

# IT and Security: BFFs?

Align with Active Vulnerability Management

Nathan Palanov, Solutions Marketing Manager



Gain the clarity, command, and confidence to embrace innovation and drive your business forward. Rapid7 transforms your data and uncertainty into answers.

# We can help you with...



Vulnerability  
Management



SIEM



Application  
Security



IT Operations



User Behavior  
Analytics



Penetration  
Testing



Managed Services



Security Advisory  
Services

# IT and Security: BFFs?

Align with Active Vulnerability Management

Nathan Palanov, Solutions Marketing Manager

# IT & Security: Differing Goals?



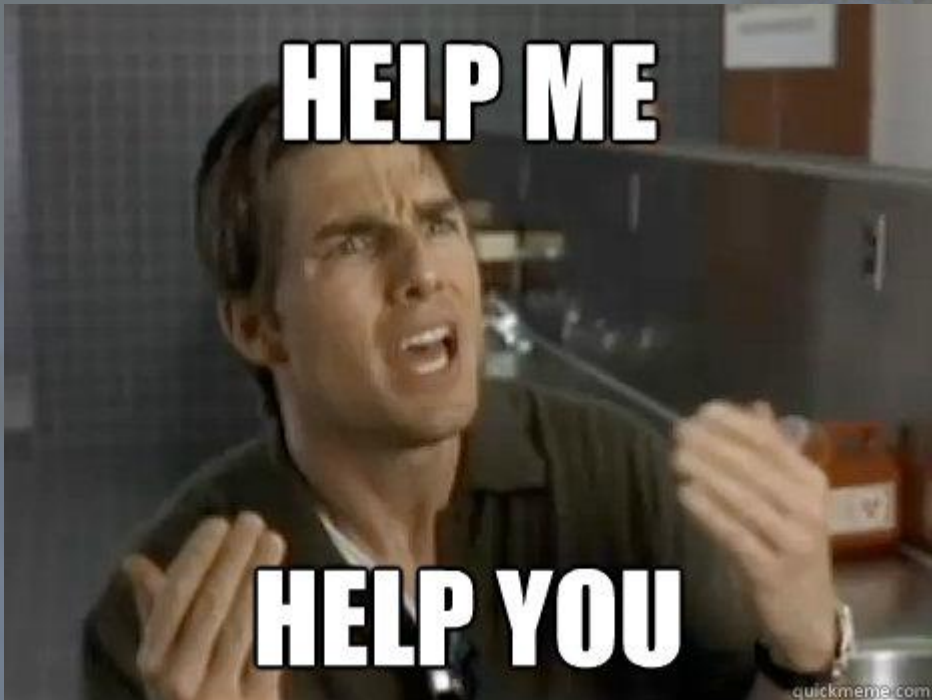
- Keep things running
- Precise Instructions
- Use existing ticketing workflow
- Remediation is secondary



- Keep things secure
- Detailed information
- Use whatever tool that works
- Remediation is primary

# In Reality...We Go Great Together

Business needs to optimize availability and security



Need the right information to understand how to  
prioritize and be efficient

Want to work together, not separately

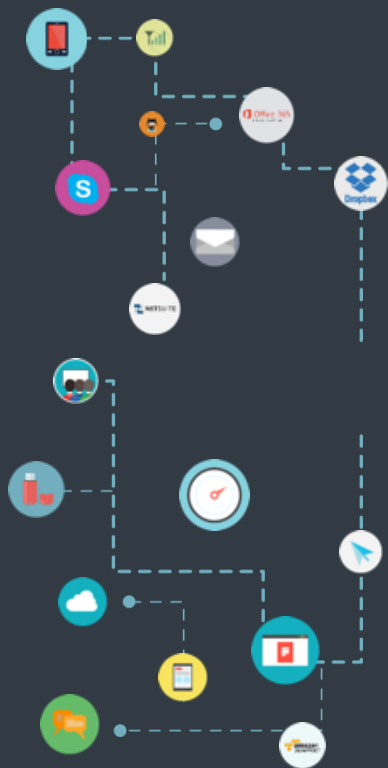
Remediation takes time and is an ongoing effort

# Security's Current Process is Tough

Teams are understaffed



Networks are alive



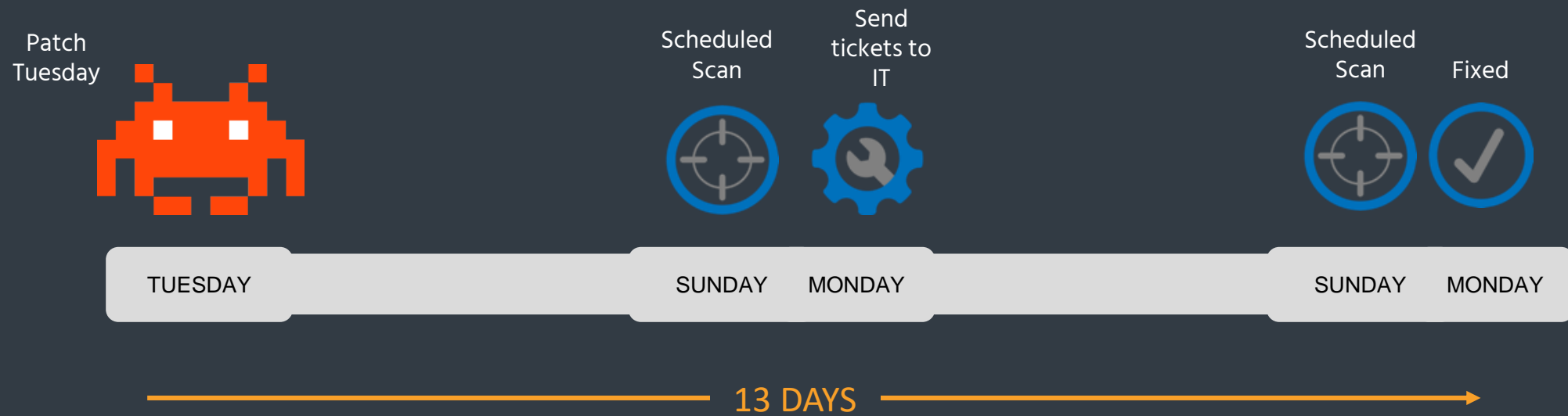
Tools Are passive and reactive



Security professionals are trapped waiting for scans



# Then





+ Add Card



WHAT'S NEW

CVE-2016-2428 May 9, 2016  
Affects Media Files processing

ImageTragick May 5, 2016  
Affects Image manipulation software

Critical MS Remote Code Exec Vulnerability Apr 7, 2016  
Affects Microsoft Windows

Expand Card >

AGENTS®

4074 Agents

Monitoring remote endpoints

Expand Card >

TOP TRENDING VULNERABILITIES

Name	New Instances	Total Instances	Risk Score Increase
MS16-057: Security Update for Windows Shell (31...	660	660	566k ^
MS16-044: Security Update for Microsoft Office 2013...	440	440	496k ^
APSB16-02: Security Updates Available for Adobe...	390	390	329k ^
MS16-046: Security Update for SAM and LSAD Re...	196	283	197k ^
RHSA-2010.0652: ImageMagick security and bug f...	96	280	160k ^

Expand Card >

NUMBER OF ASSETS

7145 Assets

↑ 11% change

in the past 30 days

AVERAGE VULNERABILITY AGE BY SEVERITY

Age in Days/Severity	Moderate	Severe	Critical
0-29	25	131	72
30-59	44	103	35
60-90	31	69	12
>90	28	44	18

NUMBER OF VULNERABILITIES

24851 Vulnerabilities

↑ 15% change

in the past 30 days

2k Critical

5k Severe

17k Moderate

nexpose

Transforming vulnerability data into prioritized answers and actions

My Liveboard

+ ADD CARD

TOTAL ASSET TRENDS

56.75k

Total Assets

↑ 1704 (3% change)

in the past 30 days

Expand Card

ASSETS BY LAST SCAN DATE

61% of my assets have not been scanned in >120 days.

Time	Count
0-30 Days	~6k
30-60 Days	~3k
60-90 Days	~3k
90-120 Days	~4k
> 120 Days	~26k

Expand Card

ASSETS RUNNING OBSOLETE OPERATING SYSTEMS

7%

of assets running obsolete OS

Expand Card

ASSETS WITH EXPIRED SSL CERTIFICATES

1.86k

Assets

With Expired SSL certificates

Expand Card

ASSETS WITH EXPIRING SSL CERTIFICATES

15

Assets

With Expiring SSL certificates

in the next 30 days

Expand Card

EXPLOITABLE ASSETS BY SKILL LEVEL

19% of assets in your environment can be exploited by a novice

Expand Card

ASSETS BY AUTHENTICATION STATUS

7% of my assets had failed logins

Expand Card

ASSETS BY OPERATING SYSTEM

51.50% of my assets are running the Microsoft Operating System

Operating System	Assets
Microsoft	~28k
Ubuntu	~10k
Linux	~5k
Unknown OS	~2k
Debian	~1k
Cisco	~1k
Red Hat	~1k
Sun	~1k
VMware	~1k
Other	~2k

Expand Card

NEWLY DISCOVERED ASSETS

ASSETS WITH DEFAULT ACCOUNT VULNERABILITIES

TOP RISKIEST ASSETS

Asset	IP Address	Vulnerabilities	Risk Score
thunderbird-u.vuln.lax.rapid7_	10.4.18.70	10	6.29t

ASSETS WITH CRITICAL RISK VULNERABILITIES

TOTAL ASSET TRENDS

56.75k

Total Assets

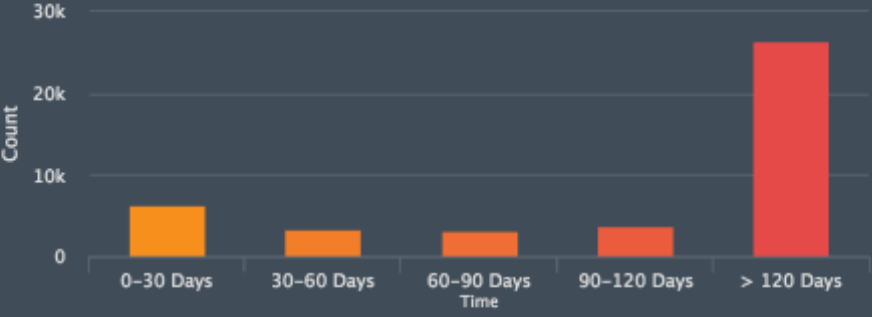
↑ 1704 (3% change)

in the past 30 days

Expand Card >


ASSETS BY LAST SCAN DATE

61% of my assets have not been scanned in >120 days.



Expand Card >

ASSETS RUNNING OBSOLETE OPERATING SYSTEMS



7%

of assets running obsolete OS

Expand Card >

ASSETS WITH EXPIRED SSL CERTIFICATES

1.86k

Assets

With Expired SSL certificates

Expand Card >

ASSETS WITH EXPIRING SSL CERTIFICATES

15

Assets


With Expiring SSL certificates

in the next 30 days

Expand Card >

EXPLOITABLE ASSETS BY SKILL LEVEL


19% of assets in your environment can be exploited by a novice



Expand Card >

ASSETS BY AUTHENTICATION STATUS

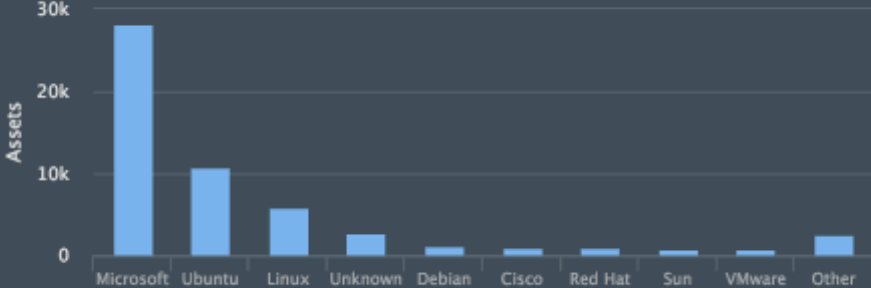
7% of my assets had failed logins



Expand Card >

ASSETS BY OPERATING SYSTEM

51.50% of my assets are running the Microsoft Operating System



Expand Card >

NEWLY DISCOVERED ASSETS

ASSETS WITH DEFAULT ACCOUNT VULNERABILITIES

TOP RISKIEST ASSETS

Asset	IP Address	Vulnerabilities	Risk Score
thunderbird-u.vuln.lax.rapid7	10.4.18.70	10	6.29

ASSETS WITH CRITICAL RISK VULNERABILITIES



Total Asset Trends - *edited*

SAVE CARD

CLOSE

heartbleed

asset.vulnerability.description CONTAINS "heartbleed"

SAVE FILTER

APPLY

1,893

Total Assets  
↑ 185 (11% change)  
in the past 30 days

☐

Remediate

(0 of 185 selected)

	IP Address	Asset	Operating System	Vulnerabilities	Risk Score	Exploit Count	Malware Count
<input type="checkbox"/>	10.4.26.7	freebsd-10-fake-u.vuln.lax.rapid7.com	FreeBSD 10.0-RELEASE	2403	1.19m	742	61
<input type="checkbox"/>	10.4.24.62	freebsd-10-hb-port-u.vuln.lax.rapid7.com	FreeBSD 10.0-RELEASE-p1	2393	1.19m	738	61
<input type="checkbox"/>	10.4.27.15	fake-fusion-414	Apple Mac OS X 10.5.8	2127	1.15m	225	38
<input type="checkbox"/>	10.4.17.44	my51-centos6-64-u.vuln.lax.rapid7.com	CentOS Linux 6.0	1521	610.61k	164	65
<input type="checkbox"/>	10.4.25.225	SAMBA300S-CENTO	CentOS Linux 6.0	1431	597.3k	164	65
<input type="checkbox"/>	10.4.25.66	samba300s-centos.vuln.lax.rapid7.com	CentOS Linux 6.0	1432	597.29k	164	65
<input type="checkbox"/>	10.4.19.182	samba200s-centos	CentOS Linux 6.0	1420	593.07k	172	65
<input type="checkbox"/>	10.4.28.211	osuse13-en1-64-u.vuln.lax.rapid7.com	OpenSUSE Linux 13.1	1575	508.69k	177	3



My Liveboard

+ ADD CARD

TOTAL ASSET TRENDS

56.75k

Total Assets

↑ 1704 (3% change)

in the past 30 days

Expand Card >

ASSETS BY LAST SCAN DATE



Expand Card >

ASSETS RUNNING OBSOLETE OPERATING SYSTEMS



Expand Card >

ASSETS WITH EXPIRED SSL CERTIFICATES

1.86k

Assets

With Expired SSL certificates

Expand Card >

ASSETS WITH EXPIRING SSL CERTIFICATES

15

Assets

With Expiring SSL certificates

in the next 30 days

Expand Card >

EXPLOITABLE ASSETS BY SKILL LEVEL

19% of assets in your environment can be exploited by a novice



Expand Card >

ASSETS BY AUTHENTICATION STATUS

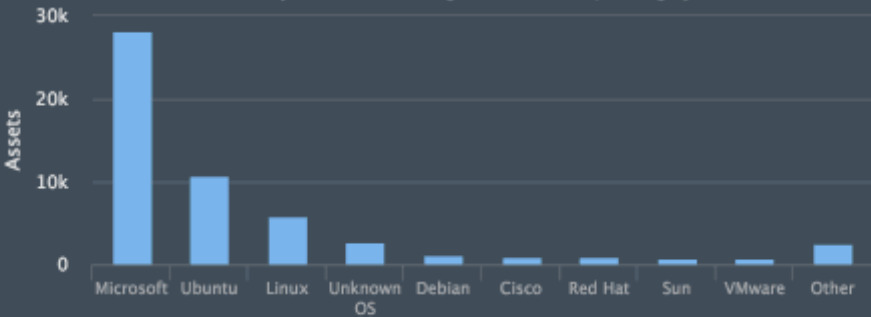
7% of my assets had failed logins



Expand Card >

ASSETS BY OPERATING SYSTEM

51.50% of my assets are running the Microsoft Operating System



Expand Card >

NEWLY DISCOVERED ASSETS

ASSETS WITH DEFAULT ACCOUNT VULNERABILITIES

TOP RISKIEST ASSETS

Asset	IP Address	Vulnerabilities	Risk Score
thunderbird-u.vuln.lax.rapid7_	10.4.18.70	10	6.29t

ASSETS WITH CRITICAL RISK VULNERABILITIES





My Liveboard

+ ADD CARD

TOTAL ASSET TRENDS

56.75k

Total Assets

↑ 1704 (3% change)

in the past 30 days

Expand Card >

ASSETS BY LAST SCAN DATE



Expand Card >

ASSETS RUNNING OBSOLETE OPERATING SYSTEMS



Expand Card >

ASSETS WITH EXPIRED SSL CERTIFICATES

1.86k

Assets

With Expired SSL certificates

Expand Card >

ASSETS WITH EXPIRING SSL CERTIFICATES

15

Assets

With Expiring SSL certificates

in the next 30 days

Expand Card >

EXPLOITABLE ASSETS BY SKILL LEVEL

19% of assets in your environment can be exploited by a novice



Expand Card >

ASSETS BY AUTHENTICATION STATUS

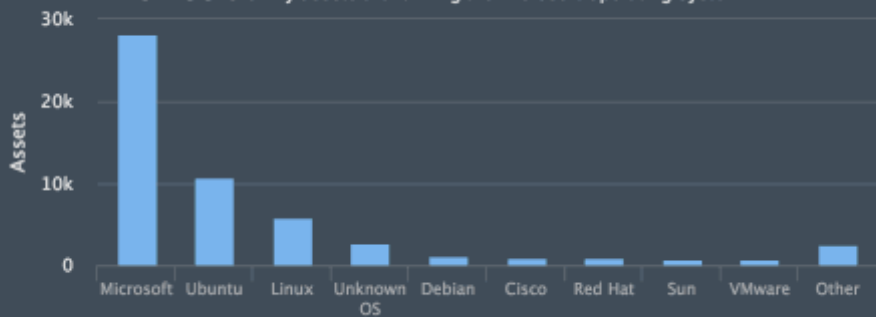
7% of my assets had failed logins



Expand Card >

ASSETS BY OPERATING SYSTEM

51.50% of my assets are running the Microsoft Operating System



Expand Card >

NEWLY DISCOVERED ASSETS

ASSETS WITH DEFAULT ACCOUNT VULNERABILITIES

TOP RISKIEST ASSETS

Asset	IP Address	Vulnerabilities	Risk Score
thunderbird-u.vuln.lax.rapid7...	10.4.18.70	10	6.29t

ASSETS WITH CRITICAL RISK VULNERABILITIES





Assets by Last Scan Date - *edited*

SAVE CARD CLOSE

heartbleed

asset.vulnerability.description CONTAINS "heartbleed"

SAVE FILTER

APPLY



☐ Remediate (0 of 56747 selected)

	IP Address	Asset	Operating System	Vulnerabilities	Risk Score	Exploit Count	Malware Count
<input type="checkbox"/>	10.4.26.7	freebsd-10-fake-u.vuln.lax.rapid7.com	FreeBSD 10.0-RELEASE	2403	1.19m	742	61
<input type="checkbox"/>	10.4.24.62	freebsd-10-hb-port-u.vuln.lax.rapid7.com	FreeBSD 10.0-RELEASE-p1	2393	1.19m	738	61
<input type="checkbox"/>	10.4.19.182	samba200s-centos	CentOS Linux 6.0	1421	1.18m	166	65
<input type="checkbox"/>	10.4.27.15	fake-fusion-414	Apple Mac OS X 10.5.8	2127	1.15m	225	38
<input type="checkbox"/>	10.4.26.7	freebsd-10-fake-u.vuln.lax.rapid7.com	FreeBSD 10.0-RELEASE	2090	1.11m	714	61
<input type="checkbox"/>	10.4.24.62	freebsd-10-hb-port-u.vuln.lax.rapid7.com	FreeBSD 10.0-RELEASE-p1	2086	1.11m	710	61

🏠

My Liveboard

+ ADD CARD

TOTAL ASSET TRENDS

56.75k

Total Assets

↑ 1704 (3% change)

in the past 30 days

Expand Card >

ASSETS BY LAST SCAN DATE

61% of my assets have not been scanned in >120 days.

Time	Count
0-30 Days	~6k
30-60 Days	~3k
60-90 Days	~3k
90-120 Days	~4k
> 120 Days	~26k

Expand Card >

ASSETS RUNNING OBSOLETE OPERATING SYSTEMS

7%

of assets running obsolete OS

Expand Card >

ASSETS WITH EXPIRED SSL CERTIFICATES

1.86k

Assets

With Expired SSL certificates

Expand Card >

ASSETS WITH EXPIRING SSL CERTIFICATES

15

Assets

With Expiring SSL certificates

in the next 30 days

Expand Card >

EXPLOITABLE ASSETS BY SKILL LEVEL

19% of assets in your environment can be exploited by a novice

Expand Card >

ASSETS BY AUTHENTICATION STATUS

7% of my assets had failed logins

Expand Card >

ASSETS BY OPERATING SYSTEM

51.50% of my assets are running the Microsoft Operating System

Operating System	Assets
Microsoft	~28k
Ubuntu	~10k
Linux	~5k
Unknown OS	~2k
Debian	~1k
Cisco	~1k
Red Hat	~1k
Sun	~1k
VMware	~1k
Other	~2k

Expand Card >

NEWLY DISCOVERED ASSETS

ASSETS WITH DEFAULT ACCOUNT VULNERABILITIES

TOP RISKIEST ASSETS

Asset	IP Address	Vulnerabilities	Risk Score
thunderbird-u.vuln.lax.rapid7_	10.4.18.70	10	6.29t

ASSETS WITH CRITICAL RISK VULNERABILITIES

?





✓ Remediation project LA Windows to fix was created successfully. [Click here to view your new project.](#)

Assets Running Obsolete Operating Systems - *edited*

SAVE CARD

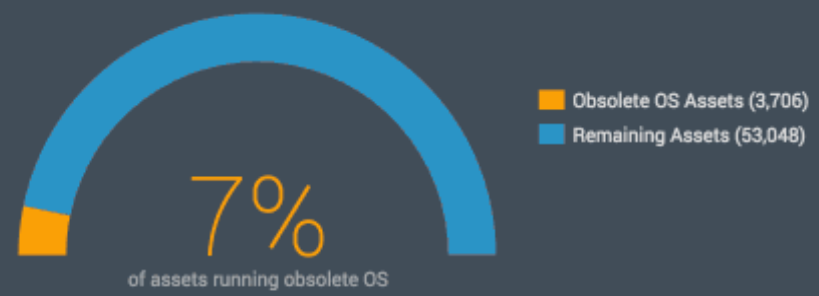
CLOSE

Microsoft

asset.os <=> ( vendor = "microsoft" ) AND asset.sites IN [ "los angeles - full audit" ]

SAVE FILTER

APPLY



☒ ☐

☐ ☐

☒ Remediate ☐ (1586 of 1586 selected)

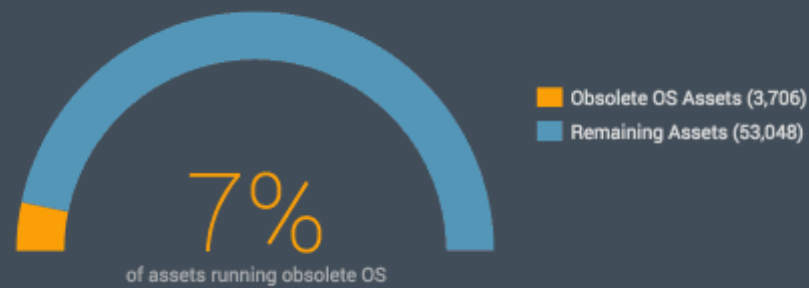
	IP Address	Asset	Operating System	Vulnerabilities	Risk Score	Exploit Count	Malware Count
<input checked="" type="checkbox"/>	10.4.19.33	dsgnr13sp1-6-u	Microsoft Windows 7 Enterprise Edition SP1	1506	1.53m	404	32
<input checked="" type="checkbox"/>	10.4.19.26	W7X64-KOREAN	Microsoft Windows 7 Enterprise Edition SP1	1468	1.5m	394	32
<input checked="" type="checkbox"/>	10.4.19.114	VLC-P	Microsoft Windows 7 Enterprise Edition SP1	1468	1.5m	392	32
<input checked="" type="checkbox"/>	10.4.19.120	FLASH11-W7-6-U	Microsoft Windows 7 Enterprise Edition SP1	1467	1.5m	392	32
<input checked="" type="checkbox"/>	10.4.19.191	C2-2003-SP2-3P	Microsoft Windows Server 2003, Enterprise Edition SP2	1429	1.5m	356	89
<input checked="" type="checkbox"/>	10.4.19.191	C2-2003-SP2-3P	Microsoft Windows Server 2003, Enterprise Edition SP2	1429	1.5m	346	89



✓ Remediation project LA Windows to fix was created successfully. [Click here to view your new project.](#)

Assets Running Obsolete Operating Systems - *edited* SAVE CARD CLOSE

Microsoft asset.os <=> ( vendor = "microsoft" ) AND asset.sites IN [ "los angeles - full audit" ] SAVE FILTER APPLY



☒ Remediate (1586 of 1586 selected)

	IP Address	Asset	Operating System	Vulnerabilities	Risk Score	Exploit Count	Malware Count
<input checked="" type="checkbox"/>	10.4.19.33	dsgnr13sp1-6-u	Microsoft Windows 7 Enterprise Edition SP1	1506	1.53m	404	32
<input checked="" type="checkbox"/>	10.4.19.26	W7X64-KOREAN	Microsoft Windows 7 Enterprise Edition SP1	1468	1.5m	394	32
<input checked="" type="checkbox"/>	10.4.19.114	VLC-P	Microsoft Windows 7 Enterprise Edition SP1	1468	1.5m	392	32
<input checked="" type="checkbox"/>	10.4.19.120	FLASH11-W7-6-U	Microsoft Windows 7 Enterprise Edition SP1	1467	1.5m	392	32
<input checked="" type="checkbox"/>	10.4.19.191	C2-2003-SP2-3P	Microsoft Windows Server 2003, Enterprise Edition SP2	1429	1.5m	356	89
		SP2-3P	Microsoft Windows Server 2003, Enterprise Edition SP2	1429	1.5m	346	89



Remediation Projects (beta)

CREATE A PROJECT

34 Projects

26  
Open

8  
Owned by Me

1  
Assigned to Me

☐

▼

🗑

✎

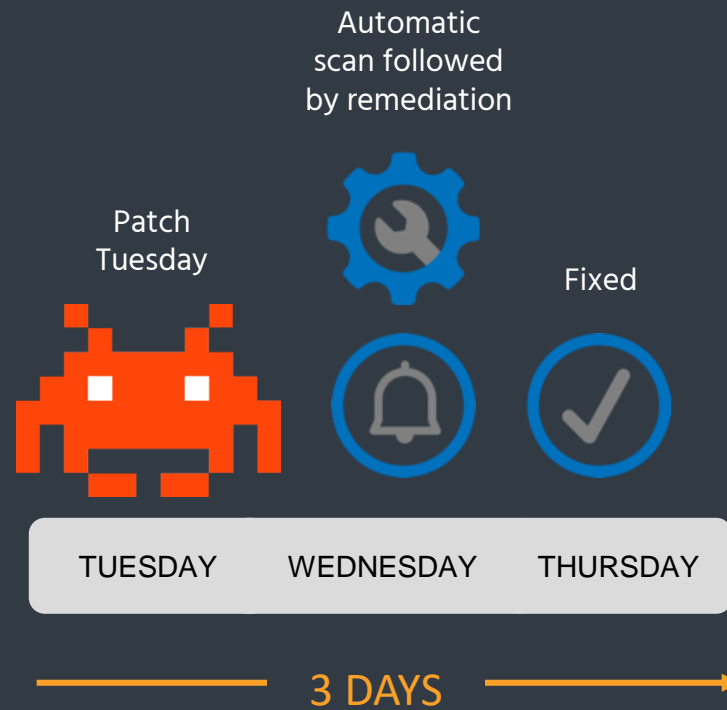
Update Status ▼

Remediation Projects (beta) (0 of 34 selected)

	Project Name	Progress	Solutions Resolv...	Remaining Ti...	Due On	Assets Affect...	Assignees	Type	Stat...
<input type="checkbox"/>	from assets with critical risk vulns	<div><div></div></div> 54%	807 of 1505	-	-	11	aebiko, amassoudi, B...	Dynamic	Open
<input type="checkbox"/>	from assets with expiring certs 2	<div><div></div></div> 22%	2984 of 13568	-	-	266	bb2, butterfly1, binish...	Static	Open
<input type="checkbox"/>	from assets with expiring ssl certs	<div><div></div></div> 22%	2984 of 13568	-	-	265	-	Static	Open
<input type="checkbox"/>	LA Windows to fix	<div><div></div></div> 0%	0 of 5771	a month	Tue, Feb 28, 2017	84	admin	Static	Open
<input type="checkbox"/>	Linux Riskiest Assets	<div><div></div></div> 56%	2260 of 4057	Past Due	Mon, Oct 31, 2016	213	aadmin	Static	Open
<input type="checkbox"/>	Linux Riskiest Assets 2	<div><div></div></div> 0%	0 of 13	Past Due	Mon, Oct 31, 2016	12	admin	Static	Open
<input type="checkbox"/>	Marilyn's Project	<div><div></div></div> 9%	1 of 11	Past Due	Wed, Oct 26, 2016	21	servicenowtagging	Static	Open
<input type="checkbox"/>	match_all_test	<div><div></div></div> 0%	0 of 3	Past Due	Thu, Dec 29, 2016	1	-	Static	Open
<input type="checkbox"/>	Obsolete Microsoft OS Assets	<div><div></div></div> 0%	2 of 413	Past Due	Wed, Nov 9, 2016	1478	Conor, admin	Dynamic	Closed
<input type="checkbox"/>	Patch Tues Priority - 2	<div><div></div></div> 3%	30 of 1108	-	-	1409	-	Dynamic	Open
<input type="checkbox"/>	patch tues priority 3	<div><div></div></div> 20%	40 of 202	-	-	47	-	Dynamic	Open
<input type="checkbox"/>	Patch Tuesday - Sept 2016	<div><div></div></div> 2%	83 of 3336	Past Due	Mon, Oct 3, 2016	411	jliou	Static	Open
<input type="checkbox"/>	Patch Tuesday Riskiest Assets	<div><div></div></div> 40%	30 of 75	Past Due	Sat, Oct 1, 2016	2	kmizota	Dynamic	Closed



# Now





## BFFs Again!

- Translate complex requests into simple and precise tasks
- Integrate with existing ticketing systems to avoid emergency meetings and back and forth
- Understand clearly where projects stand and how to align resources
- Get home to your family on time!

# Thank You