SOFTPROM

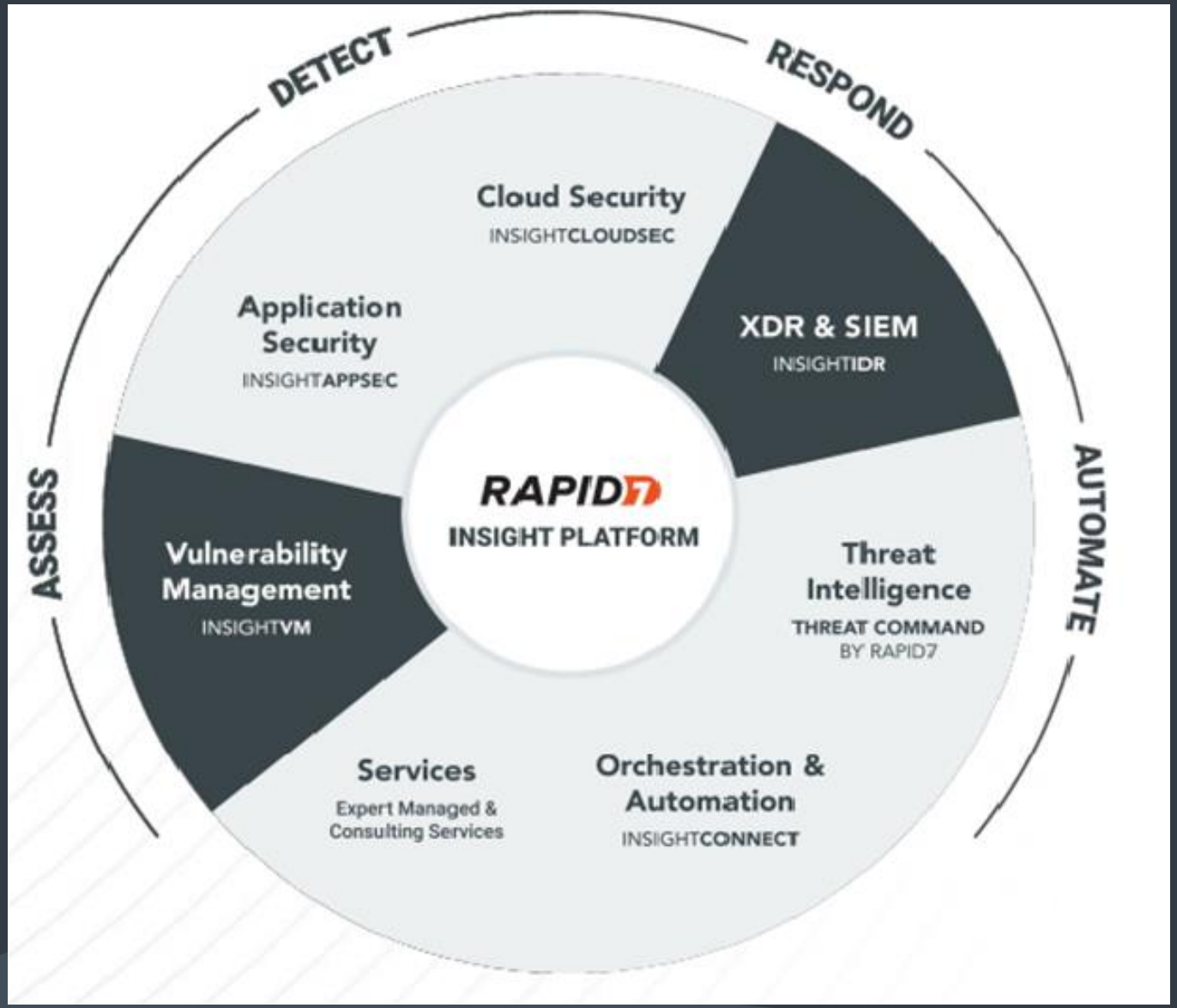
RAPID7

RAPID7 INSIGHT PLATFORM. USE CASE

Subhan Sharifov
Head of Information Security Department
at Bank of Baku

SECURITY FORUM
BAKU • APRIL 23

Продуктовая линейка



- InsightVM
- InsightAppsec
- InsightIDR (SIEM + XDR + honeypots)
- InsightCloudSec
- InsightConnect (SOAR)

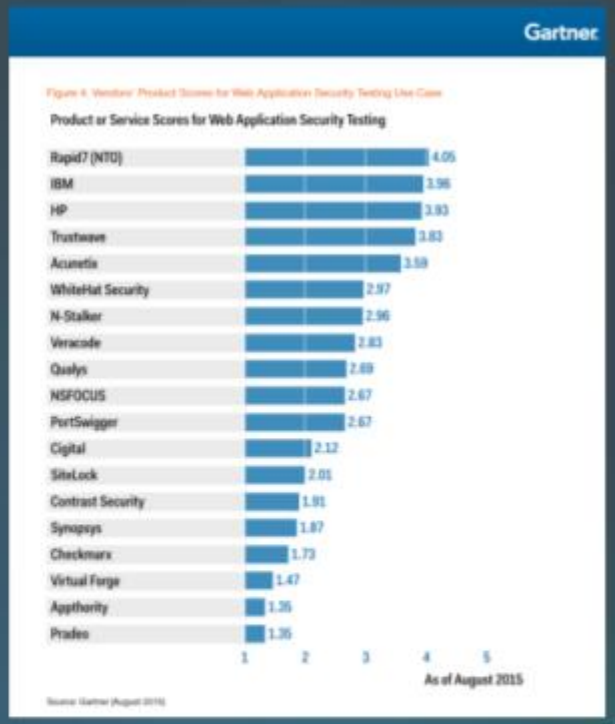
- Metasploit

RAPID7

Отраслевое лидерство

SIEM Magic Quadrant
- Gartner

Vulnerability Risk Management
- Forrester Wave



Critical Capabilities for
Application Security Testing
- Gartner

RAPID7

insightVM

nexpose®

Vulnerability Risk Management

COLLECT C

Автоматический сбор, мониторинг и анализ всей вашей сети на предмет новых и существующих рисков.

PRIORITIZE P

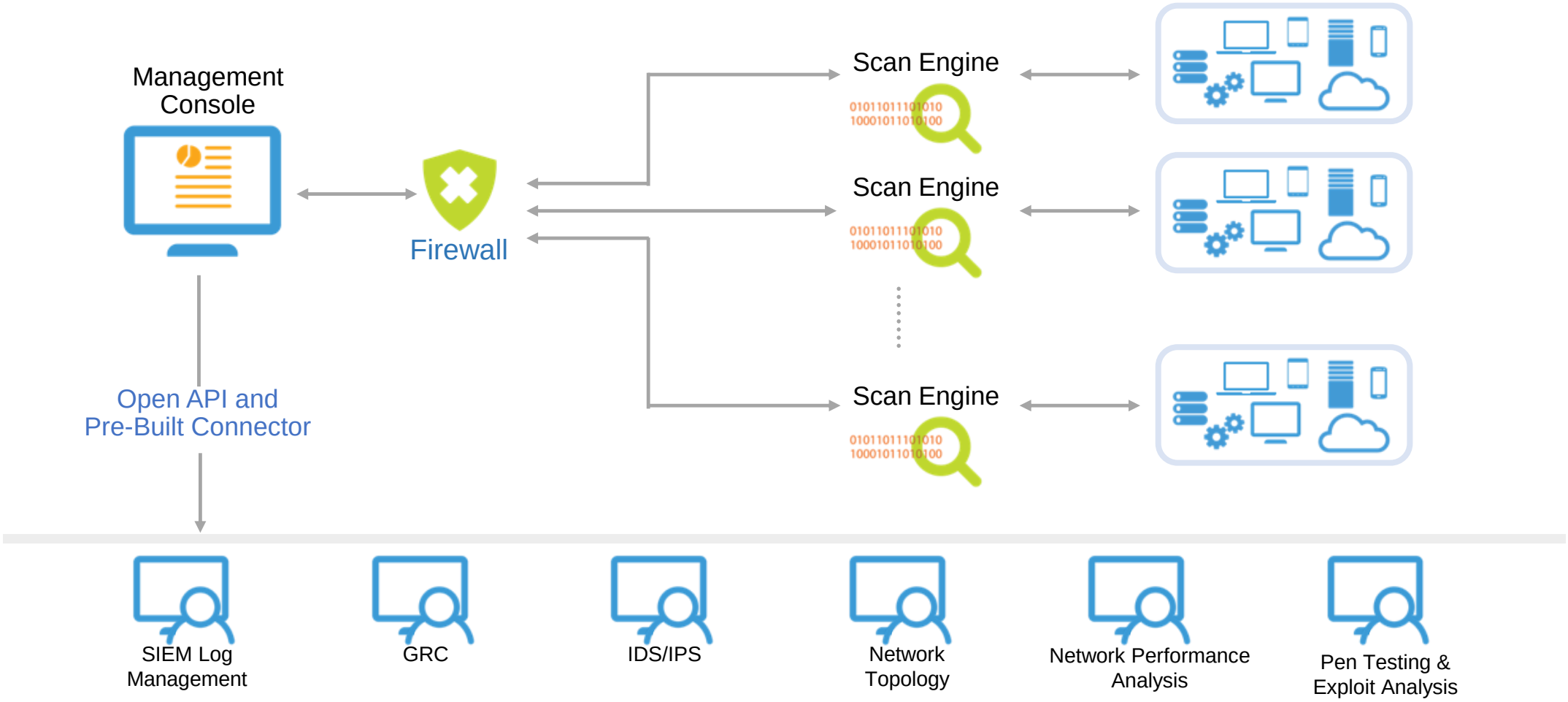
Выйдите **за пределы** только CVSS-методов, чтобы помочь вам **сосредоточиться** на наиболее важных уязвимостях, так же как это делает злоумышленник.

REMEDIATE R

Оптимизируйте **рабочий процесс исправления (устранения уязвимостей)**, чтобы сделать его вашим лучшим другом и **отслеживать прогресс** в режиме реального времени.

RAPID7

Гибкая и масштабируемая архитектура Nexpose

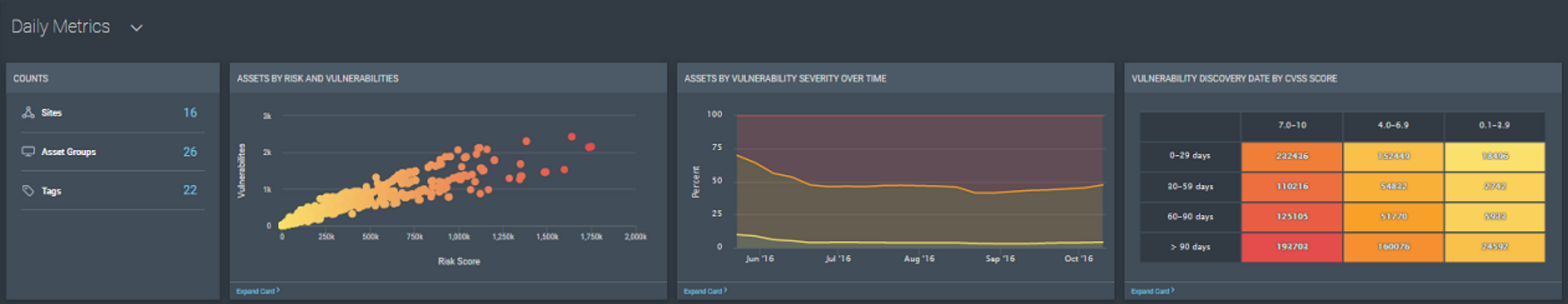


RAPID7

ОСНОВНЫЕ ОТЛИЧИЯ КОТОРЫЕ ЕСТЬ ТОЛЬКО IVM – но нет в NEXPOSE!

Liveboards – New Generation Reporting

Отслеживайте риски в реальном времени



Моментальная аналитика данных сканирования.

Визуализация результатов анализа в интерактивных карточках позволяющих моментально реагировать на изменения в инфораструктуре

RAPID7

Liveboards – New Generation Reporting

Отчеты больше не нужны

Глубокий анализ данных
Интеллектуальная система фильтров
Находите быстро то что важно!

RAPID7

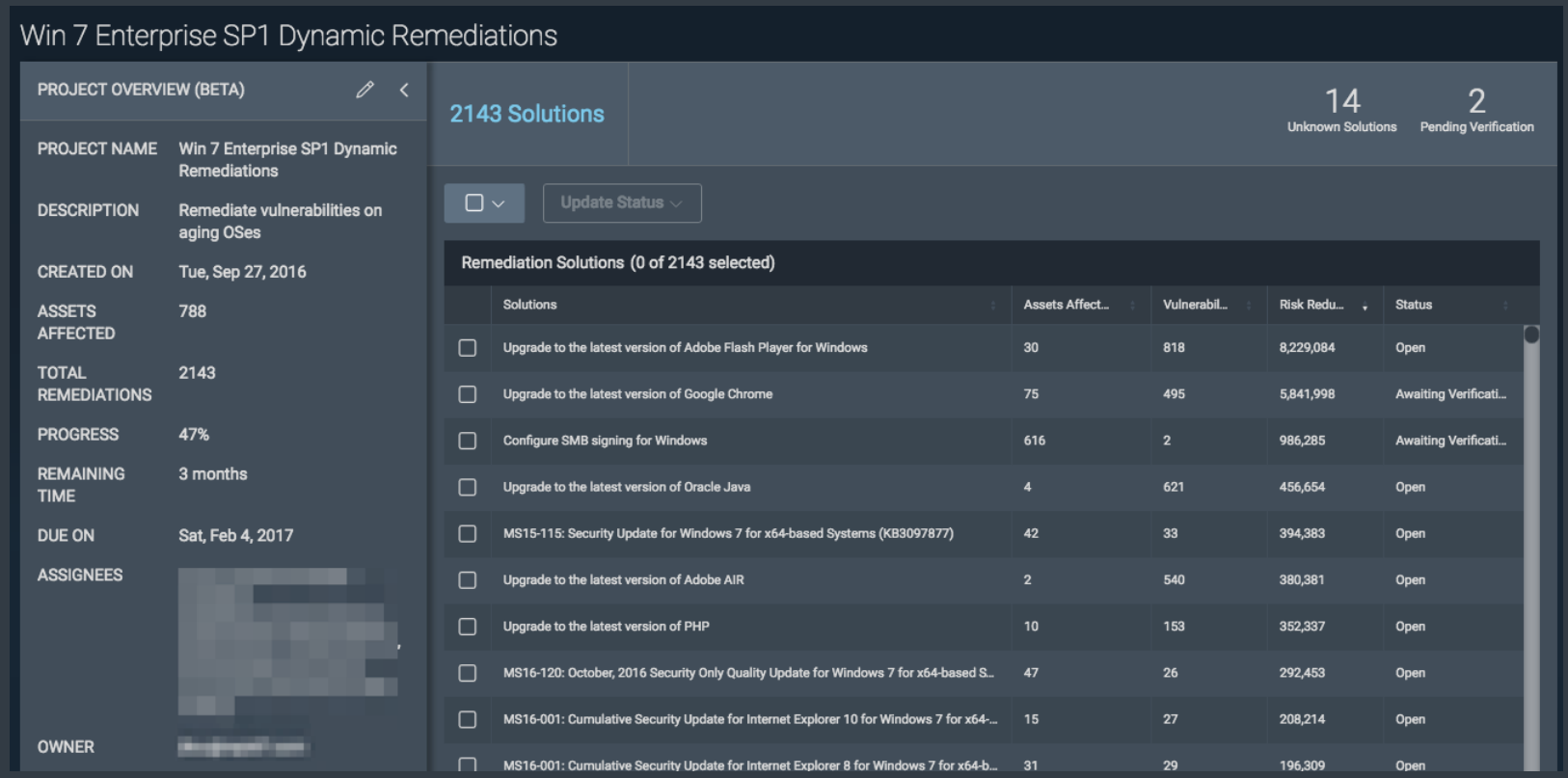
Remediation Workflows

Мгновенная реакция на риск.

Автоматические создание проектов

Контроль выполнение заданий

Автоматическое распределение заданий.



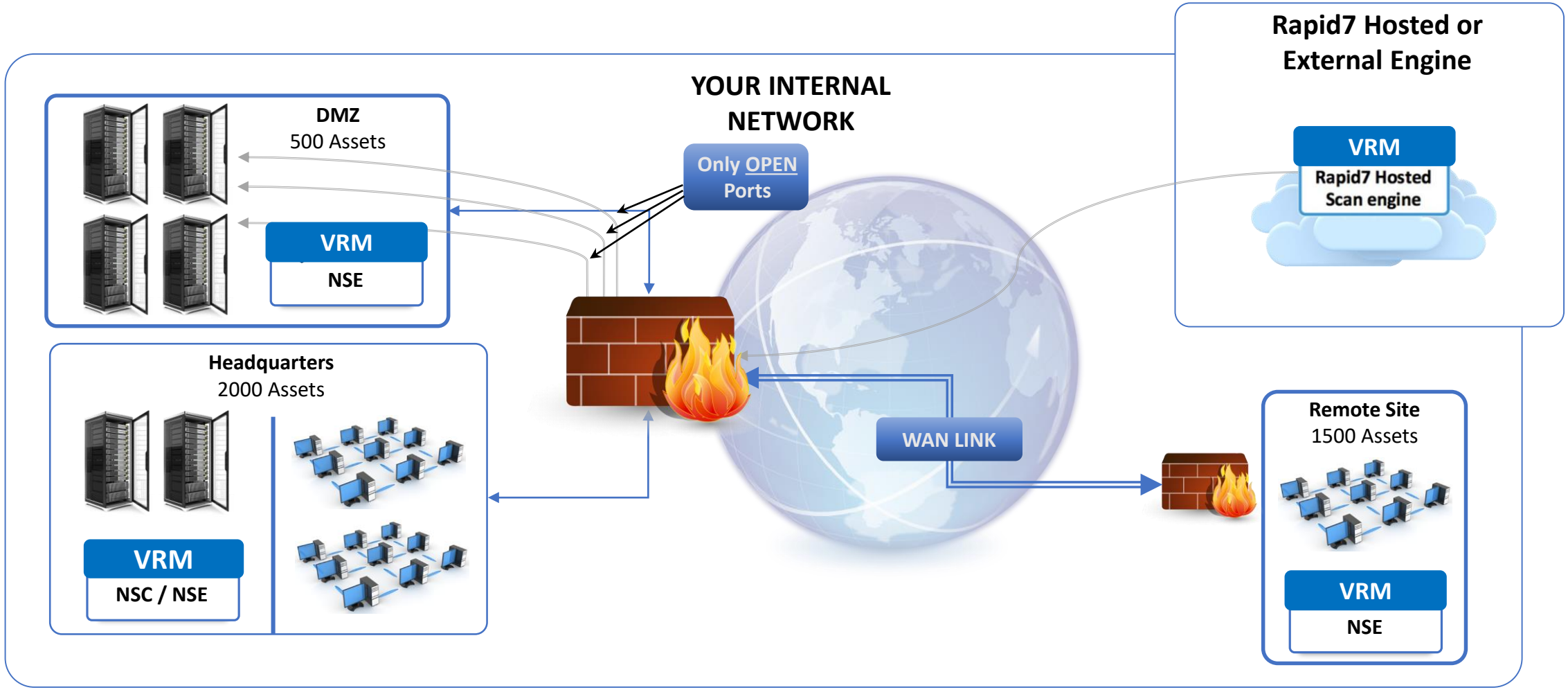
Go beyond understanding risk: Get to the fix.

RAPID7

Agents

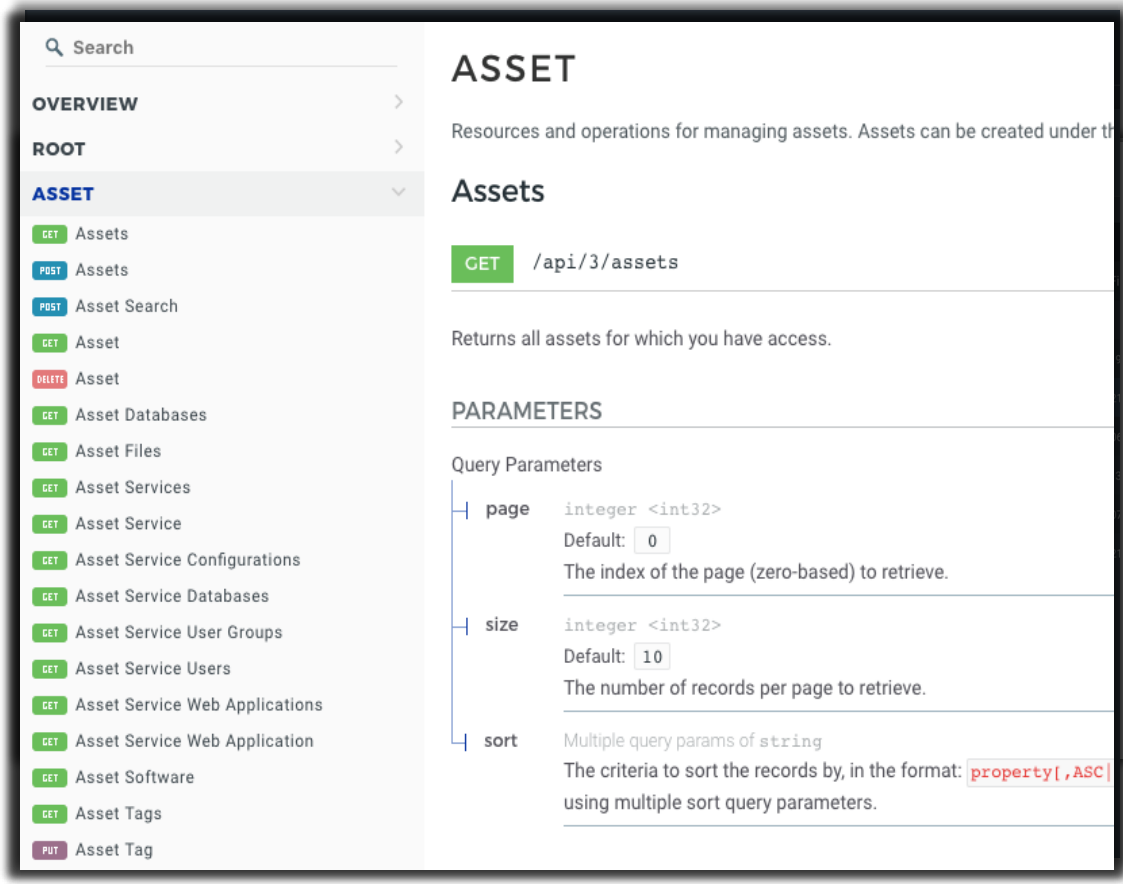
- Хосты за пределами сети
- Часто выключаемые хосты
- Хосты которые нельзя сканировать

Рекомендуемые виды Сканирования *(Internal & External Scans)*



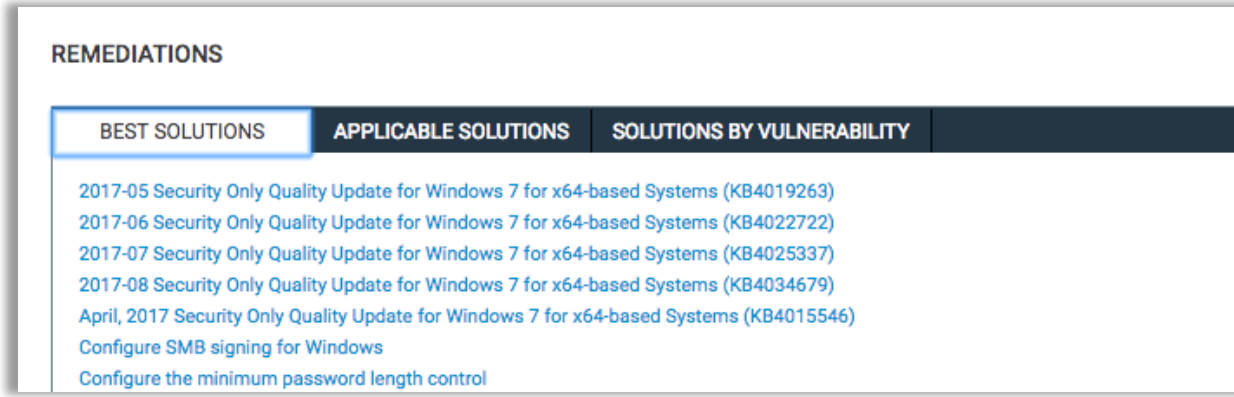
Автоматизация – ключ к эффективности

- **Автоматическое обнаружение** хостов и динамические сканы
- **Динамическая** группировка хостов
- Сканирования по расписанию
- **Адаптивный мониторинг** безопасности и Автоматическая реакция на триггеры
- Workflow **Orchestration (IVM)**
- Ticketing integration
- Restfull API
- **Интеллектуальная методика** оценки рисков
- Эффективная, многоуровневая отчетность

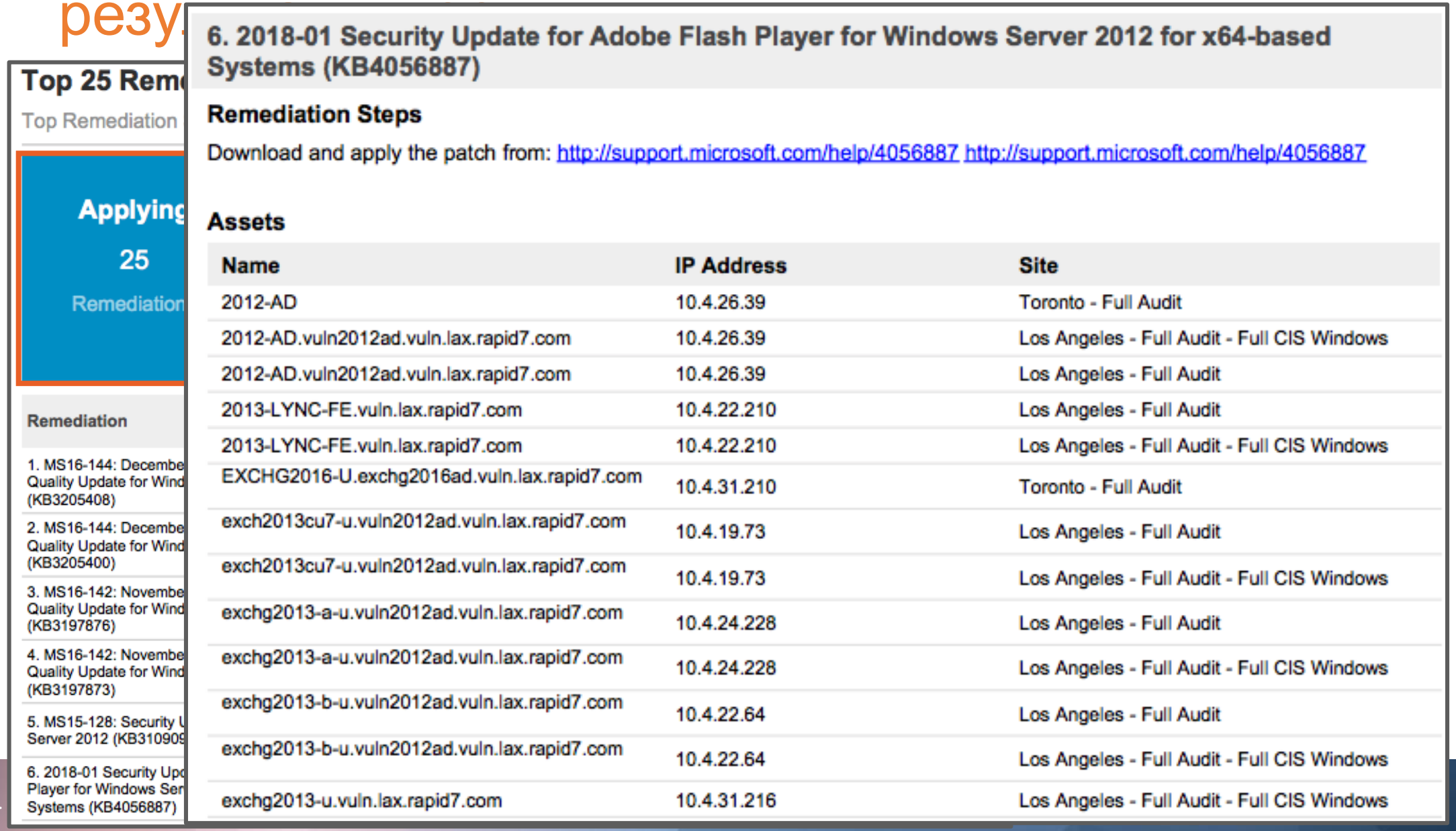


Структурированные решения по исправлению (Remediation)

- Выберите из различных типов решений для исправления.
- Отчет об **основных** исправлениях показывает единственное лучшее решение для каждого актива.
- Получите доступ к **полному набору** применимых решений в портлете Remediations.



Отчет на основе действий. Эффективность и резу



Top 25 Reme

Top Remediation

Applying

25

Remediation

Remediation

1. MS16-144: Decembe Quality Update for Wind (KB3205408)
2. MS16-144: Decembe Quality Update for Wind (KB3205400)
3. MS16-142: Novembe Quality Update for Wind (KB3197876)
4. MS16-142: Novembe Quality Update for Wind (KB3197873)
5. MS15-128: Security U Server 2012 (KB310909
6. 2018-01 Security Upd Player for Windows Ser Systems (KB4056887)

6. 2018-01 Security Update for Adobe Flash Player for Windows Server 2012 for x64-based Systems (KB4056887)

Remediation Steps

Download and apply the patch from: http://support.microsoft.com/help/4056887 http://support.microsoft.com/help/4056887

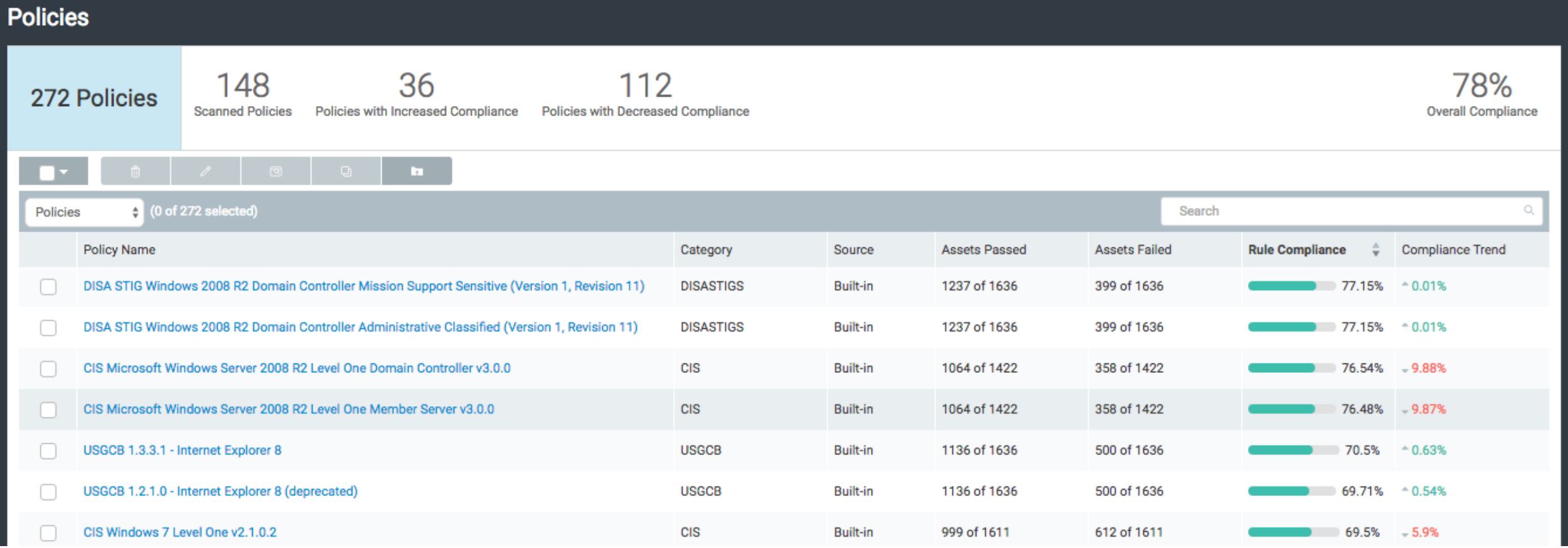
Assets

Name	IP Address	Site
2012-AD	10.4.26.39	Toronto - Full Audit
2012-AD.vuln2012ad.vuln.lax.rapid7.com	10.4.26.39	Los Angeles - Full Audit - Full CIS Windows
2012-AD.vuln2012ad.vuln.lax.rapid7.com	10.4.26.39	Los Angeles - Full Audit
2013-LYNC-FE.vuln.lax.rapid7.com	10.4.22.210	Los Angeles - Full Audit
2013-LYNC-FE.vuln.lax.rapid7.com	10.4.22.210	Los Angeles - Full Audit - Full CIS Windows
EXCHG2016-U.exchg2016ad.vuln.lax.rapid7.com	10.4.31.210	Toronto - Full Audit
exch2013cu7-u.vuln2012ad.vuln.lax.rapid7.com	10.4.19.73	Los Angeles - Full Audit
exch2013cu7-u.vuln2012ad.vuln.lax.rapid7.com	10.4.19.73	Los Angeles - Full Audit - Full CIS Windows
exchg2013-a-u.vuln2012ad.vuln.lax.rapid7.com	10.4.24.228	Los Angeles - Full Audit
exchg2013-a-u.vuln2012ad.vuln.lax.rapid7.com	10.4.24.228	Los Angeles - Full Audit - Full CIS Windows
exchg2013-b-u.vuln2012ad.vuln.lax.rapid7.com	10.4.22.64	Los Angeles - Full Audit
exchg2013-b-u.vuln2012ad.vuln.lax.rapid7.com	10.4.22.64	Los Angeles - Full Audit - Full CIS Windows
exchg2013-u.vuln.lax.rapid7.com	10.4.31.216	Los Angeles - Full Audit - Full CIS Windows

Политики соответствия (стандарты)

Визуализация

“Мне нужно быстро увидеть свое состояние соответствия для всех политик.”



Политики соответствия (стандарты)

Отчетность

Быстрые исправления, и для политик также!

Top Policy Remediations with Details — September 12, 2016 14:39:23 GMT

Policy Remediations with details

Applying	Will Remediate	Affecting
25	86 %	2119
Top Remediations	of the Total 29 Rule Failures in the Report	Assets

Policy Name	Rule Name	# Assets	Rule Compliance
CIS Microsoft SQL Server 2008 R2 Database Engine v1.2.0	1.1. Install the Latest SQL Server Service Packs and Hotfixes	506	↑ 3.448 %
CIS Microsoft SQL Server 2008 R2 Database Engine v1.2.0	1.2 Install on dedicated single-function member servers	506	↑ 3.448 %
CIS Microsoft SQL Server 2008 R2 Database Engine v1.2.0	2.1. Set the 'Ad Hoc Distributed Queries' Server Configuration Option to 0	506	↑ 3.448 %
CIS Microsoft SQL Server 2008 R2 Database Engine v1.2.0	2.2. Set the 'CLR Enabled' Server Configuration Option to 0	506	↑ 3.448 %

Rule Breakdown Summary — March 9, 2016 10:13:51 PST

10.4.25.14 w2k8-cis-c.vuln.lax.rapid7.com Microsoft Windows Server 2008 Enterprise Edition SP2

92.24 % Compliant

2 Scanned Policies with 580 Rules

535 of 580 Rules Passed

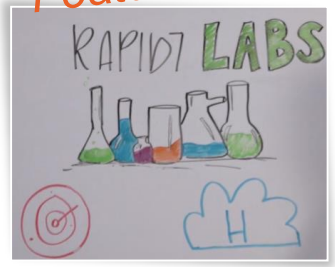
Policy Breakdown	Rules	Passed	Failed
CIS Windows 2008 Domain Controller Level One v2.1.0.1		295	40
Computer Configuration > Windows Settings > Security Settings > System Services		78	22
1.1.1.1.1. Set 'Function Discovery Resource Publication' to 'Manual'			
1.1.1.1.10. Set 'UPnP Device Host' to 'Disabled'			
1.1.1.1.100. Set 'IKE and AuthIP IPsec Keying Modules' to 'Automatic'			
1.1.1.1.11. Set 'System Event Notification Service' to 'Automatic'			
1.1.1.1.12. Set 'Windows Color System' to 'Manual'			
1.1.1.1.13. Set 'Active Directory Domain Services' to 'Automatic'			

Приоритезация. RealRisk

Rapid7 **Risk Score** (шкала от 0 до 1000) отображае

- > CVSS Score (from 0 to 10)
- > Как давно известна эта уязвимость
- > Как давно эта уязвимость в нашей сети
- > Наличие эксплойтов и malware
- > Насколько легко эксплуатируется
- > Информация с Rapid7 Labs
- > Пользовательский контекст (Критичность актива)

Featured by

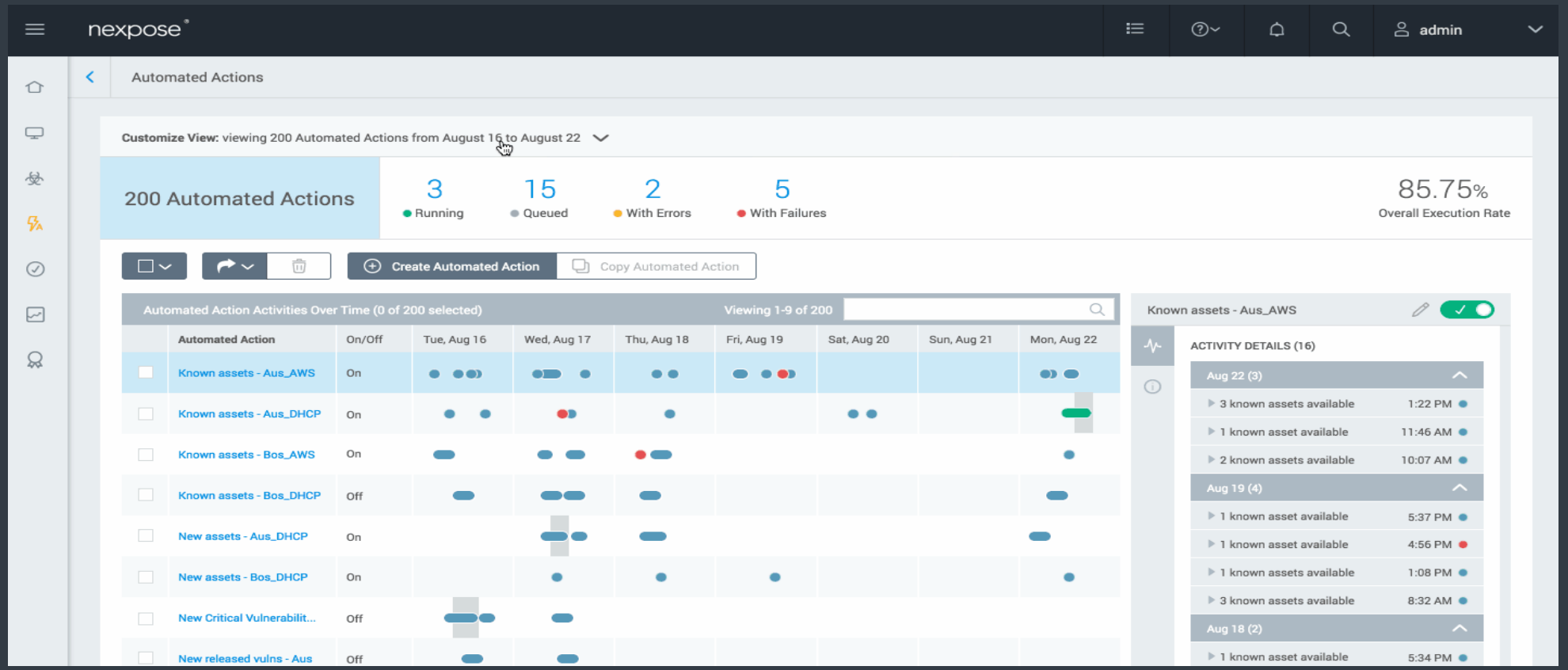


Адаптивная безопасность

Реагируйте автоматически.

Узнавайте о новых рисках сразу после их появления.

Актуализируйте список хостов без необходимости дополнительной инвентаризации.



Безопасность на основе оценки рисков

Старая модель :
Prevention-Based Security

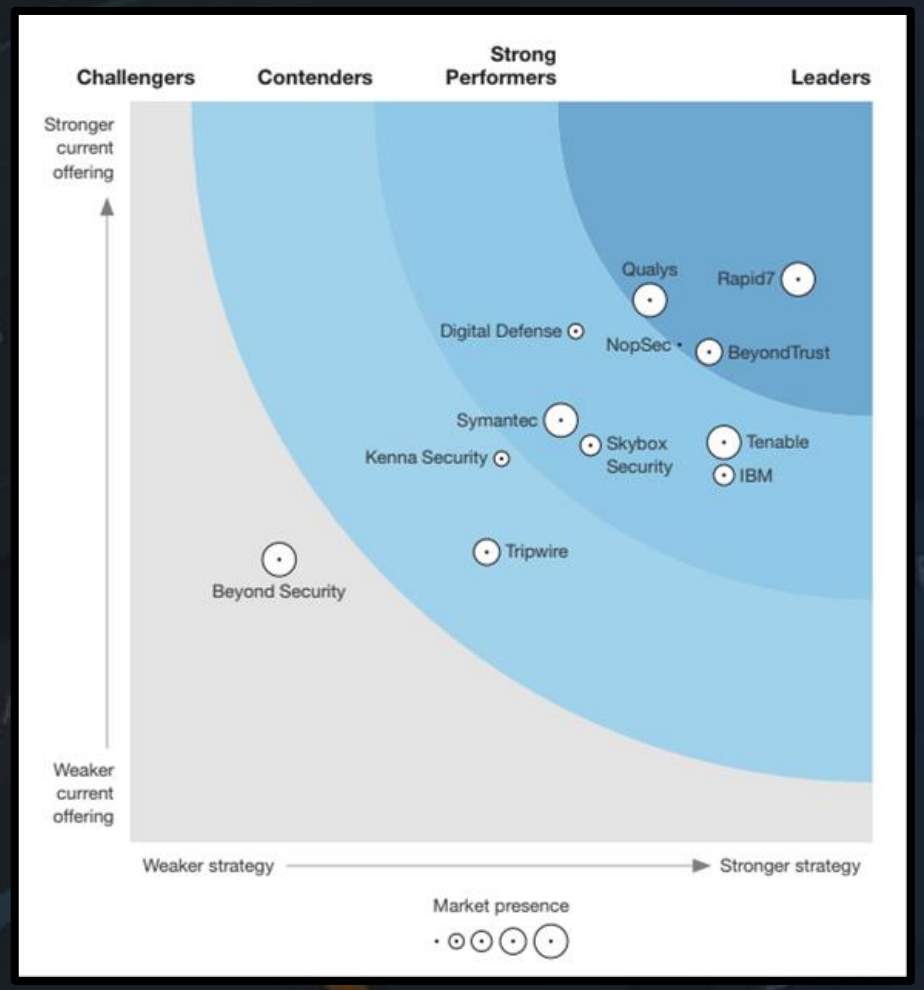
Новая модель :
Risk-Based Security

К 2020,

60%

средств корпоративной информационной безопасности будет выделено на **быстрое обнаружение и реагирование** по сравнению с менее чем 20% в 2016 году.

- *Gartner: "Special Report: Cybersecurity at the Speed of Digital Business", May 26, 2016*



“Rapid7 уже реализовал то, как VRM будет выглядеть в будущем”

- Forrester Wave for Vulnerability Risk Management, Q1 2018

Гибкая и масштабируемая архитектура

Множество вариантов разворачивания

Автоматизация

Динамические сканы

THANK YOU

New Generation Reports

Агенты

Vulnerability Validation

Сканирование мобильных устройств

Не только логи

RAPID7