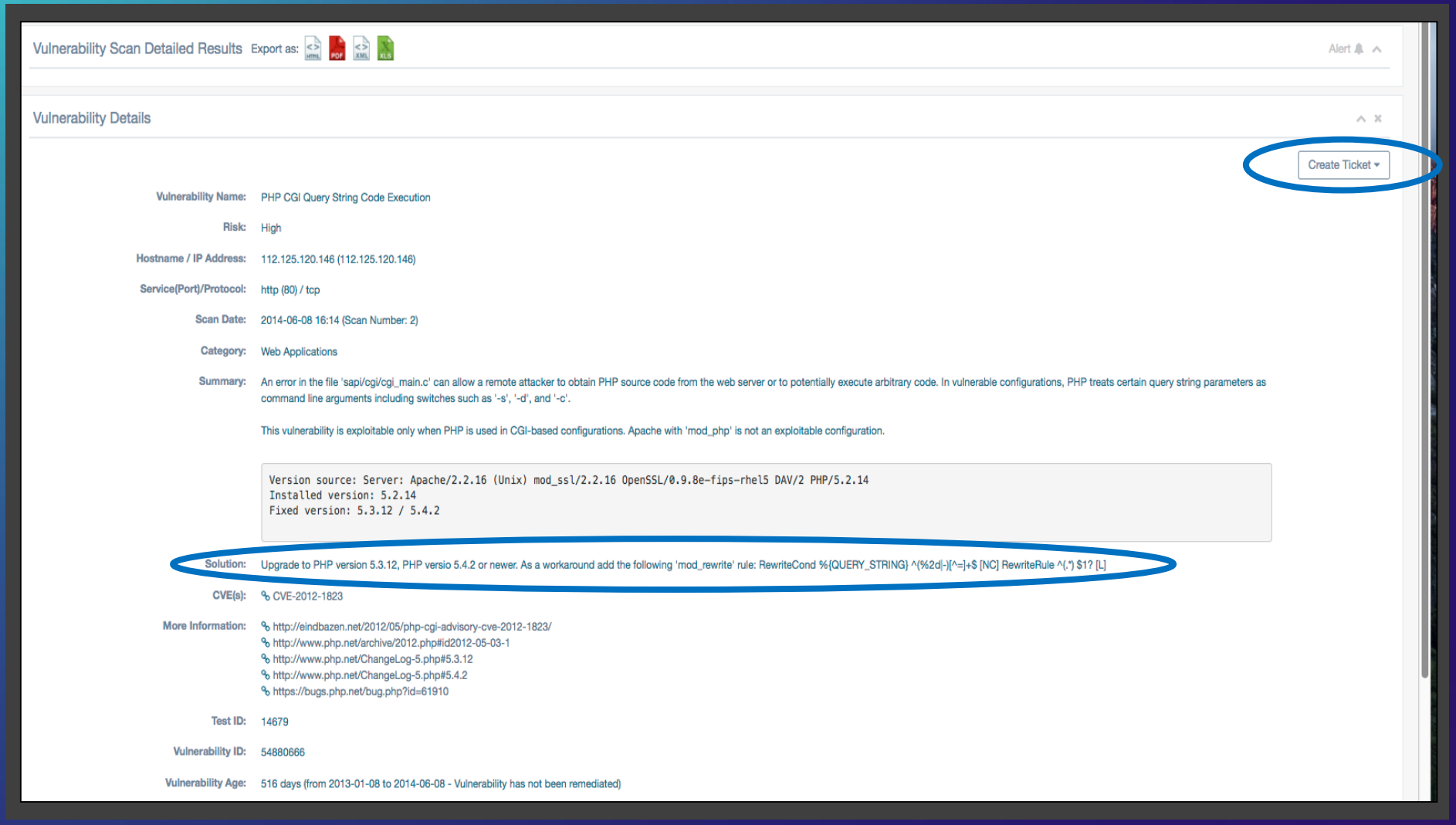
Выберите свою личную панель управления
Все панели мониторинга доступны для нажатия - разверните, чтобы получить дополнительную техническую информацию Управляйте и планируйте сканирование сети и веб-приложений с помощью Quick Add



Drill-Down for more Technical Information – Step 1..



Drill-Down for more Technical Information – Step 3..



Vulnerability Scan Detailed Results Export as:

Alert

Vulnerability Details

Create Ticket

Vulnerability Name: PHP CGI Query String Code Execution

Risk: High

Hostname / IP Address: 112.125.120.146 (112.125.120.146)

Service(Port)/Protocol: http (80) / tcp

Scan Date: 2014-06-08 16:14 (Scan Number: 2)

Category: Web Applications

Summary: An error in the file 'sapi/cgi/cgi_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.

This vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

```
Version source: Server: Apache/2.2.16 (Unix) mod_ssl/2.2.16 OpenSSL/0.9.8e-fips-rhel5 DAV/2 PHP/5.2.14
Installed version: 5.2.14
Fixed version: 5.3.12 / 5.4.2
```

Solution: Upgrade to PHP version 5.3.12, PHP versio 5.4.2 or newer. As a workaround add the following 'mod_rewrite' rule: RewriteCond %{QUERY_STRING} ^(%2d|-)[^=]+$ [NC] RewriteRule ^(.*) $1? [L]

CVE(s): CVE-2012-1823

More Information:
- http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
- http://www.php.net/archive/2012.php#id2012-05-03-1
- http://www.php.net/ChangeLog-5.php#5.3.12
- http://www.php.net/ChangeLog-5.php#5.4.2
- https://bugs.php.net/bug.php?id=61910

Test ID: 14679

Vulnerability ID: 54880666

Vulnerability Age: 516 days (from 2013-01-08 to 2014-06-08 - Vulnerability has not been remediated)

INTEGRATION PARTNERS

Ticketing, SIEM, IPS, WAF Integration Partners, and more….

Compliancy Reports

Thank you!

KNOW THAT YOU'RE SAFE

Аношко Володимир

vanoshko@nwu.com.ua

beyond