IT Security: a practical approach

IEEE Information Technology Professional Conference at TCF

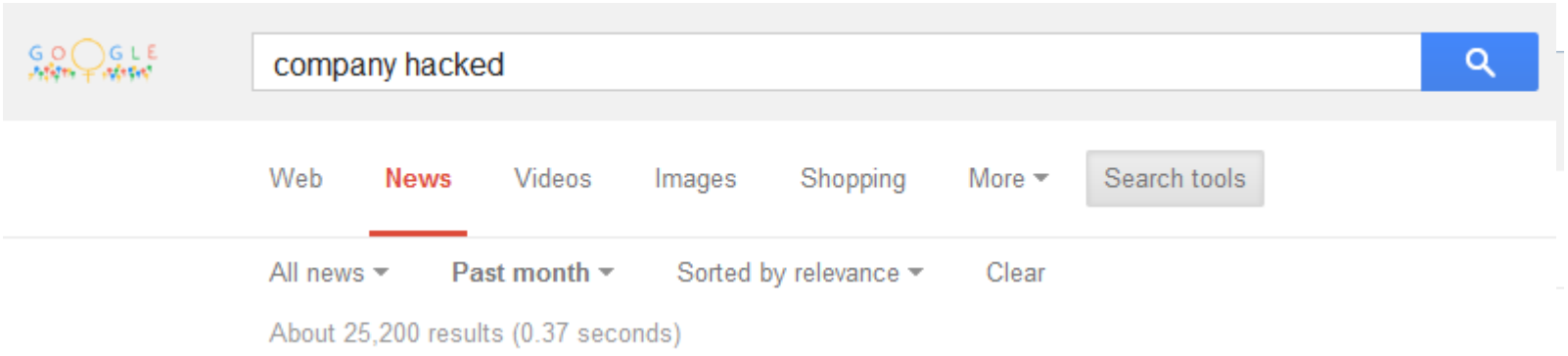
March 14, 2014

Ivan Dell'Era
Security Architect, IBM
ivd@us.ibm.com

Agenda

- Media coverage of security news
- Keeping up with changes
- Hacking university
- Tools and solution used at IBM Research
- Conclusion
- Q&A

Cyber Security (or lack of) is in the news



Microsoft's Internet Explorer 10 **Exploited** To **Hack** Military Website
Design & Trend - Feb 14, 2014
By using a zero-day **exploit** on Microsoft's Internet Explorer 10, the attackers sought to cause a drive-by download and install a backdoor called ...

Silk Road 2 **Hacked**, Over 4000 Bitcoin Allegedly Stolen
TechCrunch - by John Biggs - Feb 13, 2014
Silk Road 2 moderator Defcon reported in a forum post that hackers have used a transaction malleability **exploit** to **hack** the marketplace.
$2.7 million-worth of Bitcoin stolen as successor to dark web market ...
The Independent In-Depth - Daily Mail - Feb 14, 2014

BidorBuy forums hit with stealth **hack**
MyBroadband - by Jan Vermeulen - Feb 14, 2014
The **exploit** also didn't trigger if your browser already had cookies from the ... This means that the **hack** was trying to hide itself from regular ...

Syrian Electronic Army Threatens to **Hack** CENTCOM
Defense One - by Patrick Tucker - Mar 3, 2014
Syrian Electronic Army Threatens to **Hack** CENTCOM ... "If SEA has found a seam to **exploit**, expect that seam to be fixed and any defaced sites ...

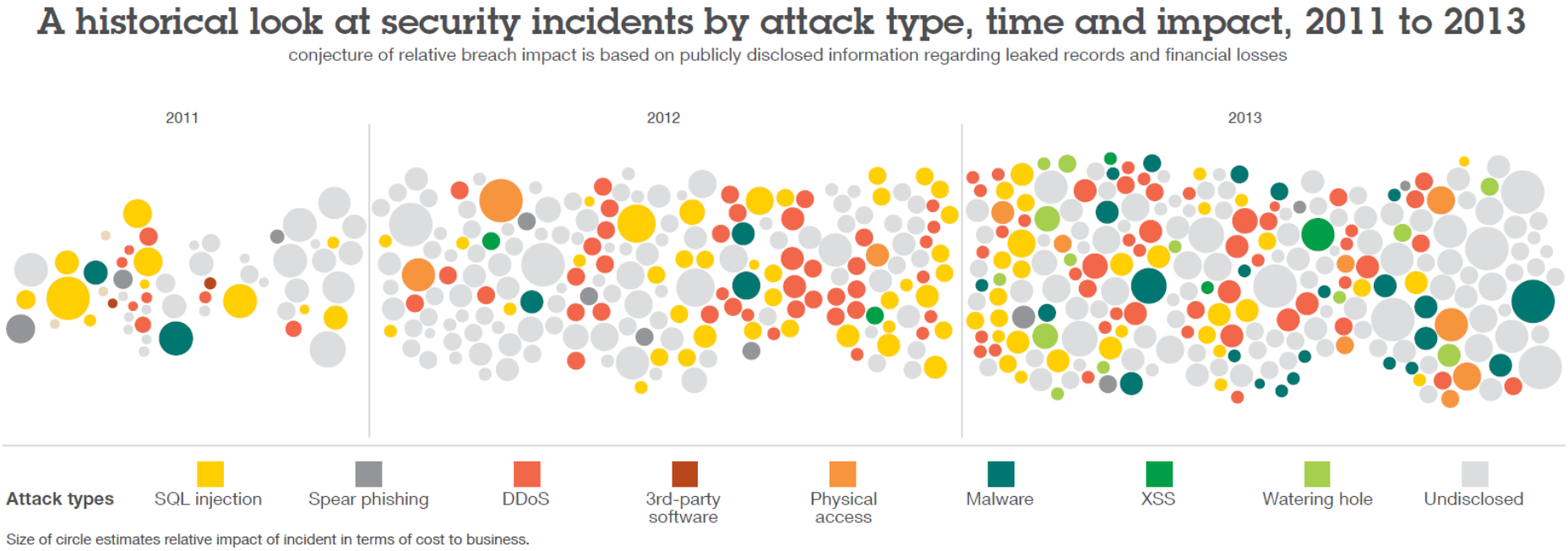
Apple Security Flaw Could Be Backdoor For NSA
Eurasia Review - Feb 25, 2014
Was the National Security Agency **exploiting** two just-discovered security flaws to **hack** into the iPhones and Apple computers of certain targets ...

AFP

The Mask **Hack** "Beyond Anything We've Seen So Far"
PC Magazine - Feb 11, 2014
Attackers used an **exploit** which targeted a vulnerability in Adobe Flash Player which lets attackers then bypass the sandbox in Google Chrome.

Data breaches likely as hackers stay a step ahead
Allentown Morning Call - 14 hours ago
"They couldn't trace where the **hacking** took place." ... sophisticated software to identify and **exploit** weaknesses in computer network security.

A look at recent cyber security incidents

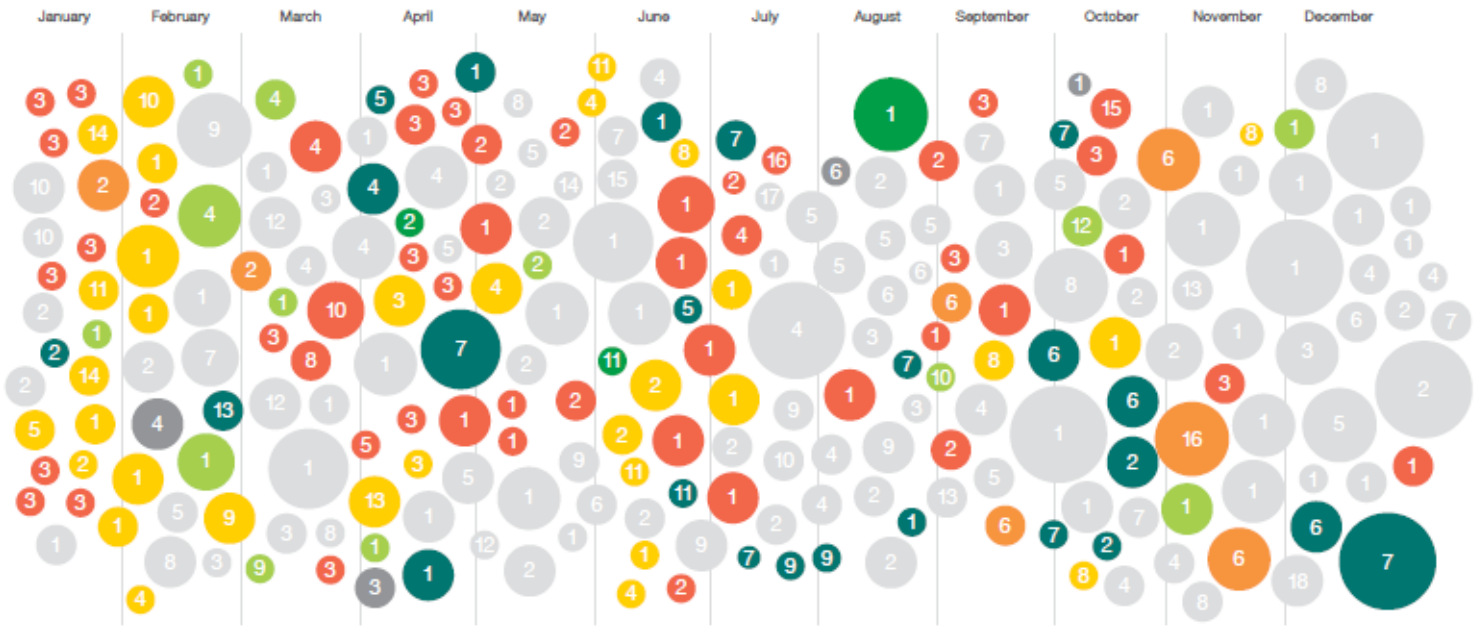


Source: IBM X-Force www.ibm.com/security/xforce/

- How often do we hear on the news of computers being compromised?
- Why can't Security Specialists prevent this?
- Which system is immune from attacks?
- How can I reasonably be protected against compromise?

Sampling of 2013 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

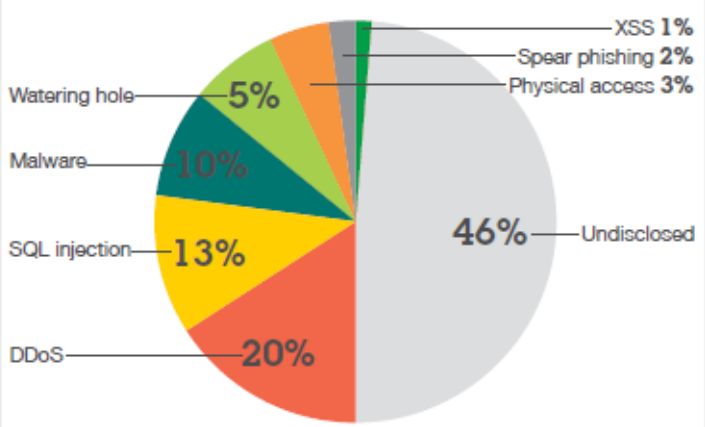


Size of circle estimates relative impact of incident in terms of cost to business.

Most-commonly attacked industries

28%	Computer Services (1)
15%	Government (2)
12%	Financial Markets (3)
9%	Media & Entertainment (4)
7%	Education (5)
5%	Healthcare (6), Retail (7), Telecommunications (8)
3%	Consumer Products (9)
2%	Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
1%	Industrial Products (14), Travel & Transportation (15), Wholesale Distribution & Services (16)
<1%	Aerospace & Defense (17), Insurance (18)

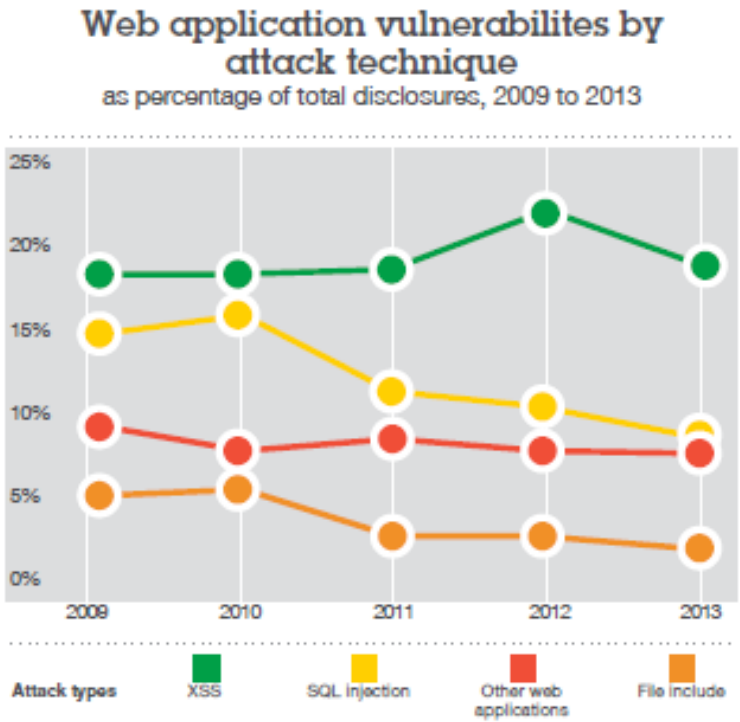
Most-common attack types

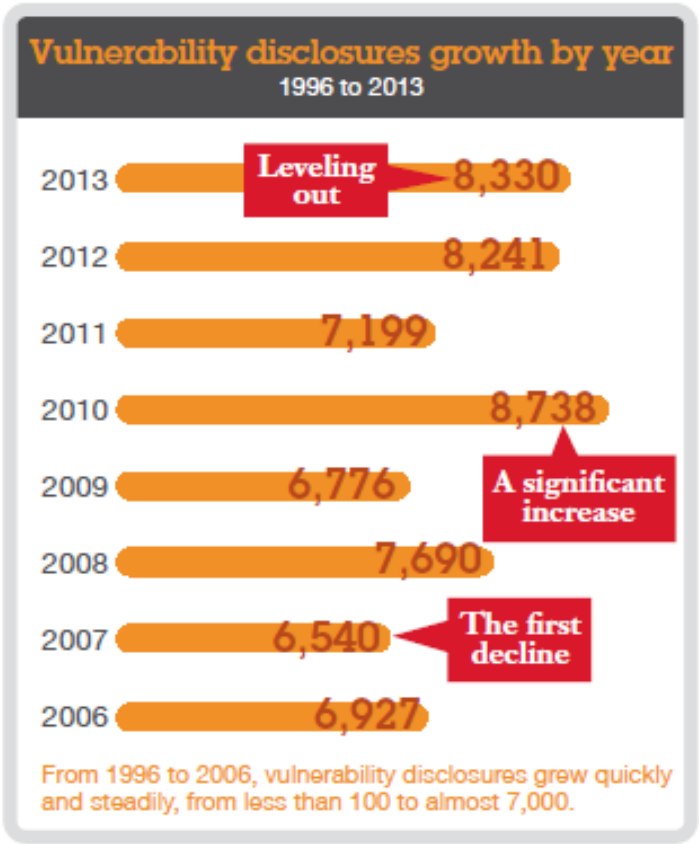


Source: IBM X-Force www.ibm.com/security/xforce/

Update, update and update again

- How often should systems and applications be updated?
- How do you know which ones are vulnerable?
- Are the IT professionals taking care of all systems?
  - And what about end users?

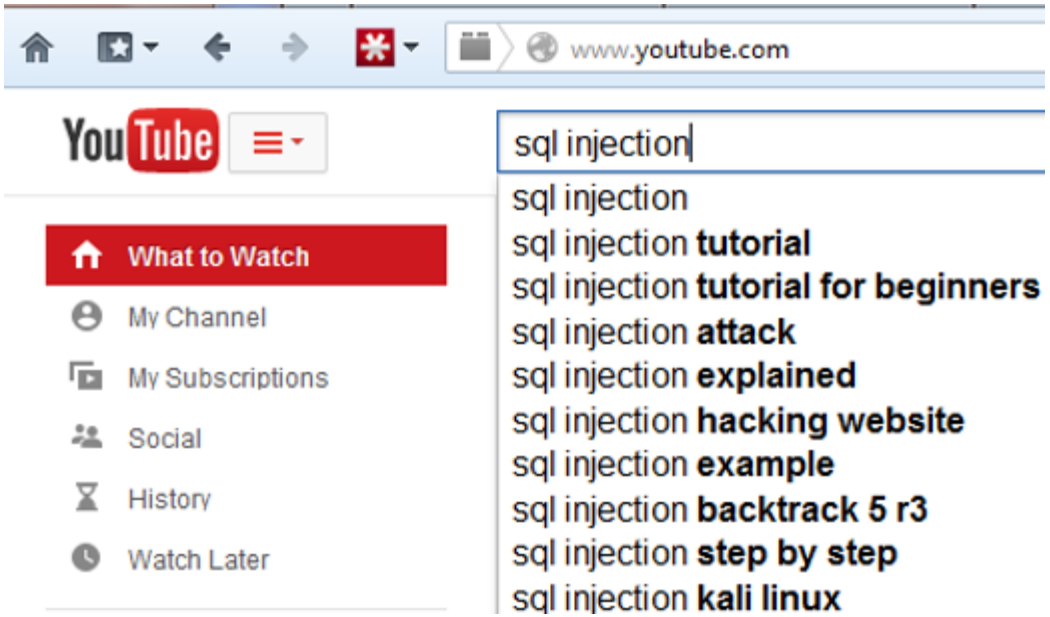




Source: IBM X-Force www.ibm.com/security/xforce/

Security – hacking university (the sad reality)

- Unpatched systems are easy targets
- Security patches are issued daily
- Once a security vulnerability fix is released, often an attack is available within hours
- Exploit tools are updated by thousands of hackers and made available online, as a freely available download
- Hacking is now as easy as the how to video on sending in a text message



People are the weakest link in the security chain

It’s human nature: why fix something if you don’t think it’s broken – or vulnerable

Some misconceptions and funny quotes I heard recently:

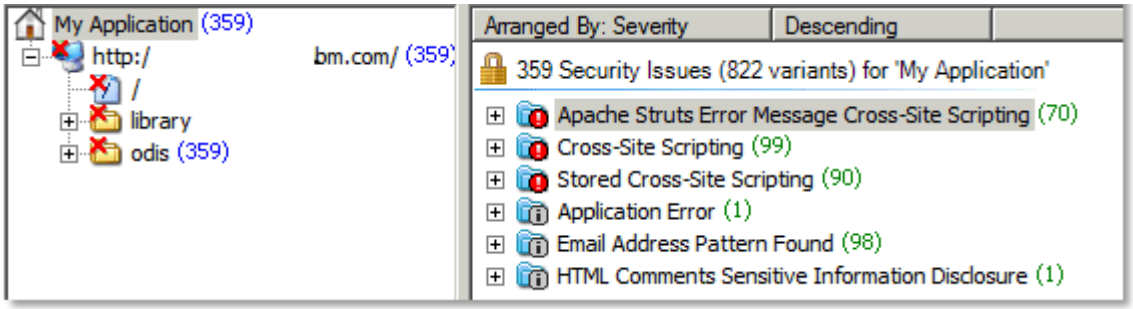
- I don’t need to install patches, my system is behind a firewall
- My project is very critical and time sensitive, so my manager and I decided to ask for a security exception
- No, really, tell me what the absolute deadline is to perform this security work
- What a fat lie: prove to me my system is vulnerable! It hasn’t been on the network for weeks...
- We never patched this issue and we were never hacked, I don’t understand why it’s so urgent now

Or some bullying:

- I’m ready to escalate all the way up to the top, my team is too busy to be concerned with security issues

Identify application weaknesses

- IBM Security AppScan identifies potential security vulnerabilities in web applications
  - Improves quantity and quality of exploits with every update (in other words, it implements new technique and exploits used by the bad guys)
  - Good practice to retest periodically
    - *After an application upgrade*
    - *When new features are added (even if it's 'just' an addition of some text pages)*
  - This step is often forgotten



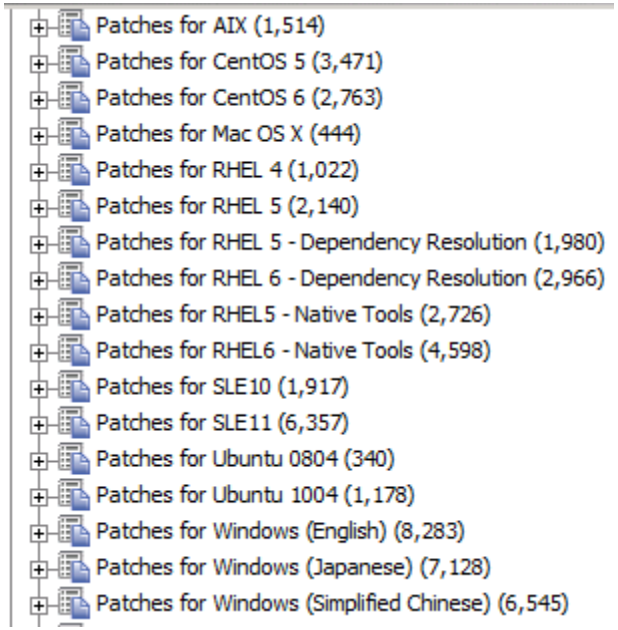
IP vulnerability scanning

- IP Vulnerability Scanner identifies services with unpatched vulnerabilities and security exposures
  - This is one of the tools used also by hackers to find exploitable issues
  - Generates a comprehensive report of every port listening on the target system
  - Identifies services and version by fingerprint, not port number
  - Finds potential vulnerabilities non-aggressively (without causing a DoS attack)
  - Identifies information leakage
    - *i.e. web servers with debugging information pages installed, providing valuable information about the environment*
  - Tests for default accounts
    - *did you remember to change the admin password?*
- Automated notification of identified issues to interested parties
  - Email contains links to knowledge base with instructions on how to fix

IBM Endpoint Manager – global view

- Formerly BigFix Endpoint Protection – acquired by IBM in 07/2010
- Provides a global view of various security aspects
- Highly customizable reports and actions
- Cross platform support (Windows, various Linux distributions, Unix, Mac, VMware, etc.)

From all security and bug fixes - to the applicable subset



IBM Endpoint Manager – applicable fixes

Bug fixes

Name
RHBA-2014:0098 - P11-Kit Bug Fix Update - Red Hat Enterprise 6.0 (x86_64)
RHBA-2014:0101 - Tzdata Enhancement Update - Red Hat Enterprise 6.0 (noarch)
RHBA-2014:0158 - Nss Bug Fix Update - Red Hat Enterprise 6.0 (SERVER/WORKSTATION) (x86_64)
RHBA-2014:0190 - Initscripts Bug Fix Update - Red Hat Enterprise 6.0 (x86_64)
RHBA-2014:0191 - Postfix Bug Fix Update - Red Hat Enterprise 6.0 (x86_64)
RHBA-2014:0199 - Psmisc Bug Fix Update - Red Hat Enterprise 6.0 (x86_64)
RHBA-2014:0203 - Upstart Bug Fix Update - Red Hat Enterprise 6.0 (x86_64)

Security vulnerability patches

Name
RHSA-2014:0159 - Kernel Security and Bug Fix Update - Red Hat Enterprise 6.0 (x86_64)
RHSA-2014:0246 - Gnutls Security Update - Red Hat Enterprise 6.0 (SERVER/WORKSTATION) (x86...

Name	Source Severity	Site	Applicable Com...	Source Release Date
2934088: Vulnerability in Internet Explorer could allow remote code execution - Enable MSHTM...	N/A	Patches for Windo...	55 / 173	2/19/2014
MS14-010: Cumulative Security Update for Internet Explorer - IE 8 - Windows 7 SP1 (x64)	Critical	Patches for Windo...	4 / 173	2/11/2014
MS14-011: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBSc...	Critical	Patches for Windo...	4 / 173	2/11/2014
MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution - Windows 7 SP1 (x64)	Critical	Patches for Windo...	4 / 173	2/11/2014
MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution - Windows Server 200...	Critical	Patches for Windo...	21 / 173	2/11/2014
MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution - Windows Server 201...	Critical	Patches for Windo...	2 / 173	2/11/2014

Name	Source Severity	Site	Applicable Com...	Source Rele
RHBA-2014:0256 - Libvirt Bug Fix Update - Red Hat Enterprise 6.0 (SERVER/WORKSTATION) (...	<Unspecified>	Patches for RHEL ...	218 / 430	3/6/2014
RHSA-2014:0255 - Subversion Security Update - Red Hat Enterprise 6.0 (SERVER/WORKSTATI...	Moderate	Patches for RHEL ...	1 / 430	3/5/2014
RHSA-2014:0255 - Subversion Security Update - Red Hat Enterprise 6.0 (SERVER/WORKSTATI...	Moderate	Patches for RHEL ...	109 / 430	3/5/2014
RHSA-2014:0246 - Gnutls Security Update - Red Hat Enterprise 6.0 (SERVER/WORKSTATION)	Important	Patches for RHEL ...	1 / 430	3/3/2014
RHSA-2014:0246 - Gnutls Security Update - Red Hat Enterprise 6.0 (SERVER/WORKSTATION) ...	Important	Patches for RHEL ...	366 / 430	3/3/2014
RHSA-2014:0222 - Libtiff Security Update - Red Hat Enterprise 6.0 (SERVER/WORKSTATION)	Moderate	Patches for RHEL ...	1 / 430	2/27/2014
RHSA-2014:0222 - Libtiff Security Update - Red Hat Enterprise 6.0 (SERVER/WORKSTATION) (...	Moderate	Patches for RHEL ...	364 / 430	2/27/2014

The growing burden of security

- IT, project groups and application owners have different priorities
- Users are not invested updating and installing security fixes each week
- In general, they are overwhelmed by the amount of security updates and different classification levels by vendors
  - Critical, Important, Moderate, Low
  - Critical, Security, General
  - Critical, Moderate, Low
  - Severity 1, 2, 3, 4
  - Urgent, High, Medium, Low
  - High, Medium, Low
- They are concerned about security patches breaking their environment, research, or affecting their results

Security automation

- Security automation needs to offer options and flexibility for users
  - Opt-in, opt-out, change windows, exceptions, custom configurations
  - Extremely user friendly
- Conform to the company security compliance requirements
  - Understand the difference between different classes of systems
    - *Production vs test and development*
    - *Accessible from the Internet (DMZ) vs in the company intranet*
- Minimize manual intervention
- Continuous Compliance and Monitoring to identify new security exposures

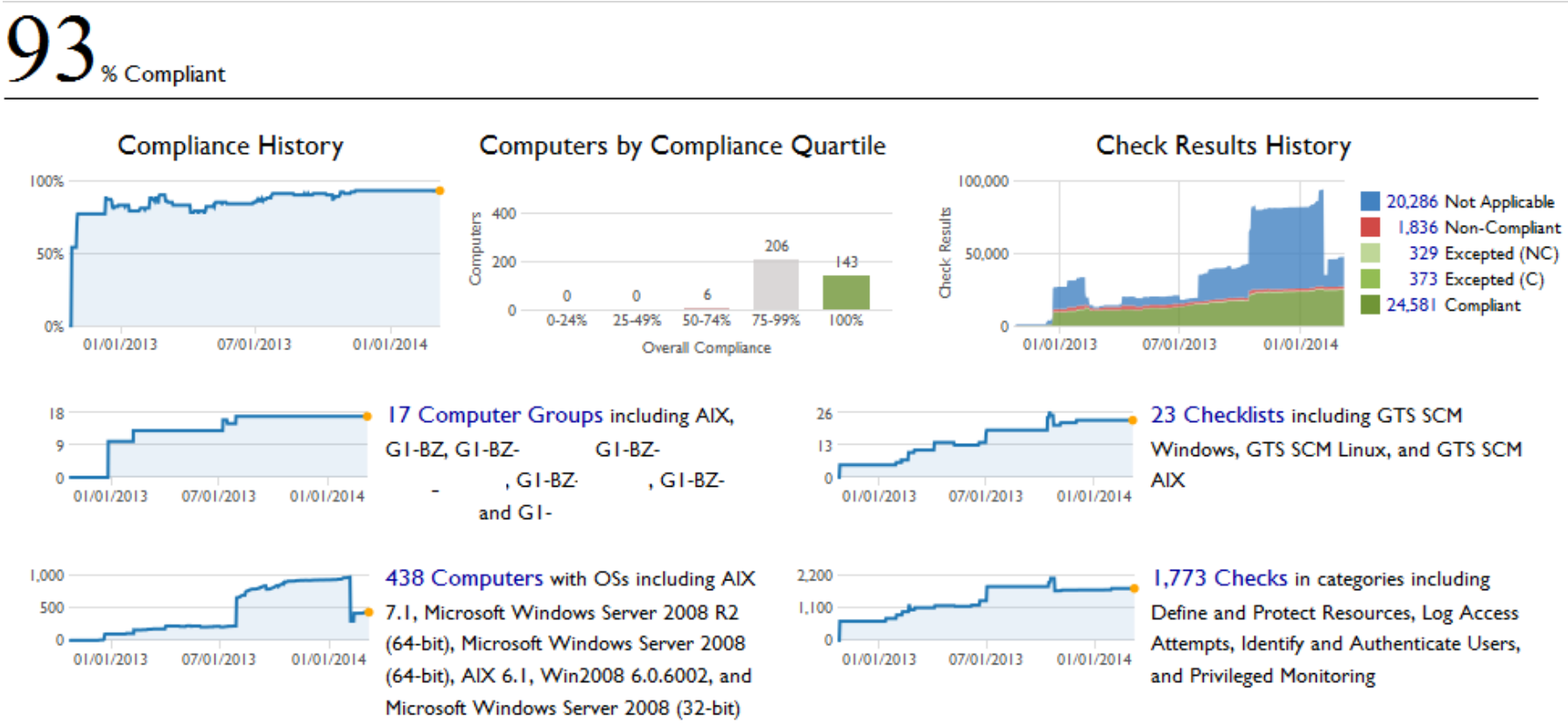
Patch correlation and remediation

- Corporate system repository contains system classification and ownership information
- Corporate security advisory classifies vulnerabilities with due dates, based on severity and system classification
- IBM Endpoint Manager identify applicable updates and security fixes
- Patch correlation and remediation tool (under development) brings them together
  - Provides list of what, why and when
  - Will allow to create policies to automate remediation based on end-user requirements

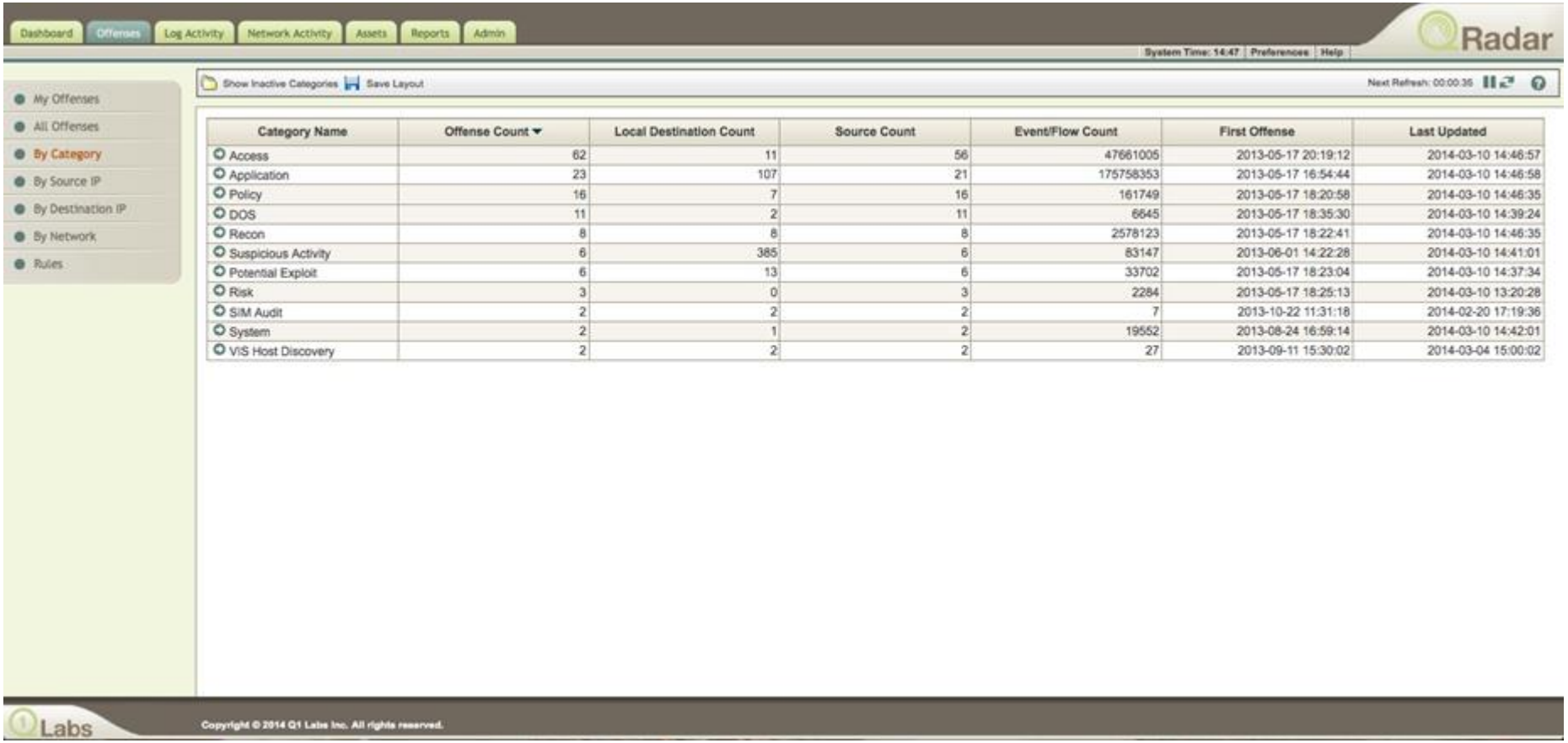
Identifier	Type	Description	Severity	Target Date	State
1	process	Initiated on Mon Mar 3 2014 20:55:35 GMT	Security	...	...
MSS-OAR-E01-2012:3823.1	patch	[RHSA-2012:1461-01] Moderate: libproxy security update	High	Sun Nov 18 2012 13:01:23 GMT	Superseded by RHSA-2013:0271
MSS-OAR-E01-2012:2382.1	patch	[RHSA-2012:1081-01] Moderate: sudo security update	Low	Thu Aug 16 2012 12:01:15 GMT	Superseded by RHSA-2012:1149
MSS-OAR-E01-2014:0347.1	patch	[RHSA-2014:0185-01] Moderate: openswan security update	Low	Fri Mar 21 2014 13:00:22 GMT	Relevant
MSS-OAR-E01-2014:0306.1	patch	[RHSA-2014:0159-01] Important: kernel security and bug fix update	Low	Fri Mar 14 2014 13:00:17 GMT	Relevant
MSS-OAR-E01-2014:0317.1	patch	[RHSA-2014:0164-01] Moderate: mysql security and bug fix update	Medium	Thu Feb 20 2014 13:00:28 GMT	Relevant
MSS-OAR-E01-2014:0287.1	patch	[RHSA-2014:0151-01] Low: wget security and bug fix update	Medium	Tue Feb 18 2014 13:00:10 GMT	Relevant
MSS-OAR-E01-2014:0226.1	patch	[RHSA-2014:0127-01] Moderate: librsvg2 security update	Low	Thu Mar 6 2014 13:00:25 GMT	Relevant
MSS-OAR-E01-2014:0235.1	patch	[RHSA-2014:0132-01] Critical: firefox security update	Medium	Wed Feb 12 2014 13:00:19 GMT	Relevant
MSS-OAR-E01-2014:0223.1	patch	[RHSA-2014:0126-01] Moderate: openldap security and bug fix update	Low	Thu Mar 6 2014 13:01:56 GMT	Relevant
MSS-OAR-E01-2014:0189.1	patch	[RHSA-2014:0097-01] Important: java-1.6.0-openjdk security update	Low	Thu Feb 27 2014 13:00:05 GMT	Superseded by RHEA-2014:0116

Security and Compliance Analytics

- Daily monitoring and reporting of security compliance and health checking

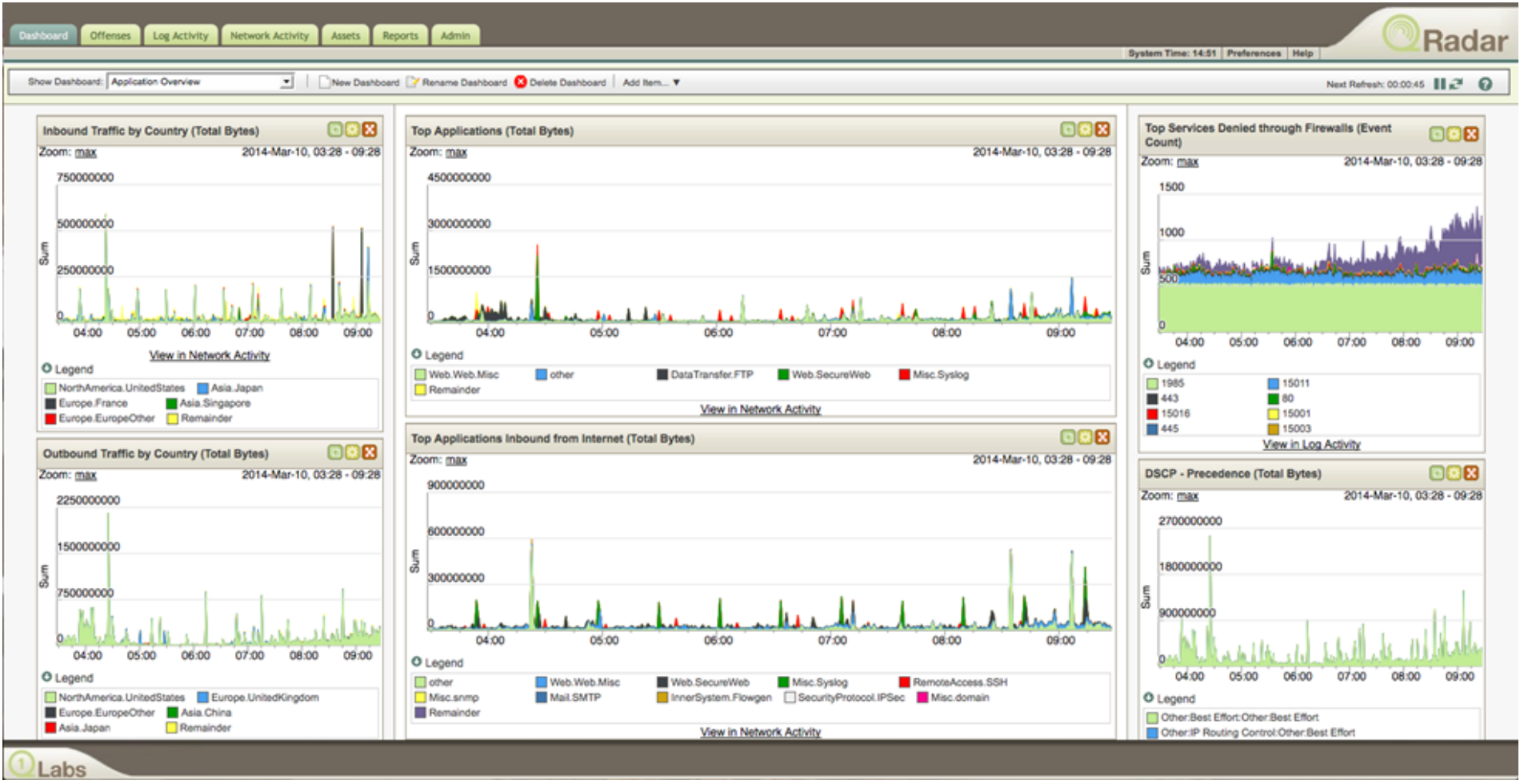


Q-Radar – Offenses by category



Category Name	Offense Count	Local Destination Count	Source Count	Event/Flow Count	First Offense	Last Updated
Access	62	11	56	47661005	2013-05-17 20:19:12	2014-03-10 14:46:57
Application	23	107	21	175758353	2013-05-17 16:54:44	2014-03-10 14:46:58
Policy	16	7	16	161749	2013-05-17 18:20:58	2014-03-10 14:46:35
DOS	11	2	11	6645	2013-05-17 18:35:30	2014-03-10 14:39:24
Recon	8	8	8	2578123	2013-05-17 18:22:41	2014-03-10 14:46:35
Suspicious Activity	6	385	6	83147	2013-06-01 14:22:28	2014-03-10 14:41:01
Potential Exploit	6	13	6	33702	2013-05-17 18:23:04	2014-03-10 14:37:34
Risk	3	0	3	2284	2013-05-17 18:25:13	2014-03-10 13:20:28
SIM Audit	2	2	2	7	2013-10-22 11:31:18	2014-02-20 17:19:36
System	2	1	2	19552	2013-08-24 16:59:14	2014-03-10 14:42:01
VIS Host Discovery	2	2	2	27	2013-09-11 15:30:02	2014-03-04 15:00:02

Q-Radar – Application Overview



Automation of compliance and health checking remediation

- We developed automation using Puppet Labs (Open Source)
  - Currently under evaluation
  - Checks and automatically applies security and compliance policy
  - Enforces security configuration, even when user (or attacker) changes configuration
  - Immediately activates when a new component is installed, applying settings to comply with policy requirements
  - Corrective actions are continuously enhanced with common issues identified by scanning and monitoring tools

Account management

- Microsoft Active Directory isn’t always the best solution
  - Corporate policy may not allow use in DMZ
  - MSAD may not retain all required approval and revalidation audit trail
  - Not all applications support MSAD
- Local ID management tool allows to bridge the gap
  - Lightweight agent
  - Customized approval process for ID creation for general and privileged users
  - Account expiration and revalidation against corporate directory
  - Unapproved local ID creation and detection
    - *Reconciliation for approved IDs*

Food for thought

- You can only protect what you know about
  - What you know is often not enough
- Security is a point in time statement, never an absolute value
- Maintaining and improving security posture is an involved process
- A few IT professionals cannot outsmart a multitude of hackers
  - However we can make their task much harder
  - Have them look for easier targets elsewhere
- If you don’t need a service, remove it
- Don’t put all of your eggs in one basket
  - Use different tools to asses risks
- Firewall and Intrusion Prevention Systems are always a good first line of defense
  - Systems behind these devices need to be secure too
- Past experience is not a guarantee of future performance


Q
A