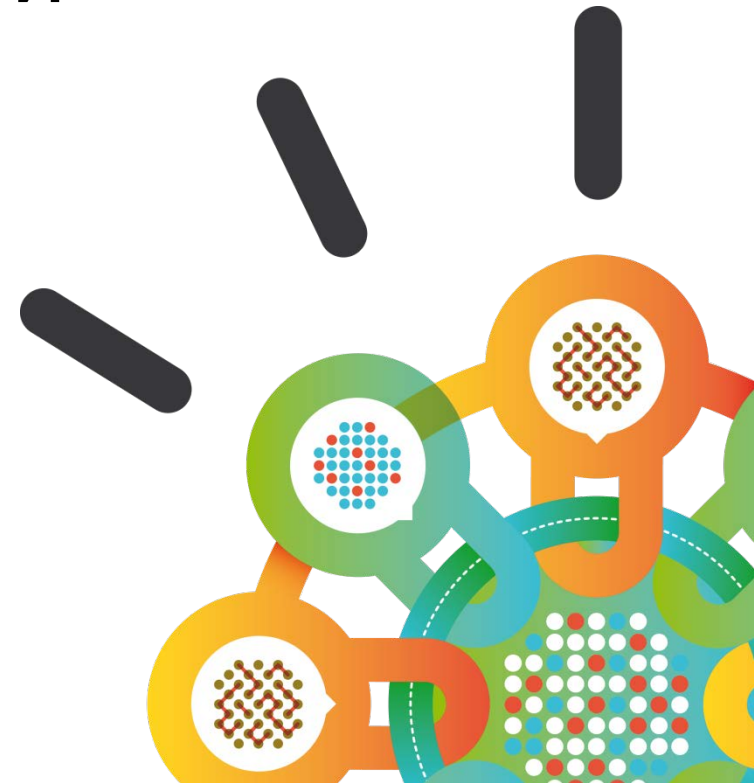


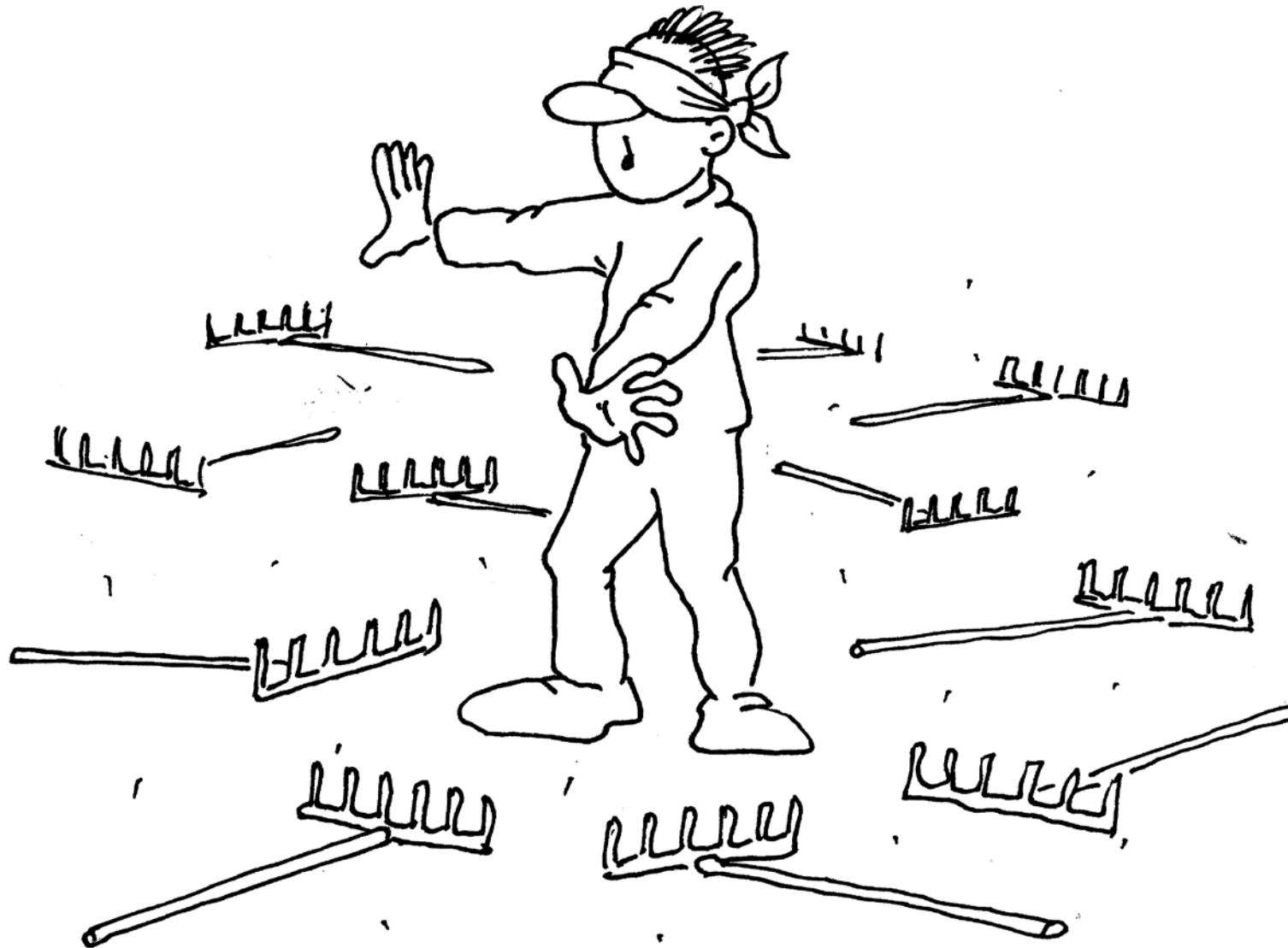
Security Intelligence.
Think Integrated.

Безопасность платежных сервисов с момента зарождения идеи

Антон Менчиц
IBM Security



Опять те же грабли...



Целевые атаки становятся всё популярнее и популярнее

Operational Sophistication

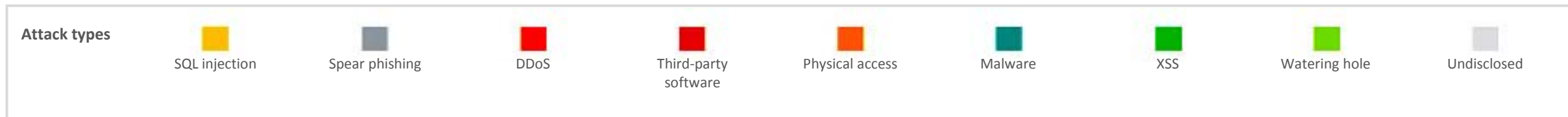
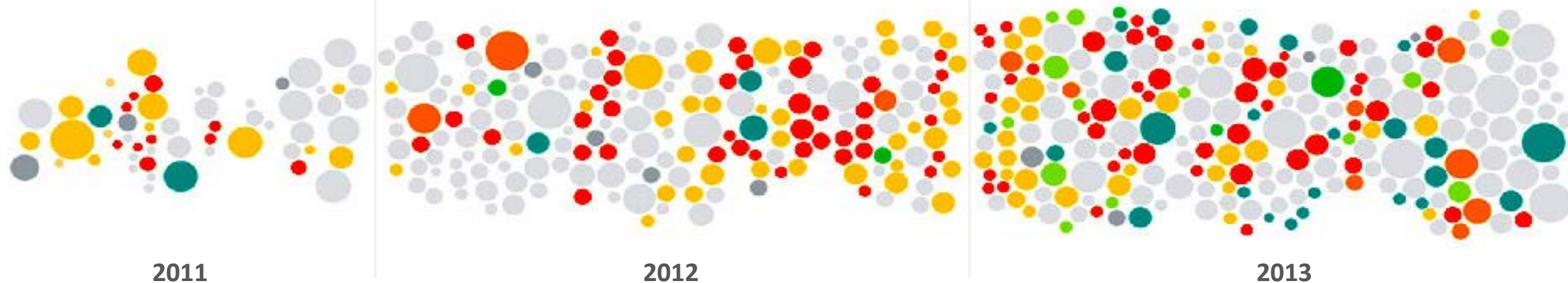
IBM X-Force® declared
Year of the Security Breach

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

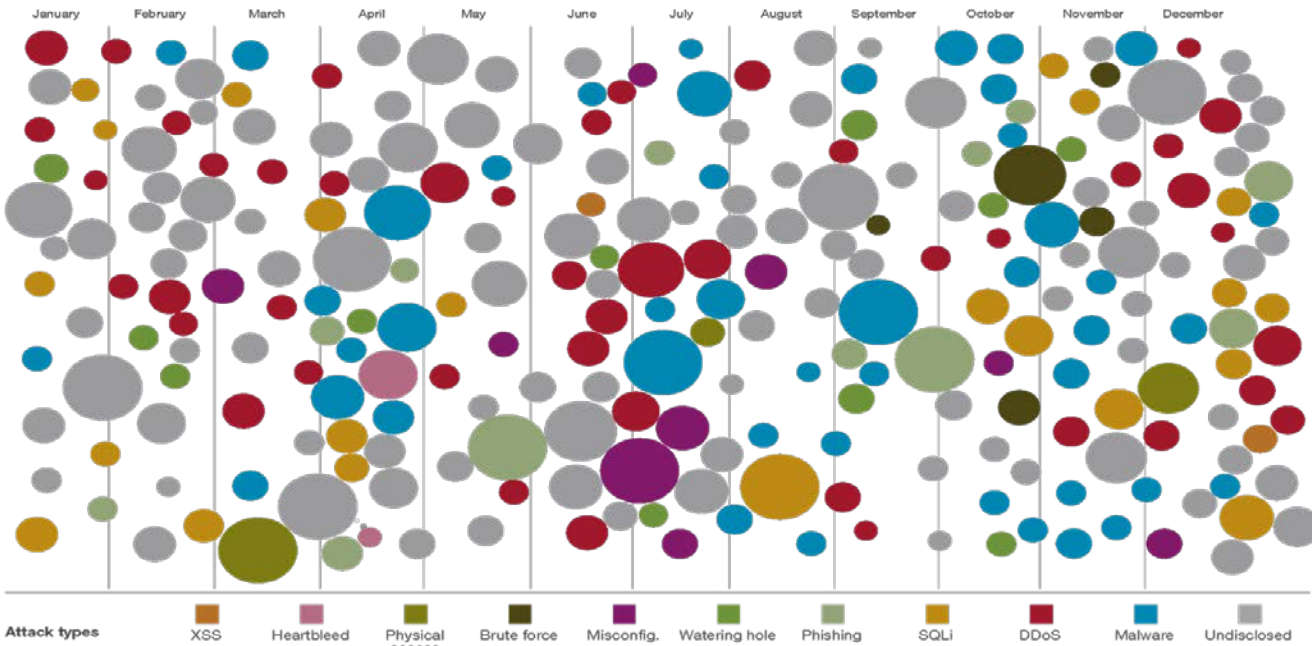


Note: Size of circle estimates relative impact of incident in terms of cost to business.

Новые и старые методы атак

Sampling of 2014 security incidents by attack type, time and impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



Vulnerability disclosures by category

as percentage of total disclosures in 2014

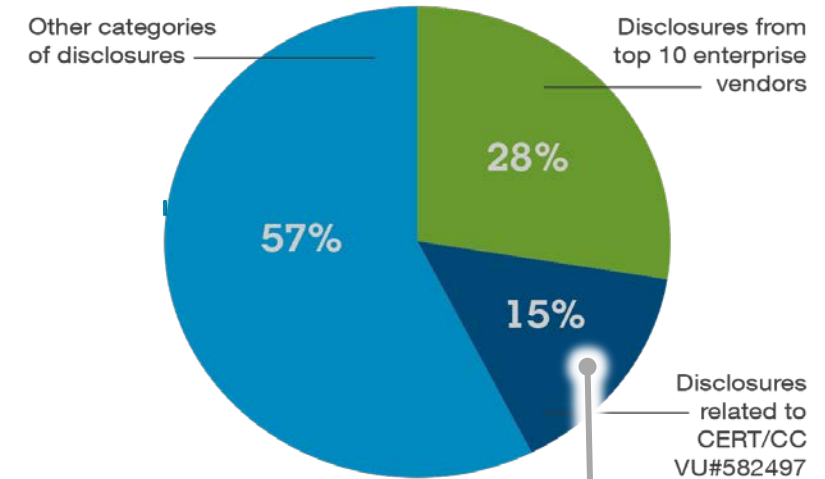
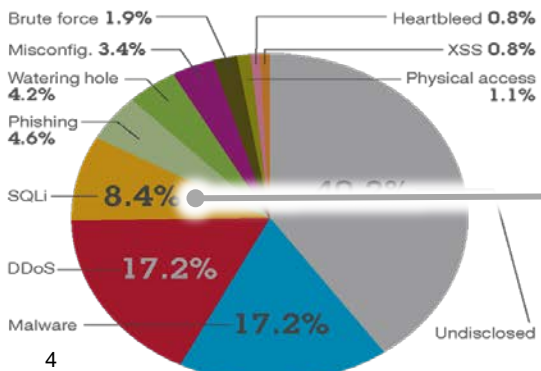


Figure 6. Vulnerability disclosures by category as percentage of total disclosures in 2014

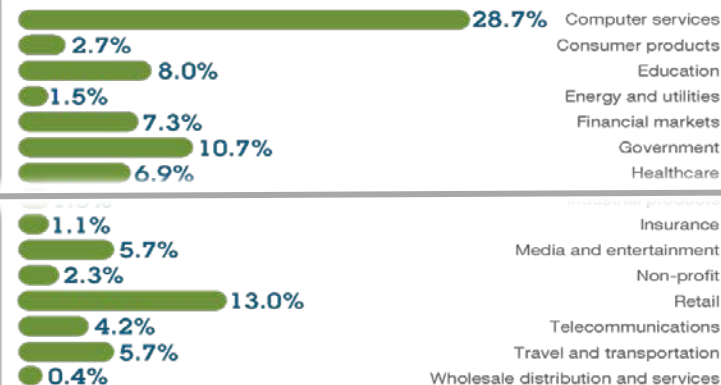
Уязвимости для платформы Android 15% из всех уязвимостей, публично опубликованных за 2014 год

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

Most-common attack types



Most-commonly attacked industries



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

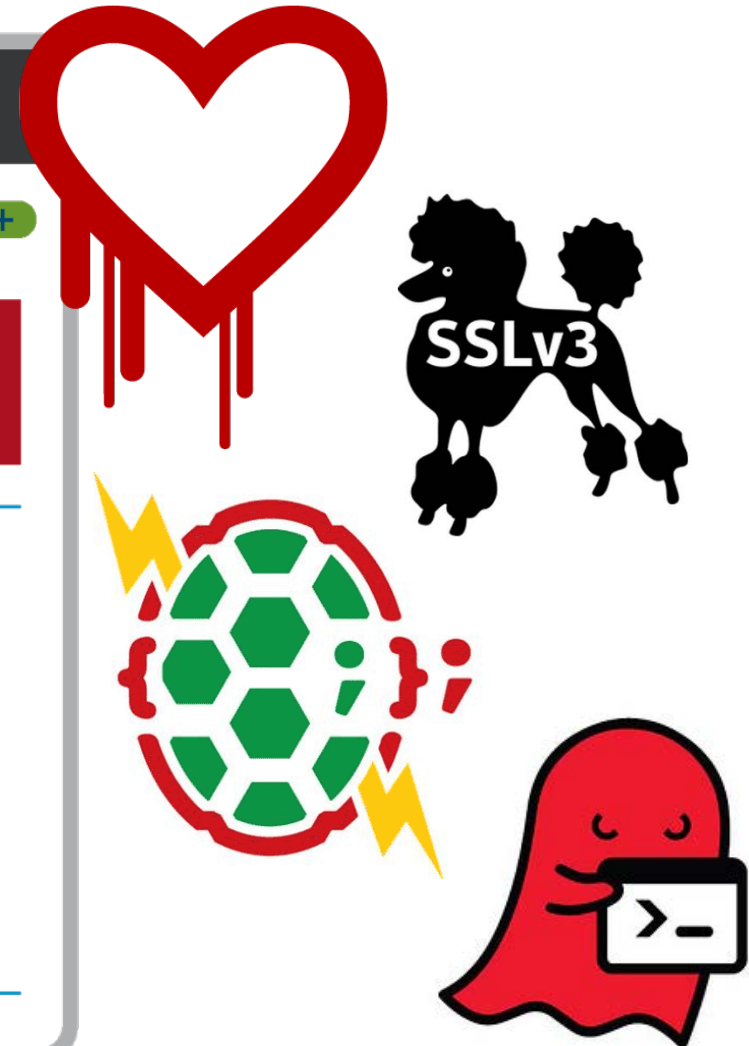
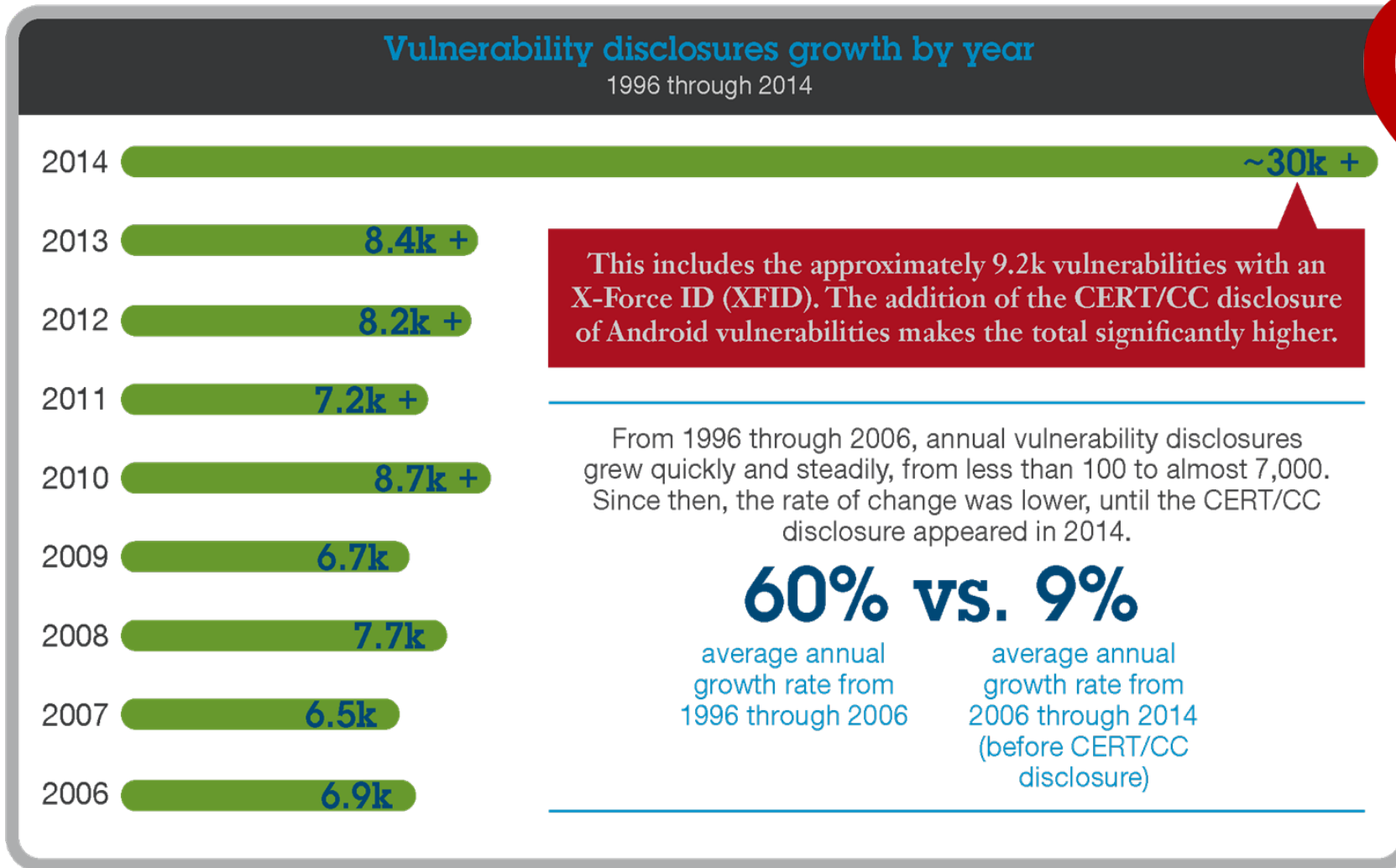
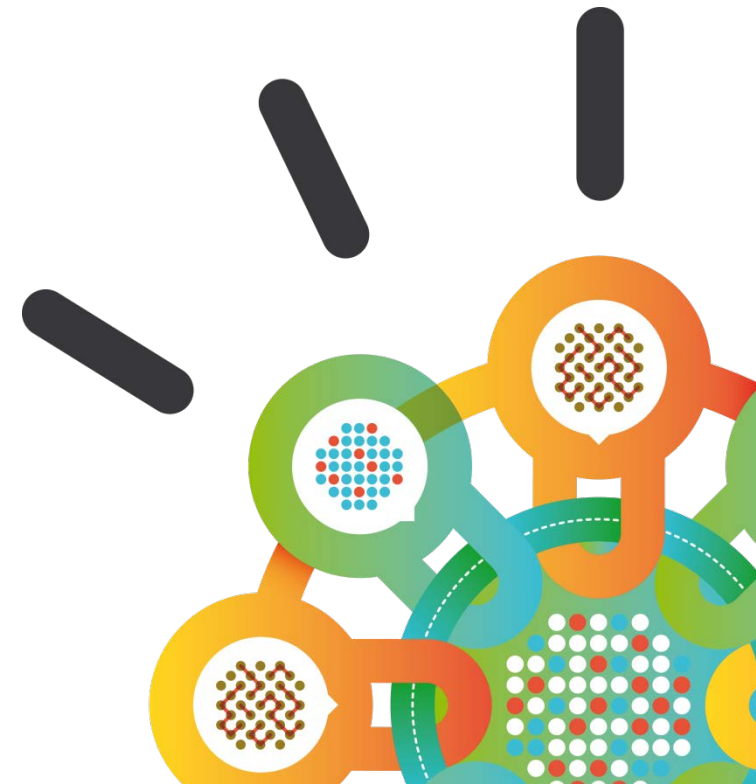


Figure 5. Vulnerability disclosures growth by year, 1996 through 2014

Что делать?

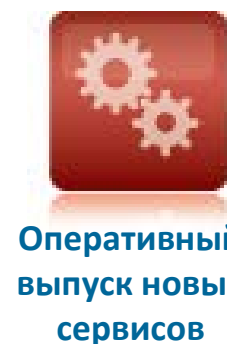
Концепция Application Security -

«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 перевода систем в продуктивную эксплуатацию
- Эффективное взаимодействие между разработчиками и безопасниками
- Видимость для руководства



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

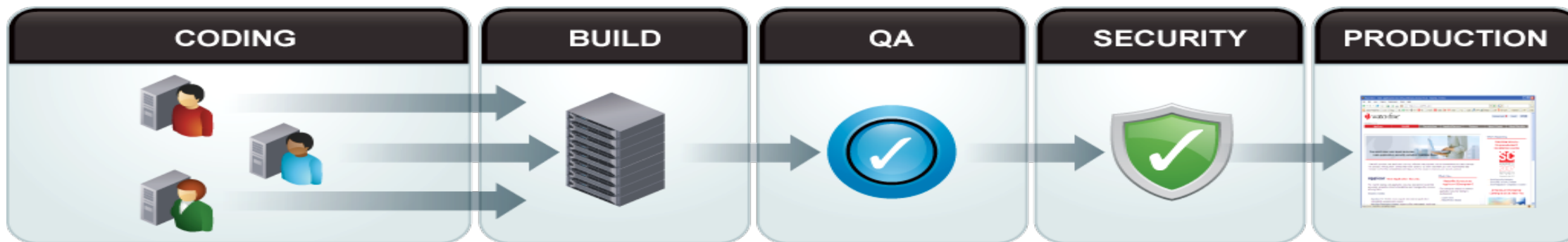


Обнаружение и устранение уязвимостей как можно раньше в процессе разработки ПО

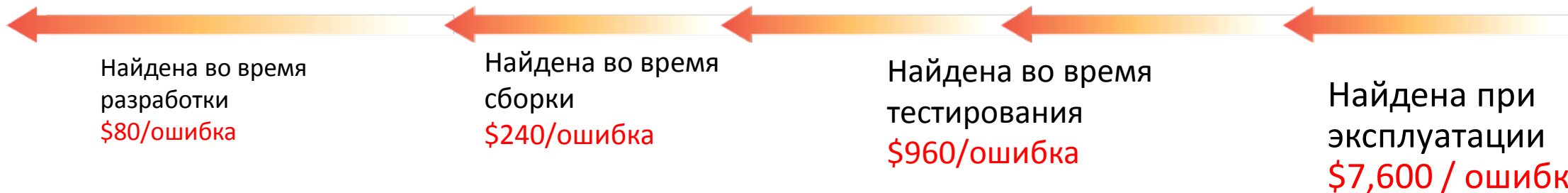
Подход Secure by Design как средство экономии!

80% затрат на разработку уходят на нахождение 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



“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

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

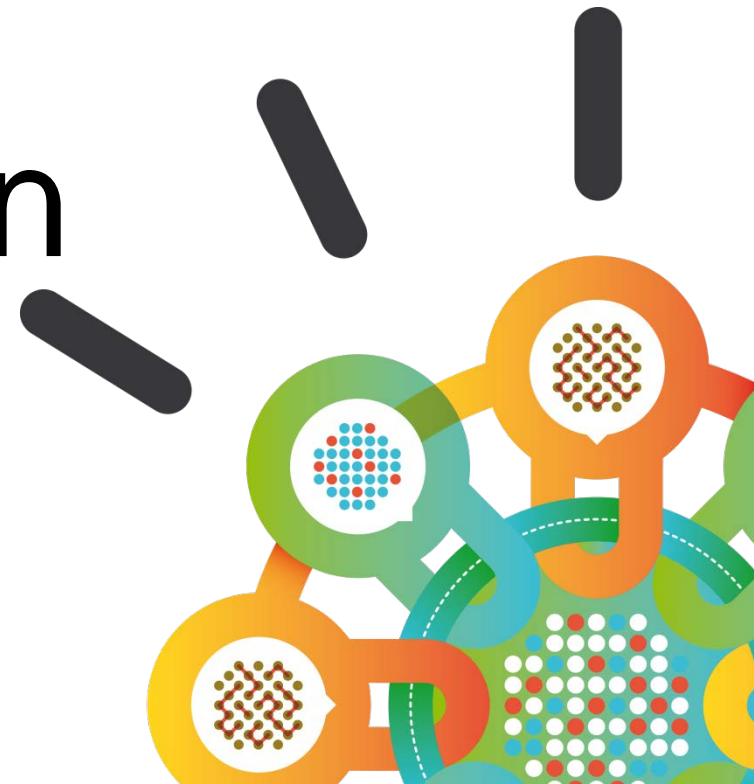


Дополнительные
расходы:

- 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.*

Важно!

IBM Security Systems

*Нехватка
ресурсов и
знаний в
области ИБ.*

Обязательно!

IBM Security Systems

Фреймворк IBM в области безопасности приложений



Технологии тестирования ПО на безопасность

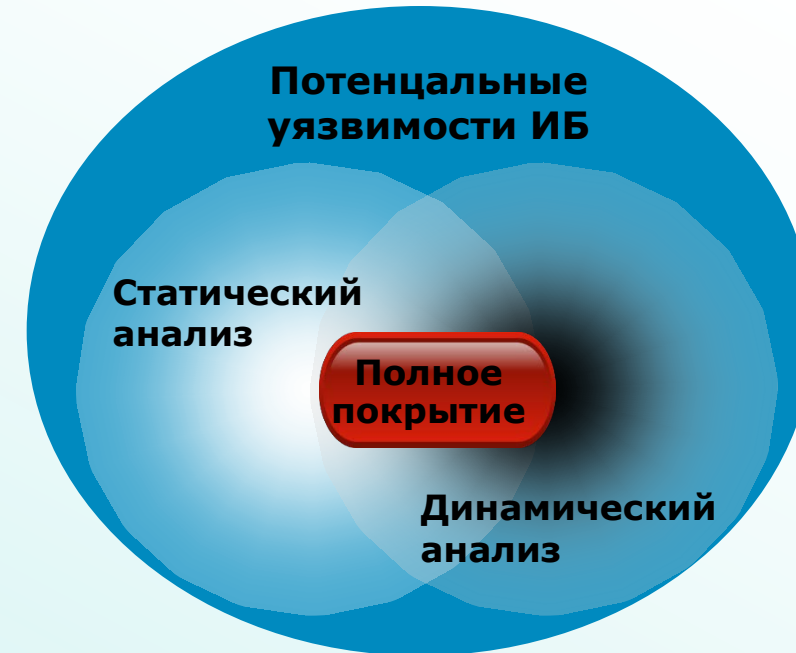
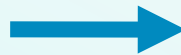
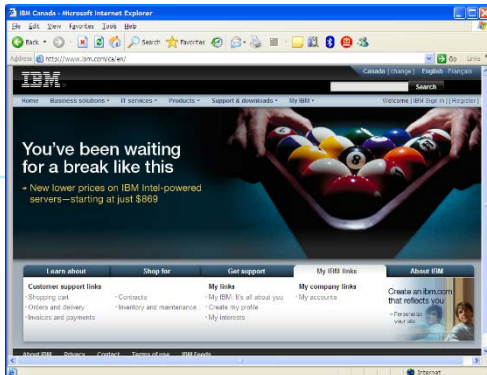
Статический анализ кода = «белый ящик»

- Смотрим на исходный код для нахождения уязвимостей ИБ

```
184 | ..... TnxCSSFontStyle .....  
|  
| constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);  
| begin  
|   inherited Create(aFontStyle);  
|   FFontStyle := aFontStyle;  
| end;  
|  
| function TnxCSSFontStyle.GetStyleValue: string;  
| begin  
|   Result := nxCSSFontStyleStrings[FontStyle];  
| end;  
|  
| procedure TnxCSSFontStyle.SetFontStyle(Value: TnxCSSFontStyleEnum);  
| begin  
|   if FFontStyle <> Value then  
|     begin
```

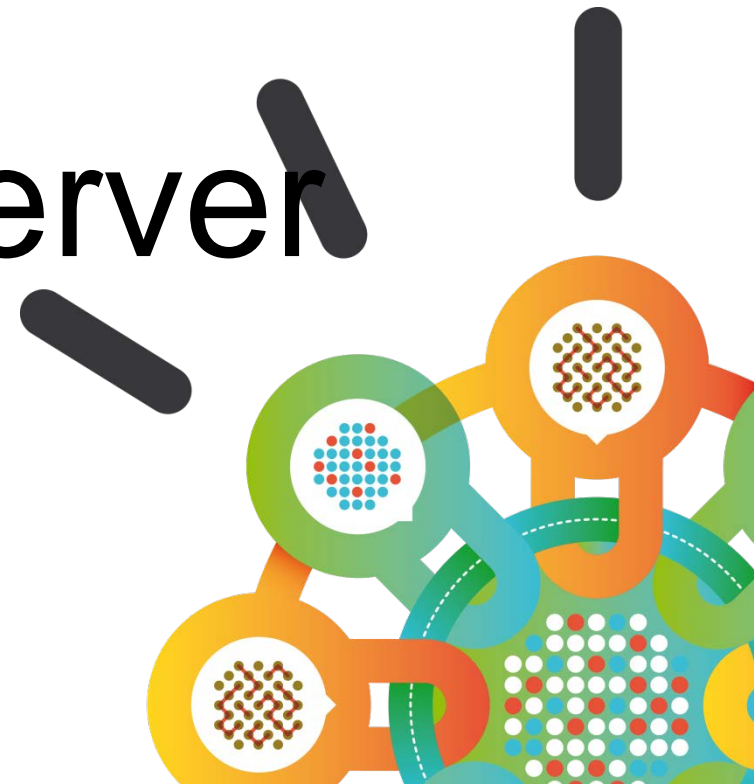
Динамический анализ = «чёрный ящик»

- Посылаем тесты в работающее приложение



AppScan Enterprise Server

Центр комплексного решения AppScan



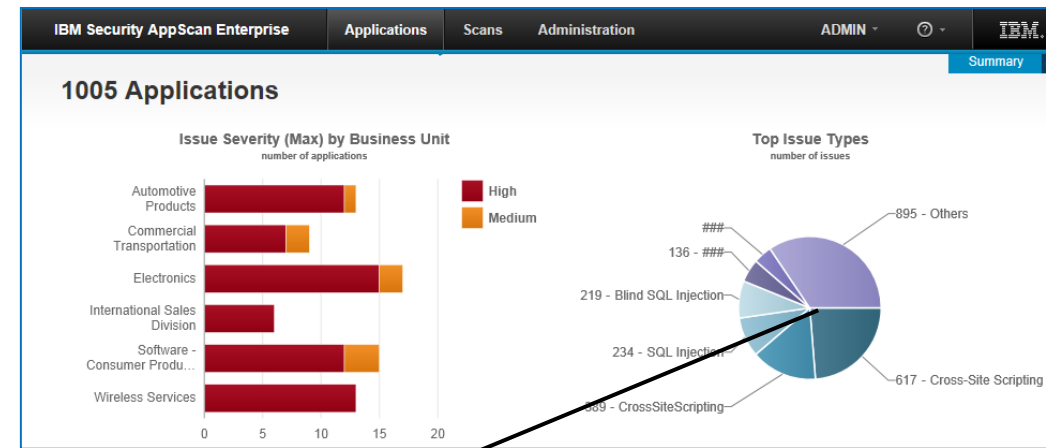
Центр решения – AppScan Enterprise Server



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?"



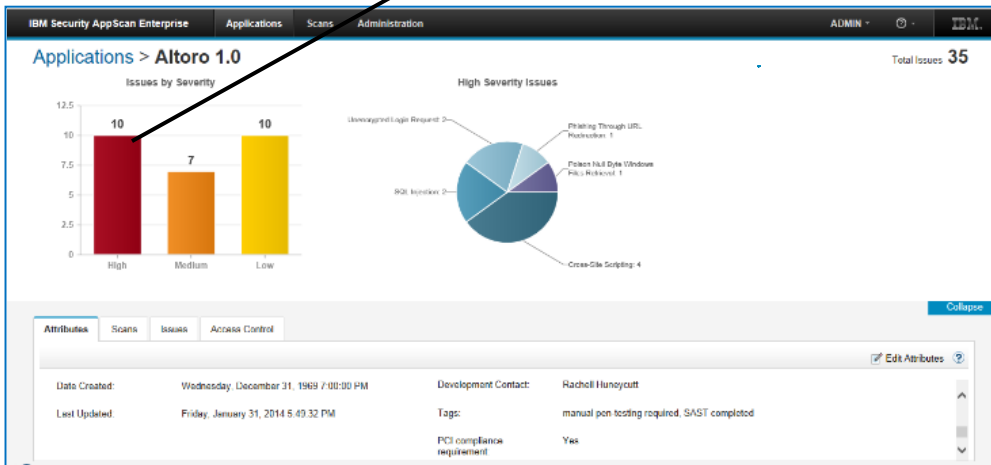
У каких приложений максимальный риск?

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?

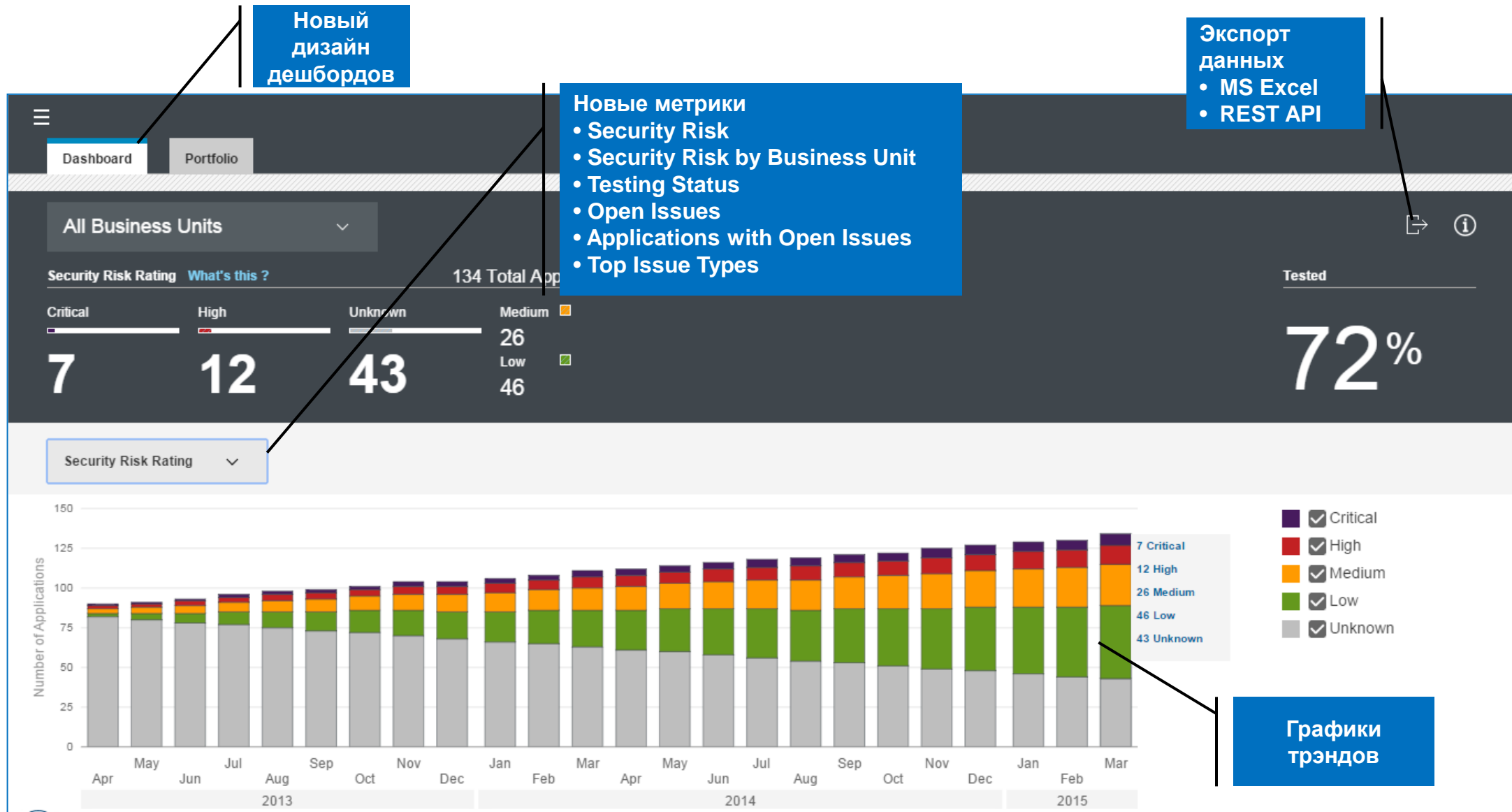


Applications
Total Applications: 13

Name	Type	Business Impact	Tested	Business Unit	Business Owner
AuthenticationMaster SSO 1.05	Web	Critical	No	Commercial Transportation	Elias Kyger
ghost	Web	Critical	Yes	Commercial Transportation	Elias Kyger
JavaBB	Web	Critical	No	Commercial Transportation	Elias Kyger
joomla	Mobile	Critical	Yes	Commercial Transportation	Elias Kyger
Altoro 1.0	Mobile	High	No	International Sales Division	Delmer Mooring
Altoro 2.0	Web	Medium	No	Software - Consumer Products	Delmer Mooring
ipt	Web	Medium	No	Wireless Services	Elias Kyger
Phpnuke	Web	Medium	No	Software - Consumer Products	Delmer Mooring
Vanilla	Web	Medium	No	Software - Consumer Products	Delmer Mooring

Total: 13 Selected: 1

AppScan Enterprise



AppScan Enterprise 9.0.2 – автоматический показ новых уязвимостей

IBM APPSCAN ENTERPRISE MONITOR

Dashboard Portfolio Altoro 1.0 **Dingsaoit Physfax 1.0** x

Dingsaoit Physfax 1.0

Commercial Transportation

Business Impact: Critical Impact
 Testing Status: Completed
 Development Contact: Cristina Sanmiguel
 Tester: Bree Beaudry

RISK RATING
2 0

There are new issues: 47

Search for a path, file, or issue type.

FILTERS #ISSUES

Status = New 47

+ Add filters

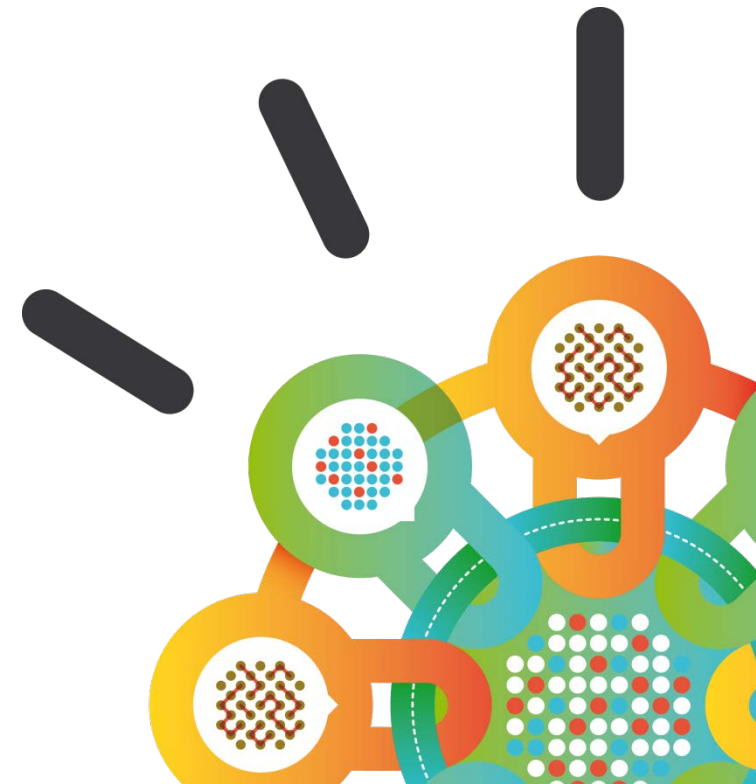
Issue	Status	CVSS	Issue Type	Location	
High (37)					
11460	New	10	Authentication.Credentials.Unprotecte	Assets.plist (26)	<input checked="" type="checkbox"/>
11466	New	10	Authentication.Credentials.Unprotecte	Assets.plist (32)	<input type="checkbox"/>
11468	New	10	Authentication.Credentials.Unprotecte	Assets.plist (43)	<input type="checkbox"/>
11485	New	10	Authentication.Credentials.Unprotecte	Assets.plist (17)	<input type="checkbox"/>
11446	New	10	BufferOverflow.FormatString	SQLInjectionExerciseC	<input type="checkbox"/>
11449	New	10	BufferOverflow.FormatString	SQLInjectionExerciseC	<input type="checkbox"/>
11457	New	10	BufferOverflow.FormatString	Asset.m (46)	<input type="checkbox"/>
11459	New	10	BufferOverflow.FormatString	SBJsonParser.m (348)	<input type="checkbox"/>

DAST

Решения по динамическому анализу

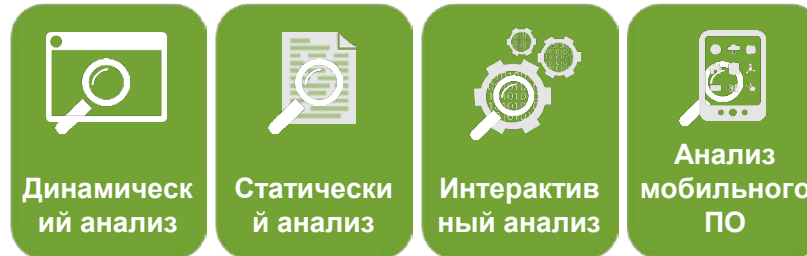
AppScan Standard

AppScan Enterprise Dynamic Analysis Scanner



Решение AppScan – Динамический анализ

Тестирование *Приложения в разработке*



AppScan Standard

- Автоматизированный инструментарий для тестирования 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

The screenshot displays the IBM Rational AppScan interface. At the top, there is a menu bar (File, Edit, View, Scan, Tools, Help) and a toolbar with icons for Scan, Pause, Manual Explore, Scan Configuration, Report, Find, Scan Log, PowerTools, and Analyze JavaScript. On the right side of the toolbar, there are buttons for Issues, Tasks, and Data.

The main area is divided into several sections:

- Left Panel:** A tree view showing the application structure under 'My Application (109)'. It lists various URLs and files, such as 'http://demo.testfire.net/' and 'bank (80)'.
- Top Center:** A list of security issues, arranged by severity (Descending). The total count is '109 Security Issues (1473 variants) for 'My Application''. Issues include 'Authentication Bypass Using SQL Injection (1)', 'Blind SQL Injection (3)', 'Cross-Site Scripting (10)', 'Database Error Pattern Found (15)', and 'DOM Based Cross-Site Scripting (2)'. A specific issue is highlighted: 'Cross-Site Scripting' at 'http://demo.testfire.net/bank/apply.aspx (1)' with a severity of 'High'.
- Bottom Center:** A detailed view of the selected 'Cross-Site Scripting' issue. It shows the URL, entity ('amCreditOffer'), and a security risk description: 'It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user...'. To the right, there is a 'CVSS Metrics Scoring (7.5)' section with a 'High' severity indicator and three bars for Base, Temporal, and Environmental metrics.
- Bottom Left:** A 'Dashboard' section with an 'Issue Severity Gauge' showing a bar chart of issue counts by severity: 49 (High), 22 (Medium), 20 (Low), and 18 (Info). It also states 'Total number of issues: 109'.
- Bottom Right:** A 'Rendered Test Response' section showing a screenshot of the 'AltoroMutual' website. A warning icon is overlaid on the page, indicating the detected issue.

Дерево приложения

Результаты сканирования

Выбор вида

Статус

Детальное описание

Статус Glass box



Новое в AppScan Standard – инструменте для пентестера

Проверка введённых данных “на лету”

Starting URL

Start the scan from this URL:



`https://demo.testfire.net`

  **Connected to server**

Starting URL

Start the scan from this URL:



`http://redf`

  **Check that URL is valid and accessible**

Starting URL

Start the scan from this URL:



`http://red`

  [Verify proxy settings](#)


Starting URL

Start the scan from this URL:

`https://portugal/certificate/cert.html`

  [Configure client-side certificate](#)

Переработанный инструмент записи сценариев

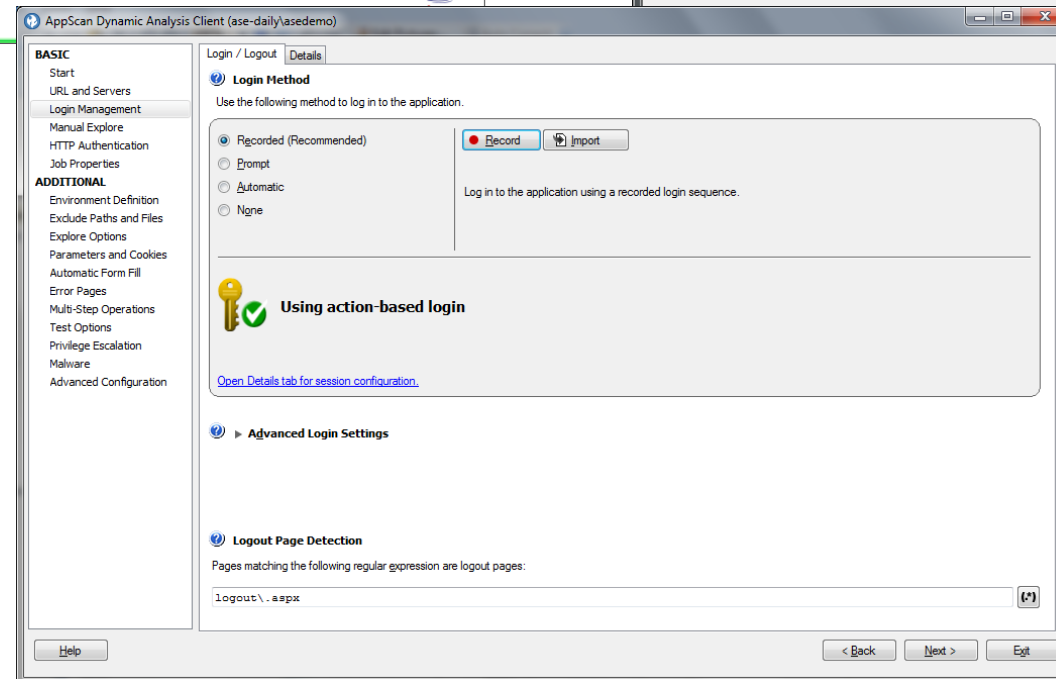
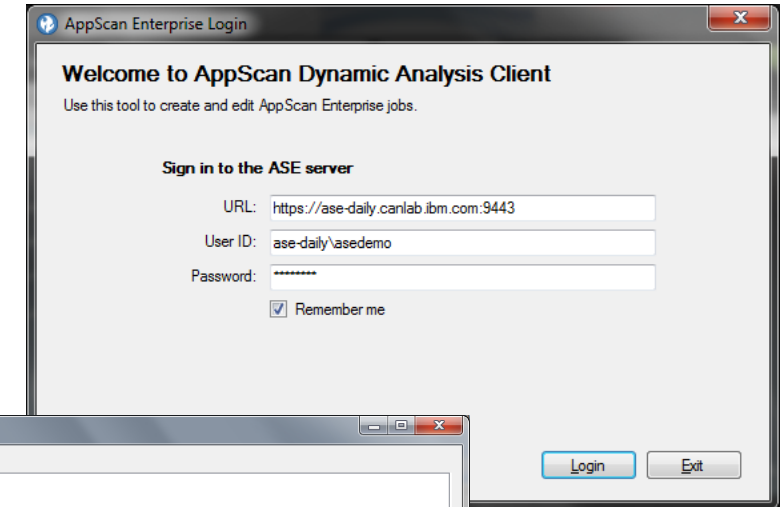
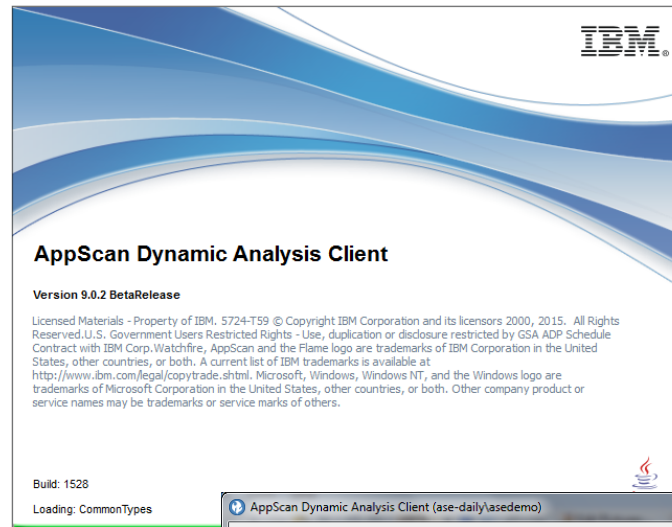


- ✓ Проще для понимания
- ✓ Подстановка SSL цепочек доверия
- ✓ Возможность показа запросов HTTP и действий браузера
- ✓ Проверка сценария логина на лету
- ✓ Лучшее распознавание шаблонов действий и предоставление подсказок по ходу работы

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.



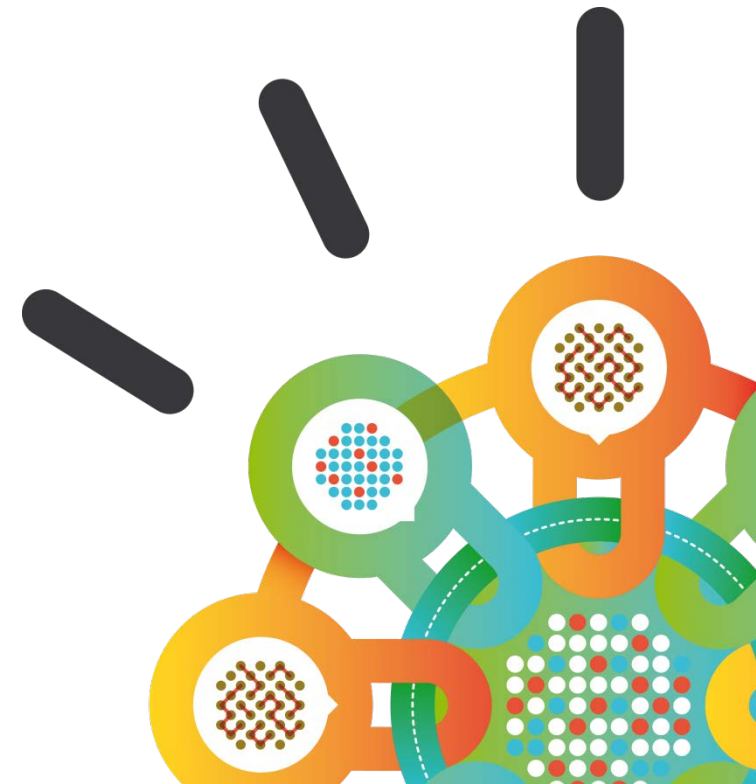
А также целый ряд новых технологий динамического тестирования в обоих продуктах

- ✓ 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

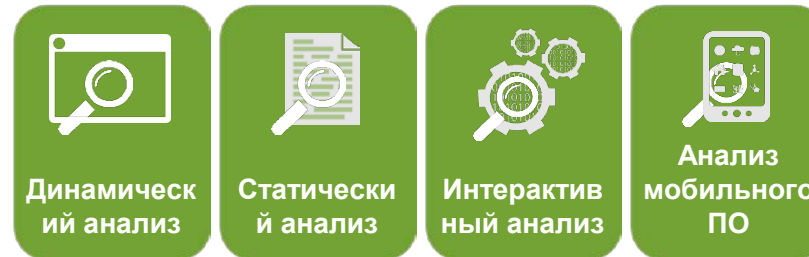
Решения по статическому анализу

AppScan Source



Решение AppScan – Статический Анализ

Тестирование *Приложения в разработке*



AppScan Source

- Наиболее эффективное с точки зрения стоимости решение по безопасности 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

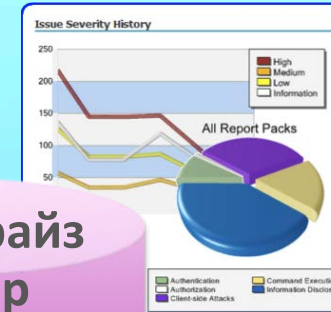
Консоль аналитика

- 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		

Отчёты для руководителя

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

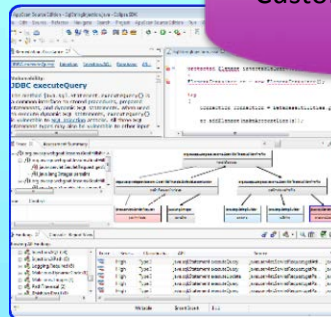


Энтерпрайз сервер

- Knowledgebase
- Assessment Database
- Custom Rules

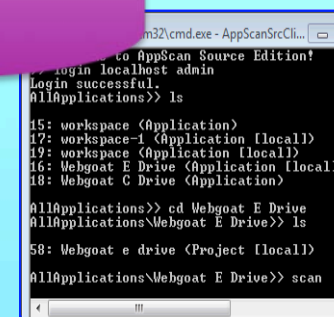
Плагины к IDE

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



Автоматизация

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



Широкая поддержка языков программирования

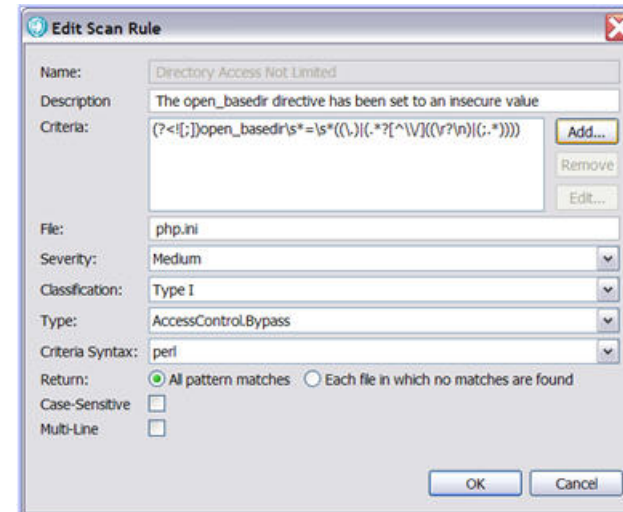
«Из коробки»

- 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

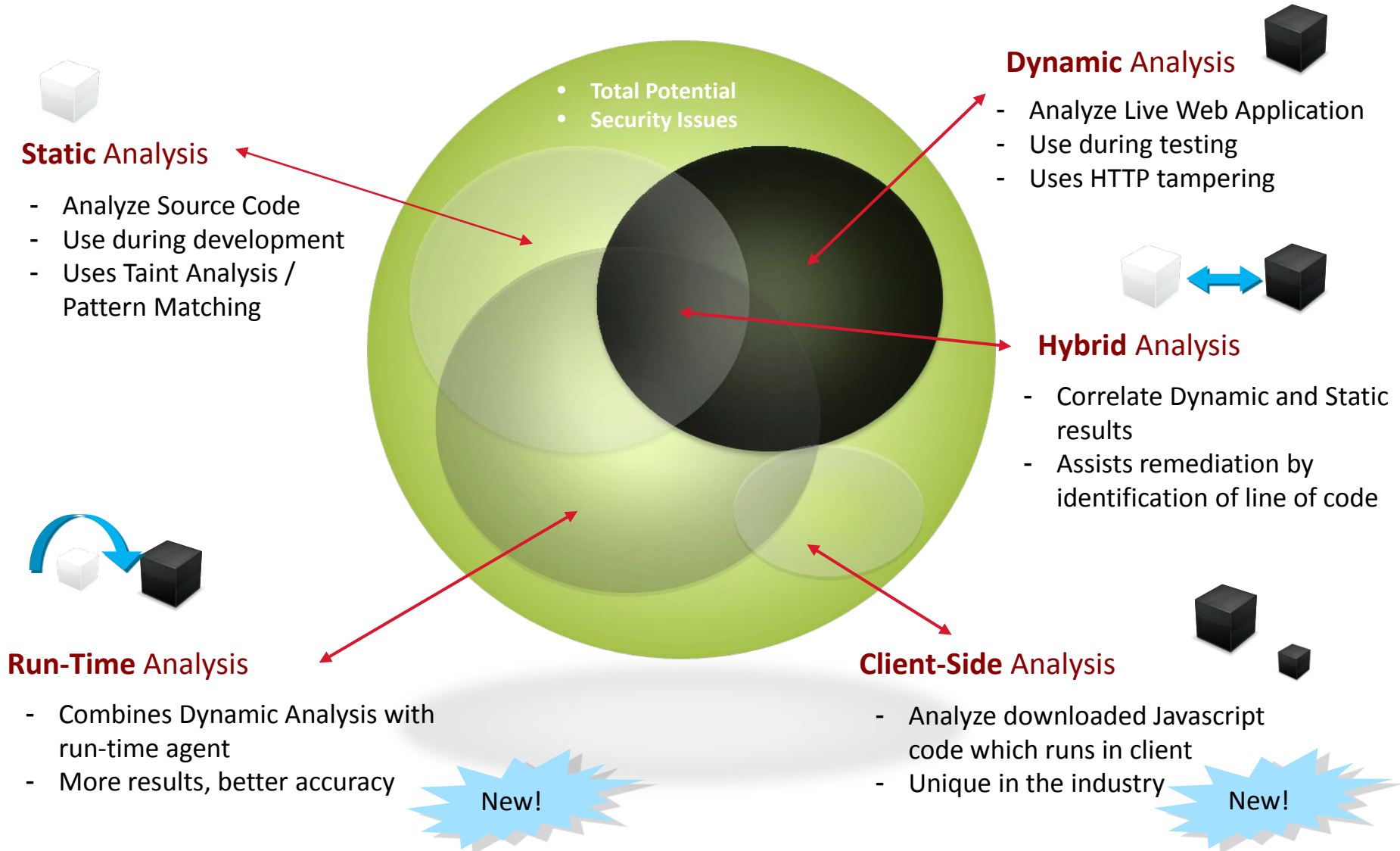
Расширяемая

Анализ регулярных выражений

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



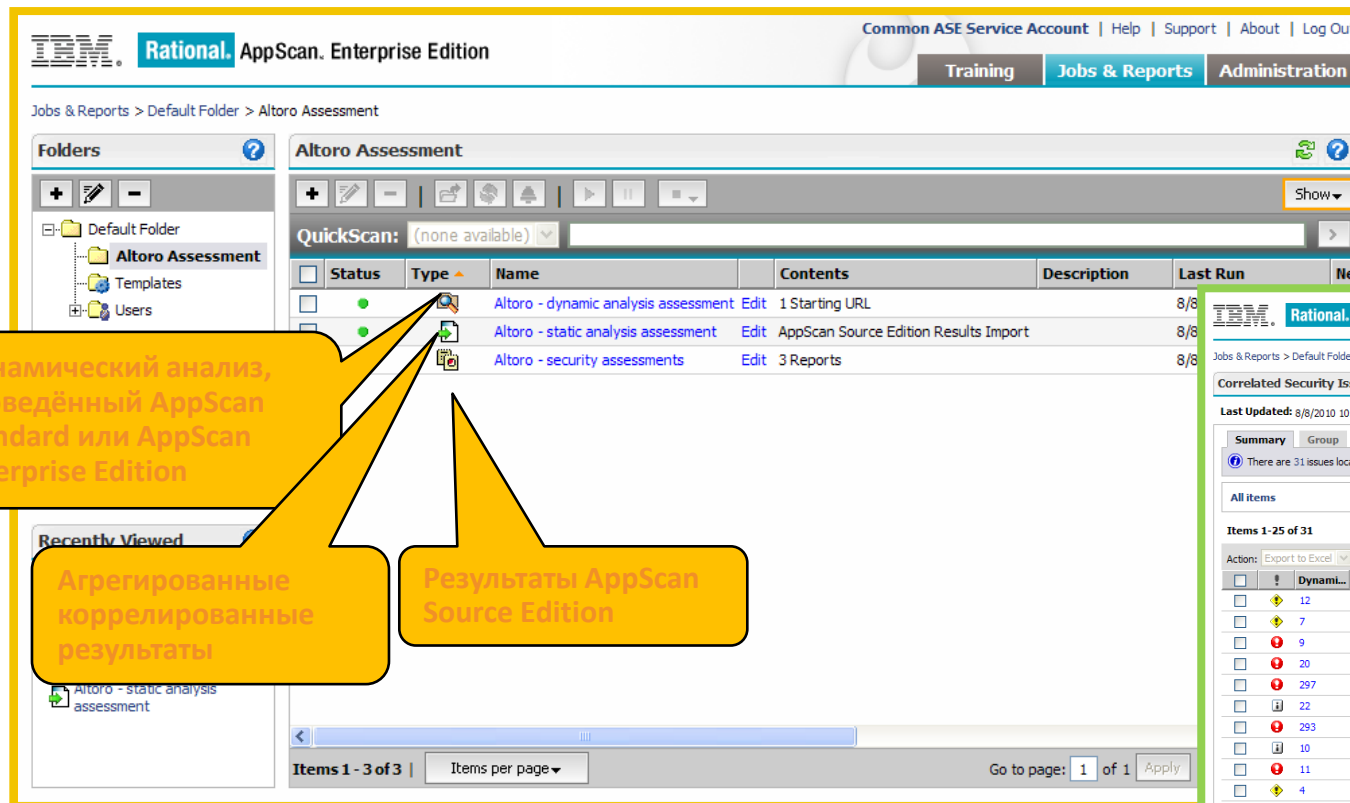
Увеличение процента найденных уязвимостей с помощью полного спектра технологий тестирования



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 приоритизации найденных уязвимостей для закрытки, то есть мы получаем подтверждение реальности проблем и метода их эксплуатации



Common ASE Service Account | Help | Support | About | Log Out

Training Jobs & Reports Administration

Jobs & Reports > Default Folder > Altoro Assessment

Folders

- Default Folder
 - Altoro Assessment
 - Templates
 - Users

Altoro Assessment

QuickScan: (none available)

Status	Type	Name	Contents	Description	Last Run
<input type="checkbox"/>		Altoro - dynamic analysis assessment	Edit	1 Starting URL	8/8
<input type="checkbox"/>		Altoro - static analysis assessment	Edit	AppScan Source Edition Results Import	8/8
<input type="checkbox"/>		Altoro - security assessments	Edit	3 Reports	8/8

Recently Viewed

- Altoro - static analysis assessment

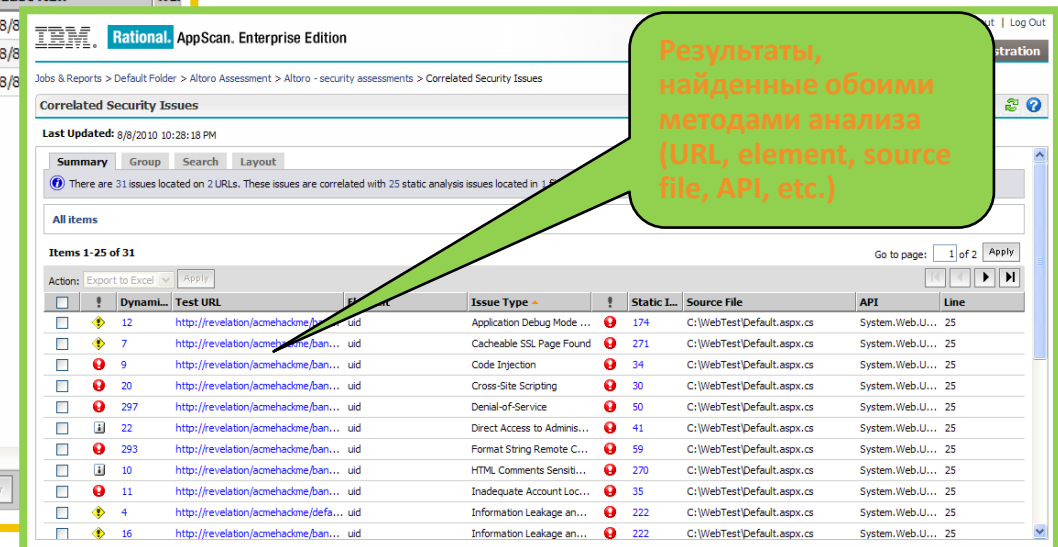
Items 1 - 3 of 3 | Items per page

Go to page: 1 of 1 Apply

Динамический анализ, проведённый AppScan Standard или AppScan Enterprise Edition

Агрегированные коррелированные результаты

Результаты AppScan Source Edition



Common ASE Service Account | Help | Support | About | Log Out

Training Jobs & Reports Administration

Jobs & Reports > Default Folder > Altoro Assessment > Altoro - security assessments > Correlated Security Issues

Correlated Security Issues

Last Updated: 8/8/2010 10:28:18 PM

Summary Group Search Layout

There are 31 issues located on 2 URLs. These issues are correlated with 25 static analysis issues located in 15

All items

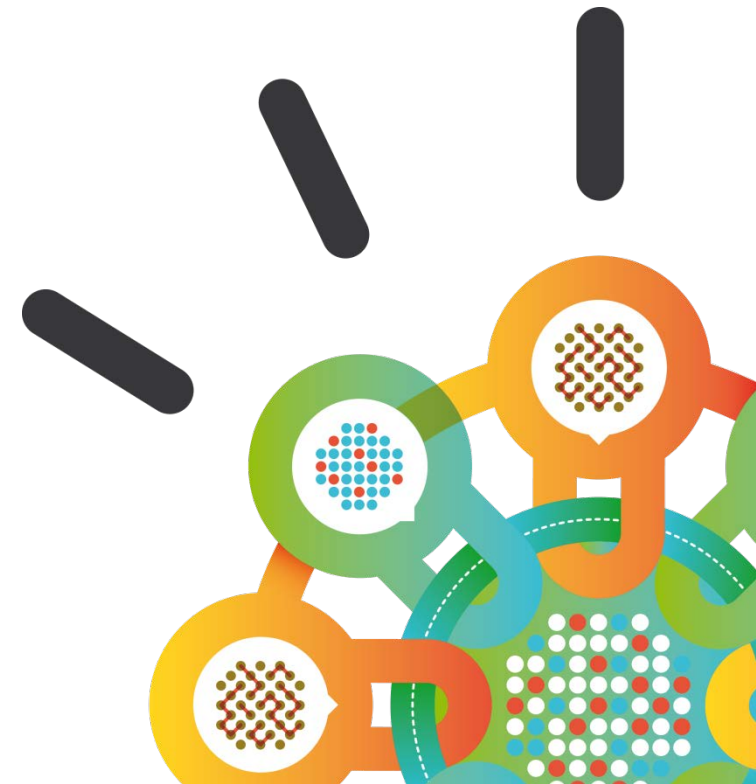
Items 1 - 25 of 31

Go to page: 1 of 2 Apply

Issue Type	Static I...	Source File	API	Line
Application Debug Mode ...	174	C:\WebTest\Default.aspx.cs	System.Web.U...	25
Cacheable SSL Page Found	271	C:\WebTest\Default.aspx.cs	System.Web.U...	25
Code Injection	34	C:\WebTest\Default.aspx.cs	System.Web.U...	25
Cross-Site Scripting	30	C:\WebTest\Default.aspx.cs	System.Web.U...	25
Denial-of-Service	50	C:\WebTest\Default.aspx.cs	System.Web.U...	25
Direct Access to Adminis...	41	C:\WebTest\Default.aspx.cs	System.Web.U...	25
Format String Remote C...	59	C:\WebTest\Default.aspx.cs	System.Web.U...	25
HTML Comments Sensiti...	270	C:\WebTest\Default.aspx.cs	System.Web.U...	25
Inadequate Account Loc...	35	C:\WebTest\Default.aspx.cs	System.Web.U...	25
Information Leakage an...	222	C:\WebTest\Default.aspx.cs	System.Web.U...	25
Information Leakage an...	222	C:\WebTest\Default.aspx.cs	System.Web.U...	25

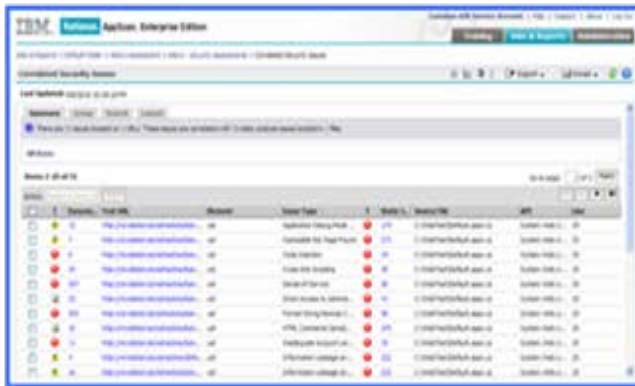
Результаты, найденные обоими методами анализа (URL, element, source file, API, etc.)

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 приоритизировать угрозы ИБ с помощью корреляции в реальном времени с результатами срабатывания систем IPS/IDS



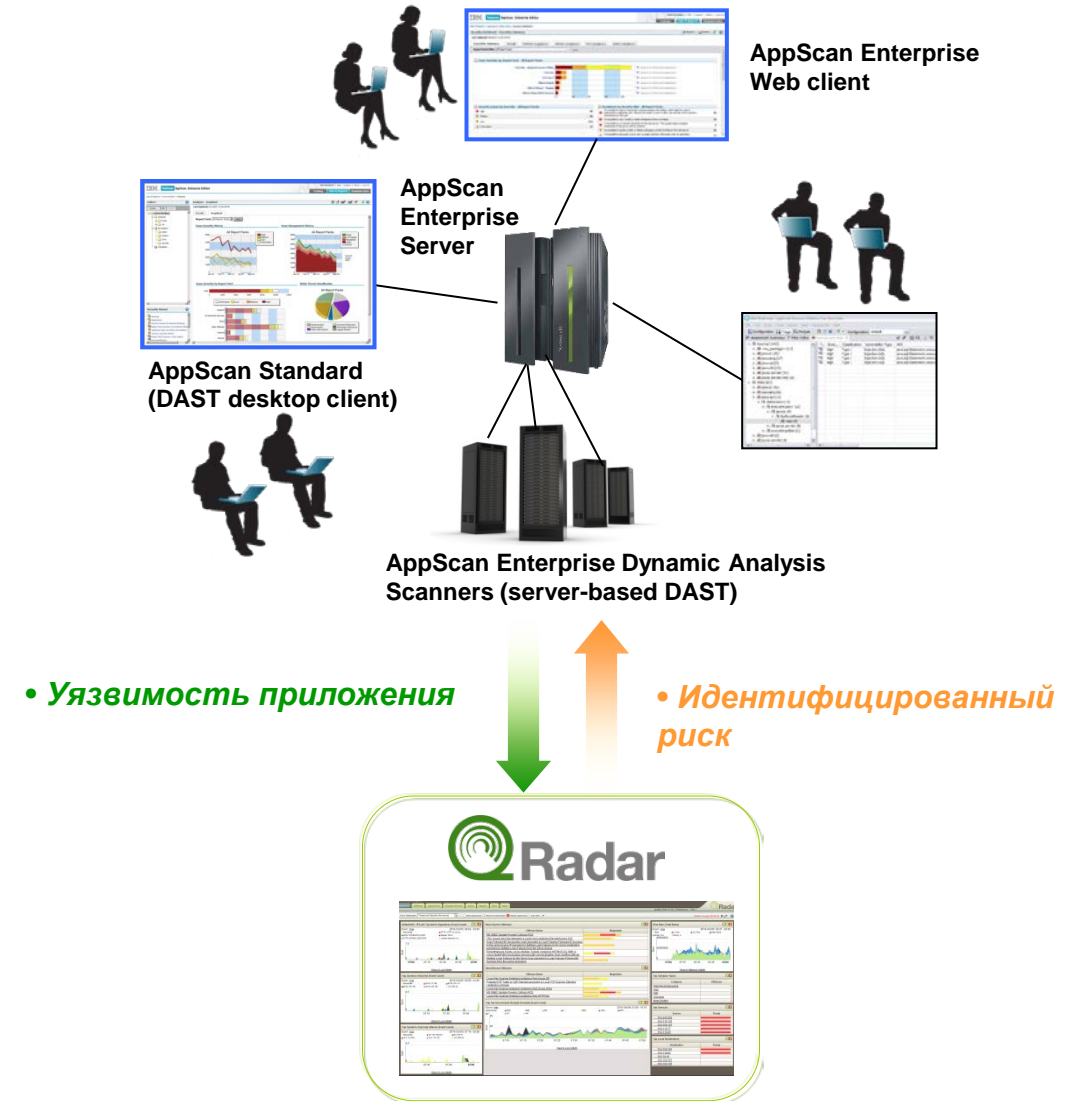
AppScan



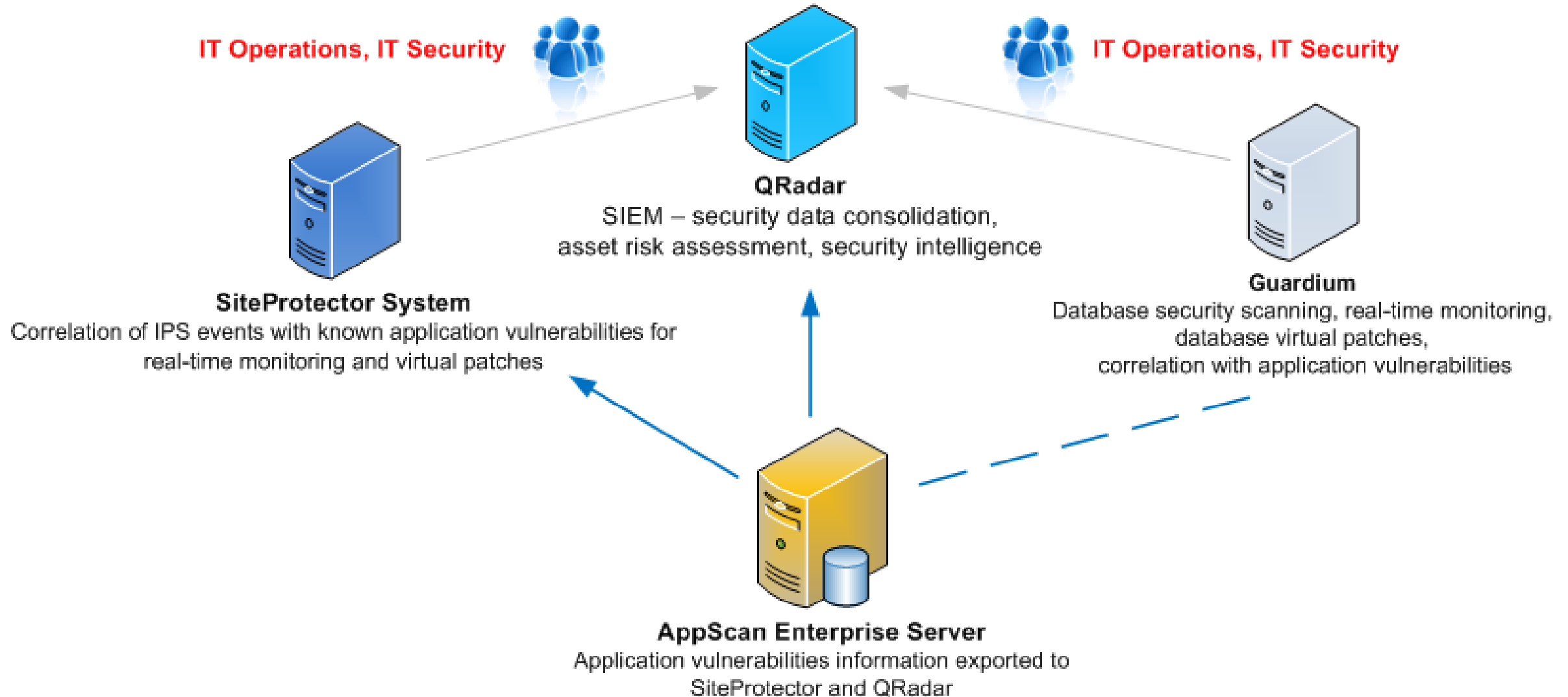
QRadar

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...