IBM Software

UKInnovate2010

The Rational Software Conference

Smarter software for a smarter planet.

IBM Software

UKInnovate2010

The Rational Software Conference

Building Managed Security Services using IBM Rational AppScan onDemand

Colin Bell
AppScan onDemand Manager, IBM
colin_bell@ie.ibm.com

Smarter software for a smarter planet.

AGENDA

Application Security Problem
IBM Rational Security Solutions
AppScan Deployment Options
AppScan Software as a Service
Case Study – Building Services at COLT Telecom
Colt an introduction (Managed Services, Products etc)
Why AppScan?
The Security workshop
The AppScan six pack walkthrough
The roll-out of AppScan
(design, build, collateral-SD, sales collateral etc)

The Costs from Security Breaches are Staggering

285 MILLION RECORDS COMPROMISED IN 2008

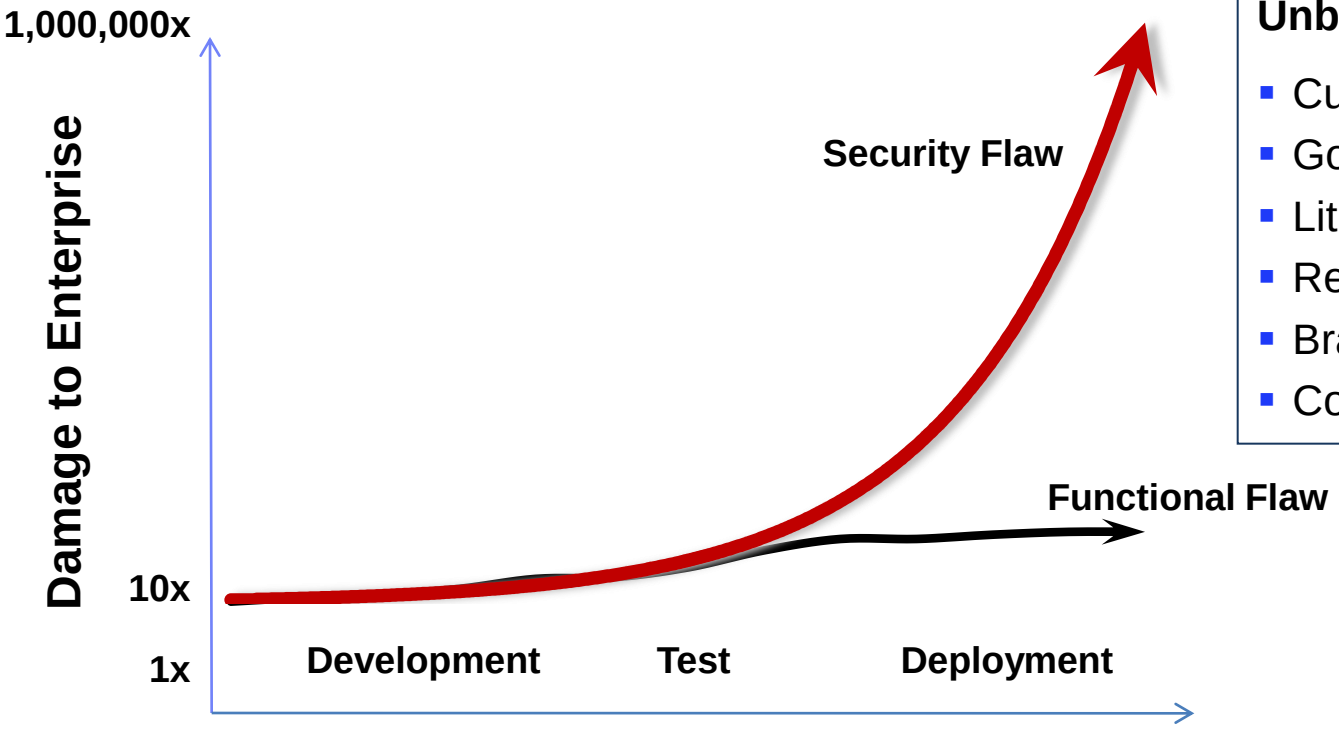
Verizon 2009 data Breach Investigations Report

$204 COST PER COMPROMISED RECORD

Ponemo+n 2009-2010 Cost of a data Breach Report

TRANSLATES TO $58.1B COST TO CORPORATIONS

Sources of Security Breach Costs



Unbudgeted Costs:

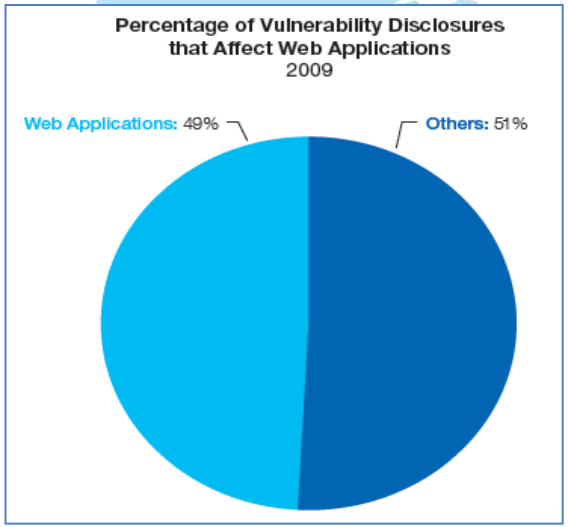
- Customer notification / care
- Government fines
- Litigation
- Reputational damage
- Brand erosion
- Cost to repair

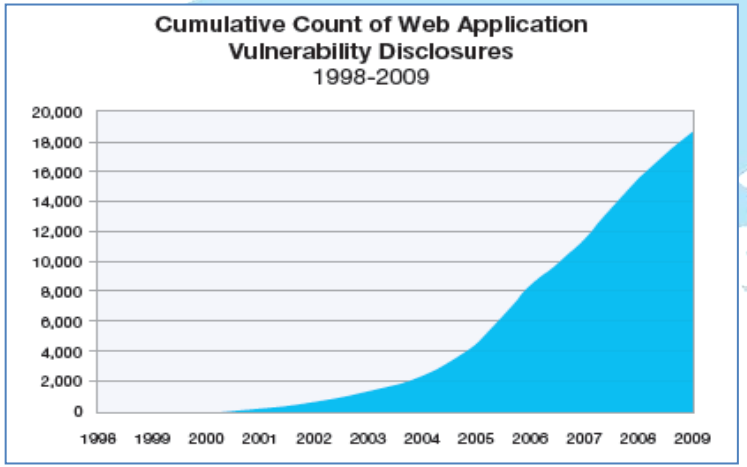
Application Vulnerabilities Continue to Dominate

Web application vulnerabilities represented the largest category in vulnerability disclosures (55% in 2008)

In 2009, 49% of all vulnerabilities are Web application vulnerabilities

SQL injection and Cross-Site Scripting are neck and neck in a race for the top spot

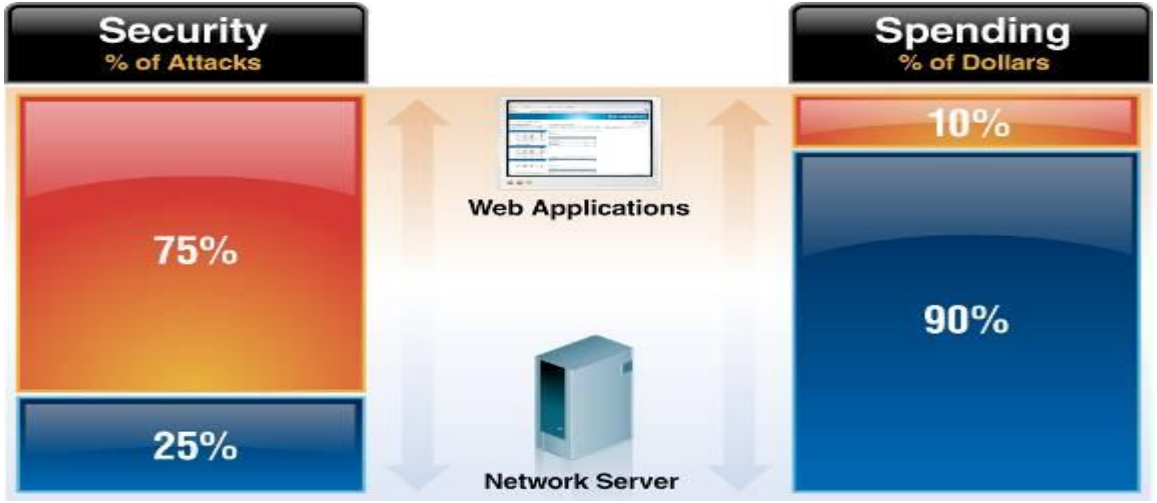




IBM Internet Security Systems 2009 X-Force® Year End Trend & Risk Report

Web App Vulnerabilities Continue to Dominate

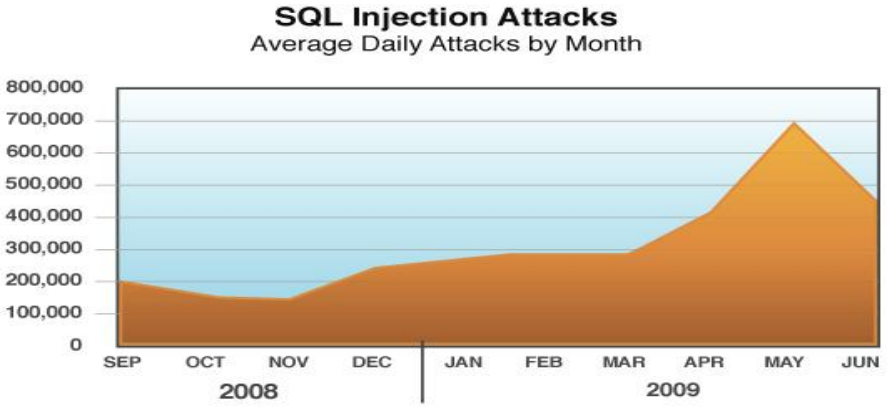
Security and Spending are Unbalanced



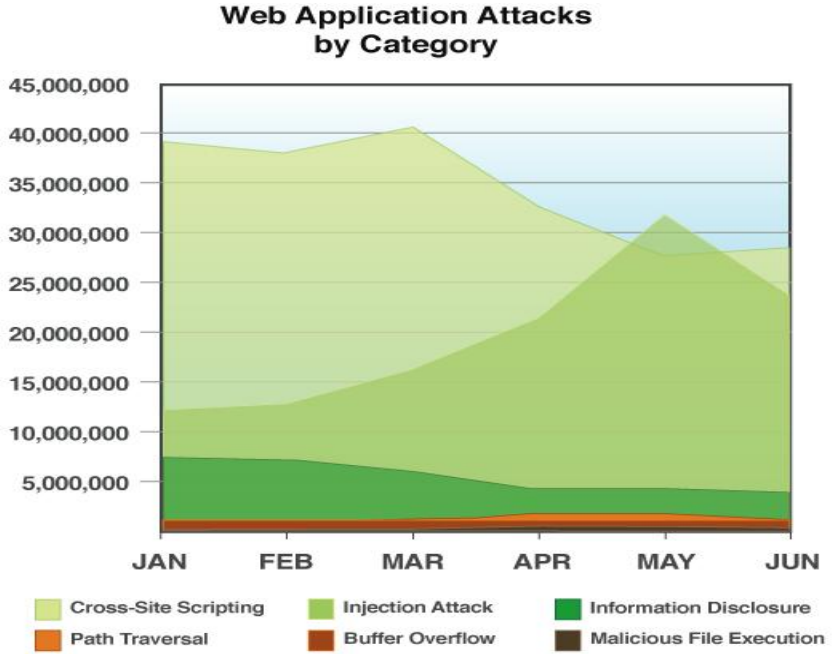
"The cleanup cost for fixing a bug in a homegrown Web application ranges anywhere from $400 to $4,000 to repair, depending on the vulnerability and the way it's fixed."
-Darkreading.com

Cross Site Scripting and Injection Attacks Continue to Dominate

- **90%** of injection attacks are attributed to SQL-related attacks
- Automated toolkits continue to flourish in 2009
- SQL injection attacks continue to grow up **50%** in Q1 2009 vs. Q4 2008 and nearly doubling in Q2 vs. Q1

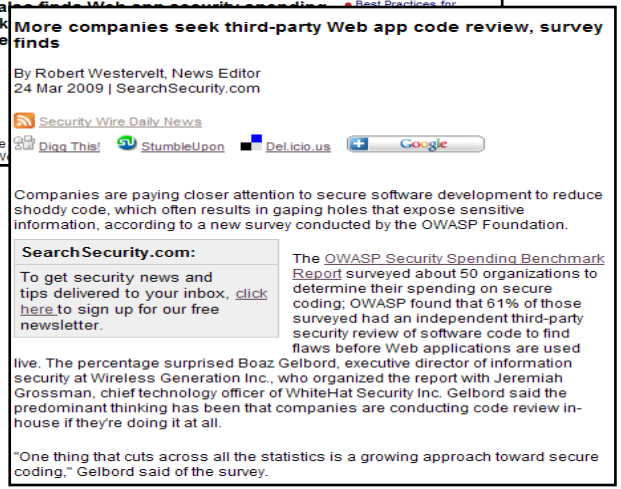


source: IBM X-Force®



source: IBM X-Force®

Headlines - Rate and Cost of Breaches Steadily Increasing



What is the Root Cause?

1. Developers not trained in security
   - Most computer science curricula have no security courses
   - Focus is on developing features

2. Under investment from security teams
   - Lack of **tools**, policies, process
   - Lack of **resources**

3. Growth in complex, mission critical online applications
   - Online banking, commerce, Web 2.0, etc

IBM Rational AppScan Suite

SECURITY

REQUIREMENTS	CODE	BUILD	QA	PRE-PROD	PRODUCTION
	AppScan Enterprise				
	AppScan Reporting Console			AppScan onDemand	
Security Requirements Definition	AppScan Source	AppScan Build	AppScan Tester	AppScan Standard	AppScan Standard
Security requirements defined before design & implementation	Build security testing into the IDE	Automate Security / Compliance testing in the Build Process	Security / compliance testing incorporated into testing & remediation workflows	Security & Compliance Testing, oversight, control, policy, audits	Outsourced testing for security audits & production site monitoring

Application Security Best Practices – Secure Engineering Framework

Flexible Deployment Options

Rational AppScan:
-Source for Automation
-Standard Ed

Configure
Scan
Triage

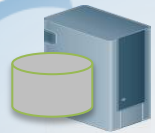
Build

Development
Rational AppScan:
- Source Ed Developer
- Source Ed Remediatio
- Enterprise QuickScan

Configure
Scan
Triage
Remediate
Verify

Configure
Scan

QA
Rational AppScan
Tester Ed for RQM



Rational AppScan
Source Ed Core

Rational AppScan
Enterprise portal &
Report Console

Functions:

Security Requirements
Configure
Scan
Triage
Remediate
Verify

Security Requirements
Configure
Scan
Triage

Security

Rational AppScan:
-Standard Ed
-Source Ed for Security

Compliance

IBM AppScan OnDemand Offerings: Software-as-a-Service

AppScan OnDemand consist of:

Software

- Appscan Standard / Enterprise (Blackbox testing)
- Appscan Source Edition (source code analysis)

Solution Management Services

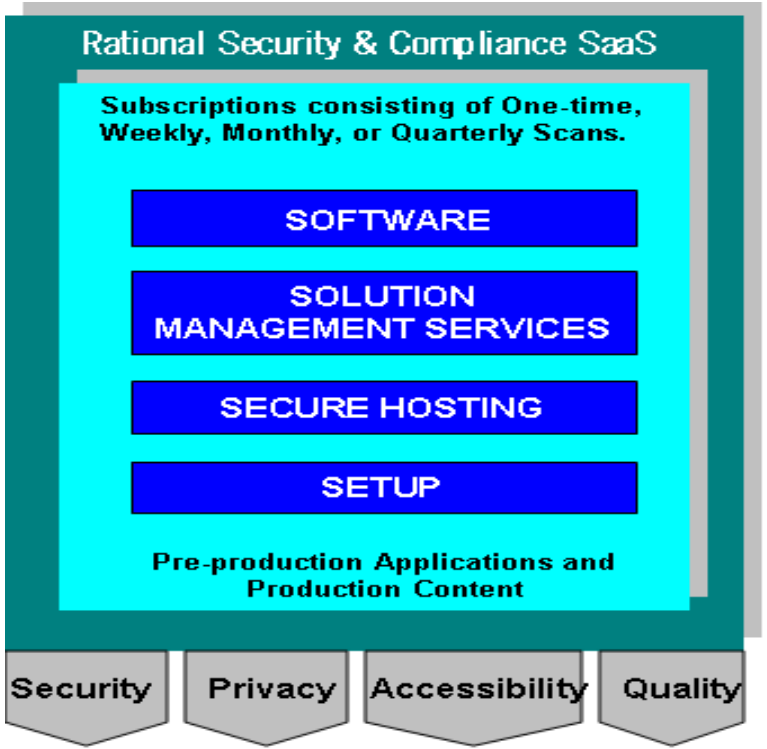
- Product experts perform product configuration
- Analyze and refine reports
- Provide subject matter expertise

Secure Hosting

- World class Data Center
- System administration, system security and availability, storage management, backup

Setup Services

- Software installation and version control
- Client access



IBM Rational Software as a Service (SaaS) Solutions

Pre-Production Testing

AppScan onDemand

- AppScan Enterprise-based
- Full test policy, monthly scans
- Full access to hosted software
- Annual contract, page based

AppScan onDemand Premium

- AppScan Standard - based
- Results via AppScan Reporting Console
- Full test policy
- Deep manual analysis & Exploitation
- One-time Application Based
- Quarterly Application Assessments

Production Testing

Production Site Monitoring

- AppScan Enterprise-based
- Limited subset of test policy *(safe for production)*
- Continuous/weekly scans
- Full access to hosted software
- Annual contract, page based

Policy Tester onDemand

- For accessibility and privacy compliance, internal quality standards
- Full test policy, monthly scans
- Full access to hosted software
- Annual contract, page based

Application Security Test – Methodology / Process

Host Discovery

Phase 1

IDENTIFY	SCOPE
Establish Target	Browse App
Meet Customer	Map Application
Agree Tests	Foot printing
Environment	Review Code
Define Dates Define	
Times	
Define Roles	
Approve Test	

Conduct Test

Phase 2

DETECT	ATTACK
Scan Ports	Plan attack
Scan Application (AppScan)	Exploit vulnerabilities
Network Enumeration	Escalate attack / privileges
Search for Vulnerabilities	Verify Risks
Identify Risks	

Report Findings

Phase 3

COLLATE	REPORT
Analyse Findings	Publish Report
List Risks	Review Report with Stake Holders (ASE Report Console)
Risk Analysis (DREAD)	Complete Action Plan
Rank Risks	Update Report with Action Plan
Develop Draft Report	Schedule Retest
	Close Assignment

CASE STUDY

Application Security Services using IBM Rational AppScan

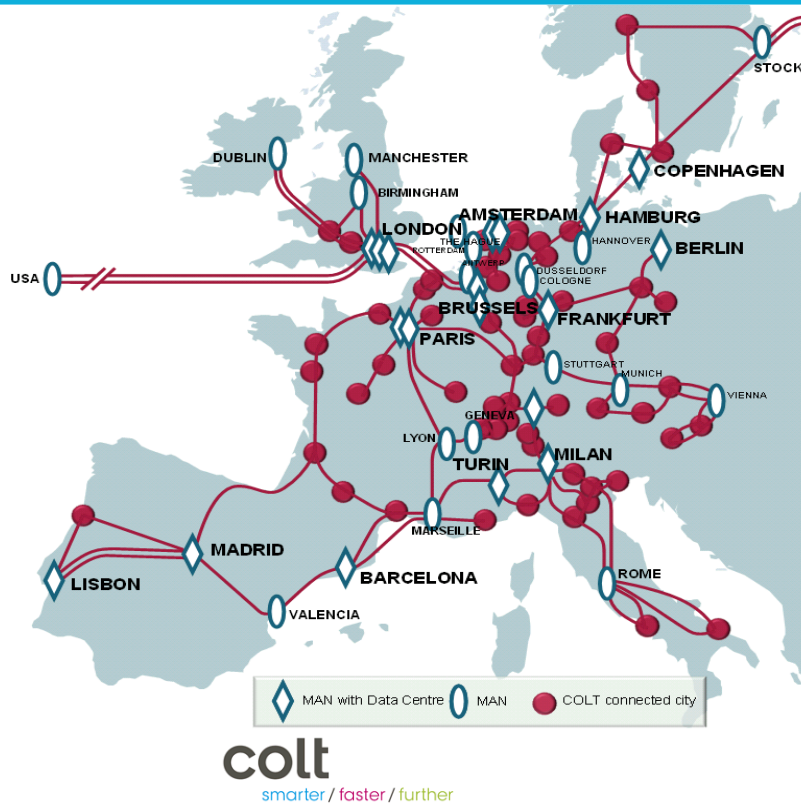
Reach and resources: COLT's network

Global reach with local knowledge:

- COLT have 3,000 people in offices across 34 of Europe's main business hubs

COLT own extensive network infrastructure across Europe:

- 25,000km European fibre network
- Connecting 34 major European cities and 15,000+ buildings
- Award-winning network throughout Europe and now the US



Resources: COLT's data centres

Purpose-built, pan-European data centres

19 fully integrated European data centre's connected by our fiber network:

23,000m^2 hosting space used

Over 5,000 customer racks

Over 25,000 devices (inc. customer)

Over 8,000 services under full management

Over 600TB of back-up monthly

24x7 dedicated Security Operations Centre:

ISO/IEC 27001 certified

24x7 Monitoring

Fault tolerant power supplies

Fully resilient air conditioning

24x7 Physical/ Logical security

Controlled access

Rapid fire suppression

colt
smarter / faster / further

Track record

colt
smarter / faster / further

Proven ability to deliver with over 40,000+ COLT customers:

Major national and multinational organisations including 3i, PwC, Fidelity; Wegener, Europ Assistance, Deutsche Börse and France 24

1000+ Finance customers including 24 of the world's top 25 financial institutions, 20 European stock exchanges

24 of the top 25 European hedge funds

All top 10 European broadcasters

Top five global providers of financial news and market data

Largest accredited SWIFT network-provider, with 750+ European clients

Why AppScan?

Security threats are a serious concern for COLT's existing or potential customers. (RFP's, bids-security)

COLT have top-class security consultants providing pen-tests and other security services -> AppScan helps us productise these services

A customer facing tool with supporting service demonstrates our security capabilities

A new service for our Sales Team- door opener

"Enabler" with huge up-sell potential.

Sales Journey

colt
smarter / faster / further

Demonstrated mid-Aug 2009

POC (2 week's in Sept 2009)

Procurement completed by end of Sept 2009 (!)

Jan – Mar 2010 productized (Colt T&C's, Book to Bill processes etc)

Workshop Objective: (Start of Productization)

> "Build a new COLT security story by defining where we are today (technology, people, capabilities) and where we want to be in the future"

Train pre-sales, sales staff.

Identify potential pilot customers

Alignment with other Colt solutions

COLT Security Services Framework

colt
smarter / faster / further

Design

- DC Architecture Design
- Security Policy Design (A)
- Compliance Consulting (A)

Implementation

- F/W IDS IPS Services and Implementation
- DC Security Controls Implementation
- Compliance Implementation (A)

Assessment

- Application scanning/assessments (A)
- Process assessments (A)
- Compliance Assessments (A)
- Network Infrastructure assessments (A)
- Forensic Investigations (A)

•Red Current
•Blue Next year

Managed Services

- F/W IDS IPS
- On-going assessments (A)
- Managed Strong Authentication
- Anti-Spam Content Security
- WAF UTM DDoS
- Log Analysis and Reporting (A)
- Compliance Reporting (A)
- On-Demand Services/ Virtualisation Services (A)

Content Overview for COLT Solutions/ Services

colt
smarter / faster / furth

COLT Advanced Security Services (CASS) - WEB Security Assessment

Description

•This service provides security tests of a client's critical web based application(s). A consultant will test the designated application(s) using IBM Rational AppScan products, additional manual testing will be performed.

•This service is ideal for onetime assessments or regular quarterly security assessments of critical applications.

•This can help a client to meet a compelling deadline such as a PCI audit or other compliance conditions.

Solution Components

Services
•Standalone Engagements
- Basic (3 Days)
- Comprehensive (5 Days)
- Advanced (10 Days)

•Re-occurring/Subscription Based
- Quarterly, Yearly

•Report and Presentation with Risk Analysis

Up-Sell / Cross-Sell
•Other COLT Security Services
•Compliance pre-Audit
•Risk Management

Customer Benefits

- Identification of vulnerability of publicly available and internal web based applications.
- Periodic re-test to demonstrate improvement
- Monitors issues arising from new releases or newly identified attack strategies.
- Client is provided with a detailed walkthrough session to outline and explain the findings, discuss remediation and prioritizing of actions arising from the test.

Customer Profile

Target Customers
•Existing COLT customers
•Companies already using Managed Services in other areas.

Who?
•CIO, CSO, IT Manager, Application Owners

Compelling Business Drivers
•Assistance with Compliance
•Ongoing Application Risk Assessment
•Security Validation on new Applications and Services

Competitive Landscape

Not for publication

References

- **COLT OnLine**
- Read Success Story
- Read Success Story

The roll-out of Rational AppScan

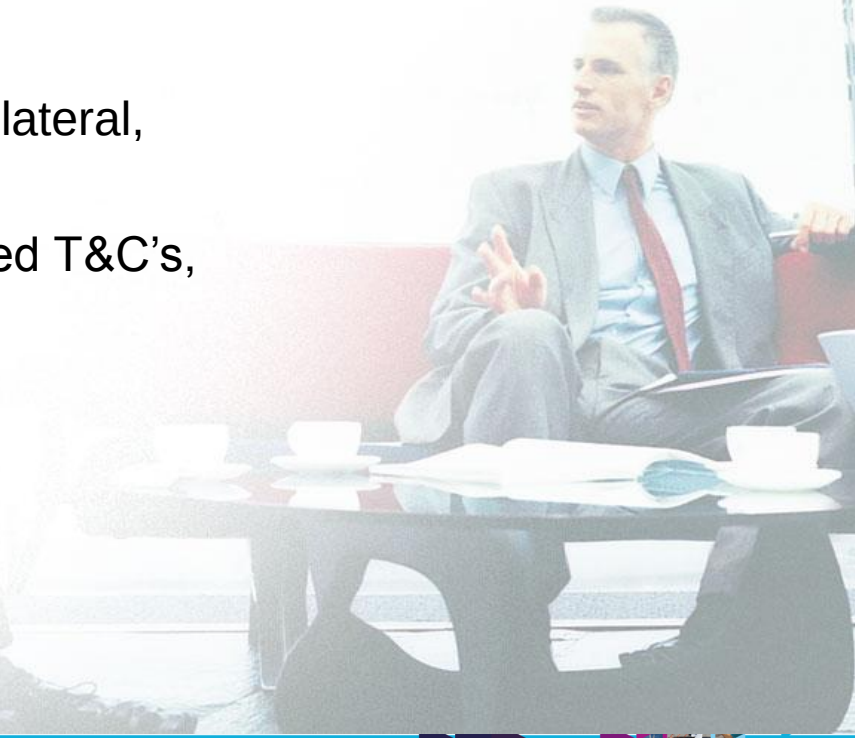
colt
smarter / faster / further

Design, Build, Operate Service (2 months)

Productization: Service Description, Sales Collateral, Marketing etc. (2 months)

Legal: General Terms & Conditions, Specialised T&C's, Waiver and SoW (2 months)

Training: 2 day training session



First Customers

Illustrates that Colt have top quality Security Consultants & a state of the art Security Portfolio.

First step into on-boarding onto their Cloud Solutions

Major “up-sell” opportunities

Lessons Learned

Catalyst for bundling solutions together e.g. auditing & security solutions

Assisted Colt build a compelling Security Story

Providing our Sales Team with new “door opener” services

AppScan Best of Breed of pen-test tools

Excellent support from IBM.


Questions

www.ibm.com/software/rational

IBM Software

UKInnovate2010

The Rational Software Conference

Smarter software for a smarter planet.