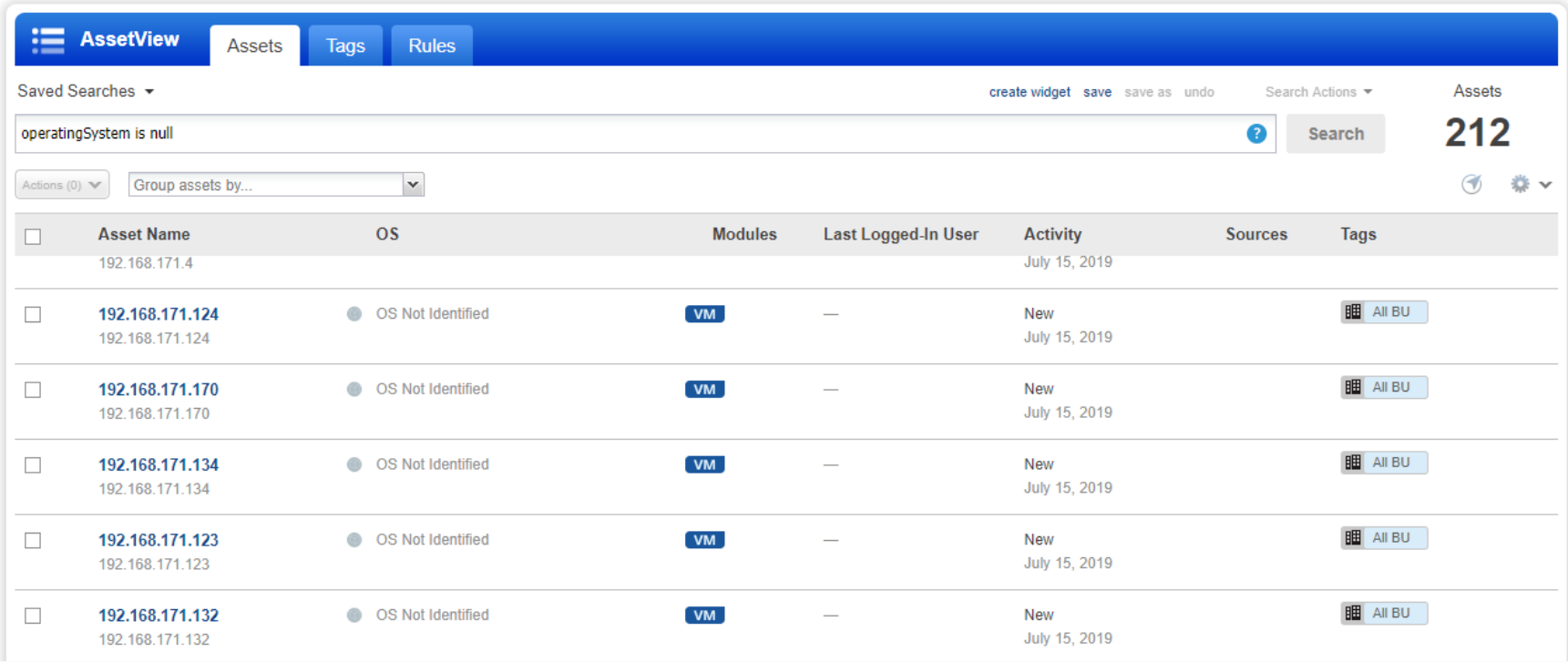
Facts, Myths and Questions in a Qualys Customer's Mind

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

Data Quality

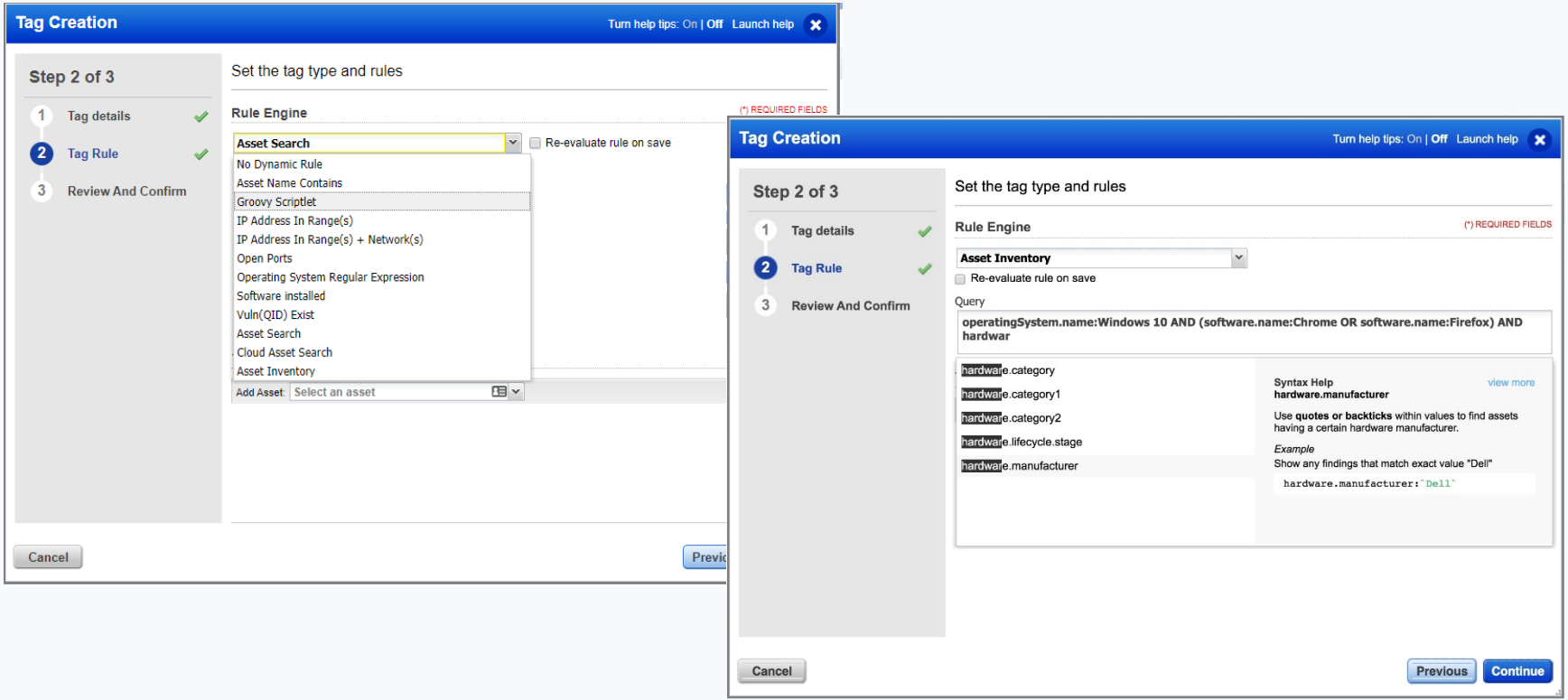
Rubbish In = Rubbish Out



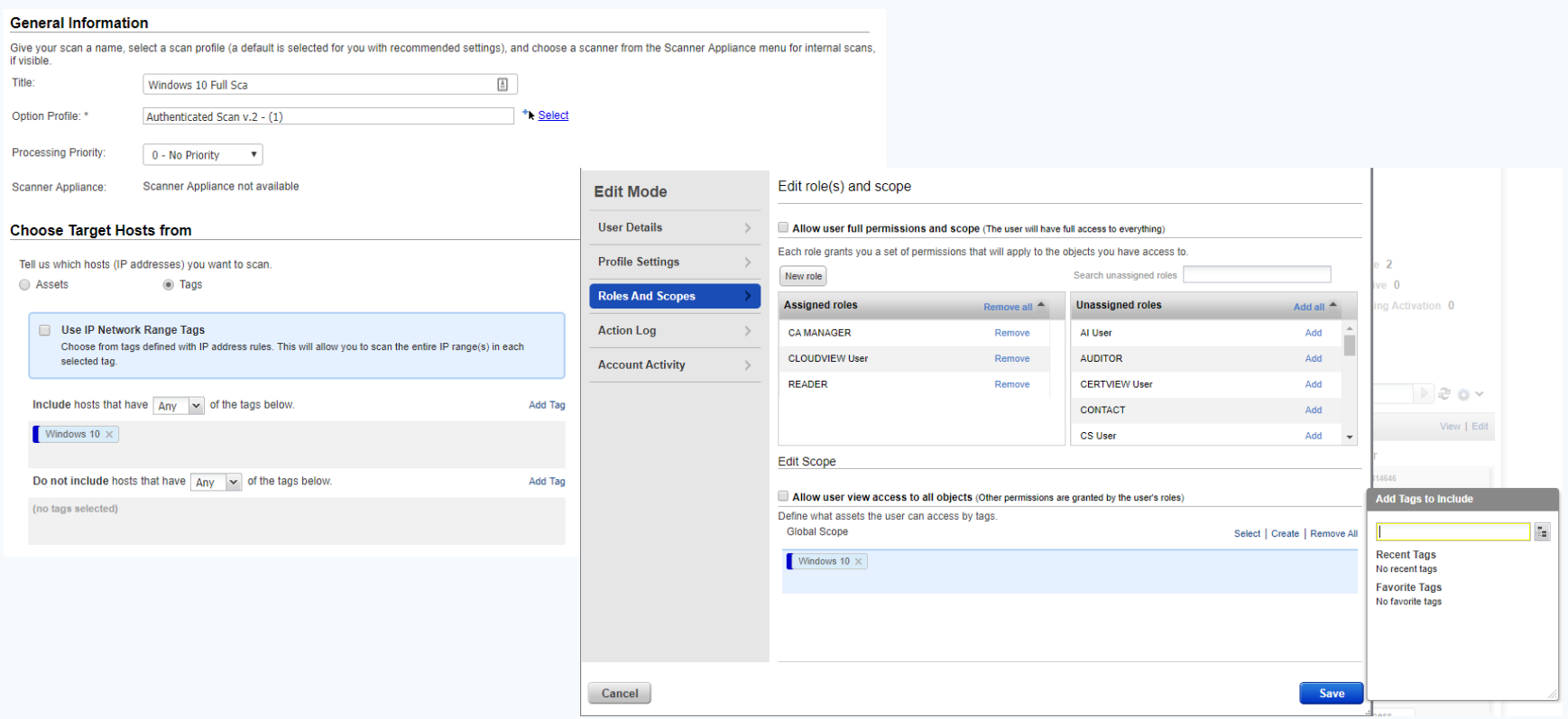
Qualys.

Tags and Asset Groups

Tag Creation



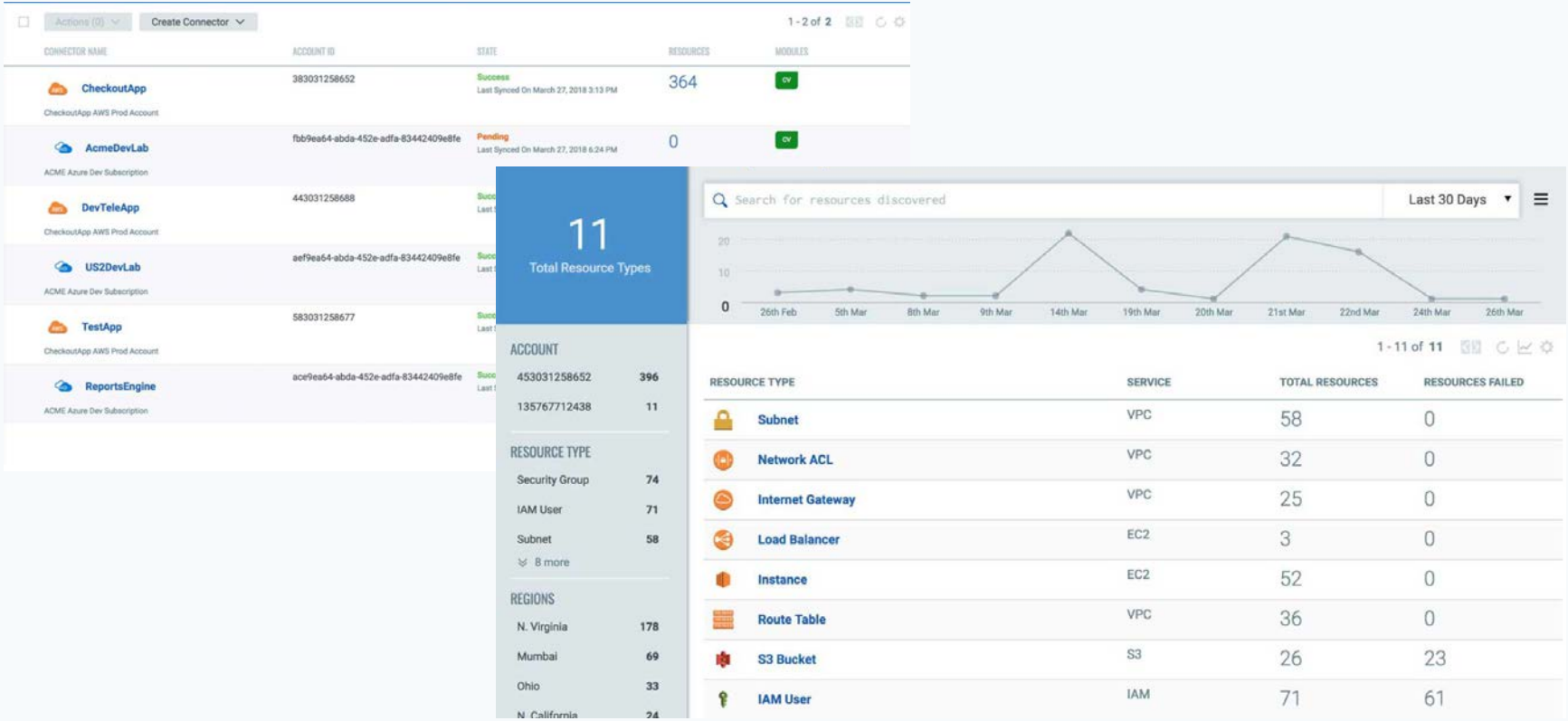
Tag Uses



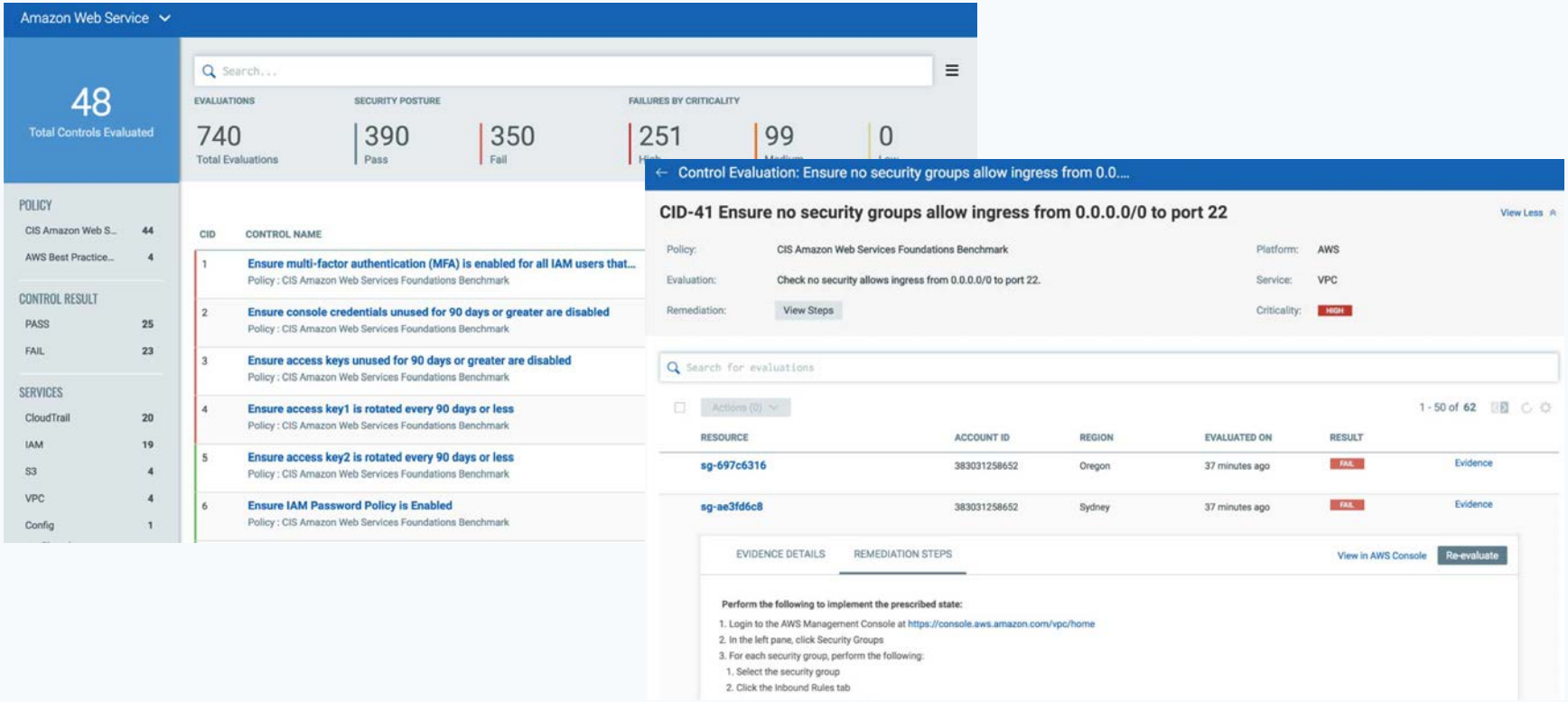
Qualys.

Cloud Integrations

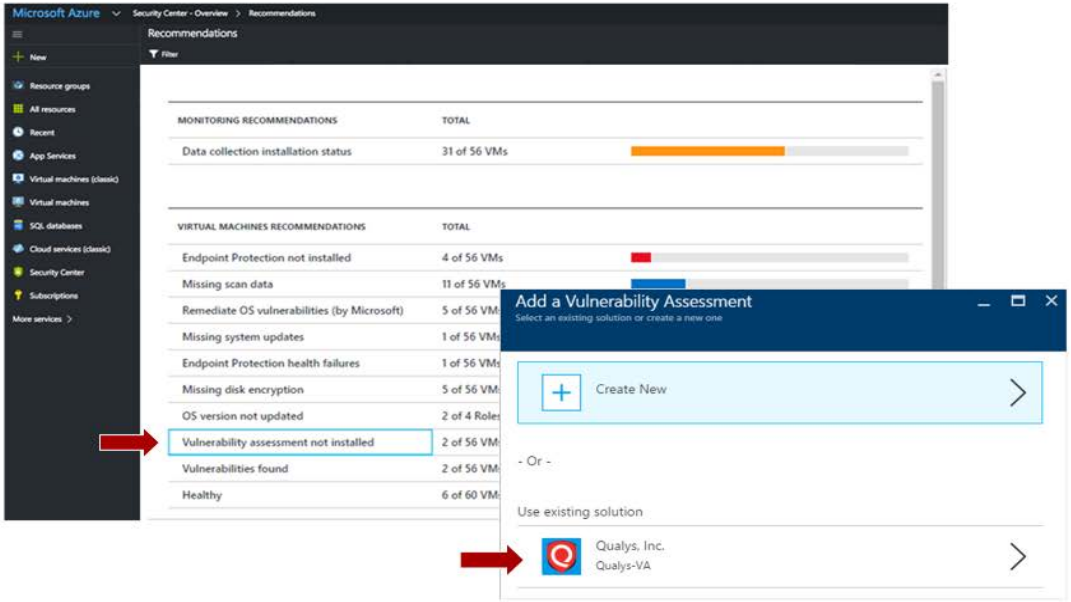
Cloud Inventory

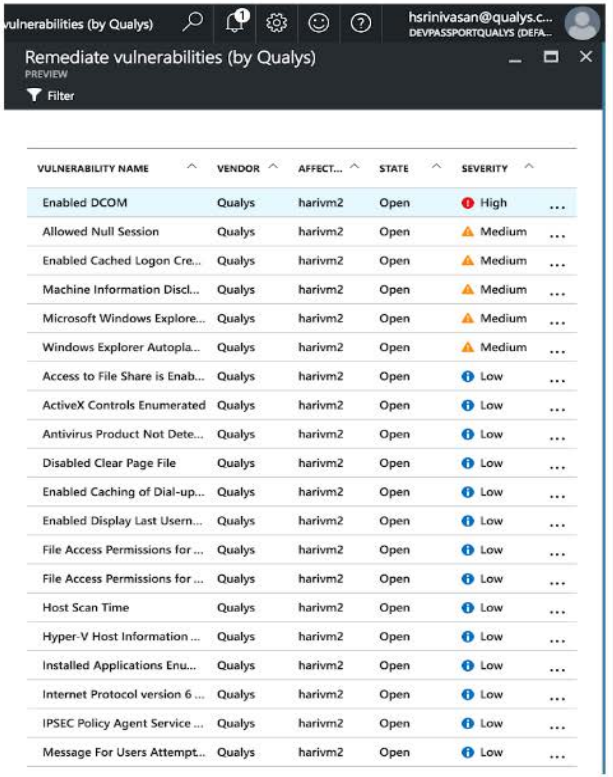


Cloud Assessment



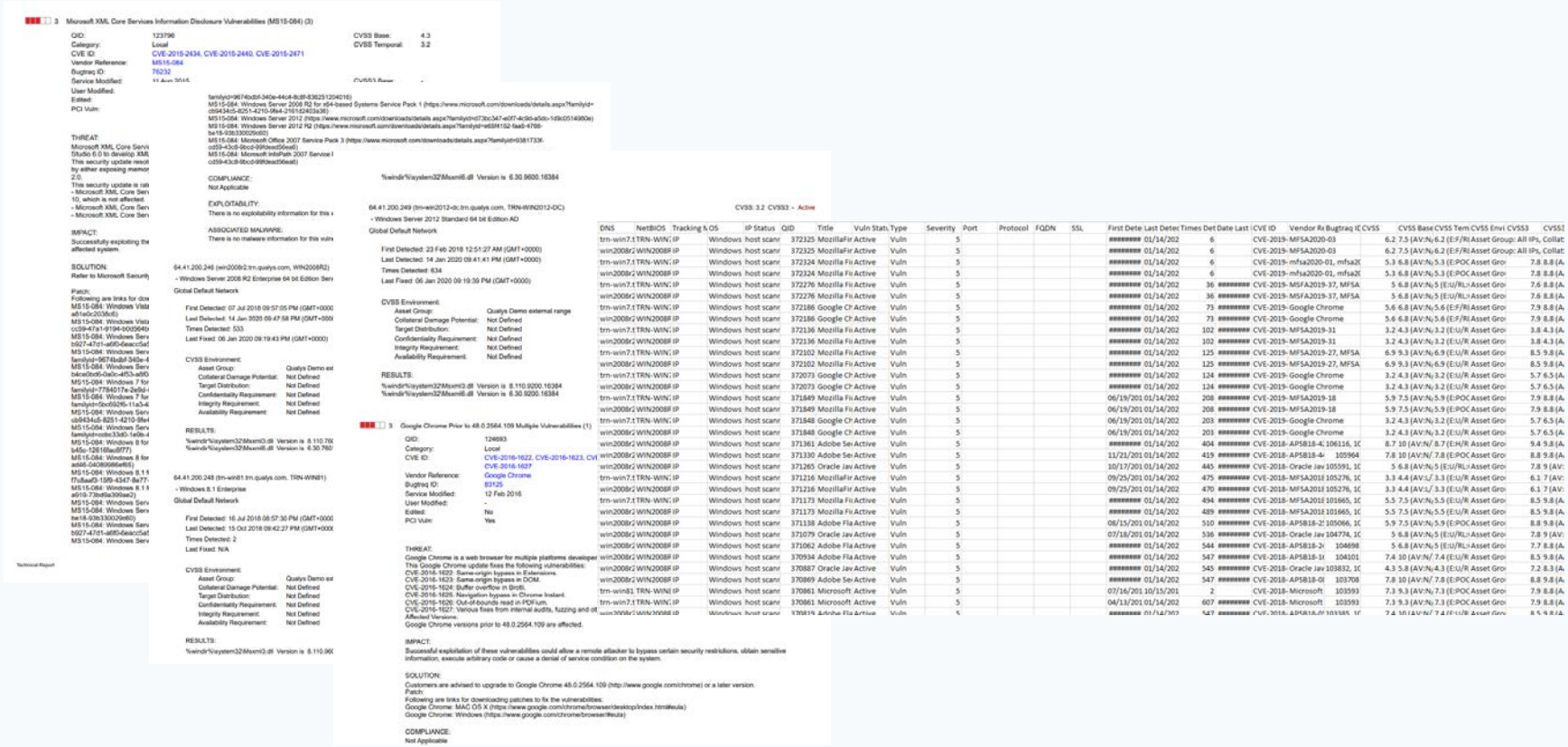
Azure Integration





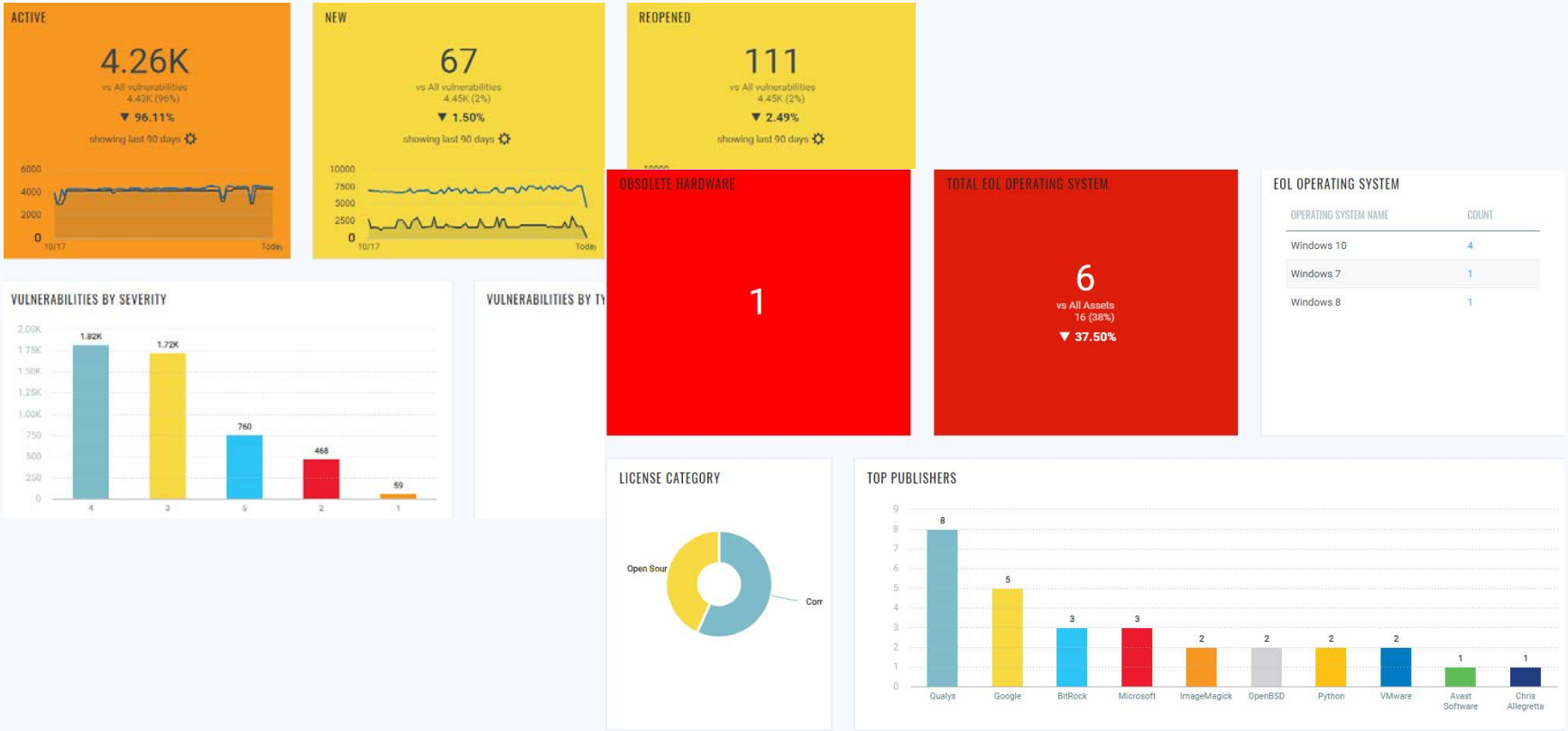
Reporting

Static Reports

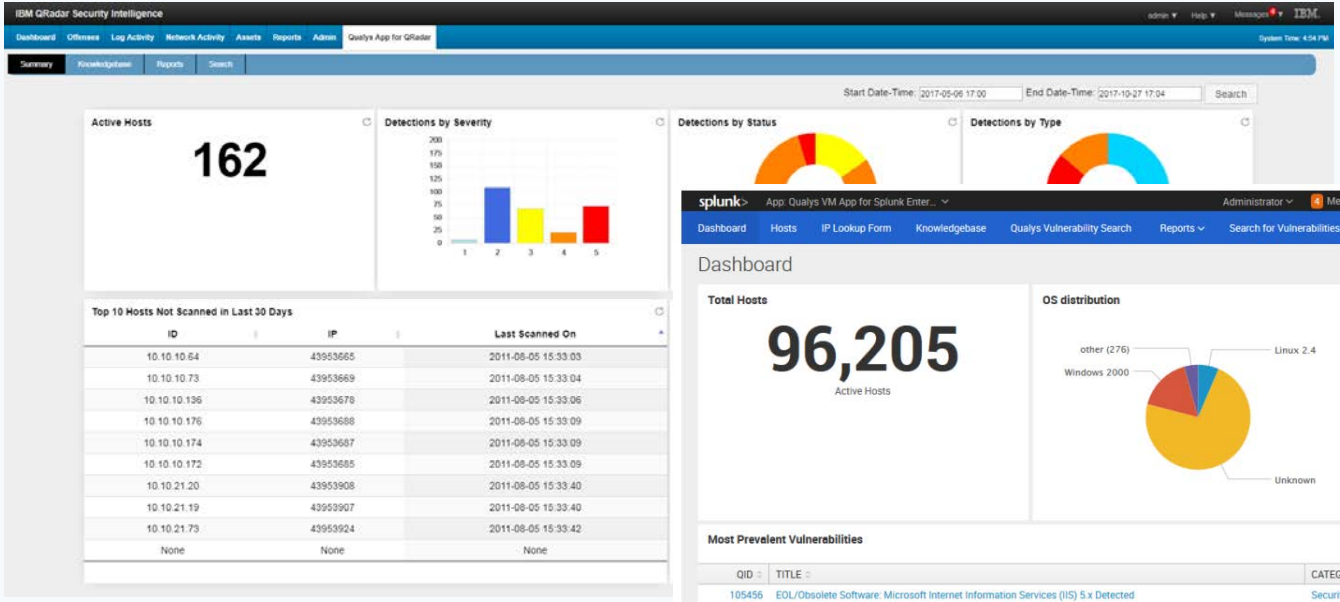


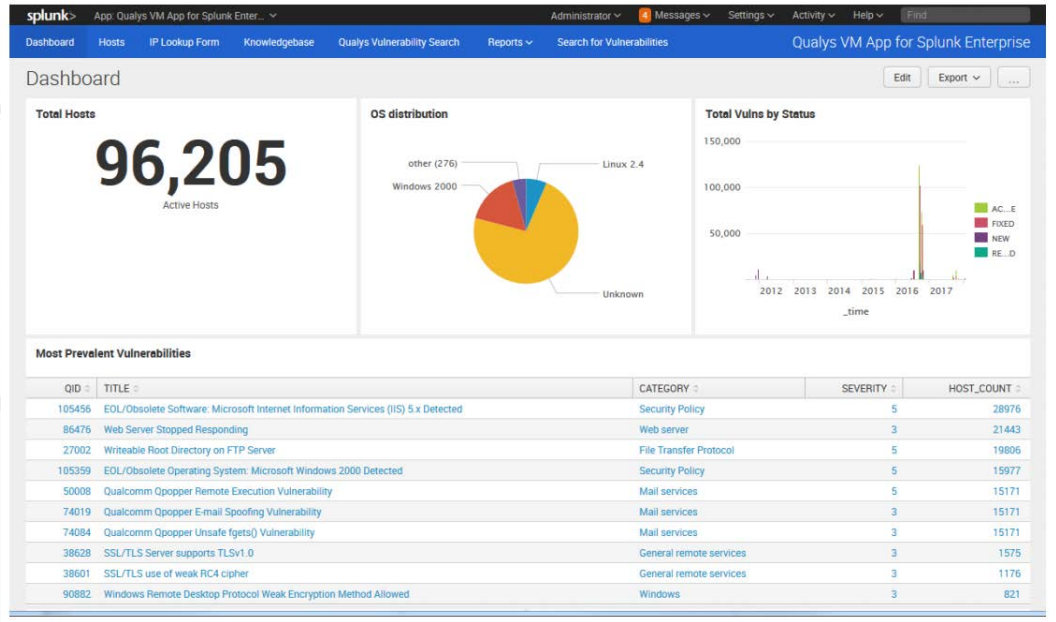
Qualys.

Dashboards


ACTIVE
4.26K
vs All vulnerabilities
4.42K (96%)
▼ 96.11%
showing last 90 days
NEW
67
vs All vulnerabilities
4.45K (2%)
▼ 1.50%
showing last 90 days
REOPENED
111
vs All vulnerabilities
4.45K (2%)
▼ 2.49%
showing last 90 days
OBSOLETE HARDWARE
1
TOTAL EOL OPERATING SYSTEM
6
vs All Assets
16 (38%)
▼ 37.50%
EOL OPERATING SYSTEM
OPERATING SYSTEM NAME
COUNT
Windows 10
4
Windows 7
1
Windows 8
1
VULNERABILITIES BY SEVERITY
1.82K
1.72K
760
468
59
LICENSE CATEGORY
Open Sour
Corr
TOP PUBLISHERS
Qualys
Google
BitRock
Microsoft
ImageMagick
OpenBSD
Python
VMware
Avast Software
Chris Allegretta

API / Plugins


IBM QRadar Security Intelligence
Qualys App for QRadar
Start Date-Time: 2017-05-06 17:00
End Date-Time: 2017-10-27 17:04
Search
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 43953665 2011-08-05 15:33:03
10.10.10.73 43953669 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
10.10.21.73 43953924 2011-08-05 15:33:42
None None None


splunk>
App: Qualys VM App for Splunk Enter...
Administrator
Messages
Settings
Activity
Help
Find
Dashboard
Hosts
IP Lookup Form
Knowledgebase
Qualys Vulnerability Search
Reports
Search for Vulnerabilities
Qualys VM App for Splunk Enterprise
Dashboard
Edit
Export
Total Hosts
96,205
Active Hosts
OS distribution
other (276)
Windows 2000
Linux 2.4
Unknown
Total Vulns by Status
150,000
100,000
50,000
2012 2013 2014 2015 2016 2017
_time
AC...E
FIXED
NEW
RE...D
Most Prevalent 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 fgets() 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

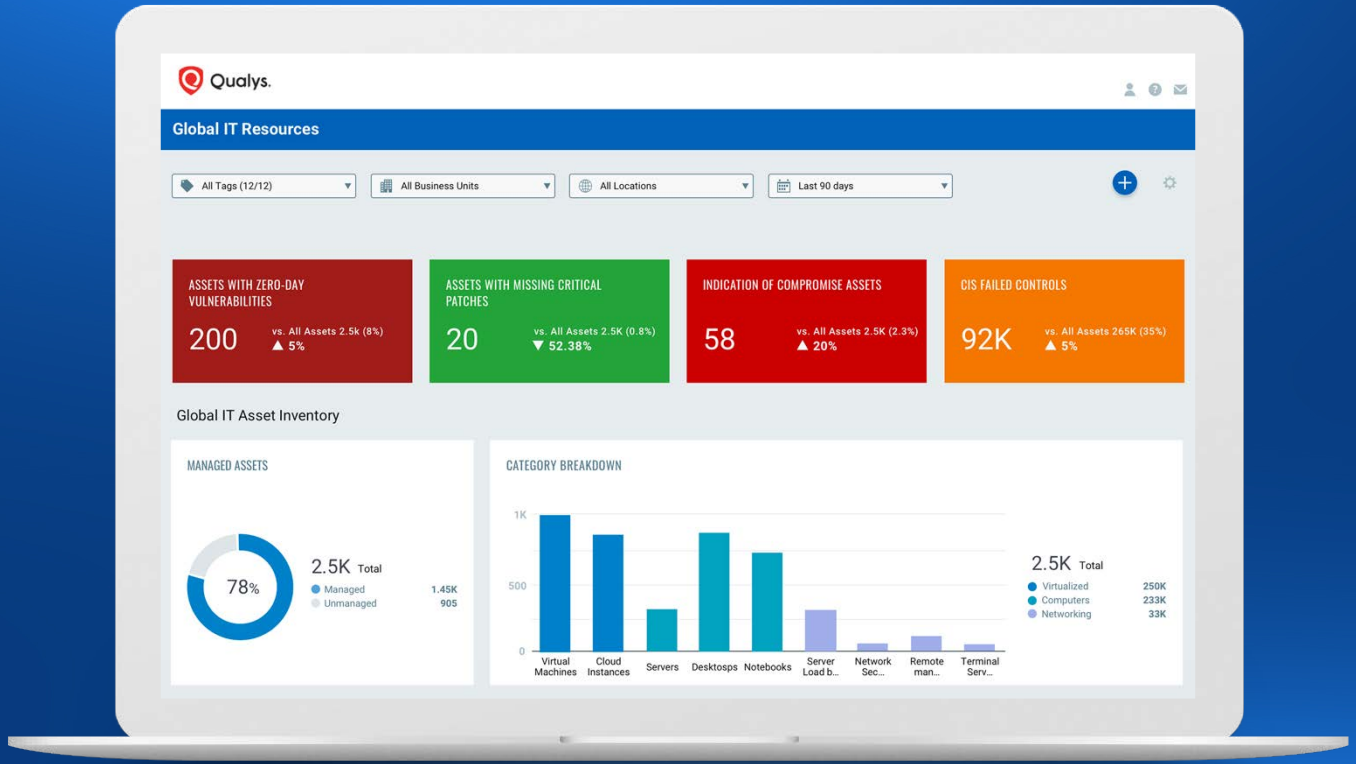
Automatic asset onboarding and clean-up (*ex: purging and adding assets*)
Qualys health check automation
(*ex: Scanner utilization tracking, API limit tracking*)
Scan/Re-scan on Demand
CI/CD Integrations (*Out-of-box and custom*)

Digital Biodiversity

Dominate the Digital Biodiversity!

Why is Qualys better?

CLOUD-BASED MICROSERVICES ARCHITECTURE


Qualys.
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
MANAGED ASSETS
78%
2.5K Total
Managed 1.45K
Unmanaged 905
CATEGORY BREAKDOWN
1K
500
0
Virtual Machines
Cloud Instances
Servers
Desktosps
Notebooks
Server Load b...
Network Sec...
Remote man...
Terminal Serv...
2.5K Total
Virtualized 250K
Computers 233K
Networking 33K

Thank You