

Behind the Analytics ...and the FUD

Matt Hathaway, Director, IDR Solutions



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

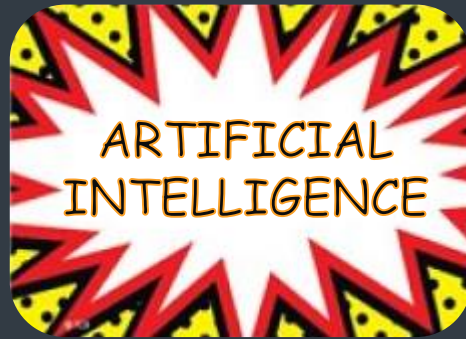


Security Advisory
Services

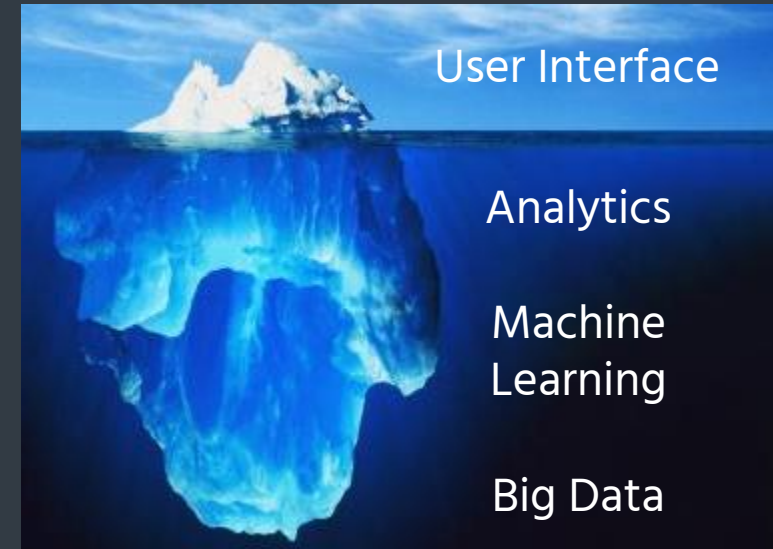
Behind the Analytics ...and the FUD

Matt Hathaway, Director, IDR Solutions

Answering the “So what?”



- You're hearing them.
- How are they **really** being used?



Home

Log Search

Dashboards

Users & Accounts

Assets & Endpoints

Investigations

FILTER BY:

RESET

DATE CREATE DATE

Dec 23, 2016

to

Jan 20, 2017

Status

Closed (5)

Open (99)

Investigations

Report Archive

Data Collection

Settings

Threats

Alert Types

Search

Account Authenticated To Critical Asset (17)

Account Authentication (1)

Account Connected To Network Honeypot

Asset Connects To Network Honeypot

Brute Force Against Domain Account (2)

Harvested Credentials (9)

Ingress From Disabled Account (2)

Ingress From Non Expiring Account (3)

Ingress From Service Account (2)

Lateral Movement Local Credentials (2)

Multiple Country Authentications (32)

Network Access For Threat (3)

Service Account Authenticated From New Source (2)

Wireless Multiple Country Authentications (3)

Created By

Scheduled Hunt

Alerts by Attack Chain

Example 1: Service Account Abuse

DEC 31, 2016

OPEN

Critical Data Server - USB Policy Enforcement at 20170103T200000.233Z

Investigation Created: 2017-01-03T20:00:00.285Z

Last Accessed: 2017-01-03T20:00:00.285Z

JAN 1, 2017

OPEN

Critical Data Server - USB Policy Enforcement at 20170101T200000.211Z

Investigation Created: 2017-01-01T20:00:00.227Z

Last Accessed: 2017-01-01T20:00:00.227Z

DEC 30, 2016

OPEN

Critical Data Server - USB Policy Enforcement at 20161230T200000.185Z

Investigation Created: 2016-12-30T20:00:00.238Z

Last Accessed: 2016-12-30T20:00:00.238Z

DEC 27, 2016

OPEN

Lateral Movement Service Account | LATERAL MOVEMENT

Service account echapman@razor.com authenticated to 2 assets from an unfamiliar source asset

Alert First Seen: 2016-12-27T16:25:41.687Z

Investigation Created: 2016-12-27T16:28:20.305Z

Last Accessed: 2017-01-19T17:23:31.175Z

Home

Log Search

Dashboards

Users & Accounts

Assets & Endpoints

Investigations

Report Archive

Data Collection

Settings

Investigations

Lateral Movement Service Account

Last Accessed: Jan 20, 2017 8:16 PM

FILTER BY:

RESET

EVENT DATETIME

Dec 27, 2016 to Dec 29, 2016

☒ Manually Added Data

☒ Alerts

☒ Notable Behaviors

END

DEC 29, 2016

10:03 PM

INGRESS FROM SERVICE ACCOUNT

Service account echapman@razor.com authenticated at least 100 times

12:28 AM

VIRUS ALERT EVENT

A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.

12:28 AM

VIRUS ALERT EVENT

A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.

12:28 AM

VIRUS ALERT EVENT

A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.

12:28 AM

VIRUS ALERT EVENT

A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.

12:28 AM

VIRUS ALERT EVENT

A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.

12:28 AM

VIRUS ALERT EVENT

A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.

12:28 AM

VIRUS ALERT EVENT

A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.

12:28 AM

VIRUS ALERT EVENT

A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.

12:28 AM

VIRUS ALERT EVENT

A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.

12:28 AM

VIRUS ALERT EVENT

A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.

INVESTIGATION ELEMENTS

Users

Eduardo Chapman

Assets

t233-4279.tor.razor.com

t586-7657.tor.razor.com

RAPID7

What went into this one alert?

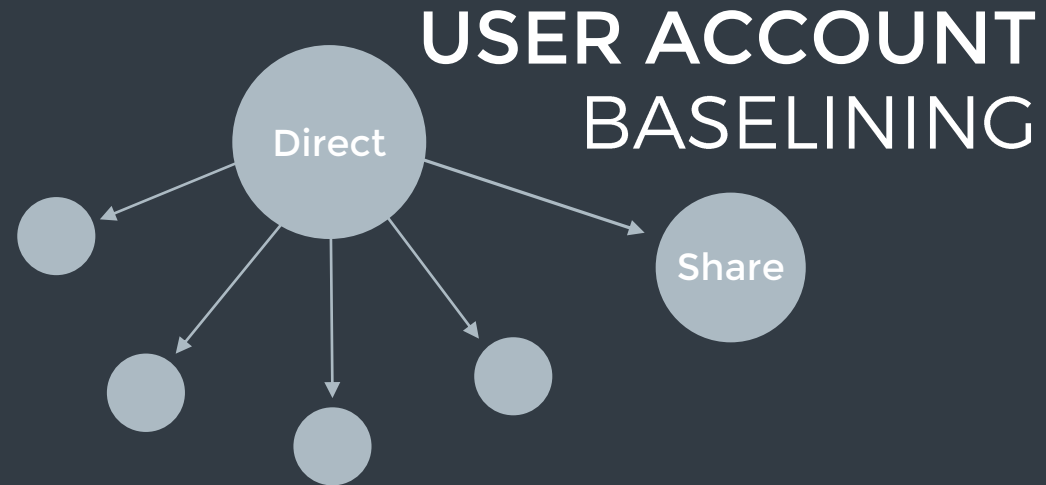
3 major components

Every account's characteristics are monitored for classification

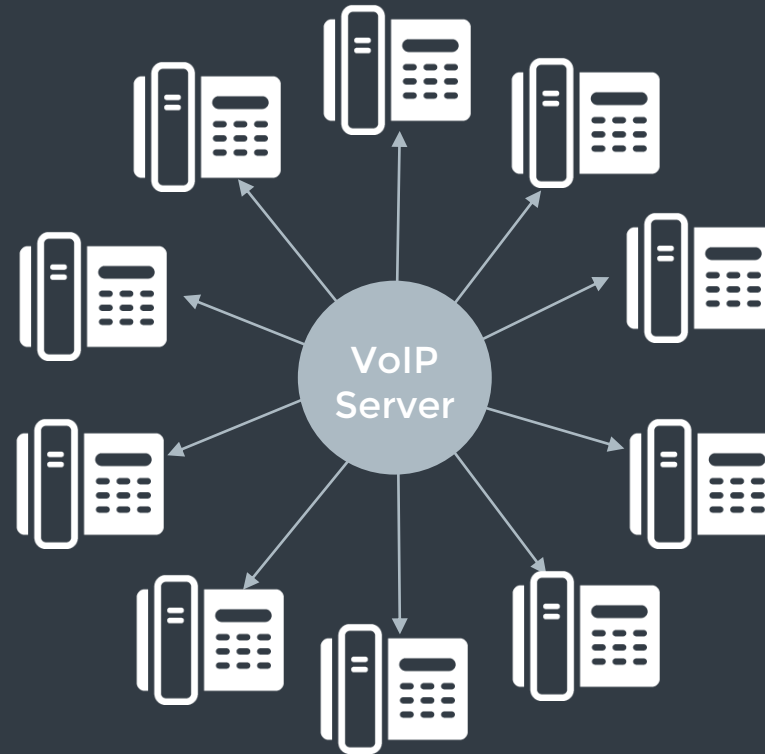
Each account's activity is baselined according to its corresponding classification

Every remote authentication is mapped between assets and compared to the baseline

Baselining Different Account Types



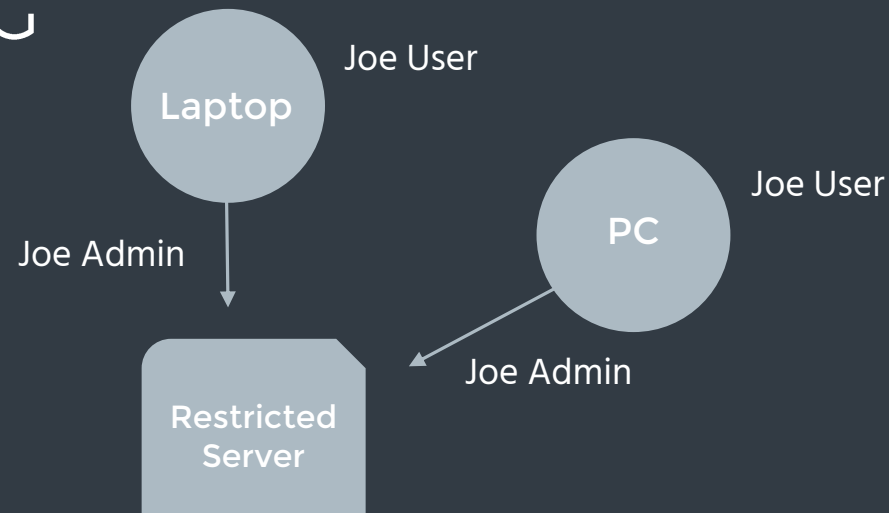
Baselining Different Account Types



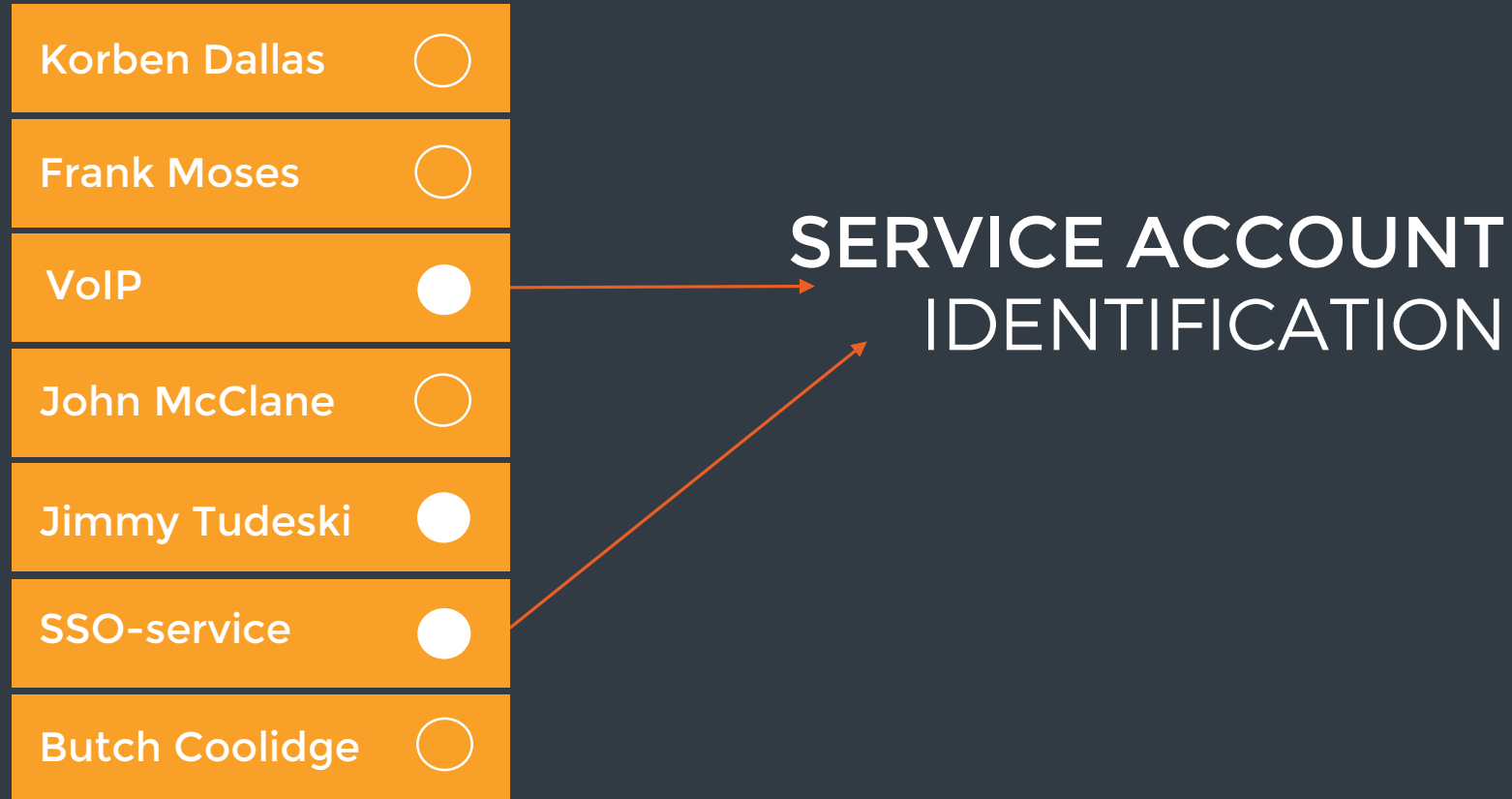
**SERVICE ACCOUNT
BASELINING**

Baselining Different Account Types

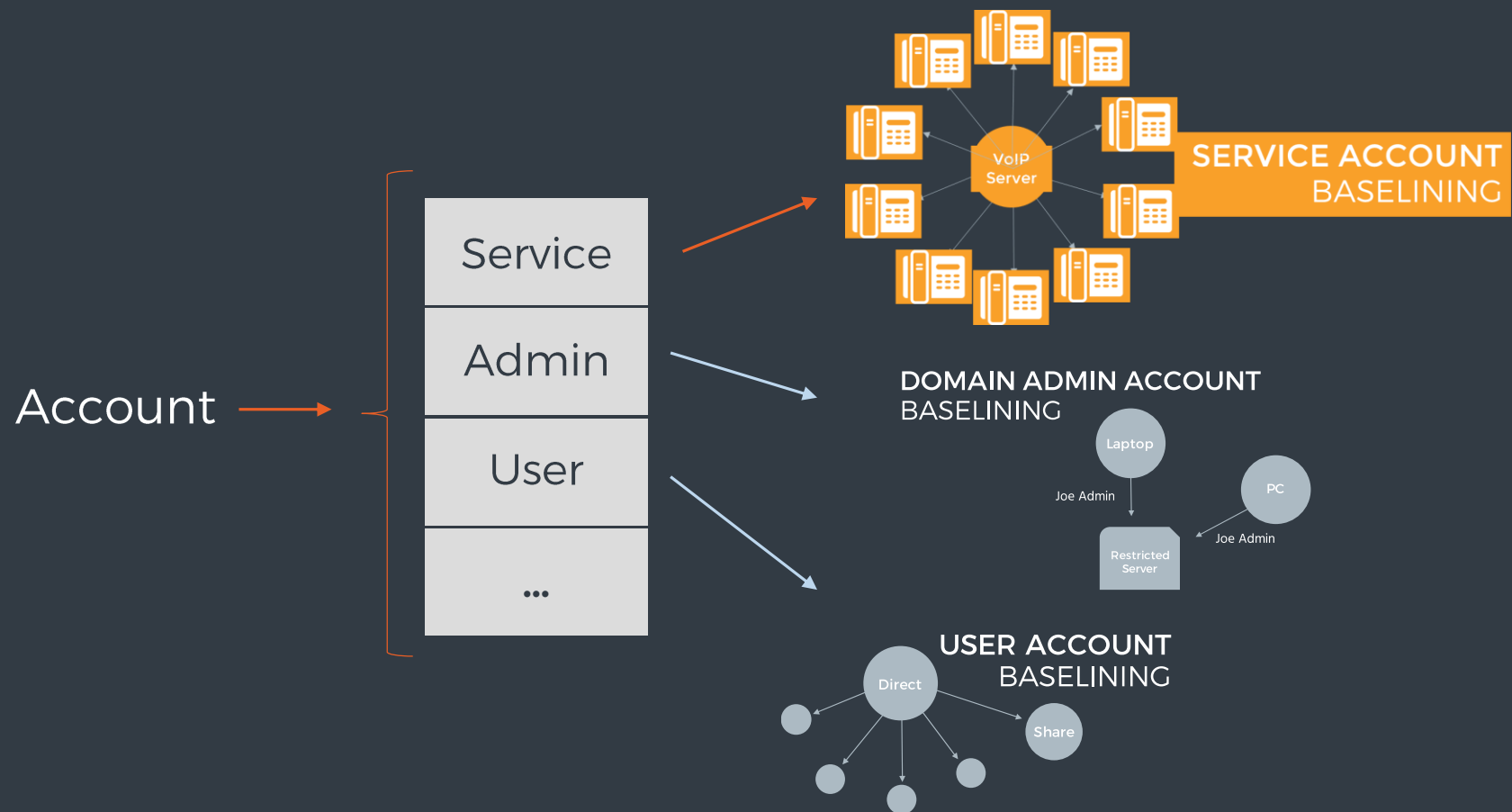
DOMAIN ADMIN ACCOUNT BASELINING



Account Characteristics



Account Classification



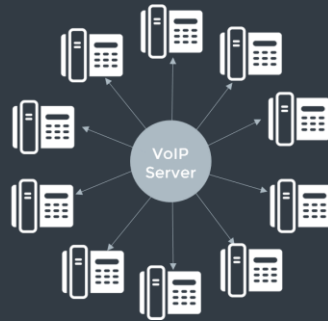


**SERVICE ACCOUNT
ANOMALY DETECTION**

With all of these together, alert

Korben Dallas	○
Frank Moses	○
VoIP	●
John McClane	○
Jimmy Tudeski	●
SSO-service	●
Butch Coolidge	○

SERVICE ACCOUNT
IDENTIFICATION



SERVICE ACCOUNT
BASELINING



SERVICE ACCOUNT
ANOMALY DETECTION



InsightIDR
ALERT

☰

nexpose

Create

?

🔍

🏠

📦

🖥️

🦠

📌

🔍

👤

📄

🔗

⚙️

Remediation Projects (beta)

CREAT

58 Projects

46
Open

17
Owned by Me

0
Assigned to Me

☐

▼

🗑️

✎

Update Status ▼

Remediation Projects (beta) (0 of 58 selected)

Project Name	Progress	Solutions Resolved	Remaining TL	Due On	Assets Affect...	Assignees	Type
☐ from assets newly discovered card	<div><div></div></div> 11%	3880 of 35291	-	-	1191	binuser, awarnick, bert...	Static
☐ Assets with easy to exploit security issues	<div><div></div></div> 68%	168 of 246	10 days	Thu, Dec 20, 2016	43	ae...	Static
☐ from assets with expiring ssl certs	<div><div></div></div> 22%	2984 of 13568	-	-	265	-	Static
☐ from assets with expiring certs 2	<div><div></div></div> 22%	2984 of 13568	-	-	266	bb2, butterfly1, binish, ...	Static
☐ Linux Riskiest Assets	<div><div></div></div> 56%	2260 of 4057	Past Due	Mon, Oct 31, 2016	213	asadmin	Static
☐ Small set of assets with easy to exploit vulns	<div><div></div></div> 15%	1040 of 6883	-	-	7	jliou	Static
☐ Win 7 Enterprise SP1 Dynamic Remediations	<div><div></div></div> 48%	1029 of 2155	10 days	Sat, Feb 4, 2017	836	chewlie, cucumber~Q...	Static
☐ Critical Vulnerabilities on Business Critical Assets	<div><div></div></div> 67%	861 of 1289	Past Due	Mon, Oct 31, 2016	2	awarnick, agencyuser	Static
☐ from assets with critical risk vulns	<div><div></div></div> 54%	807 of 1505	-	-	11	aebiko, amassoudi, Be...	Dynamic
☐ static bigsite1	<div><div></div></div> 2%	669 of 33945	2 years	Sun, Dec 2, 2018	1354	thing1	Static
☐ SSL CERT	<div><div></div></div> 70%	521 of 740	Past Due	Fri, Sep 30, 2016	2	nxadmin	Static
☐ Riskiest Ubuntu	<div><div></div></div> 51%	369 of 717	Past Due	Sun, Oct 30, 2016	83	admin	Static

Example 2: Remediation priorities



from assets with critical risk vulns

PROJECT OVERVIEW (BETA) ✎ <

PROJECT NAME

from assets with critical risk vulns

DESCRIPTION

-

CREATED ON

Tue, Sep 27, 2016

ASSETS AFFECTED

11

TOTAL REMEDIATIONS

1505

PROGRESS

54%

REMAINING TIME

-

DUE ON

-

ASSIGNEES

Akihito Ebiko, Arian Massoudi, Bear, bin2

OWNER

jliou@rapid7.com

TYPE

Dynamic

CARD ASSET FILTER

(asset.vulnerability.severity = 'CRITICAL') && (asset.vulnerability.title CONTAINS 'cve-2016-6662' || asset.vulnerability.title CONTAINS 'cve-2016-6663')

ASSET FILTER

asset.vulnerability.title CONTAINS 'cve-2016-6662' || asset.vulnerability.title CONTAINS 'cve-2016-6663'

VULNERABILITY FILTER

-

1508 Solutions

1075 Unknown Solutions0 Pending Verification

☐ ▾

Update Status ▾

Remediation Solutions (0 of 1508 selected)					
	Solutions	Assets Affect...	Vulnerabil...	Risk Redu...	Status
<input type="checkbox"/>	Upgrade to the latest version of Oracle MySQL	11	310	389,877	Open
<input type="checkbox"/>	Upgrade to the latest version of Google Chrome	1	802	370,897	Open
<input type="checkbox"/>	Upgrade to the latest version of Mozilla Firefox	1	738	361,751	Open
<input type="checkbox"/>	Upgrade to the latest version of Oracle Java	1	432	212,805	Open
<input type="checkbox"/>	Upgrade to the latest version of PHP	2	151	125,039	Open
<input type="checkbox"/>	Configure SMB signing for Windows	11	2	17,744	Open
<input type="checkbox"/>	MS16-001: Cumulative Security Update for Internet Explorer 8 for Windows 7 (KB3124275)	3	29	16,256	Open
<input type="checkbox"/>	MS16-001: Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB31242...	1	28	15,732	Open
<input type="checkbox"/>	MS14-039: Security Update for Windows Server 2008 R2 x64 Edition (KB2973201)	1	21	13,034	Open
<input type="checkbox"/>	MS16-106: Security Update for Windows 7 (KB3185911)	3	24	12,387	Open
<input type="checkbox"/>	MS15-085: Security Update for Windows Server 2008 R2 x64 Edition (KB3071756)	1	20	9,993	Open
<input type="checkbox"/>	MS16-044: Security Update for Windows 7 (KB3146706)	3	19	8,837	Open
<input type="checkbox"/>	Disable Insecure TLS/SSL protocol support	11	4	7,909	Open
<input type="checkbox"/>	MS16-144: December, 2016 Security Only Quality Update for Windows 7 (KB3205394)	3	20	7,797	Open
<input type="checkbox"/>	MS15-080: Security Update for Windows 7 (KB3078601)	3	12	6,581	Open

What went into this list of priorities?

3 major components

Every project is a series of remediation solutions with a live total Risk Reduction

Each solution has a live total Risk Reduction achieved if completed

The Risk Reduction is the combined total of each vulnerability's Real Risk score

Remediation Projects

1. Traders environment	35,291
2. Linux riskiest assets	13,567
3. Static bigsite	12,654
4. Corporate sales remediations	7,985
5. Riskiest ubuntu	4,325
6. Assets with medium vulns	1,509
7. Assets with expiring certs	665

Priority #1

Traders environment	Total: 35,291
1. Upgrade to latest version of Oracle	10,434
2. Configure SMB signing for Windows	5,437
3. Upgrade to latest version of Firefox	4,903
4. MS16-001: Security update	2,101
5. MS16-106: Security update for Windows 7	323
6. MS15-085: Security update for Internet Exp	224

CVSS
AGE
EXPLOIT EASE
EXPLOITS KNOWN

**VULNERABILITY
RISK SCORE**



Superseding
vulnerability
patched




Solution
implemented



Asset
criticality
changed



Remediation Projects



1. Traders environment	35,291
2. Linux riskiest assets	13,567
3. Static bigsite	12,654
4. Corporate sales remediations	7,985
5. Riskiest ubuntu	4,325
6. Assets with medium vulns	1,509
7. Assets with expiring certs	665

Priority #1

Corporate sales remediations Total: 35,291



1. Upgrade to latest version of Google Chrome	12,686
2. Configure SMB signing for Windows	15,437
3. Upgrade to latest version of PHP	8,943
4. Upgrade to latest version of Oracle Java	2,101
5. MS16-106: Security update for Windows 7	732
6. MS15-09: Security update for Windows Server	523

CVSS
AGE
EXPLOIT EASE
EXPLOITS KNOWN

VULNERABILITY
RISK SCORE

Superseding
vulnerability
patched



Solution
implemented



Change in
asset
criticality



In Summary

- Analytics \neq Superpowers
- They are effective when targeted
- 90% of work is beneath the surface

Thank You!