



QUALYS SECURITY CONFERENCE 2020

# Facts, Myths and Questions in a Qualys Customer's Mind

Kevin O'Keefe, Giorgio Gheri and Marco Rottigni  
Qualys, Inc.

The background is a solid blue color with a subtle pattern of small white dots arranged in a grid. A large, faint, light blue circle is centered behind the text, creating a gradient effect that is brightest in the center and fades towards the edges.

# Data Quality

# Rubbish In = Rubbish Out

The screenshot shows the Qualys AssetView interface. At the top, there are tabs for 'Assets', 'Tags', and 'Rules'. Below the tabs, there is a search bar containing the query 'operatingSystem is null'. To the right of the search bar, there is a 'Search' button and a large number '212' indicating the number of assets found. Below the search bar, there are options for 'Actions (0)' and 'Group assets by...'. The main part of the interface is a table with the following columns: 'Asset Name', 'OS', 'Modules', 'Last Logged-In User', 'Activity', 'Sources', and 'Tags'. The table contains six rows of data, each representing an asset with an IP address, an OS status of 'OS Not Identified', a 'VM' module, and an activity of 'New' on 'July 15, 2019'. Each row also has a 'Sources' column with 'All BU' and a 'Tags' column with a grid icon.

Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
192.168.171.4				July 15, 2019		
<b>192.168.171.124</b> 192.168.171.124	● OS Not Identified	VM	—	New July 15, 2019		All BU
<b>192.168.171.170</b> 192.168.171.170	● OS Not Identified	VM	—	New July 15, 2019		All BU
<b>192.168.171.134</b> 192.168.171.134	● OS Not Identified	VM	—	New July 15, 2019		All BU
<b>192.168.171.123</b> 192.168.171.123	● OS Not Identified	VM	—	New July 15, 2019		All BU
<b>192.168.171.132</b> 192.168.171.132	● OS Not Identified	VM	—	New July 15, 2019		All BU

# Tags and Asset Groups

# Tag Creation

### Tag Creation

Turn help tips: On | Off Launch help

Step 2 of 3 Set the tag type and rules

1 Tag details ✓  
2 Tag Rule ✓  
3 Review And Confirm

Rule Engine (\*) REQUIRED FIELDS

Asset Search  Re-evaluate rule on save

- No Dynamic Rule
- Asset Name Contains
- Groovy Scriptlet
- IP Address In Range(s)
- IP Address In Range(s) + Network(s)
- Open Ports
- Operating System Regular Expression
- Software installed
- Vuln(QID) Exist
- Asset Search
- Cloud Asset Search
- Asset Inventory

Add Asset: Select an asset

Cancel Previous

### Tag Creation

Turn help tips: On | Off Launch help

Step 2 of 3 Set the tag type and rules

1 Tag details ✓  
2 Tag Rule ✓  
3 Review And Confirm

Rule Engine (\*) REQUIRED FIELDS

Asset Inventory  Re-evaluate rule on save

Query

operatingSystem.name:Windows 10 AND (software.name:Chrome OR software.name:Firefox) AND hardware

hardware.category  
hardware.category1  
hardware.category2  
hardware.lifecycle.stage  
hardware.manufacturer

Syntax Help [view more](#)  
**hardware.manufacturer**  
Use quotes or backticks within values to find assets having a certain hardware manufacturer.  
*Example*  
Show any findings that match exact value "Dell"  
hardware.manufacturer: 'Dell'

Cancel Previous Continue

# Tag Uses

## General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal scans, if visible.

Title:

Option Profile: \*  [Select](#)

Processing Priority:

Scanner Appliance: Scanner Appliance not available

## Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

- Assets  Tags

Use IP Network Range Tags  
Choose from tags defined with IP address rules. This will allow you to scan the entire IP range(s) in each selected tag.

Include hosts that have  of the tags below. [Add Tag](#)

Do not include hosts that have  of the tags below. [Add Tag](#)

(no tags selected)

### Edit Mode

- User Details >
- Profile Settings >
- Roles And Scopes >**
- Action Log >
- Account Activity >

### Edit role(s) and scope

Allow user full permissions and scope (The user will have full access to everything)

Each role grants you a set of permissions that will apply to the objects you have access to.

New role  Search unassigned roles

Assigned roles	Remove all	Unassigned roles	Add all
CA MANAGER	Remove	AI User	Add
CLOUDVIEW User	Remove	AUDITOR	Add
READER	Remove	CERTVIEW User	Add
		CONTACT	Add
		CS User	Add

### Edit Scope

Allow user view access to all objects (Other permissions are granted by the user's roles)

Define what assets the user can access by tags.

Global Scope [Select](#) | [Create](#) | [Remove All](#)

### Add Tags to Include

Recent Tags  
No recent tags

Favorite Tags  
No favorite tags

[Cancel](#) [Save](#)

The background is a solid blue color with a subtle pattern of small white dots arranged in a grid. A large, faint, light blue circle is centered behind the text, creating a gradient effect that is brightest in the center and fades towards the edges.

# Cloud Integrations

# Cloud Inventory

Actions (0)
Create Connector

1 - 2 of 2

CONNECTOR NAME	ACCOUNT ID	STATE	RESOURCES	MODULES
<b>CheckoutApp</b> <small>CheckoutApp AWS Prod Account</small>	383031258652	<span style="color: green;">Success</span> <small>Last Synced On March 27, 2018 3:13 PM</small>	364	<span style="color: green;">OK</span>
<b>AcmeDevLab</b> <small>ACME Azure Dev Subscription</small>	fb99ea64-abde-452e-adfa-83442409e8fe	<span style="color: red;">Pending</span> <small>Last Synced On March 27, 2018 6:24 PM</small>	0	<span style="color: green;">OK</span>
<b>DevTeleApp</b> <small>CheckoutApp AWS Prod Account</small>	443031258688	<span style="color: green;">Success</span> <small>Last Synced On March 27, 2018 3:13 PM</small>	364	<span style="color: green;">OK</span>
<b>US2DevLab</b> <small>ACME Azure Dev Subscription</small>	aef9ea64-abde-452e-adfa-83442409e8fe	<span style="color: green;">Success</span> <small>Last Synced On March 27, 2018 3:13 PM</small>	364	<span style="color: green;">OK</span>
<b>TestApp</b> <small>CheckoutApp AWS Prod Account</small>	583031258677	<span style="color: green;">Success</span> <small>Last Synced On March 27, 2018 3:13 PM</small>	364	<span style="color: green;">OK</span>
<b>ReportsEngine</b> <small>ACME Azure Dev Subscription</small>	ace9ea64-abde-452e-adfa-83442409e8fe	<span style="color: green;">Success</span> <small>Last Synced On March 27, 2018 3:13 PM</small>	364	<span style="color: green;">OK</span>

11

Total Resource Types

Last 30 Days

1 - 11 of 11

RESOURCE TYPE	SERVICE	TOTAL RESOURCES	RESOURCES FAILED
<b>Subnet</b>	VPC	58	0
<b>Network ACL</b>	VPC	32	0
<b>Internet Gateway</b>	VPC	25	0
<b>Load Balancer</b>	EC2	3	0
<b>Instance</b>	EC2	52	0
<b>Route Table</b>	VPC	36	0
<b>S3 Bucket</b>	S3	26	23
<b>IAM User</b>	IAM	71	61

ACCOUNT	TOTAL RESOURCES
453031258652	396
135767712438	11

RESOURCE TYPE	TOTAL RESOURCES
Security Group	74
IAM User	71
Subnet	58
8 more	

REGIONS	TOTAL RESOURCES
N. Virginia	178
Mumbai	69
Ohio	33
N. California	24



# Cloud Assessment

The screenshot displays the Amazon Web Service Security Center console. The top navigation bar shows 'Amazon Web Service' with a dropdown arrow. On the left, a blue sidebar contains a large '48' representing 'Total Controls Evaluated'. Below this, there are sections for 'POLICY', 'CONTROL RESULT', and 'SERVICES'. The 'CONTROL RESULT' section shows 'PASS' with 25 items and 'FAIL' with 23 items. The 'SERVICES' section lists 'CloudTrail' (20), 'IAM' (19), 'S3' (4), 'VPC' (4), and 'Config' (1).

The main content area features a search bar and three summary cards: 'EVALUATIONS' (740 Total Evaluations), 'SECURITY POSTURE' (390 Pass, 350 Fail), and 'FAILURES BY CRITICALITY' (251 High, 99 Medium, 0 Low). A blue header for a control evaluation reads 'Control Evaluation: Ensure no security groups allow ingress from 0.0.0.0/0...'. The control details for 'CID-41 Ensure no security groups allow ingress from 0.0.0.0/0 to port 22' are shown, including the policy name, evaluation description, remediation link, platform (AWS), service (VPC), and criticality (HIGH).

Below the control details is a table of evaluations. The table has columns for 'RESOURCE', 'ACCOUNT ID', 'REGION', 'EVALUATED ON', and 'RESULT'. Two rows are visible, both showing a 'FAIL' result. The first row is for resource 'sg-697c6316' in the 'Oregon' region, and the second row is for resource 'sg-ae3fd6c8' in the 'Sydney' region. Both were evaluated 37 minutes ago. A 'View Steps' button is present for the first row.

At the bottom, the 'REMEDiation STEPS' section provides instructions on how to resolve the issue, including logging into the AWS Management Console and navigating to the Security Groups page.

# Azure Integration

Microsoft Azure Security Center - Overview > Recommendations

Recommendations

MONITORING RECOMMENDATIONS TOTAL

Recommendation	Total
Data collection installation status	31 of 56 VMs

VIRTUAL MACHINES RECOMMENDATIONS TOTAL

Recommendation	Total
Endpoint Protection not installed	4 of 56 VMs
Missing scan data	11 of 56 VMs
Remediate OS vulnerabilities (by Microsoft)	5 of 56 VMs
Missing system updates	1 of 56 VMs
Endpoint Protection health failures	1 of 56 VMs
Missing disk encryption	5 of 56 VMs
OS version not updated	2 of 4 Roles
<b>Vulnerability assessment not installed</b>	2 of 56 VMs
Vulnerabilities found	2 of 56 VMs
Healthy	6 of 60 VMs

Add a Vulnerability Assessment

Select an existing solution or create a new one

+ Create New >

- Or -

Use existing solution

- Qualys, Inc. Qualys-VA >

Remediate vulnerabilities (by Qualys)

PREVIEW

Filter

VULNERABILITY NAME	VENDOR	AFFECT...	STATE	SEVERITY
Enabled DCOM	Qualys	harivm2	Open	High
Allowed Null Session	Qualys	harivm2	Open	Medium
Enabled Cached Logon Cre...	Qualys	harivm2	Open	Medium
Machine Information Discl...	Qualys	harivm2	Open	Medium
Microsoft Windows Explore...	Qualys	harivm2	Open	Medium
Windows Explorer Autopla...	Qualys	harivm2	Open	Medium
Access to File Share is Enab...	Qualys	harivm2	Open	Low
ActiveX Controls Enumerated	Qualys	harivm2	Open	Low
Antivirus Product Not Dete...	Qualys	harivm2	Open	Low
Disabled Clear Page File	Qualys	harivm2	Open	Low
Enabled Caching of Dial-up...	Qualys	harivm2	Open	Low
Enabled Display Last User...	Qualys	harivm2	Open	Low
File Access Permissions for ...	Qualys	harivm2	Open	Low
File Access Permissions for ...	Qualys	harivm2	Open	Low
Host Scan Time	Qualys	harivm2	Open	Low
Hyper-V Host Information ...	Qualys	harivm2	Open	Low
Installed Applications Enu...	Qualys	harivm2	Open	Low
Internet Protocol version 6 ...	Qualys	harivm2	Open	Low
IPSEC Policy Agent Service ...	Qualys	harivm2	Open	Low
Message For Users Attempt...	Qualys	harivm2	Open	Low

# Reporting

# Static Reports

**Microsoft XML Core Services Information Disclosure Vulnerabilities (MS15-084) (3)**

**QID:** 123796  
**Category:** Local  
**CVE ID:** CVE-2015-2434, CVE-2015-2440, CVE-2015-2421  
**Vendor Reference:** MS15-084  
**Bugtraq ID:** 76232  
**Edited:** 14 Jun 2016  
**User Modified:**  
**PCV User:**

**CVSS Base:** 4.3  
**CVSS Temporal:** 3.2

**CVSS3 Base:** -

**THREAT:**  
 Microsoft XML Core Serv  
 Studio 6.0 to Service MS15-084: Windows Server 2008 R2 for x64-based Systems Service Pack 1 (https://www.microsoft.com/downloads/details.aspx?familyid=95145420-4710-4642-9442-000000000000)  
 MS15-084: Windows Server 2012 (https://www.microsoft.com/downloads/details.aspx?familyid=73634747-4656-4660-990051480000)  
 MS15-084: Windows Server 2012 R2 (https://www.microsoft.com/downloads/details.aspx?familyid=91011000-10ad-4700-b415-000000000000)  
 MS15-084: Microsoft Office 2007 Service Pack 3 (https://www.microsoft.com/downloads/details.aspx?familyid=03817336-0259-4320-89c0-9990a5050eaf)  
 MS15-084: Microsoft Intune 2013 Service 1 (https://www.microsoft.com/downloads/details.aspx?familyid=03817336-0259-4320-89c0-9990a5050eaf)  
 MS15-084: Windows Server 2008 R2 for x64-based Systems Service Pack 1 (https://www.microsoft.com/downloads/details.aspx?familyid=95145420-4710-4642-9442-000000000000)

**COMPLIANCE:**  
 Not Applicable

**EXPLOITABILITY:**  
 There is no exploitability information for this vulnerability.

**ASSOCIATED MAILINGS:**  
 There is no mailing information for this vulnerability.

**IMPACT:**  
 Successful exploitation of this vulnerability may allow an attacker to bypass certain security restrictions, obtain sensitive information, execute arbitrary code or cause a denial of service condition on the system.

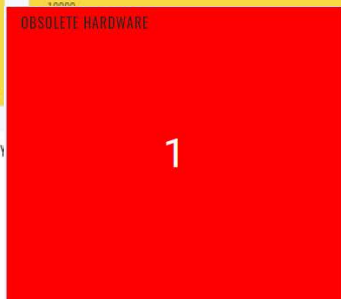
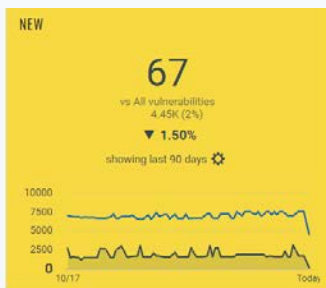
**SOLUTION:**  
 Customers are advised to upgrade to Google Chrome 48.0.2564.109 (http://www.google.com/chrome/) or a later version. Patch: Following are links for downloading patches to fix the vulnerabilities: Google Chrome: MAG OS X (https://www.google.com/chrome/browser/desktop/updates.html#links) Google Chrome: Windows (https://www.google.com/chrome/browser/desktop/updates.html#links)

**COMPLIANCE:**  
 Not Applicable

**Global Default Network**

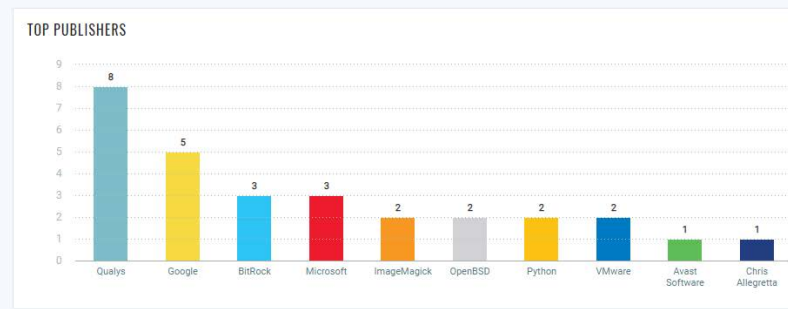
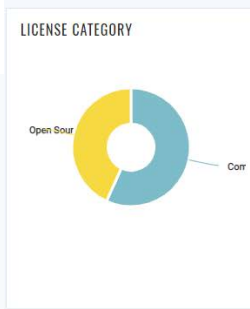
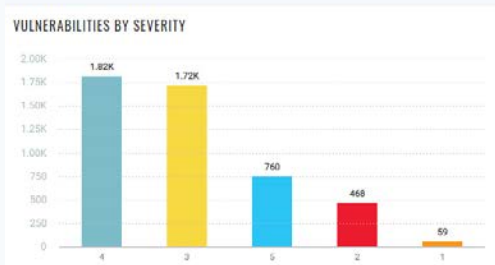
DNS	NetBIOS	Tracking & OS	IP Status	QID	Title	Vuln Stat.	Type	Severity	Port	Protocol	FQDN	SSL	First Detect	Last Detect	Times	Det Date Last	CVE ID	Vendor ID	Bugtraq ID	CVSS	CVSS Base	CVSS Temp	CVSS Env	CVSS3	CVSS3 Collat		
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	372325	Mozilla/Fi Active	Vuln	S	*****	*****	01/14/2012	6	6	6	CVE-2015-MFSA2020-03	6.2.7.5	[AV]/N/6.2	[E/F]/Ri	Asset Group: All IPs, Collat	6.2.7.5	6.2	6.2	6.2		
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	372326	Mozilla/Fi Active	Vuln	S	*****	*****	01/14/2012	6	6	6	CVE-2015-MFSA2020-03	6.2.7.5	[AV]/N/6.2	[E/F]/Ri	Asset Group: All IPs, Collat	6.2.7.5	6.2	6.2	6.2		
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	372324	Mozilla/Fi Active	Vuln	S	*****	*****	01/14/2012	6	6	6	CVE-2015-mfsa2020-01_mfsa20	5.3	6.8	[AV]/N/5.3	[E/POC]	Asset Group: 7.8.8.8 (A)	5.3	6.8	5.3		
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	372324	Mozilla/Fi Active	Vuln	S	*****	*****	01/14/2012	6	6	6	CVE-2015-mfsa2020-01_mfsa20	5.3	6.8	[AV]/N/5.3	[E/POC]	Asset Group: 7.8.8.8 (A)	5.3	6.8	5.3		
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	372276	Mozilla/Fi Active	Vuln	S	*****	*****	01/14/2012	36	36	36	CVE-2015-MFSA2019-37_MFSA	5.6.8	[AV]/N/5.6	[E/UR]	Asset Group: 7.8.8.8 (A)	5.6.8	[AV]/N/5.6	[E/UR]	Asset Group: 7.8.8.8 (A)		
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	372276	Mozilla/Fi Active	Vuln	S	*****	*****	01/14/2012	36	36	36	CVE-2015-MFSA2019-37_MFSA	5.6.8	[AV]/N/5.6	[E/UR]	Asset Group: 7.8.8.8 (A)	5.6.8	[AV]/N/5.6	[E/UR]	Asset Group: 7.8.8.8 (A)		
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	372186	Google Cr Active	Vuln	S	*****	*****	01/14/2012	73	73	73	CVE-2015-Google Chrome	3.6	6.8	[AV]/N/3.6	[E/F]/Ri	Asset Group: 7.8.8.8 (A)	3.6	6.8	3.6		
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	372186	Google Cr Active	Vuln	S	*****	*****	01/14/2012	73	73	73	CVE-2015-Google Chrome	3.6	6.8	[AV]/N/3.6	[E/F]/Ri	Asset Group: 7.8.8.8 (A)	3.6	6.8	3.6		
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	372136	Mozilla/Fi Active	Vuln	S	*****	*****	01/14/2012	102	102	102	CVE-2015-MFSA2019-31	3.2	4.3	[AV]/N/3.2	[E/UR]	Asset Group: 3.8.4.1 (A)	3.2	4.3	3.2		
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	372136	Mozilla/Fi Active	Vuln	S	*****	*****	01/14/2012	102	102	102	CVE-2015-MFSA2019-31	3.2	4.3	[AV]/N/3.2	[E/UR]	Asset Group: 3.8.4.1 (A)	3.2	4.3	3.2		
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	372102	Mozilla/Fi Active	Vuln	S	*****	*****	01/14/2012	125	125	125	CVE-2015-MFSA2019-27_MFSA	6.9	9.3	[AV]/N/6.9	[E/UR]	Asset Group: 8.5.8.8 (A)	6.9	9.3	6.9		
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	372102	Mozilla/Fi Active	Vuln	S	*****	*****	01/14/2012	125	125	125	CVE-2015-MFSA2019-27_MFSA	6.9	9.3	[AV]/N/6.9	[E/UR]	Asset Group: 8.5.8.8 (A)	6.9	9.3	6.9		
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	372073	Google Cr Active	Vuln	S	*****	*****	01/14/2012	124	124	124	CVE-2015-Google Chrome	3.2	4.3	[AV]/N/3.2	[E/UR]	Asset Group: 5.7.6.3 (A)	3.2	4.3	3.2		
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	372073	Google Cr Active	Vuln	S	*****	*****	01/14/2012	124	124	124	CVE-2015-Google Chrome	3.2	4.3	[AV]/N/3.2	[E/UR]	Asset Group: 5.7.6.3 (A)	3.2	4.3	3.2		
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	371849	Mozilla/Fi Active	Vuln	S	*****	*****	06/19/2011	01/14/2012	208	208	208	CVE-2015-MFSA2019-18	5.9	7.5	[AV]/N/5.9	[E/POC]	Asset Group: 7.8.8.8 (A)	5.9	7.5	5.9	
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	371849	Mozilla/Fi Active	Vuln	S	*****	*****	06/19/2011	01/14/2012	208	208	208	CVE-2015-MFSA2019-18	5.9	7.5	[AV]/N/5.9	[E/POC]	Asset Group: 7.8.8.8 (A)	5.9	7.5	5.9	
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	371848	Google Cr Active	Vuln	S	*****	*****	06/19/2011	01/14/2012	203	203	203	CVE-2015-Google Chrome	3.2	4.3	[AV]/N/3.2	[E/UR]	Asset Group: 5.7.6.3 (A)	3.2	4.3	3.2	
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	371848	Google Cr Active	Vuln	S	*****	*****	06/19/2011	01/14/2012	203	203	203	CVE-2015-Google Chrome	3.2	4.3	[AV]/N/3.2	[E/UR]	Asset Group: 5.7.6.3 (A)	3.2	4.3	3.2	
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	371361	Adobe Se Active	Vuln	S	*****	*****	01/14/2012	404	404	404	CVE-2016-ASP818-01_108414	8.7	10	[AV]/N/8.7	[E/UR]	Asset Group: 8.9.8.9 (A)	8.7	10	8.7		
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	371361	Adobe Se Active	Vuln	S	*****	*****	01/14/2012	404	404	404	CVE-2016-ASP818-01_108414	8.7	10	[AV]/N/8.7	[E/UR]	Asset Group: 8.9.8.9 (A)	8.7	10	8.7		
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	371265	Oracle Java Active	Vuln	S	*****	*****	11/21/2011	01/14/2012	415	415	415	CVE-2016-ASP818-04_105964	7.8	10	[AV]/N/7.8	[E/POC]	Asset Group: 8.9.8.9 (A)	7.8	10	7.8	
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	371265	Oracle Java Active	Vuln	S	*****	*****	11/21/2011	01/14/2012	415	415	415	CVE-2016-ASP818-04_105964	7.8	10	[AV]/N/7.8	[E/POC]	Asset Group: 8.9.8.9 (A)	7.8	10	7.8	
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	371136	Adobe Fla Active	Vuln	S	*****	*****	10/17/2011	01/14/2012	449	449	449	CVE-2016-Oracle jav 105991	5.6	8.8	[AV]/N/5.6	[E/UR]	Asset Group: 7.8.9 (AV)	5.6	8.8	5.6	
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	371136	Adobe Fla Active	Vuln	S	*****	*****	10/17/2011	01/14/2012	449	449	449	CVE-2016-Oracle jav 105991	5.6	8.8	[AV]/N/5.6	[E/UR]	Asset Group: 7.8.9 (AV)	5.6	8.8	5.6	
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	371216	Mozilla/Fi Active	Vuln	S	*****	*****	09/25/2011	01/14/2012	475	475	475	CVE-2016-MFSA2011105276	3.1	4.4	[AV]/L/3.1	[E/UR]	Asset Group: 6.1.7 (AV)	3.1	4.4	3.1	
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	371216	Mozilla/Fi Active	Vuln	S	*****	*****	09/25/2011	01/14/2012	470	470	470	CVE-2016-MFSA2011105276	3.1	4.4	[AV]/L/3.1	[E/UR]	Asset Group: 6.1.7 (AV)	3.1	4.4	3.1	
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	371173	Mozilla/Fi Active	Vuln	S	*****	*****	09/25/2011	01/14/2012	489	489	489	CVE-2016-MFSA2011101665	5.7	8.8	[AV]/N/5.7	[E/UR]	Asset Group: 8.5.8.8 (A)	5.7	8.8	5.7	
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	371173	Mozilla/Fi Active	Vuln	S	*****	*****	09/25/2011	01/14/2012	489	489	489	CVE-2016-MFSA2011101665	5.7	8.8	[AV]/N/5.7	[E/UR]	Asset Group: 8.5.8.8 (A)	5.7	8.8	5.7	
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	371138	Adobe Fla Active	Vuln	S	*****	*****	08/15/2011	01/14/2012	510	510	510	CVE-2016-ASP818-01_105066	5.9	7.5	[AV]/N/5.9	[E/POC]	Asset Group: 8.9.8.9 (A)	5.9	7.5	5.9	
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	371138	Adobe Fla Active	Vuln	S	*****	*****	08/15/2011	01/14/2012	510	510	510	CVE-2016-ASP818-01_105066	5.9	7.5	[AV]/N/5.9	[E/POC]	Asset Group: 8.9.8.9 (A)	5.9	7.5	5.9	
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	370791	Oracle Java Active	Vuln	S	*****	*****	07/18/2011	01/14/2012	536	536	536	CVE-2016-Oracle jav 104774	5.6	8.8	[AV]/N/5.6	[E/UR]	Asset Group: 7.8.9 (AV)	5.6	8.8	5.6	
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	370791	Oracle Java Active	Vuln	S	*****	*****	07/18/2011	01/14/2012	536	536	536	CVE-2016-Oracle jav 104774	5.6	8.8	[AV]/N/5.6	[E/UR]	Asset Group: 7.8.9 (AV)	5.6	8.8	5.6	
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	370966	Adobe Fla Active	Vuln	S	*****	*****	04/13/2011	01/14/2012	548	548	548	CVE-2016-ASP818-01_104898	7.4	10	[AV]/N/7.4	[E/UR]	Asset Group: 8.5.8.8 (A)	7.4	10	7.4	
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	370966	Adobe Fla Active	Vuln	S	*****	*****	04/13/2011	01/14/2012	547	547	547	CVE-2016-ASP818-01_104898	7.4	10	[AV]/N/7.4	[E/UR]	Asset Group: 8.5.8.8 (A)	7.4	10	7.4	
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	370887	Oracle Java Active	Vuln	S	*****	*****	03/15/2011	01/14/2012	545	545	545	CVE-2016-Oracle jav 103832	4.3	5.8	[AV]/N/4.3	[E/UR]	Asset Group: 7.2.8.1 (A)	4.3	5.8	4.3	
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	370887	Oracle Java Active	Vuln	S	*****	*****	03/15/2011	01/14/2012	545	545	545	CVE-2016-Oracle jav 103832	4.3	5.8	[AV]/N/4.3	[E/UR]	Asset Group: 7.2.8.1 (A)	4.3	5.8	4.3	
*****	*****	*****	*****	64.1.200.249	Trn-win7.1TRN-WIN-IP	Windows host scan	370861	Microsoft Active	Vuln	S	*****	*****	07/16/2011	10/14/2012	2	2	2	CVE-2018-Microsoft	103593	7.3	9.3	[AV]/N/7.3	[E/POC]	Asset Group: 7.8.8.8 (A)	7.3	9.3	7.3
*****	*****	*****	*****	64.1.200.249	win2008R2WIN2008R2-IP	Windows host scan	370861	Microsoft Active	Vuln	S	*****	*****	04/13/2011	01/14/2012	607	607	607	CVE-2018-Microsoft	103593	7.3	9.3	[AV]/N/7.3	[E/POC]	Asset Group: 7.8.8.8 (A)	7.3	9.3	7.3
*****																											

# Dashboards



**EOL OPERATING SYSTEM**

OPERATING SYSTEM NAME	COUNT
Windows 10	4
Windows 7	1
Windows 8	1



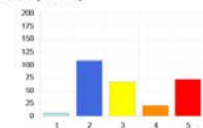
# API / Plugins

IBM QRadar Security Intelligence interface showing navigation tabs: Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Admin. The active tab is 'Qualys App for QRadar'. Search filters for Start Date-Time (2017-05-06 17:00) and End Date-Time (2017-10-27 17:04) are visible.

## Active Hosts

162

## Detections by Severity



## Detections by Status



## Detections by Type



## Top 10 Hosts Not Scanned in Last 30 Days

ID	IP	Last Scanned On
10.10.10.64	43953685	2011-08-05 15:33:03
10.10.10.73	43953689	2011-08-05 15:33:04
10.10.10.136	43953678	2011-08-05 15:33:06
10.10.10.176	43953688	2011-08-05 15:33:09
10.10.10.174	43953687	2011-08-05 15:33:09
10.10.10.172	43953685	2011-08-05 15:33:09
10.10.21.20	43953908	2011-08-05 15:33:40
10.10.21.19	43953907	2011-08-05 15:33:40
10.10.21.75	43953924	2011-08-05 15:33:42
None	None	None

Splunk dashboard for Qualys VM App for Splunk Enterprise. The dashboard includes the following sections:

- Total Hosts:** 96,205 Active Hosts.
- OS distribution:** Pie chart showing the distribution of operating systems, including Windows 2000, Linux 2.4, and Unknown.
- Total Vulns by Status:** Line chart showing the number of vulnerabilities over time (2012-2017), categorized by status: AC..E, FIXED, NEW, RE..D.
- Most Prevalent Vulnerabilities:** Table listing the top vulnerabilities.

QID	TITLE	CATEGORY	SEVERITY	HOST_COUNT
105456	EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 5 x Detected	Security Policy	5	28976
86476	Web Server: Stopped Responding	Web server	3	21443
27002	Writeable Root Directory on FTP Server	File Transfer Protocol	5	19806
105359	EOL/Obsolete Operating System: Microsoft Windows 2000 Detected	Security Policy	5	15977
50008	Qualcomm Qpopper Remote Execution Vulnerability	Mail services	5	15171
74019	Qualcomm Qpopper E-mail Spoofing Vulnerability	Mail services	3	15171
74084	Qualcomm Qpopper Unsafe fget(s) Vulnerability	Mail services	3	15171
38628	SSL/TLS Server supports TLSv1.0	General remote services	3	1575
38601	SSL/TLS use of weak RC4 cipher	General remote services	3	1176
90882	Windows Remote Desktop Protocol Weak Encryption Method Allowed	Windows	3	821

# Integrations

# Integrations / Use Cases

## Data Extraction

Long-term data retention for Audit  
Ticket generation for task tracking  
Unifying Multiple Qualys subscriptions  
Cross-correlation of enterprise data sets  
Playbook integrations (Splunk -> Phantom)  
CMDB population and data syncing

## Operational Automation

Automatic asset onboarding and clean-up (*ex: purging and adding assets*)  
Qualys health check automation  
(*ex: Scanner utilization tracking, API limit tracking*)  
Scan/Re-scan on Demand  
CI/CD Integrations (*Out-of-box and custom*)



# Digital Biodiversity

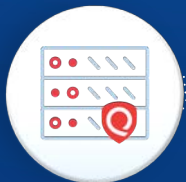
# Dominate the Digital Biodiversity!



Why is Qualys better?

# CLOUD-BASED MICROSERVICES ARCHITECTURE





### Global IT Resources

📌 All Tags (12/12) | 🏢 All Business Units | 🌐 All Locations | 📅 Last 90 days



**ASSETS WITH ZERO-DAY VULNERABILITIES**

200 vs. All Assets 2.5K (8%) ▲ 5%

**ASSETS WITH MISSING CRITICAL PATCHES**

20 vs. All Assets 2.5K (0.8%) ▼ 52.38%

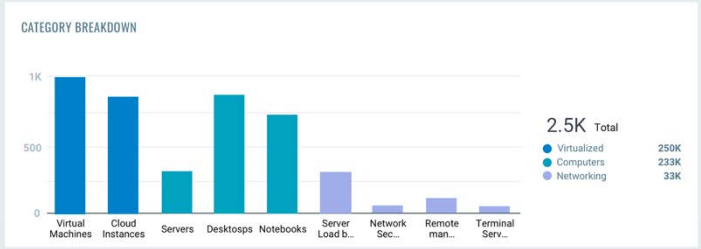
**INDICATION OF COMPROMISE ASSETS**

58 vs. All Assets 2.5K (2.3%) ▲ 20%

**CIS FAILED CONTROLS**

92K vs. All Assets 265K (35%) ▲ 5%

### Global IT Asset Inventory





QUALYS SECURITY CONFERENCE 2020

Thank You