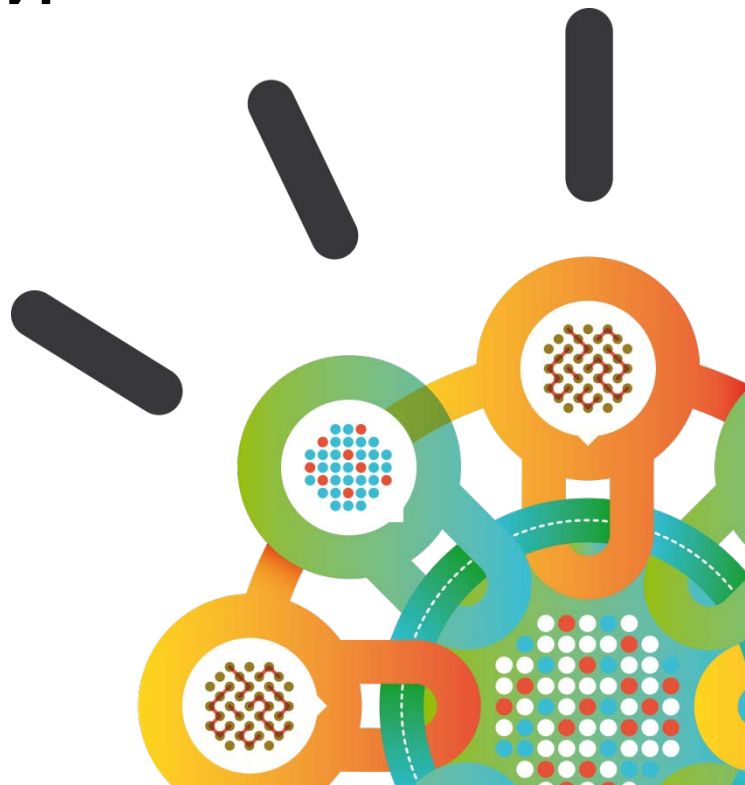
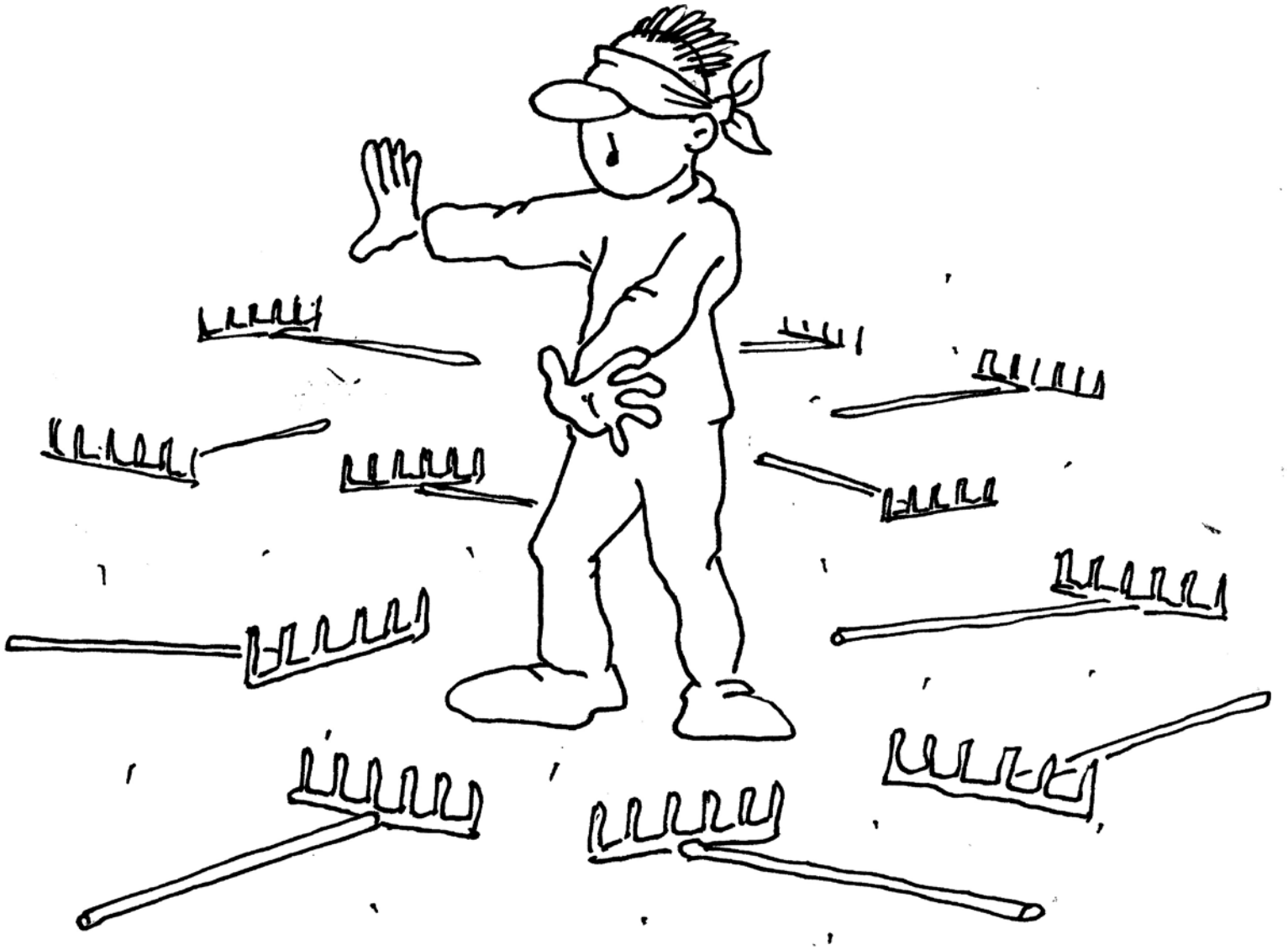
Security Intelligence.
Think Integrated.

Безопасность платежных сервисов с момента зарождения идеи



Антон Менчиц
IBM Security

Опять те же грабли…



Источник: IBM X-Force® Research 2014 Q3 Trend and Risk Report

Целевые атаки становятся всё популярнее и популярнее

Operational Sophistication

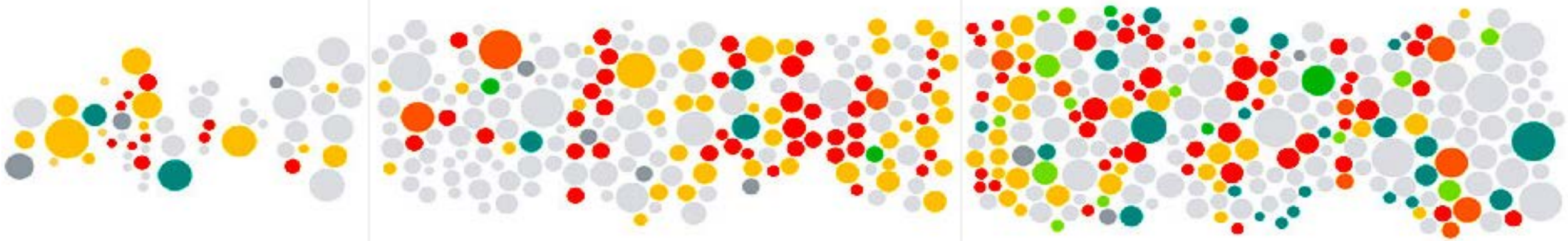
IBM X-Force® declared Year of the Security Breach

Near Daily Leaks of Sensitive Data

40% increase
in reported data breaches and incidents

Relentless Use of Multiple Methods

500,000,000+ records
were leaked, while the future shows no sign of change



2011 2012 2013

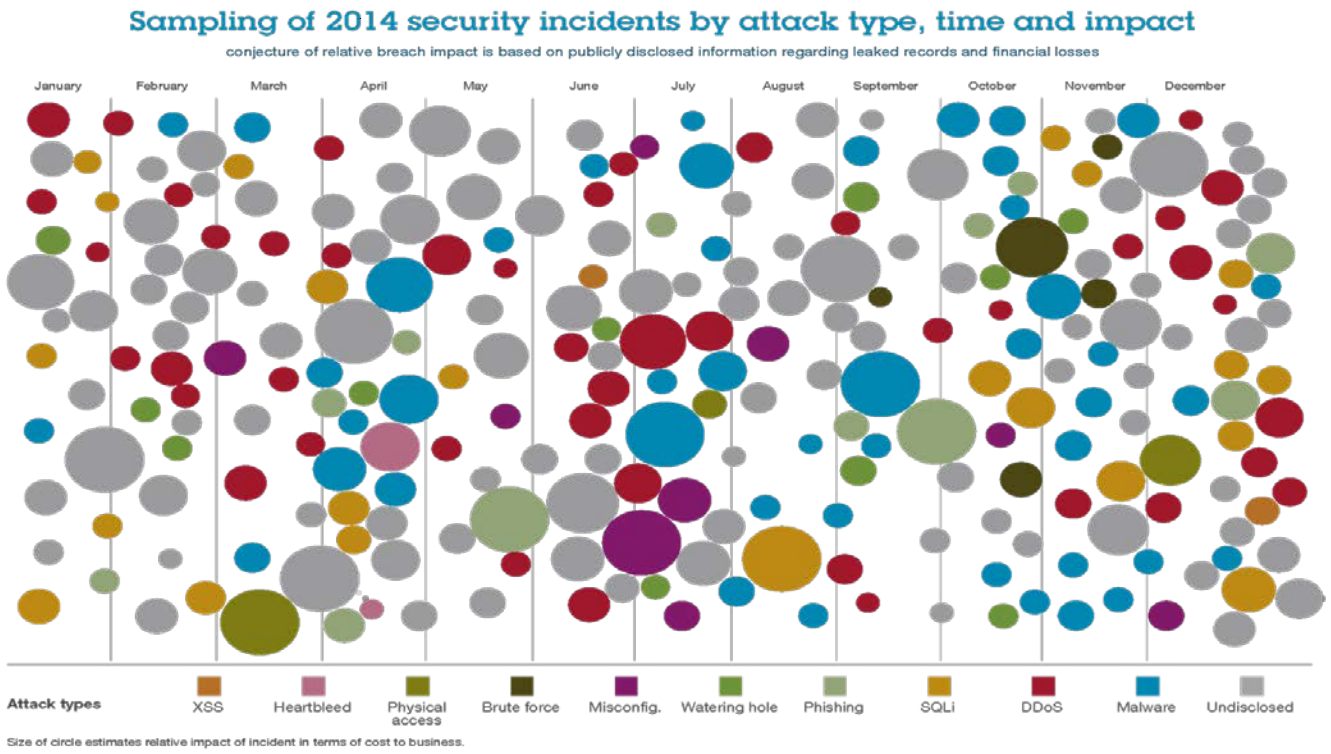
Attack types

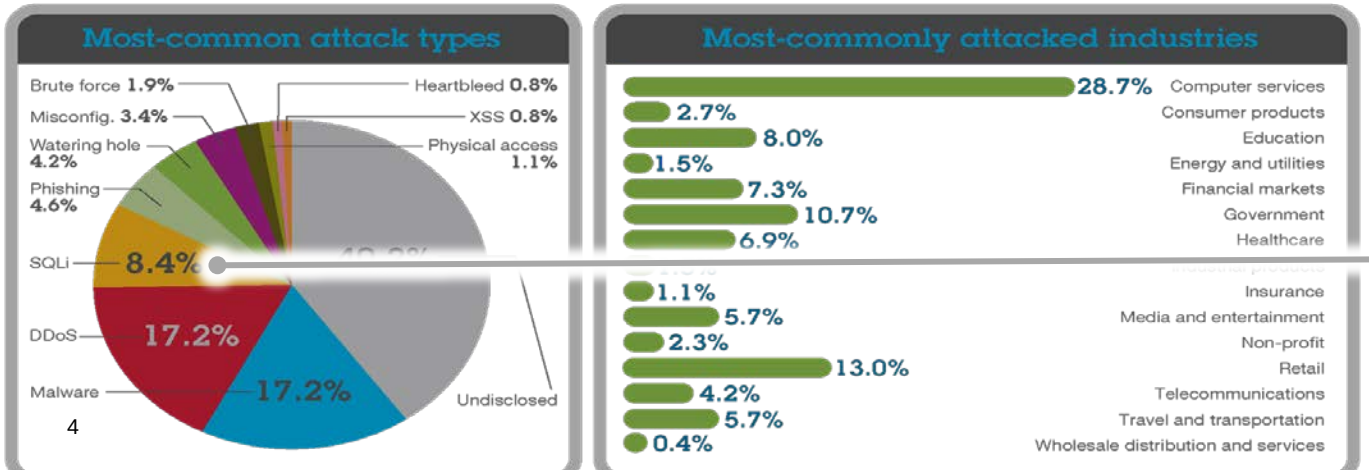
- SQL injection
- Spear phishing
- DDoS
- Third-party software
- Physical access
- Malware
- XSS
- Watering hole
- Undisclosed

Note: Size of circle estimates relative impact of incident in terms of cost to business.

Источник: IBM X-Force® Research 2014 Q3 Trend and Risk Report

Новые и старые методы атак





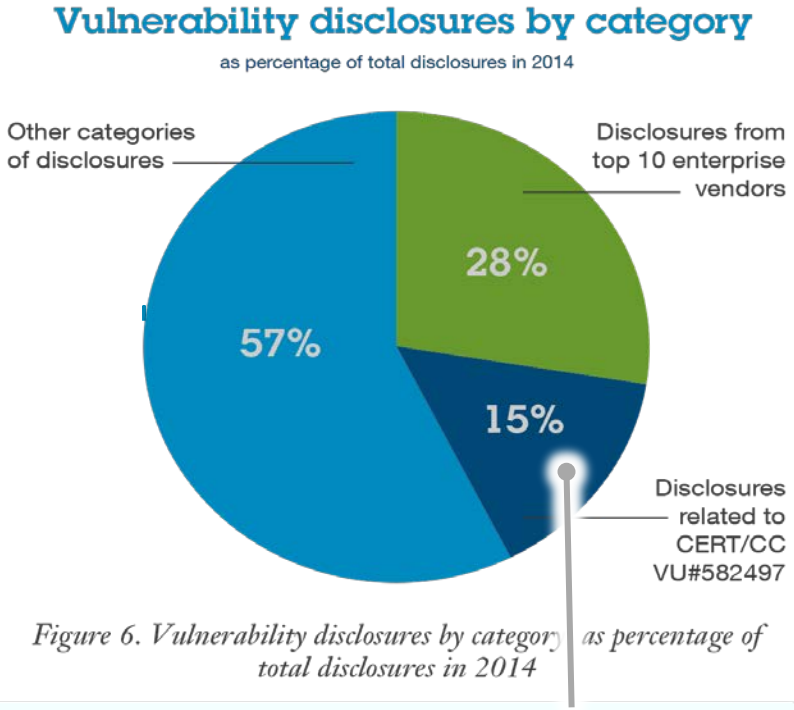


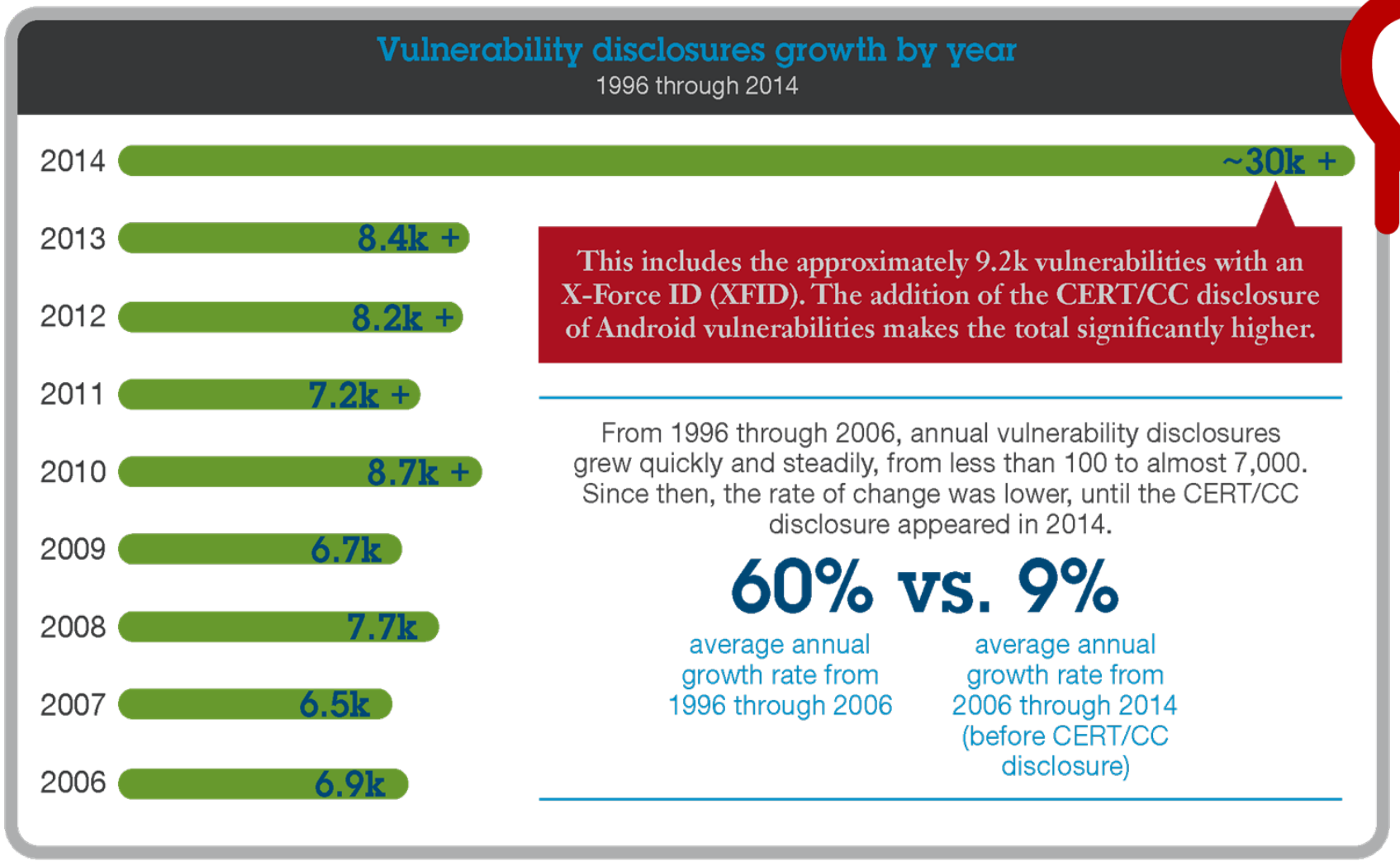
Figure 6. Vulnerability disclosures by category as percentage of total disclosures in 2014

Уязвимости для платформы Android 15% из всех уязвимостей, публично опубликованных за 2014 год

SQLi
8,4% из всех атак за прошедший 2014 год

Source: IBM X-Force 2015 Q1 Trend and Risk Report

Уязвимости в ПО – не уменьшающийся трэнд. Даже если считать только опубликованные



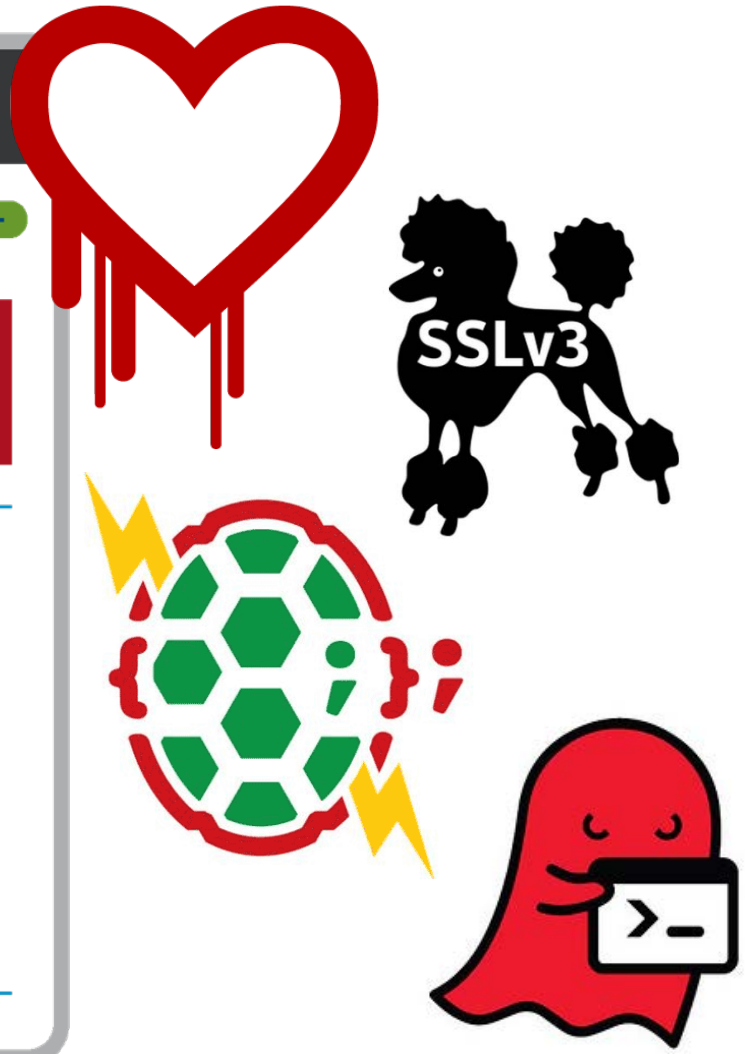


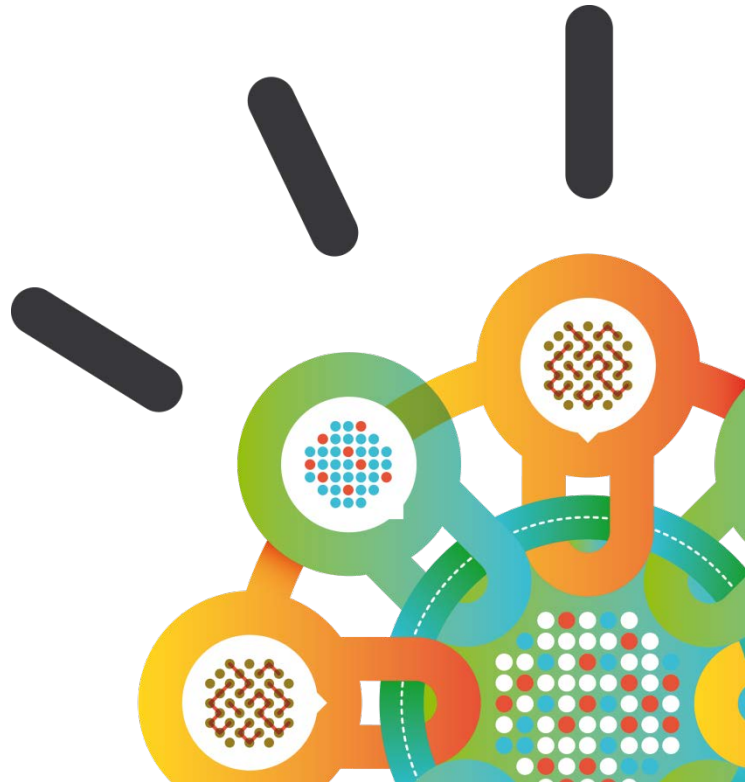
Figure 5. Vulnerability disclosures growth by year, 1996 through 2014

Source: IBM X-Force® Research and Development

Что делать?

Концепция Application Security -

«безопасность в процессе разработки»



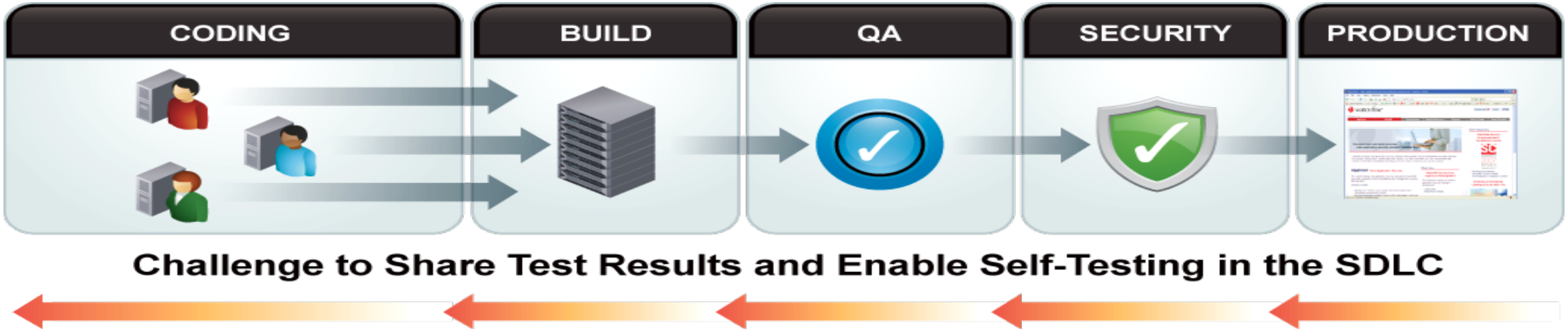
Единственный способ победить в гонке – адаптация подхода ***Secure by Design*** при проектировании и разработке приложений

- Учёт требований по ИБ в процесс разработки приложений
- Обработка уязвимостей ИБ до первода систем в продуктивную эксплуатацию
- Эффективное взаимодействие между разработчиками и безопасниками
- Видимость для руководства

Оперативный выпуск новых сервисов

Безопасные инновации

Уменьшение затрат



Обнаружение и устранение уязвимостей как можно раньше в процессе разработки ПО

Подход Secure by Design как средство экономии!

*80% затрат на разработку уходят на находжение и исправление ошибок в ПО**

Средняя цена утечки данных $7.2M**
(судебные иски, потеря доверия заказчиков, потеря доверия к бренду)

Challenge to Share Test Results and Enable Self-Testing in the SDLC

Найдена во время разработки
$80/ошибка

Найдена во время сборки
$240/ошибка

Найдена во время тестирования
$960/ошибка

Найдена при эксплуатации
$7,600 / ошибка

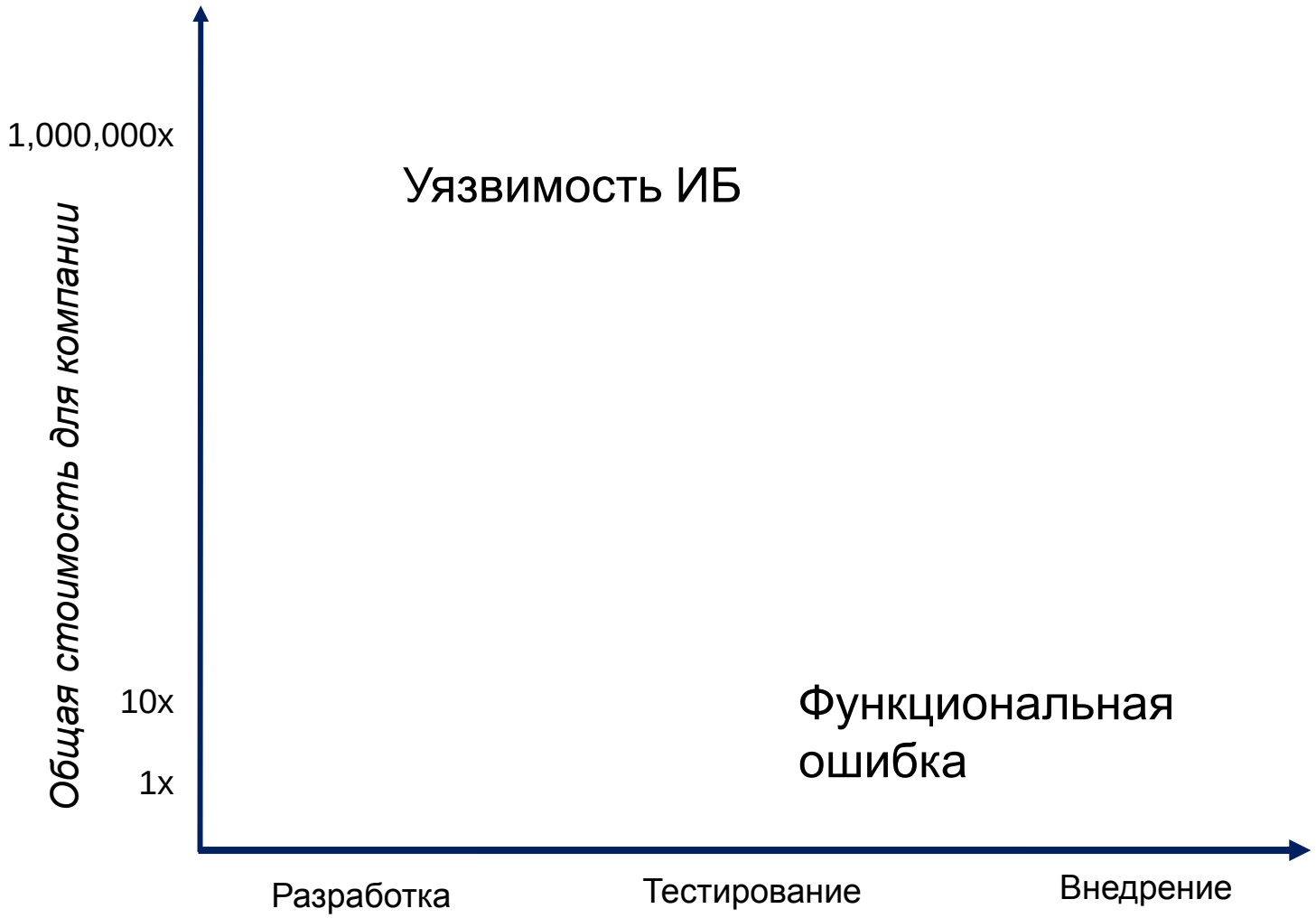
"С тех пор, как финансово мотивированные взломщики переместили свой фокус на приложения, безопасность Web-приложений стала главным вопросом дня. Тем не менее, безопасность веб-приложений не может лежать только на службе ИБ. Компании должны учитывать безопасность разработки веб-приложений как можно раньше в процессе их разработке, используя средства или услуги тестирования ПО на уязвимости."

Neil MacDonald, Gartner, 12-6-11

* Источник: National Institute of Standards and Technology

** Источник: Ponemon Institute 2009-10

Цена уязвимости ИБ — выше, чем цена обычной ошибки в ПО



Дополнительные расходы:

- Уведомление клиентов
- Штрафы
- Финансовые обязательства
- Репутация
- Цена бренда
- Стоимость восстановления

Решения IBM AppScan

как средство обеспечения подхода «безопасность в процессе разработки»

Ключевые моменты в безопасности приложений

Скорость разработки – критически важна.

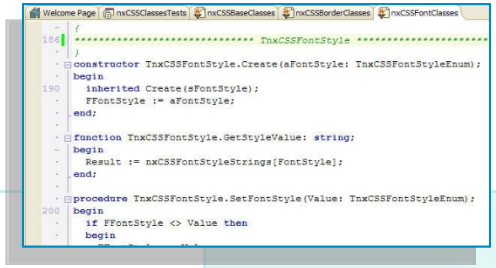
Нехватка *ресурсов* и *знаний* в области ИБ.

Фреймворк IBM в области безопасности приложений

Технологии тестирования ПО на безопасность

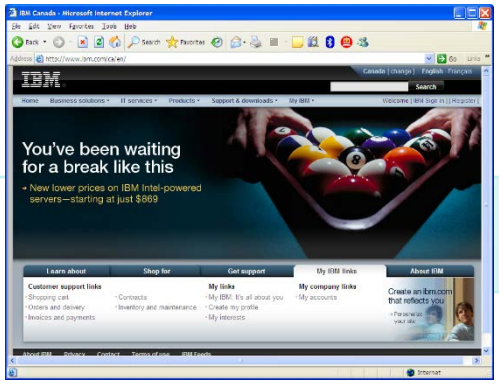
Статический анализ кода = «белый ящик»

- Смотрим на исходный код для нахождения уязвимостей ИБ



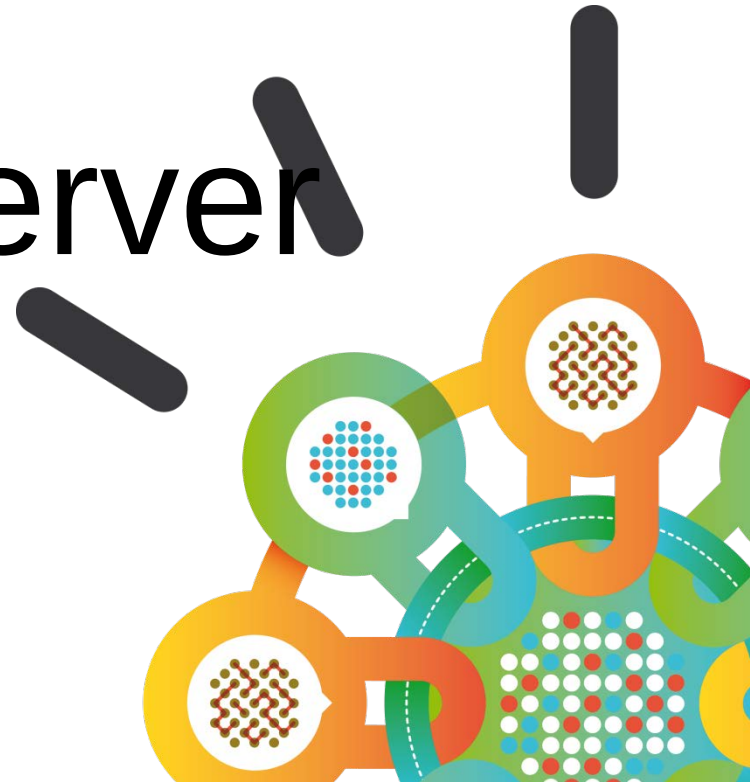
Динамический анализ = «чёрный ящик»

- Посылаем тесты в работающее приложение



AppScan Enterprise Server

Центр комплексного решения AppScan

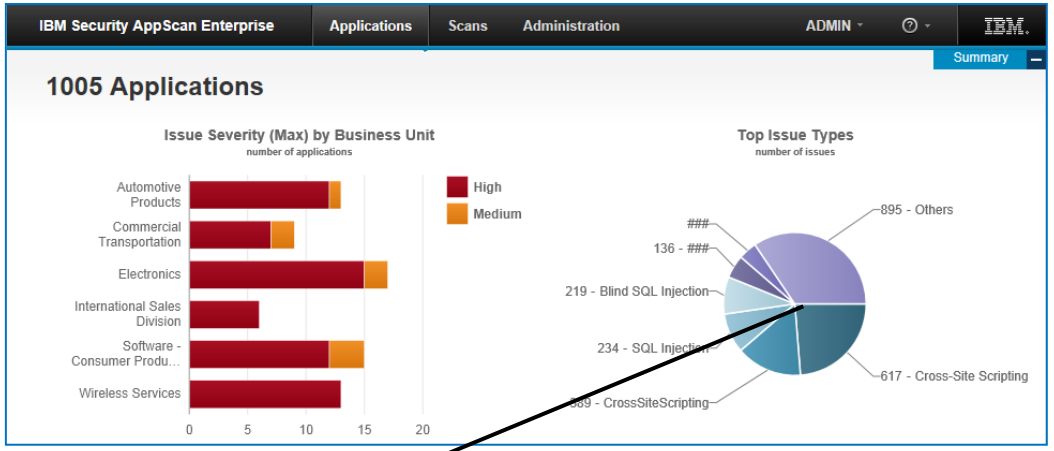


Центр решения – AppScan Enterprise Server

AppScan Enterprise Server

- Создайте список всего самописного и заказного ПО
- Приоретизируйте приложения по влиянию на бизнес
- Приоретизируйте уязвимости в контексте ПО и степени рисков
- Получите статус безопасности ПО и динамики изменений
- Получите более 40 готовых отчётов по соответствию различным стандартам

Ответ на вопрос - “Каков статус безопасности всех приложений?”



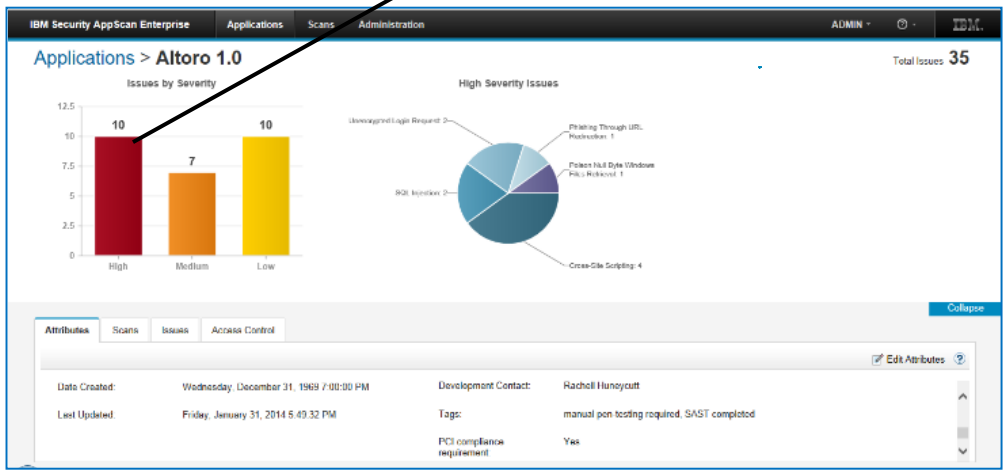
У каких приложений максимальный риск?

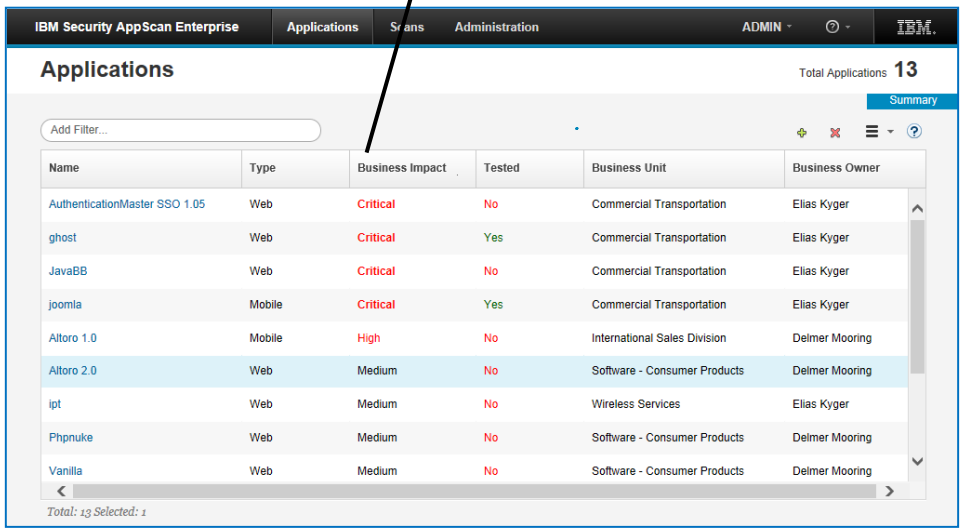
Какой процент приложений вы уже проверили?

Какие наиболее частые ошибки у ваших разработчиков?

Какие уязвимости надо закрыть первыми?

Какие из приложений — самые критичные для вас?



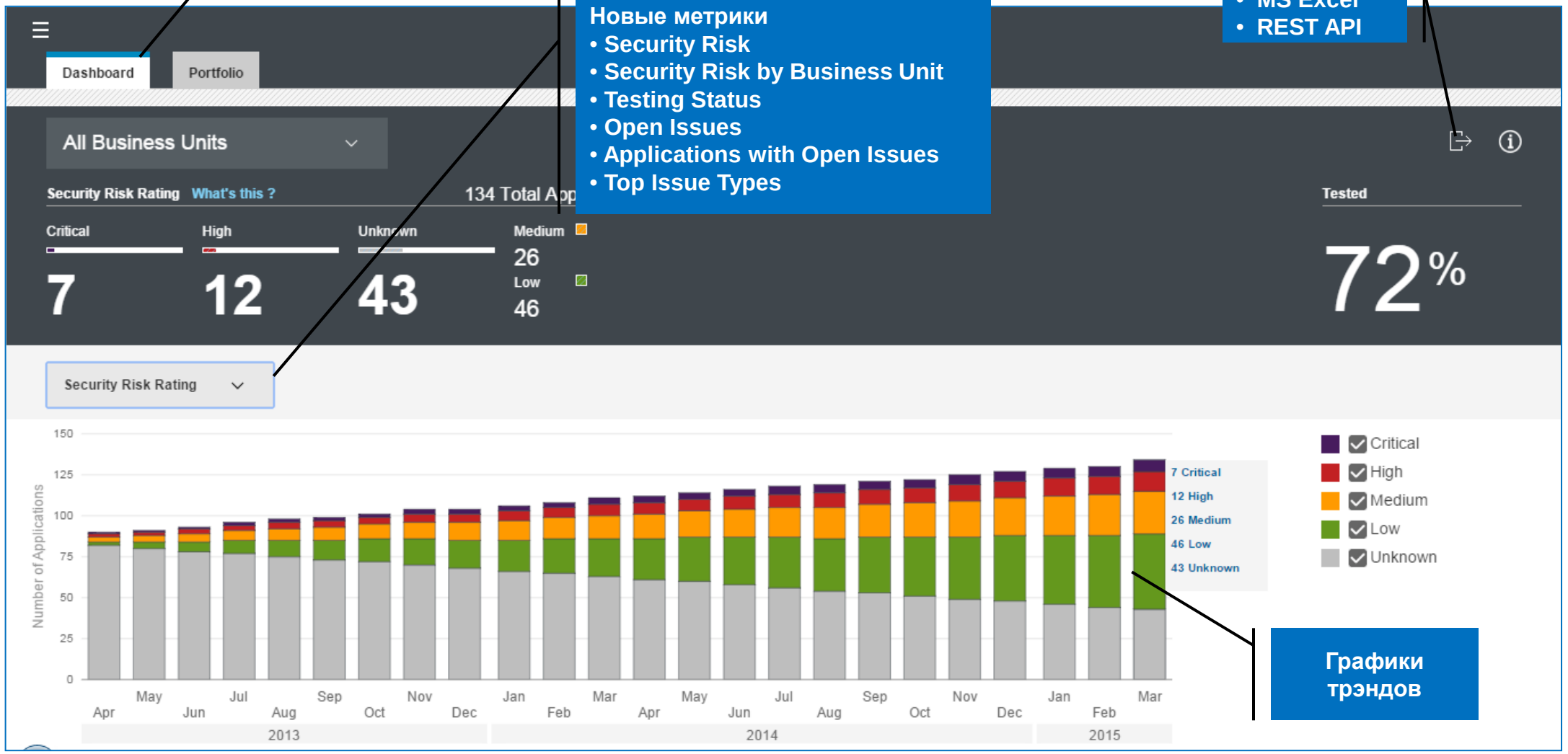


AppScan Enterprise

Новый дизайн дешбордов

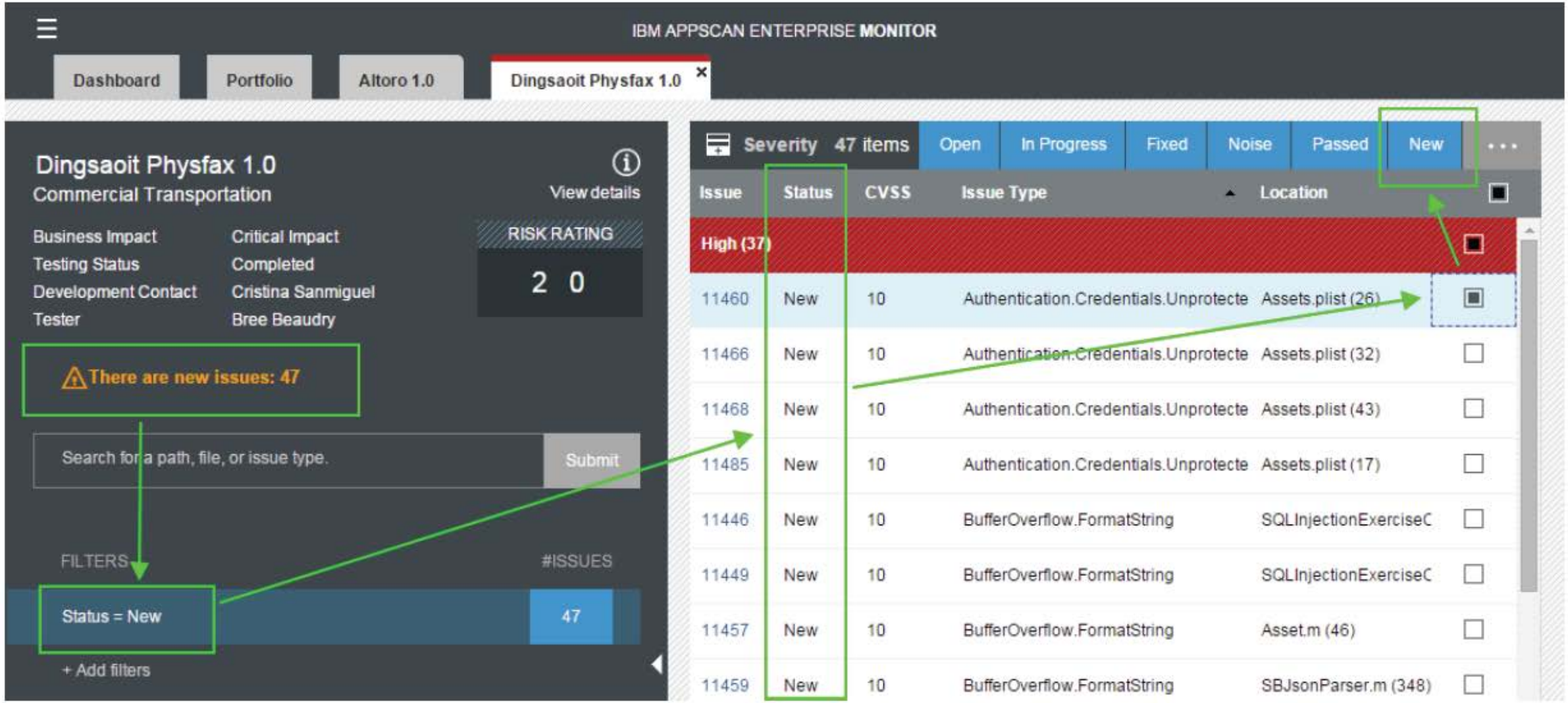
Новые метрики
- Security Risk
- Security Risk by Business Unit
- Testing Status
- Open Issues
- Applications with Open Issues
- Top Issue Types

Экспорт данных
- MS Excel
- REST API



Графики трэндов

AppScan Enterprise 9.0.2 – автоматический показ новых уязвимостей

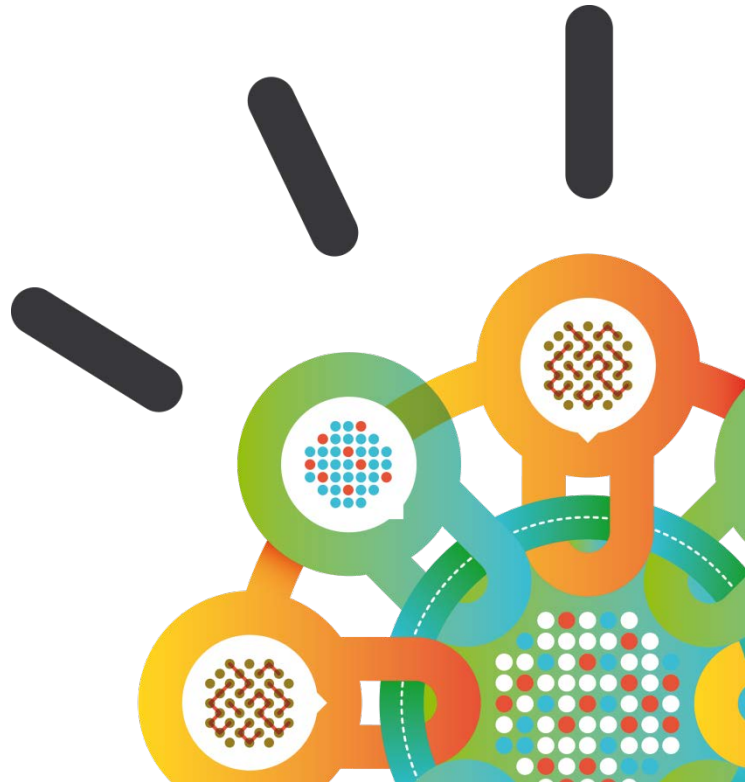


DAST

Решения по динамическому анализу

AppScan Standard

AppScan Enterprise Dynamic Analysis Scanner



Решение AppScan – Динамический анализ

Тестирование

Приложения в разработке

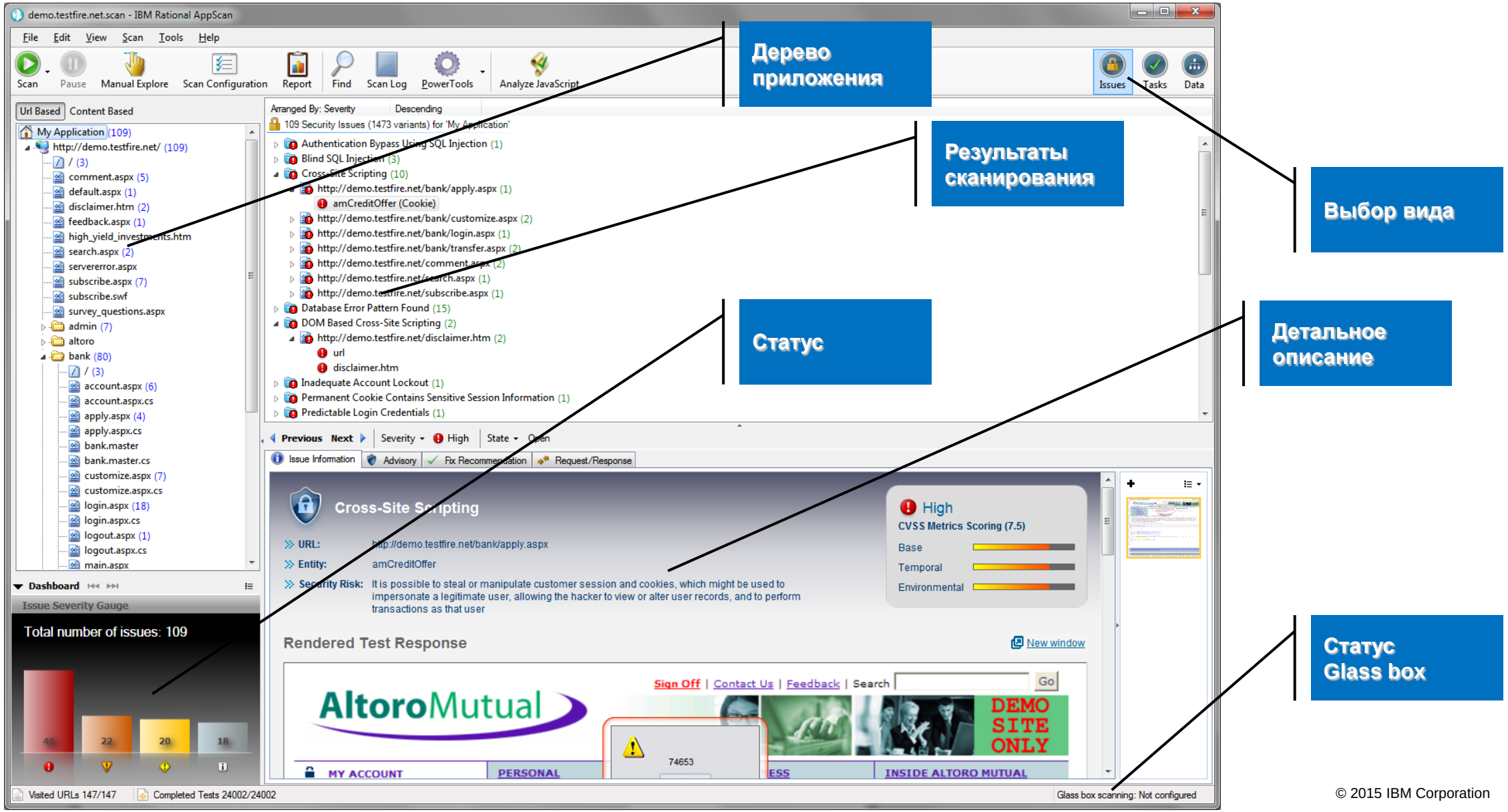
AppScan Standard

- Автоматизированный инструментарий для тестирование на проникновение
- Быстрое конфигурирование динамических тестов
- Гибкость инструментария
- Тестирование веб сервисов

AppScan Enterprise Dynamic Analysis Scanner

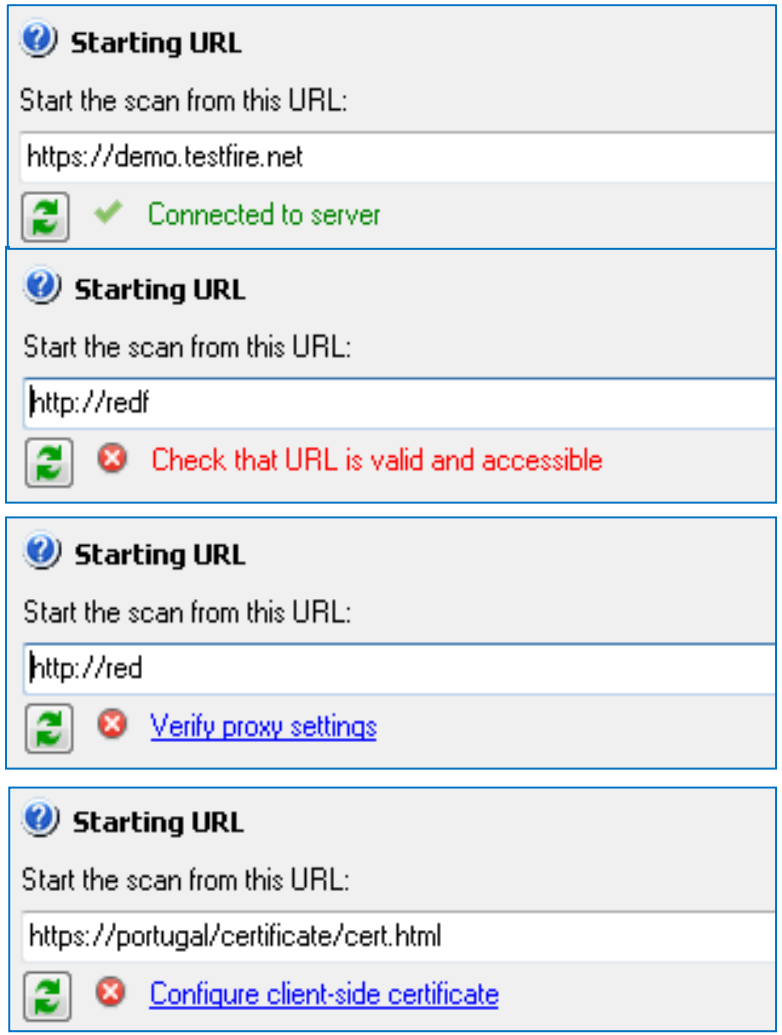
- Масштабные динамические тестирования
- Назначение политик тестирования и шаблонов на конкретных сотрудников
- Тестирование по расписанию, централизованное управление сканированиями

AppScan Standard — Простой для понимания инструмент

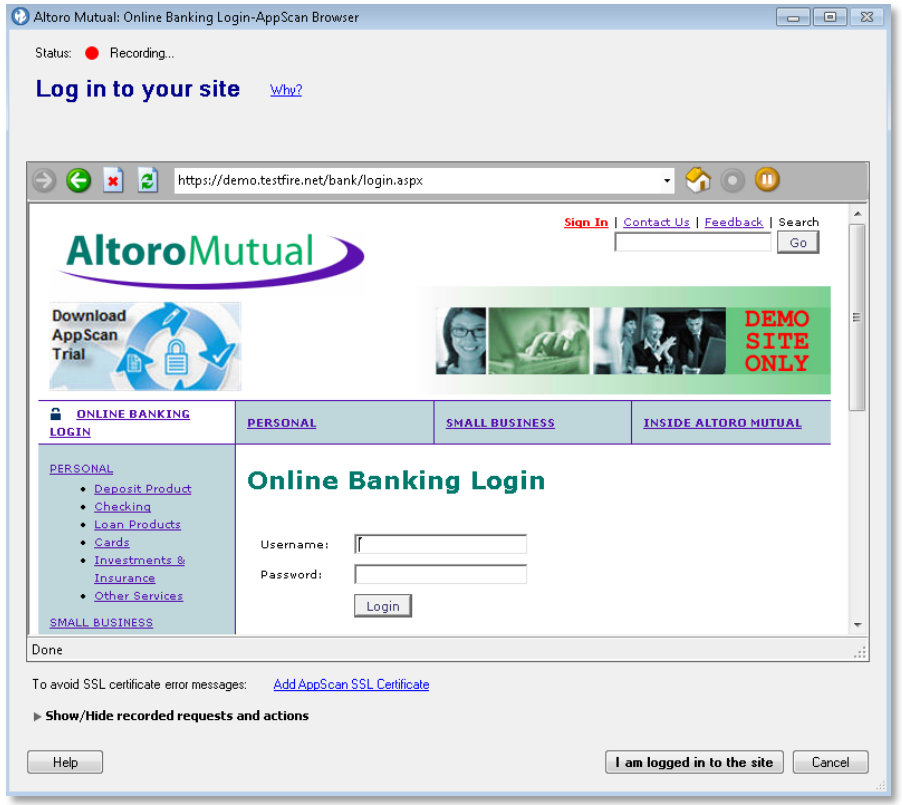


Новое в AppScan Standard – инструменте для пентестера

Проверка введённых данных “на лету”



Переработанный инструмент записи сценариев

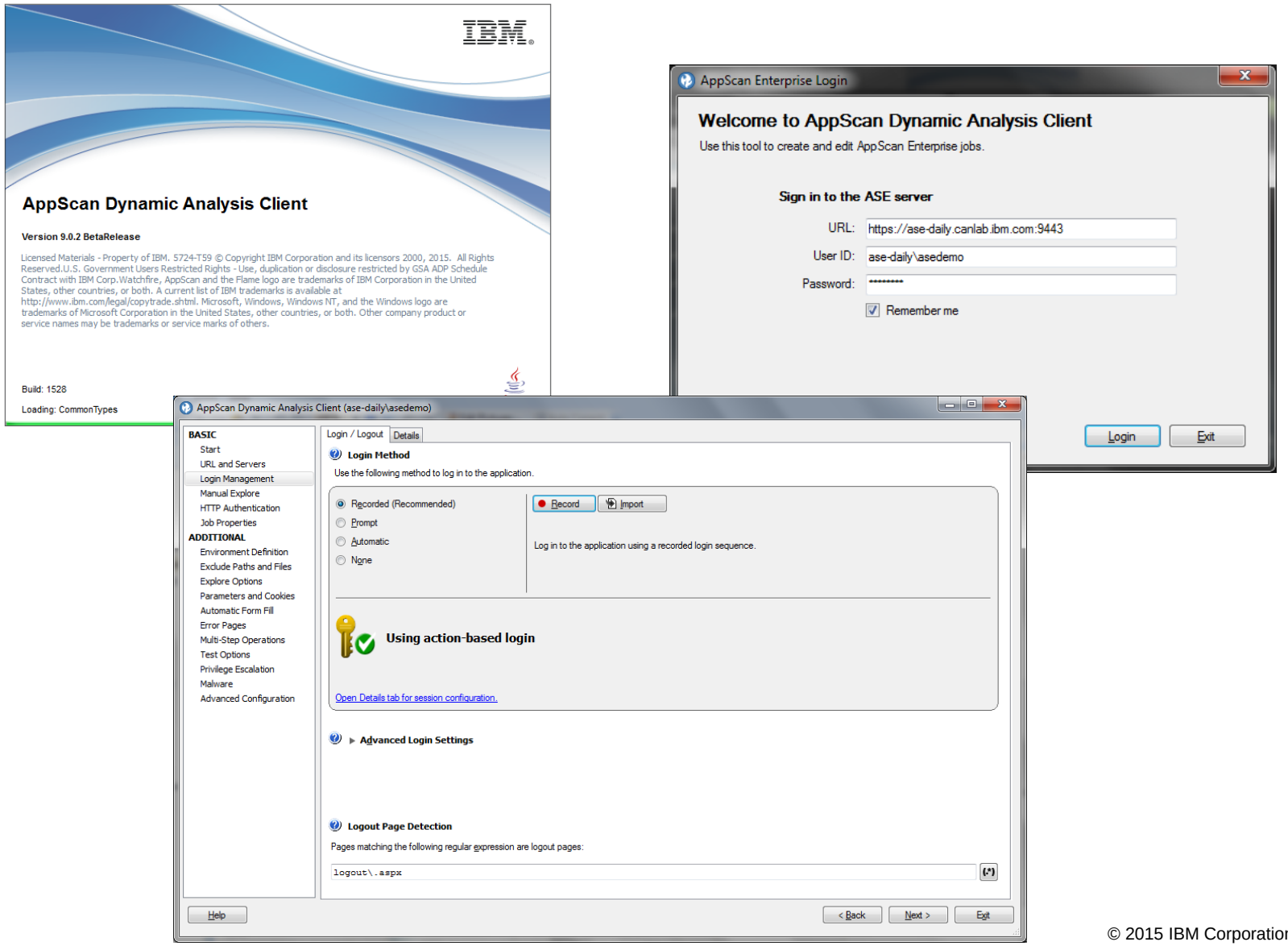


- ✓ Проще для понимания
- ✓ Подстановка SSL цепочек доверия
- ✓ Возможность показа запросов HTTP и действий браузера
- ✓ Проверка сценария логина на лету
- ✓ Лучшее распознавание шаблонов действий и предоставление подсказок по ходу работы

Новое в AppScan Enterprise DA Scanner – инструмент для разработчиков

Новый интерфейс для конфигурирования сканирований

- ✓ Основан на проверенных (простых и удобных) технологиях AppScan Standard.
- ✓ Включает настройки и конфигурации ранее недоступные для DA Scanner.
- ✓ Не требует переучиваться при переходе от AppScan Standard.



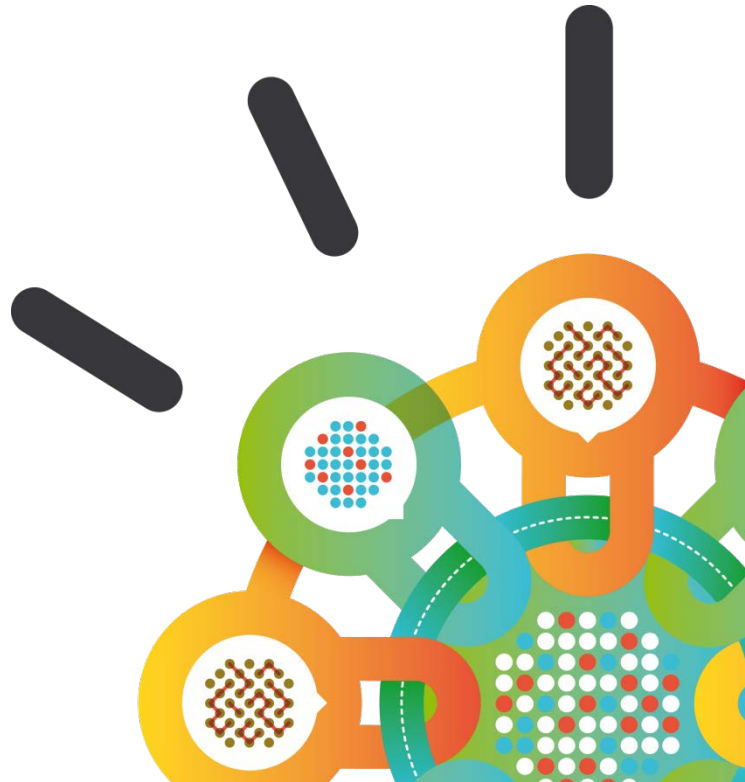
А также целый ряд новых технологий динамического тестирования в обоих продуктах

- ✓ MongoDB NoSQL Injection (Новая возможность, на текущий момент уникальная на рынке)
- ✓ Shellshock
- ✓ POODLE
- ✓ FREAK
- ✓ Deprecated SSL Version
- ✓ Link to Non-Existing Domain
- ✓ System Call Code Injection
- ✓ XML External Entity

SAST

Решения по статическому анализу

AppScan Source



Решение AppScan – Статический Анализ

Тестирование

Приложения в разработке

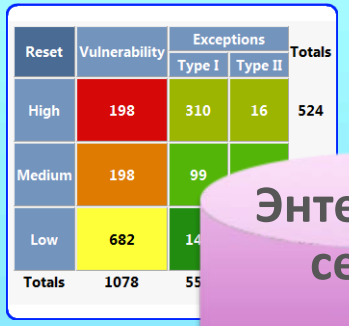
AppScan Source

- Наиболее эффективное с точки зрения стоимости решение по пезопасности ПО
- Внедрение безопасности на самых ранних стадиях цикла разработки ПО, с интеграцией в существующий инструментарий разработки
- Лучшие практики безопасности с использованием централизованного управления и политик безопасности
- Отчётность, соответствие и аудит — позволяют наладить диалог между группой разработки и группой ИБ, и поднять статус ИБ на уровень менеджмента

Компоненты IBM Security AppScan Source

Консоль аналитика

- Configure Software
- Scan
- Triage Results
- Manage Security Policies

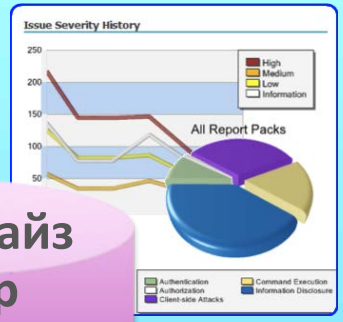


Reset	Vulnerability	Exceptions		Totals
		Type I	Type II	
High	198	310	16	524
Medium	198	99		
Low	682	14		
Totals	1078	55		

Энтерпрайз сервер

- Knowledgebase
- Assessment Database
- Custom Rules

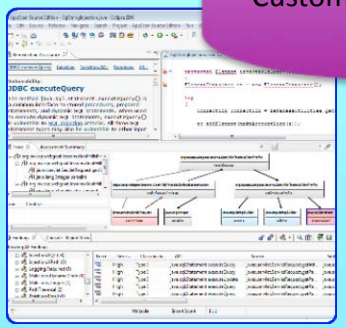
Отчёты для руководителя



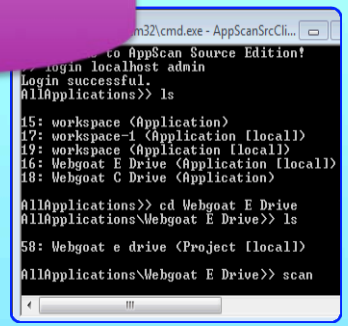
- Track Progress
- Compare Applications
- Customize Dashboards
- Manage Portfolio Risk
- Combine BB/WB results

Плагины к IDE

- Investigate Flaws
- Remediate with Guidance
- Scan
- Confirm Fix



Автоматизация



- Build integration
- Automate Scans
- ANT, Make, Maven integration
- Data Access API

27

Широкая поддержка языков программирования

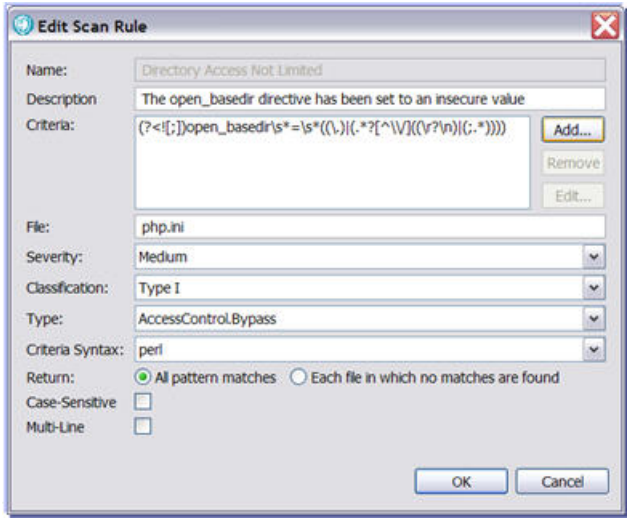
«Из коробки»

- Java
- JSP
- C
- C++
- .NET
  - C#
  - VB.NET
  - ASP.NET
- Classic ASP (VB6)
- PHP
- HTML
- Perl
- ColdFusion
- JavaScript
- VBScript
- COBOL
- PL/SQL
- T-SQL
- SAP ABAP
- *Mobile*
  - Android
  - Objective-C
  - Worklight

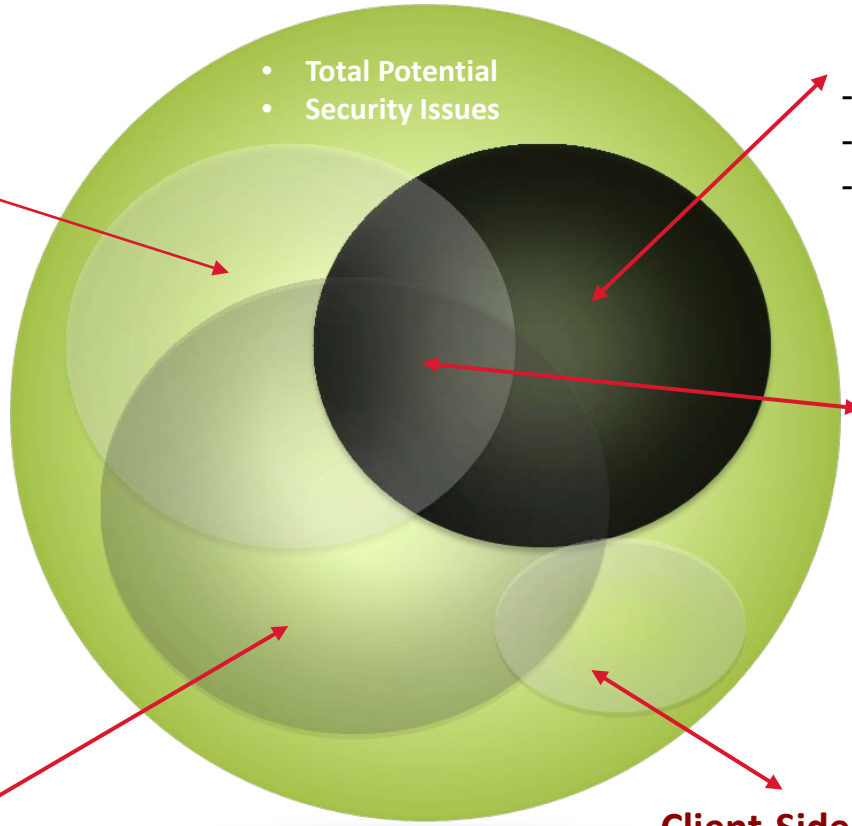
Расширяемая

Анализ регулярных выражений

- Определение собственных правил
- Использование регулярных выражений
- Ассоциирование правил с любым языком программирования



Увеличение процента найденных уязвимостей с помощью полного спектра технологий тестирования



Static Analysis

- Analyze Source Code
- Use during development
- Uses Taint Analysis / Pattern Matching

Dynamic Analysis

- Analyze Live Web Application
- Use during testing
- Uses HTTP tampering

Hybrid Analysis

- Correlate Dynamic and Static results
- Assists remediation by identification of line of code

Run-Time Analysis

- Combines Dynamic Analysis with run-time agent
- More results, better accuracy

New!

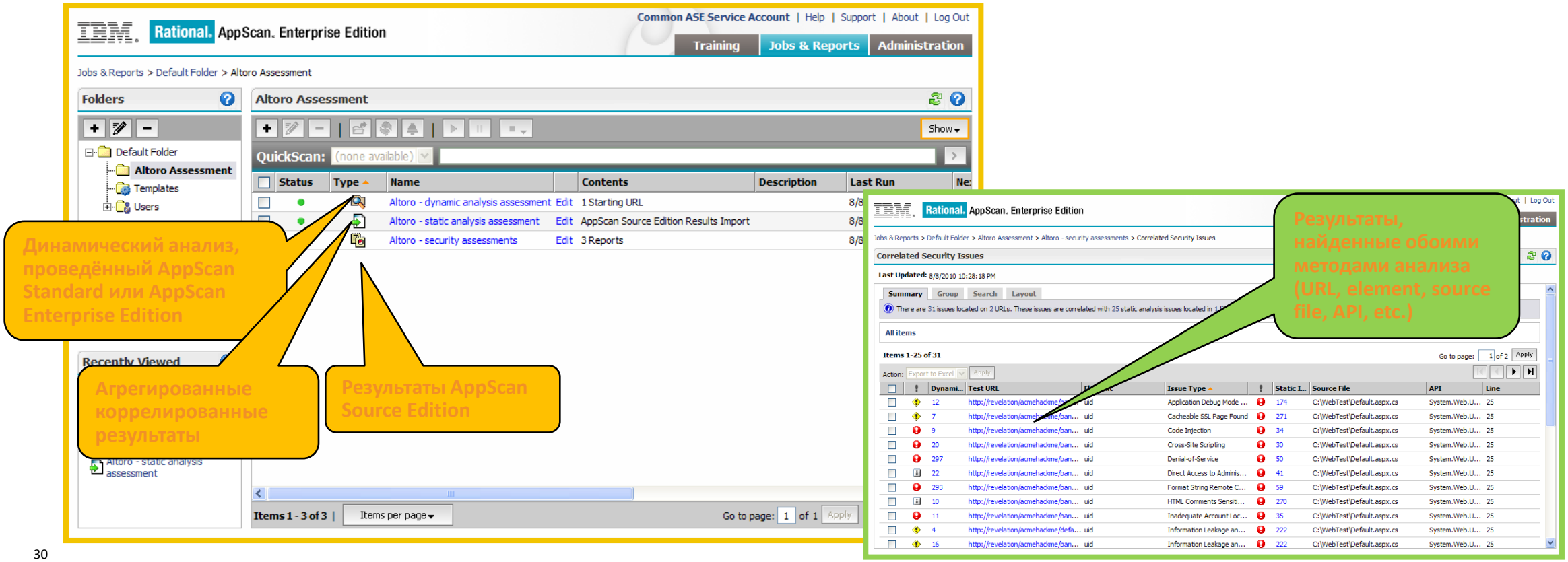
Client-Side Analysis

- Analyze downloaded Javascript code which runs in client
- Unique in the industry

New!

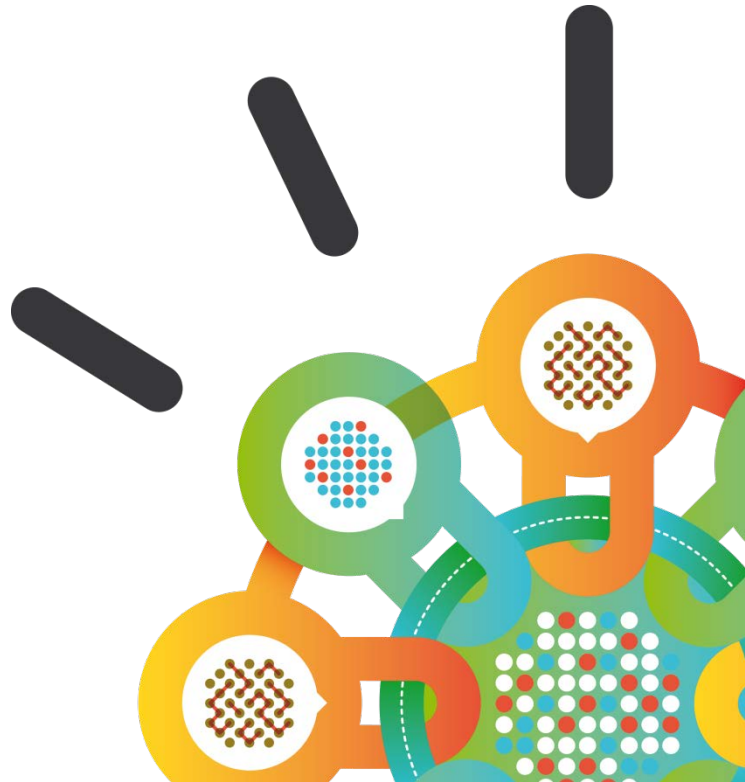
Гибридный анализ – автоматическая корреляция результатов статического и динамического анализов

- **Корреляция подходов «белого» и «чёрного» ящиков**
  - Более точные результаты, то есть мы подтверждаем валидность найденных статическим анализом уязвимостей с помощью динамического анализа
  - Помощь в приоретизации найденных уязвимостей для закрытки, то есть мы получаем подтверждение реальности проблем и метода их эксплуатации



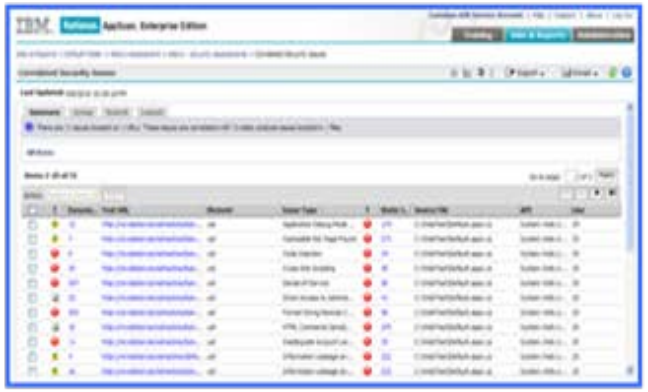
30

Интеграция



AppScan Enterprise – интеграция с QRadar

- AppScan предоставляет для Qradar данные о найденных уязвимостях ИБ в приложениях
- Позволяет лучше обнаруживать и приоритизировать инциденты информационной безопасности, в том числе проактивно работать с уязвимыми ресурсами
- Позволяет создавать более точную оценку рисков для всего списка ресурсов в QRadar SIEM
- Позволяет QRadar SIEM обнаруживать и приоретизировать угрозы ИБ с помощью корреляции в реальном времени с результатами срабатывания систем IPS/IDS

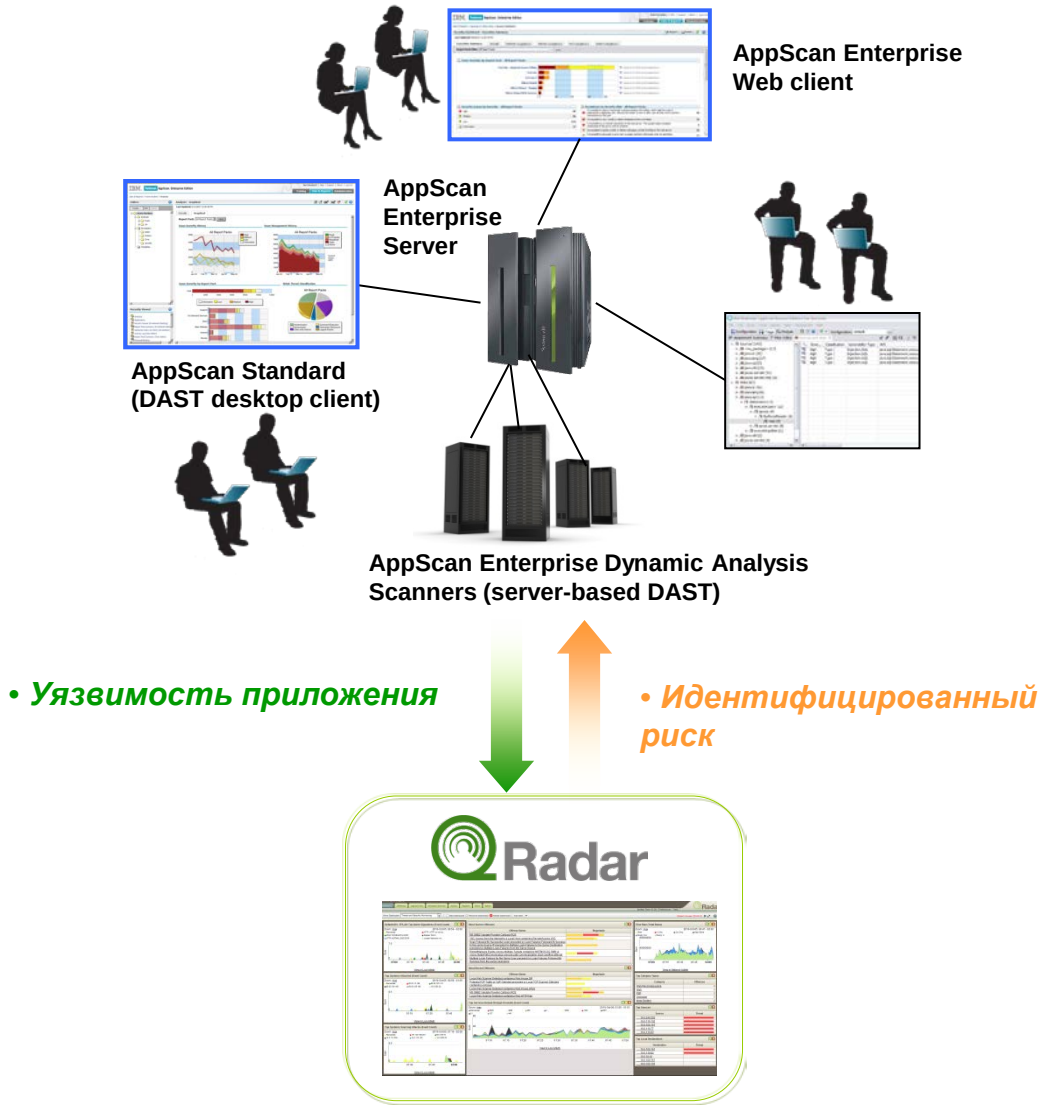


AppScan

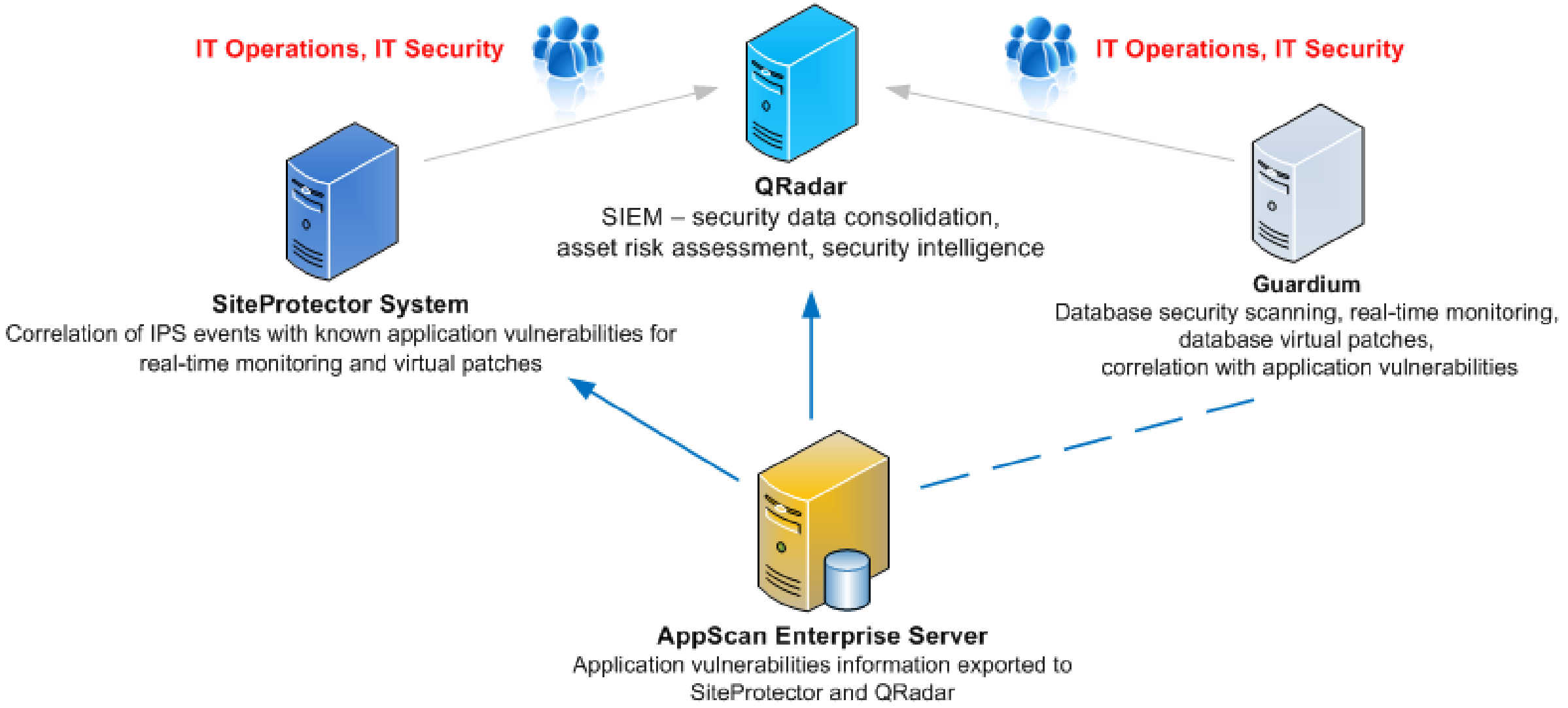
QRadar

QRadar Vulnerability Manager + App Scan (DAST) = полное видение уязвимостей

- Сканер QVM:
  - Сканирование сетевых ресурсов
  - Сканирование веб ресурсов и баз данных без логина
- IBM AppScan (DAST):
  - Подробное сканирование веб приложений с возможностью логина
- Бесшовная интеграция базы данных уязвимостей IBM AppScan в QVM
- Уязвимости, найденные AppScan используются наравне с найденными QVM во всех отчётах, дэшбордах и прочих возможностях работы с уязвимостями QRadar
- QVM позволяет накладывать сетевые потоки, контексты безопасности и угроз на уязвимости, полученные от IBM AppScan



Интеграция с IBM Security Systems SiteProtector, QRadar, Guardium



Не наступайте на грабли дважды…