

# RSAC<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SP01-T07

## Bridging the Divide between Security and Operations Teams

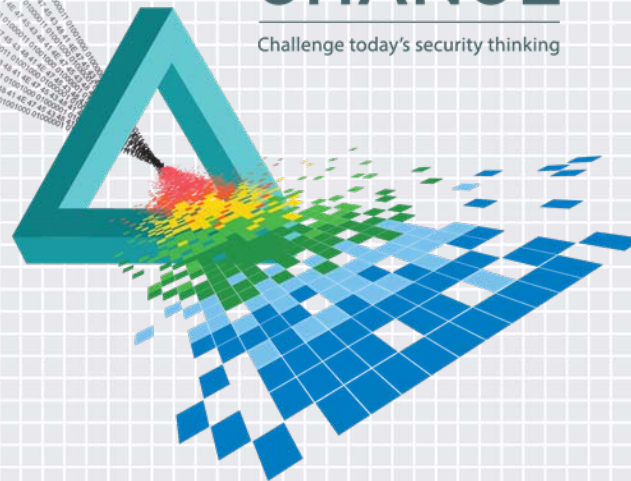
**Jonathan C. Trull**

---

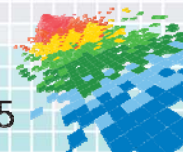
CISO  
Qualys  
@jonathantrull

# CHANGE

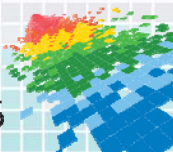
Challenge today's security thinking



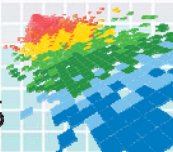
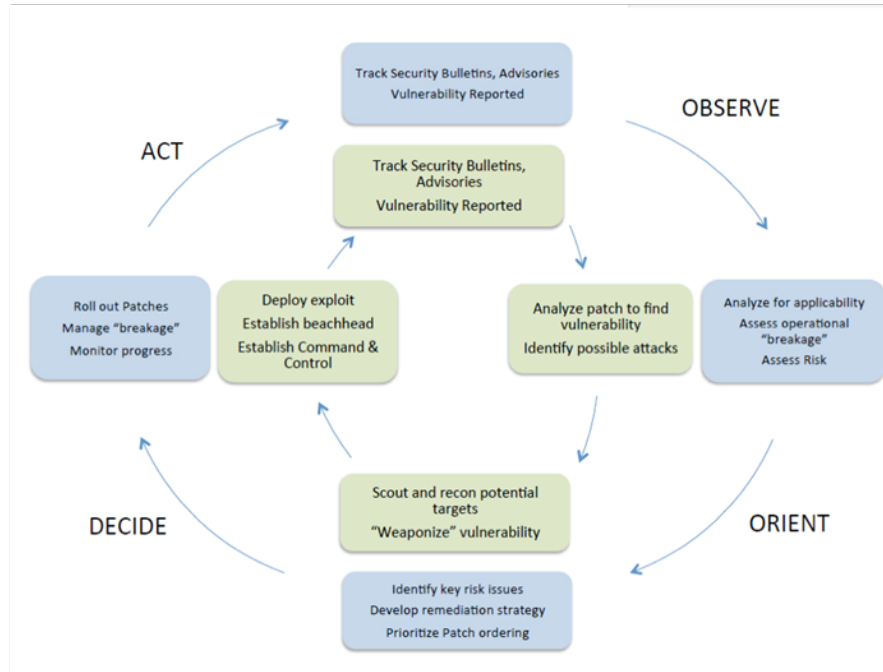
# The Great Divide



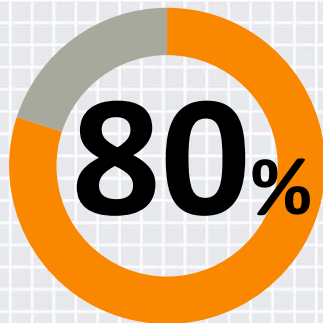
# Major Constraints on Ops and Security Teams



# Attack-Defend Cycle (OODA Loop)

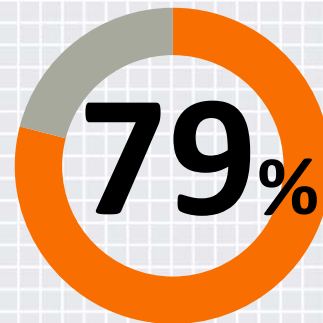


# Most breaches exploit known vulnerabilities



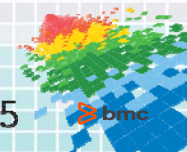
**ATTACKS**

More than 80% of attacks target **known vulnerabilities**



**PATCHES**

79% of vulnerabilities have **patches available** on day of disclosure





# Security

## Close Vulnerabilities

193 days to patch known vulnerabilities

# Operations

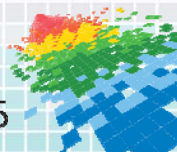
## Reduce downtime

80% of downtime due to misconfigurations

# Laws of Vulnerabilities

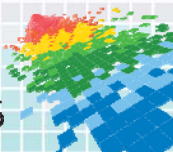
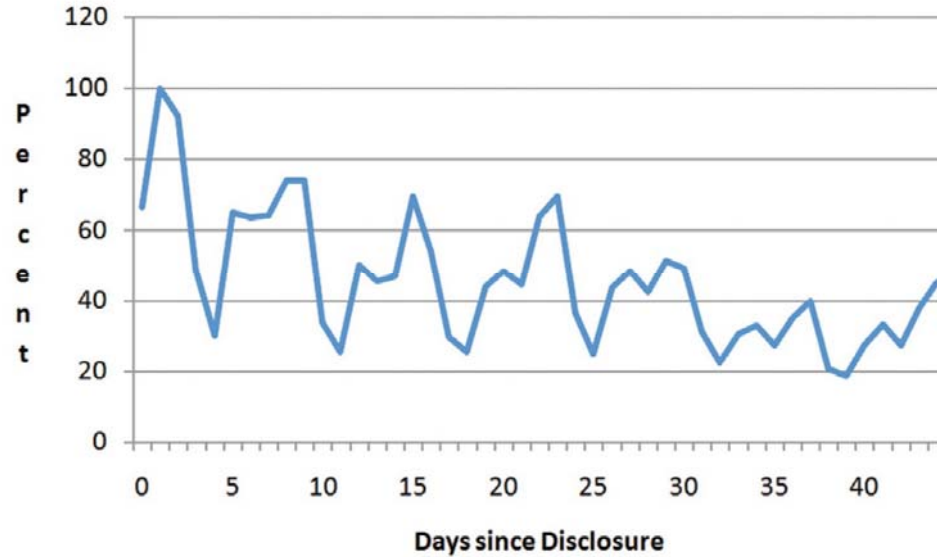
- ◆ **Half-Life** – time interval for reducing occurrence of a vulnerability by half
- ◆ **Prevalence** – turnover rate of vulnerabilities in the “Top 20” list
- ◆ **Persistence** – total lifespan of vulnerabilities
- ◆ **Exploitation** – time interval between an exploit announcement and the first attack

<https://community.qualys.com/blogs/laws-of-vulnerabilities>



# Half-Life

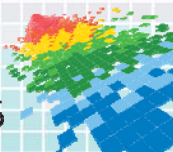
◆ 29.5 Days





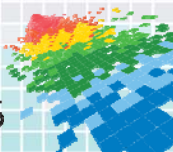
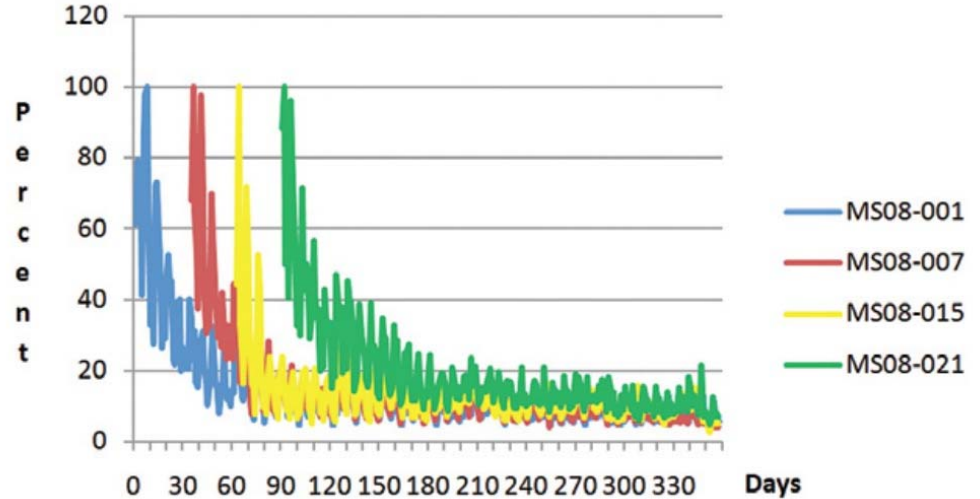
# Prevalence

- ◆ 8 critical vulnerabilities retained a constant presence in the Top 20
- ◆ Exploit Kits continuously target the same applications:
  - ◆ Java Runtime Environment
  - ◆ Adobe Flash
  - ◆ Adobe Reader
  - ◆ Internet Explorer



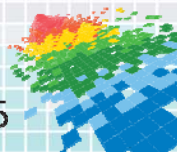
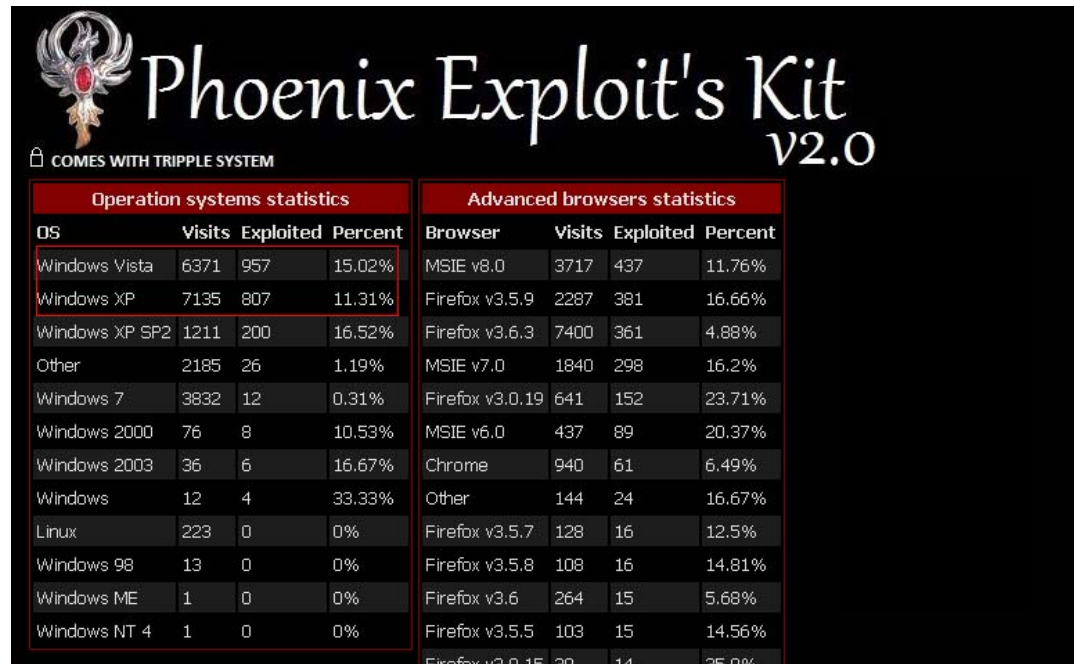
# Persistence

- ◆ Indefinite
- ◆ Stabilize at 5-10%

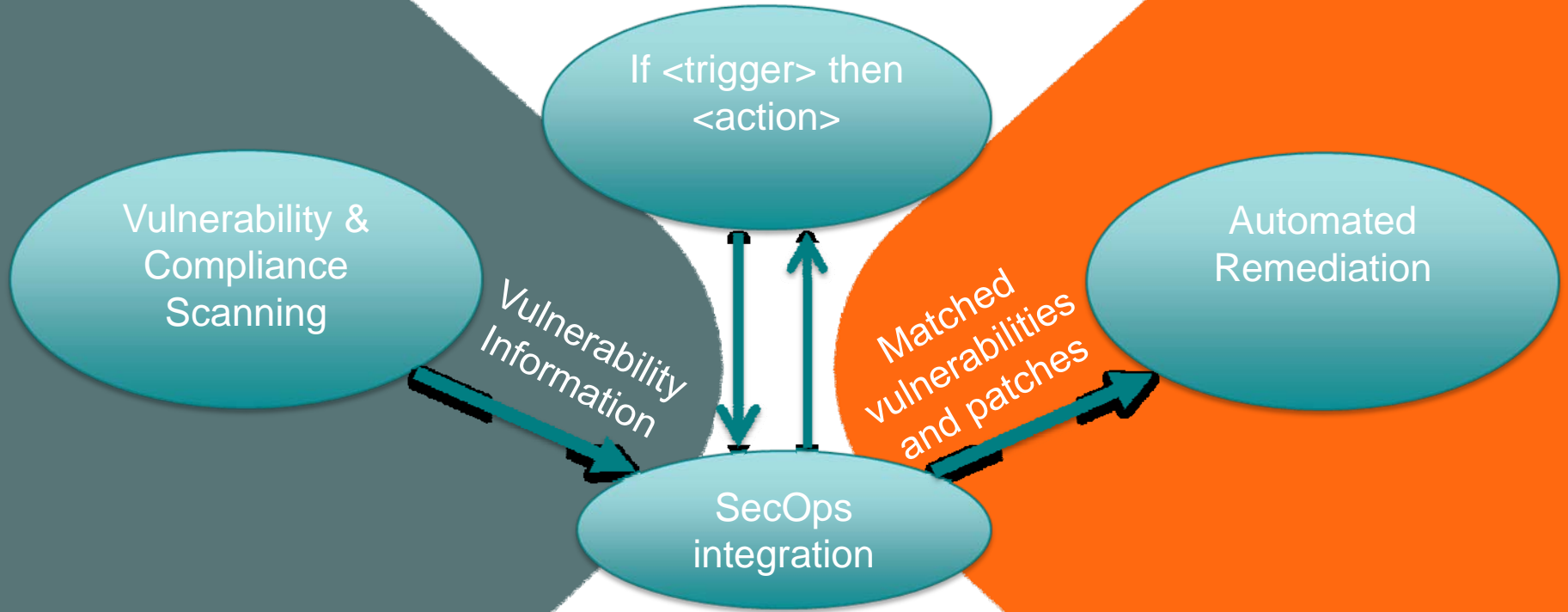


# Exploit Kits Increase Successful Attacks

- ◆ Average < 10 days
- ◆ Critical < 48 hours
- ◆ Exploit kits offer money back guarantees



# SecOps Integration



# Dashboard

Status within your permissions  
Last Updated: Today

New  
**17917**

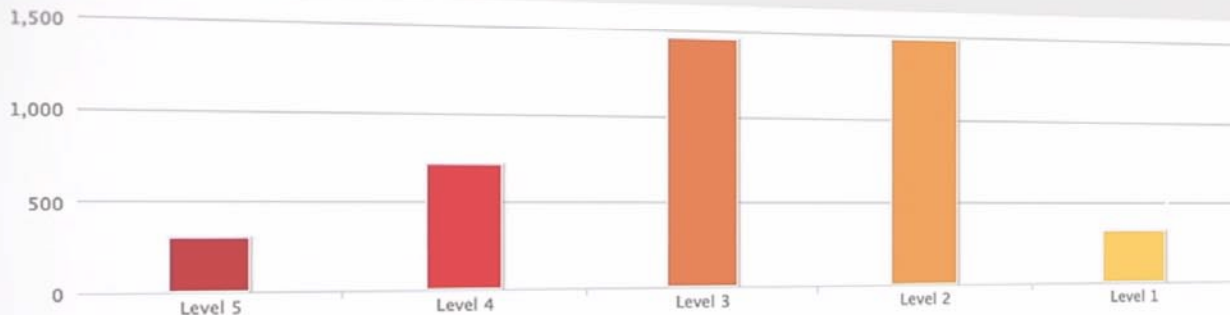
Active  
**30000**

Reopened  
**2090**

[New Scan](#)

[Schedule Scan](#)

## Vulnerabilities by severity



## Most vulnerable hosts

[View All](#)

10.10.30.117  
2K9-30-117  
10.10.10.2  
Untitled  
10.10.10.7  
STORE  
10.10.30.22  
Untitled  
10.10.34.206  
Untitled

## New MS Patch Releases

[View All](#)

Microsoft Windows Client/Server Run-Time  
Subsys...  
04/09/2013 [Info](#) | [Report](#)  
Microsoft Antimalware Client Elevation of  
Privi...  
04/09/2013 [Info](#) | [Report](#)  
HTML Sanitization Component Elevation of  
Privi...  
04/09/2013 [Info](#) | [Report](#)  
Microsoft Windows Kernel Multiple Elevation of  
...

## Latest reports

[View all](#)

VM - scheduled report  
23 Apr 2013, 16:51:09  
 DISTRIBUTION LIST - Manager  
23 Apr 2013, 16:21:09  
 VM - scheduled report  
22 Apr 2013, 16:51:09  
 DISTRIBUTION LIST - Manager  
22 Apr 2013, 16:22:10

## Your last scans

[View all](#)

Title	Date	Status
10.10.34.206	04/04/2013	Finished
10.10.30.22 - 20130403 - Init OP - 20130403	04/03/2013	Finished
10.10.30.22 - 20130403	04/03/2013	Finished
10.10.30.22 - 20130403 - Init OP	04/03/2013	Finished
10.10.30.22	04/03/2013	Finished
10.10.30.22 - 20130403 - Init OP - 20130403	04/03/2013	Finished
10.10.30.22	04/03/2013	Finished

## Most vulnerable hosts

[View all](#)

Hosts	DNS Hostname	Risk
10.10.25.219	qa.qualys.com	HIGH
10.10.10.0	balaji.qualys.com	HIGH
10.10.10.255	funkytown.vuln.qa.qualys.com	HIGH
10.10.24.0	huge.qa.qualys.com	HIGH
10.10.26.255	None	MED
10.10.30.0	ns2.vuln.qa.qualys.com	MED
10.10.30.255	STORE	MED

# Security Teams Portal

64.39.106.242 (xp-sp2, XP-SP2)

Vulnerabilities (6)

- ▶  5 Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067)
- ▶  5 EOL/Obsolete Operating System: Microsoft Windows XP Detected
- ▶  3 NetBIOS Shared Folder List Available
- ▶  3 Microsoft Windows Remote Information Disclosure (MS05-007)
- ▶  2 ICMP Based TCP Reset Denial of Service Vulnerability
- ▶  1 ICMP Timestamp Request

Potential Vulnerabilities (3)

Information Gathered (17)

64.39.106.243 (2k-sp4-oe501, 2K-SP4-OE501)

... Interface Buffer Overrun Vulnerability (MS03-026)  
... (MS03-039)

# Risk from the Security Team's Standpoint

**311**  
Hosts Scanned  
Confirmed | Potential  
5008 | 2380

[View Details](#)

**20**  
Hosts Managed  
Confirmed | Potential  
1148 | 137

[View Details](#)

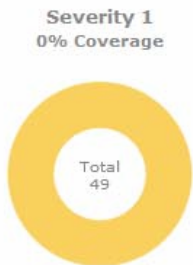
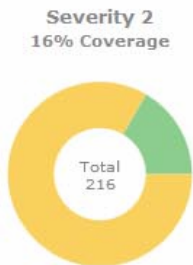
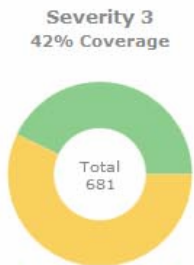
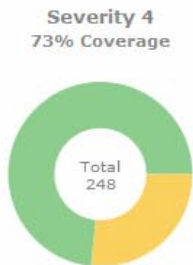
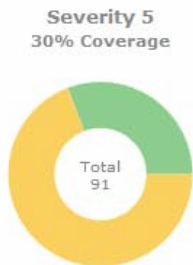
**7388**  
Total Vulnerabilities  
Managed | Unmanaged  
1285 | 6103

[View Details](#)

**2180**  
OOB Remediation  
Managed | Unmanaged  
538 | 1642

[View Details](#)

### OOB Remediation for Managed Servers





# The SecOps Portal

 Reports

 Remediate

Group By : No grouping

 Vulnerable Hosts



 Export

View 1 - 549 of 549

IP Address	HostName	OS	QID	Title	Type	Reference ID	Remediation Type	BSA Remediation	Severity	Smart Group	Qualys Tags
10.129.145.114	clm-pun-008214.bmc.com	Windows 2008	90551	Microsoft Windows GDI+ Remote Code Execution Vulnerability (MS09-062)	C	CVE-2009-2500	PATCH	✓	■■■■■	Windows	Production, Test BU and User Relation, BU_User_Relation
172.22.187.94	clm-aus-003451.bmc.com	Windows 2008	90551	Microsoft Windows GDI+ Remote Code Execution Vulnerability (MS09-062)	C	CVE-2009-2500	PATCH	✓	■■■■■	Windows	Development, Richa_CompleteScan
10.129.145.87	clm-pun-008293.bmc.com	Linux Red Hat ES 6.4	121562	Red Hat Update for Firefox (RHSA-2013-1476)	C	CVE-2013-5590	PATCH	✓	■■■■■	Linux	Development, Richa_CompleteScan, Test BU and User Relation, BU_User_Relation
10.129.145.87	clm-pun-008293.bmc.com	Linux Red Hat ES 6.4	121853	Red Hat Update for Firefox (RHSA-2014-0310)	C	CVE-2014-1493	PATCH	✓	■■■■■	Linux	Development, Richa_CompleteScan, Test BU and User Relation

# Remediation



How to schedule vulnerabilities to be fixed using patches

IPAddress	HostName	Remediation Reference	Status	Schedule Date	Notification	Ticket ID
<input checked="" type="checkbox"/> 172.22.191.79	clm-aus-003450.bmc.com	PATCH_JOB:MS09-062				

Select what to remediate

Approval Required for Remediation  Pre-Approved Remediation  Raise Change Ticket

Remediation Group Name

Patch fix

Request Approval

Emergency Fix

Schedule

2015-02-17 11:39:42

“Go Fix It button”

Applicable for Patch Remediation

# Scheduling & Approvals

⏪ Previous

[Reports](#)
[Remediate](#)

Group By: No grouping

Vulnerable Hosts

Export

1 - 5 of 5

	IPAddress	HostName	OS	QID	Title	Type	Reference ID	Remediation Type	BSA Remediation	Severity	Smart Group	Qualys Tags
<input checked="" type="checkbox"/>	192.168.100.1	onbmc-s	Windows 2008	90882	Windows Remote Desktop Protocol Weak Encryption Method Allowed	<b>C</b>		CONFIG			All Servers, Available, BSA Infrastructure	BDC, BDC Network
<input type="checkbox"/>	192.168.100.2	bl-appserver	Windows 2008	90782	Microsoft Windows DNS Server Denial of Service Vulnerability (MS12-017)	<b>P</b>	CVE-2012-0006	PATCH			All Servers, Available, BSA Infrastructure, All PCI	BDC, BDC Network
<input type="checkbox"/>	192.168.100.3	WINDB.bmc.local	Windows 2008	90882	Windows Remote Desktop Protocol Weak Encryption Method Allowed	<b>C</b>		CONFIG			All Servers, Windows Servers, Available, Backend, Corporate Website, Database Form	BDC, BDC Network

How to select and schedule vulnerabilities that can be fixed using configuration packages.

Use a Config package

## Configuration Packages

**Summary**

Patch Remediation

Config Remediation

5

Remediations Jobs

✓ 5

Jobs Completed

☑ 3

Jobs Successful

✕ 2

Jobs Failed

⚙ 0

Jobs Pending

💻 5

Servers Remediated

## Remediation Action Summary

🔍 🔄 📄 Export

Page 1 of 1

View 1 - 2 of 2

Group	Date Created	Start Time	End Time	Total Time	Job Execution Time	Server Count	Vulnerabilities	Status
CfgGrp	2015-02-17 10:59:22.705	2015-02-17 11:04:18.000	2015-02-17 11:05:34.0	6 mins 11 sec	1 mins 16 sec	3	1	COMPLETED
PatchGrp	2015-02-17 11:02:38.952	2015-02-17 11:07:34.000	2015-02-17 11:37:12.0	34 mins 33 sec	29 mins 38 sec	2	2	COMPLETED

🔍 🔄 📄 Export

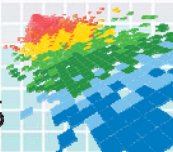
View 1 - 2 of 2

Job results for remediation group actions

# Results

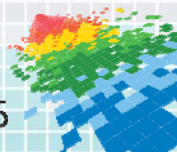
# Morningstar Case Study

- ◆ Decreased configuration compliance audit cycle from 2 months to 5 days
- ◆ Reduced audit and patch time by 97%
- ◆ Reduced compliance audit time from 5 days to 12 minutes per system
- ◆ Provided 100% SOX compliance



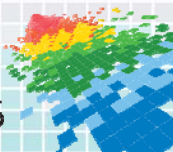
# State of Michigan Case Study

- ◆ Heartbleed – vulnerability in OpenSSL
- ◆ Needed to quickly patch servers spread across the State
- ◆ Connected VM and Patch Management solutions to remediate Heartbleed in record time



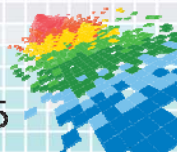
# Advantages of Bridging the Divide

- ◆ Significant decrease in configuration audit cycles
- ◆ Significant reduction in approval and patch deployment time frames
- ◆ Reduce audit remediation from months to hours
- ◆ Enhanced ability to report/communicate meaningful information to business stakeholders



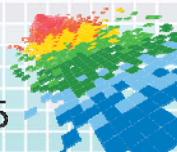
# Bridging the Divide

- ◆ Arm the security and Ops teams with the right tools for the job
- ◆ Communicate vertically and horizontally within your Organization
  - ◆ Essential to remove fear, uncertainty, and doubt
  - ◆ Embed security staff within key operational functions – e.g., CAB



# Bridging the Divide (Cont)

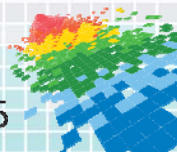
- ◆ Orchestrate/automate infrastructure security
  - ◆ Continuously enforce controls/changes
  - ◆ Validate changes through logs/audit trail
- ◆ Perform continuous compliance monitoring
  - ◆ All systems all the time
- ◆ Automate remediation based on key triggers/risks
  - ◆ If <trigger> then <action>





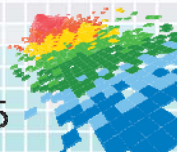
# Bridging the Divide (Cont)

- ◆ Measure the security and Ops teams' performance by the half-life results & treatment of the persistence law
  - ◆ Include results in HR performance reviews / bonuses
- ◆ Integrate VM/CM solution with patch & configuration management systems, asset inventory systems, ticketing systems, configuration systems (BMC BladeLogic / Chef / Puppet), and reporting systems



# Bridging the Divide (Cont)

- ◆ Focus patching efforts on those things that will hurt you most
- ◆ Select a VM/CM solution with strong APIs, integration, and that limits resources spent on system administration
- ◆ Learn to speak the language of the Ops team



# Apply What You Have Learned Today

- ◆ **Next week you should:**
  - ◆ Review the process by which vulnerabilities and misconfigurations are identified and delivered to your operations teams for action/remediation
- ◆ **In the first three months following this presentation you should:**
  - ◆ Identify opportunities to integrate threat and vulnerability systems with key operational systems (ticketing, CMDB, GRC, patch and configuration management)
  - ◆ In cooperation with Ops, define a core set of “if-then” rules that will automatically trigger remediation
- ◆ **Within six months you should:**
  - ◆ Define a set of agreed upon remediation metrics appropriate for different governance layers and begin tracking those metrics
  - ◆ Automate 20% of your vulnerability and configuration management workflow

