QSC 2021 VMDR

Qualys.

Course Training Documents

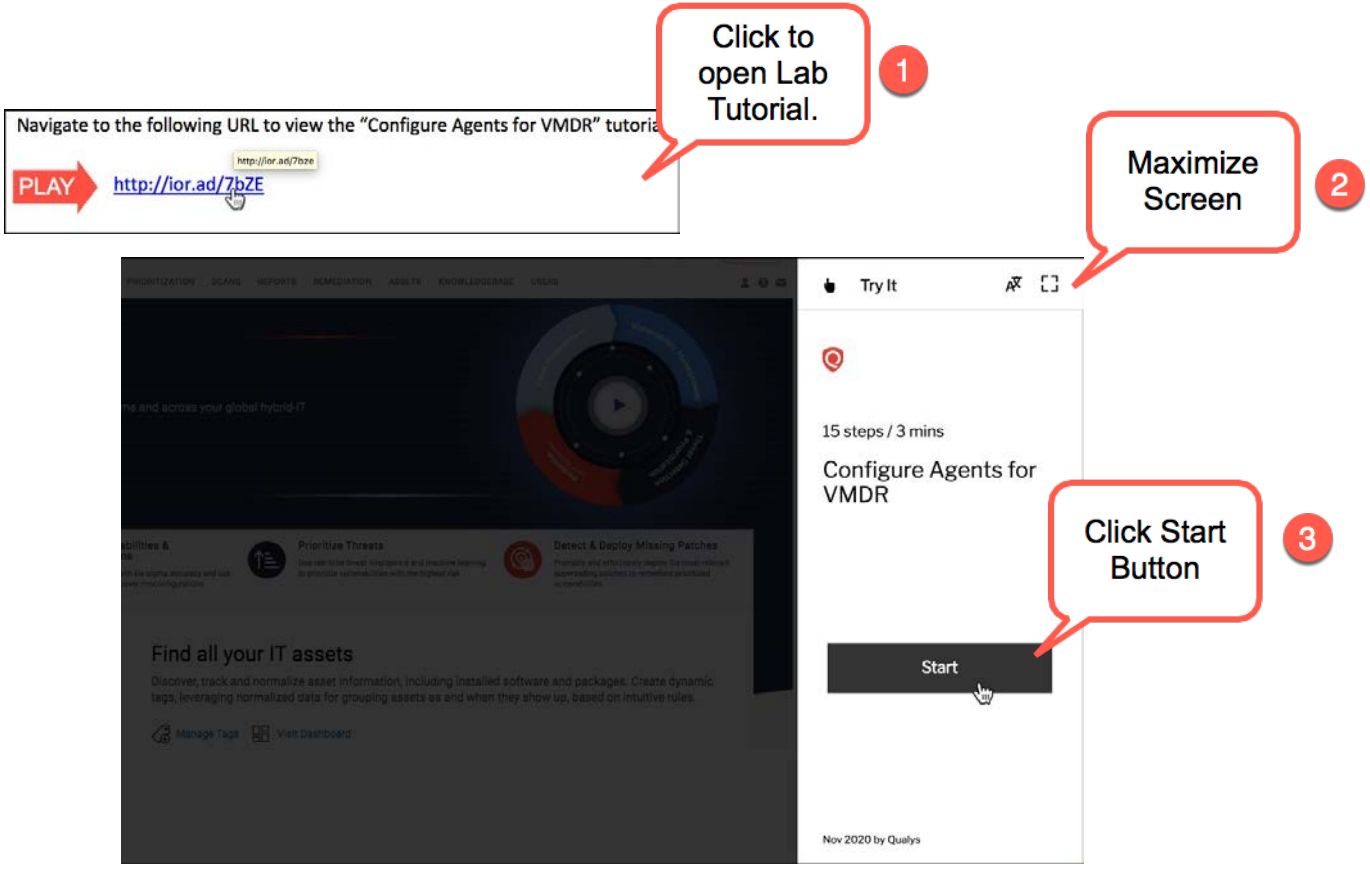
- QSC 2021 VMDR Lab Tutorial Supplement
- QSC 2021 VMDR Slides

You can download both documents from:

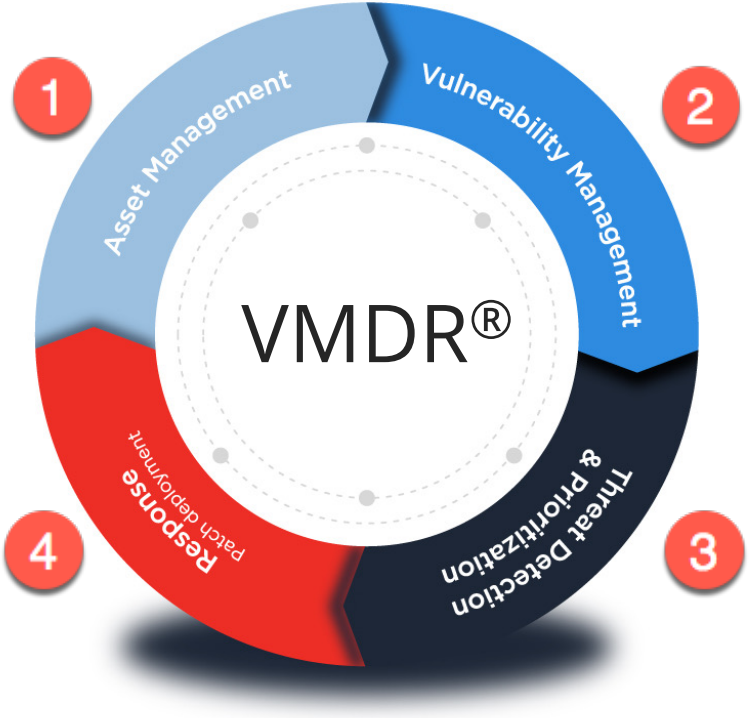
`https://bit.ly/qsc21vmdr`

Qualys.

Play Lab Tutorials



Qualys VMDR Lifecycle



Qualys.

VMDR Agenda

1. Asset Management
    - Qualys Sensor Overview
    - CyberSecurity Asset Management (CSAM)
2. Vulnerability Management (VM)
    - Vulnerability Findings
    - Dashboards & Widgets
3. Threat Detection & Prioritization (TP)
    - VMDR Threat Feed
    - VMDR Prioritization Report
4. Response – Patch Management (PM)
    - Deployment Jobs
    - Patch Catalog

Qualys.

Asset Management

Qualys.

CIS Control 1: Inventory and Control of Enterprise Assets

CIS Controls

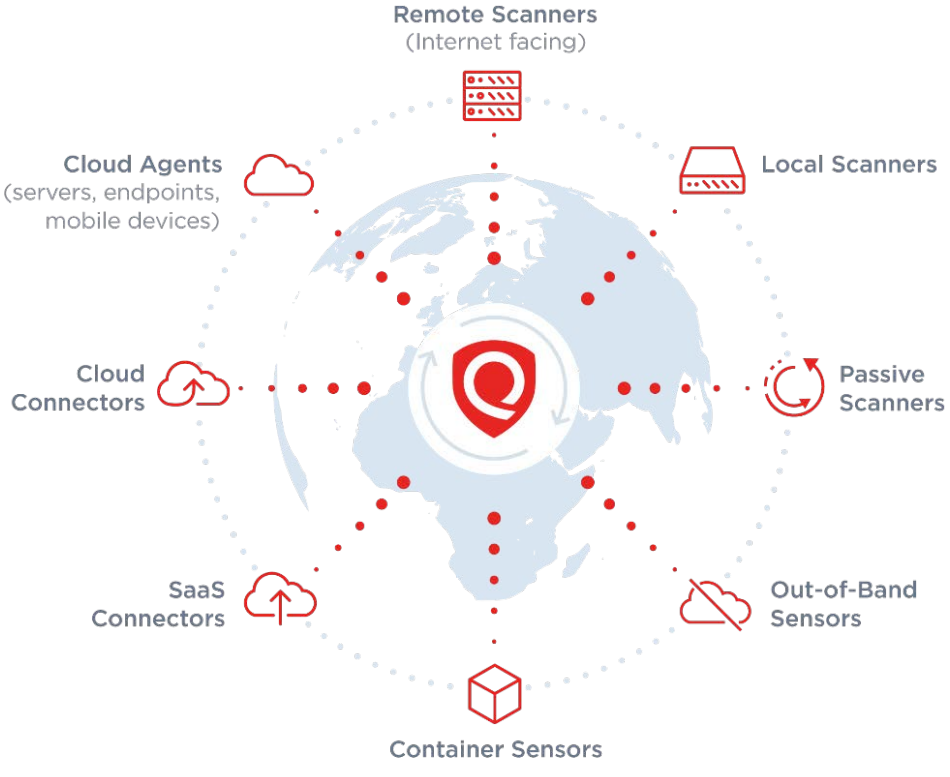
Overview

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

https://www.cisecurity.org/controls/inventory-and-control-of-enterprise-assets/

Qualys.

Qualys Sensor Platform



APIs (collect data from 3rd parties)

Qualys.

Configure Agents for VMDR

- The patching and response functions in VMDR require Cloud Agent.
- Some Agent Activation Keys may need to be updated to include the VMDR application modules (i.e., VM, CSAM, SCA, and PM).

Qualys.

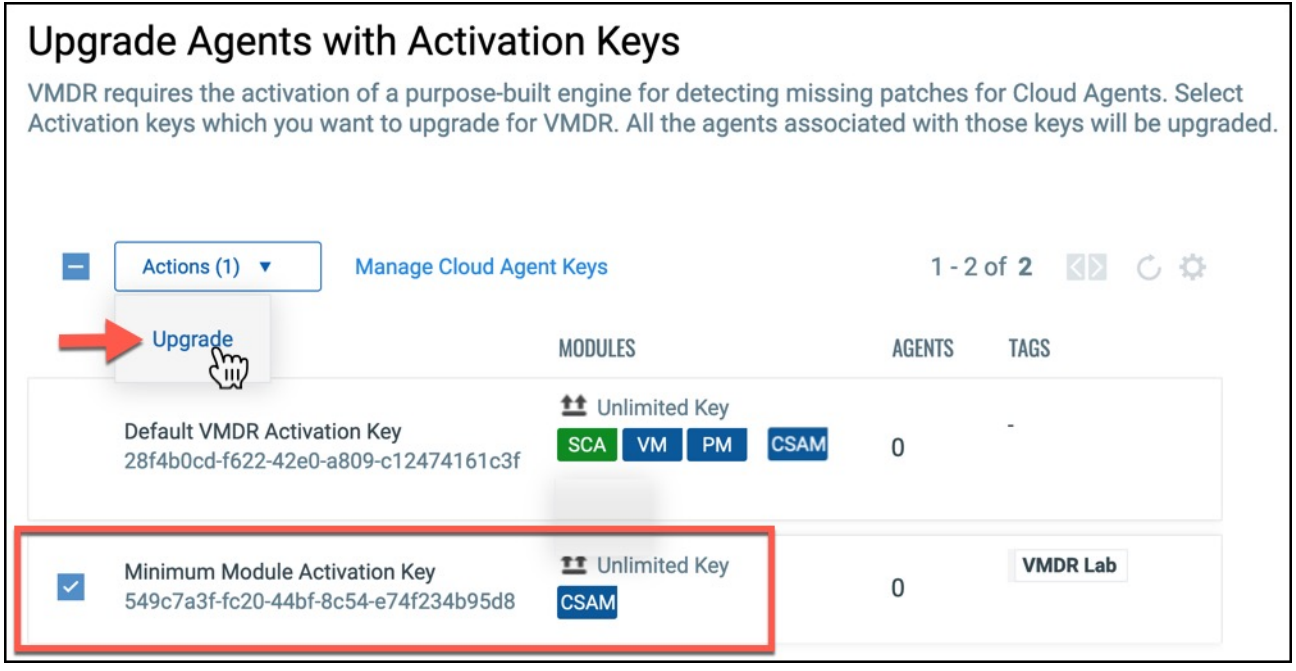
Lab 1: Configure Agents for VMDR

Please consult pages 3 to 14 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 4.

Qualys.

Upgrade Agent Activation Keys

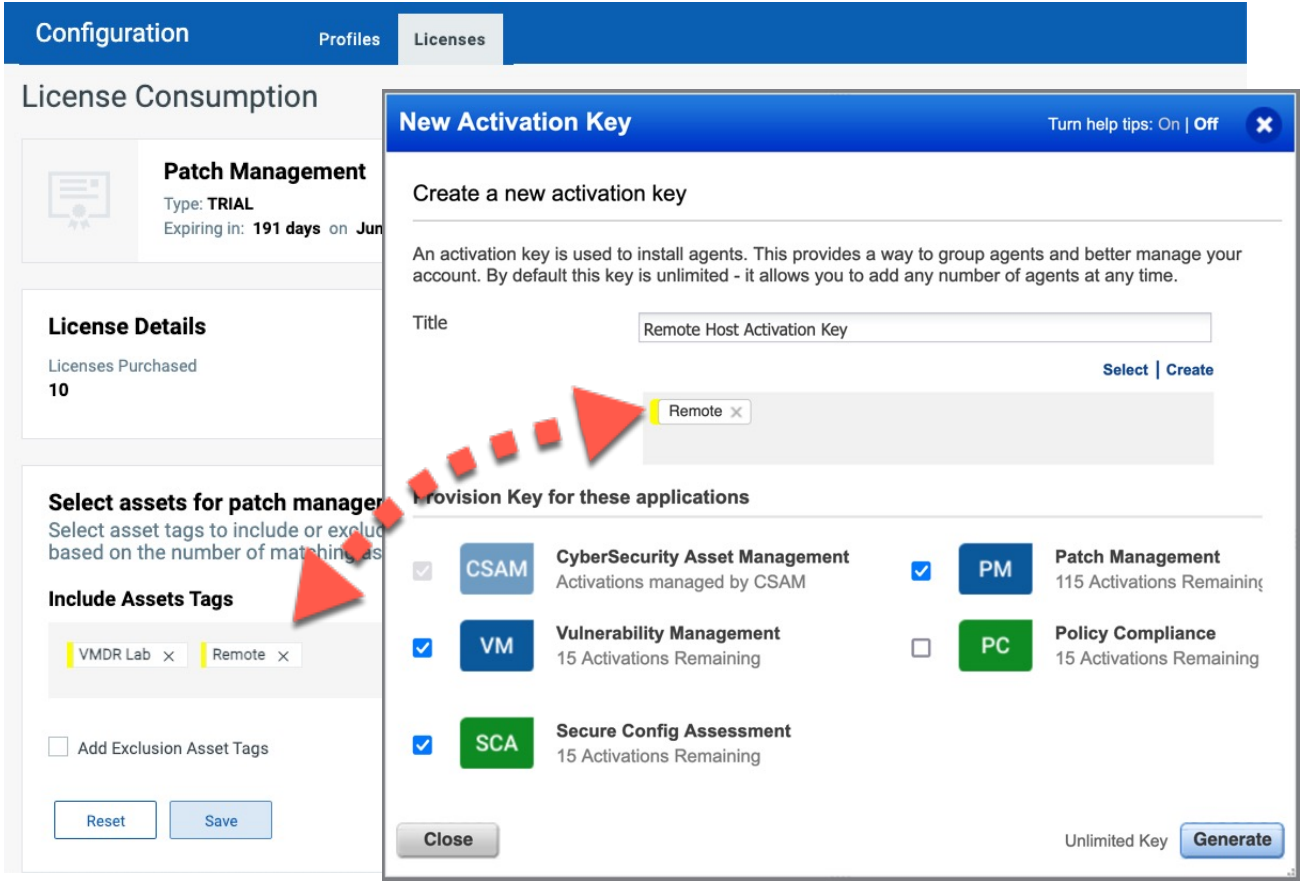


Upgrade Agent Activation Keys to include VMDR application modules (i.e., VM, SCA, PM, CSAM).

Qualys.

Activation Key Tagging Strategy

BEST PRACTICE: Assign "static" tags to agent Activation Keys and use them to ensure agent hosts receive their appropriate performance settings, patching licenses, and patch job assignments.



Qualys.

CyberSecurity Asset Management

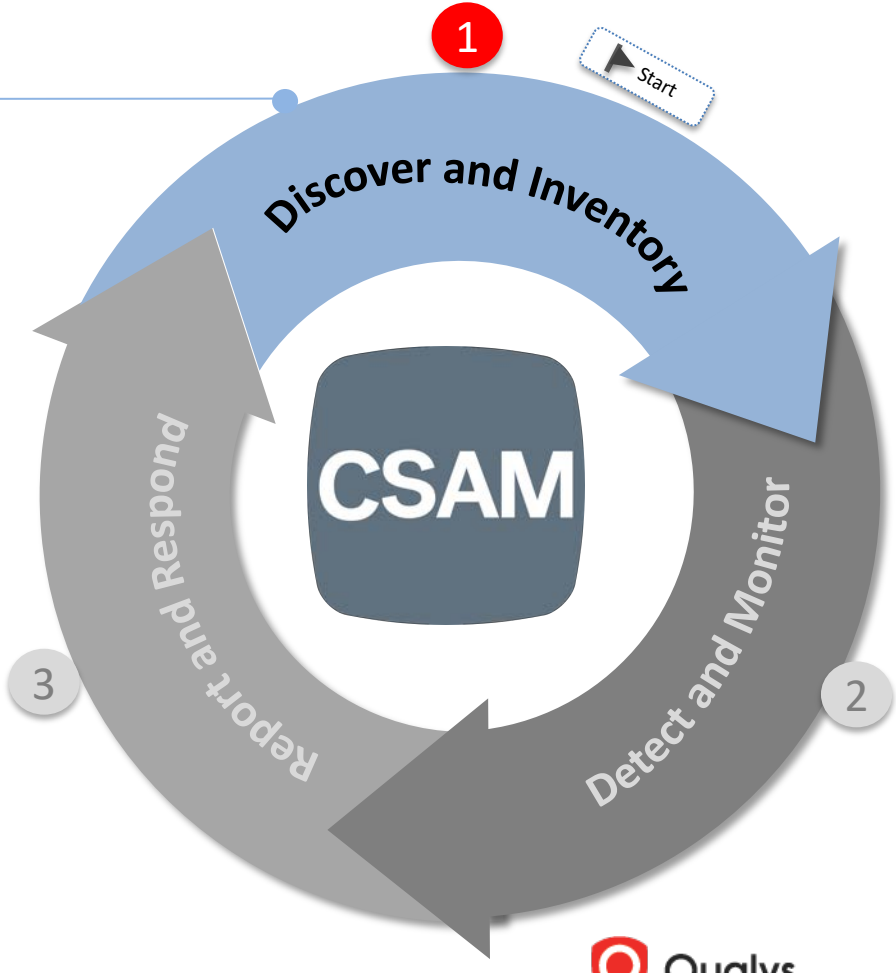
Qualys.

Discover and Inventory Assets

Asset Inventory Data Collection
- Passive Sensor
- Configure CMDB Sync (if using CMDB solution)

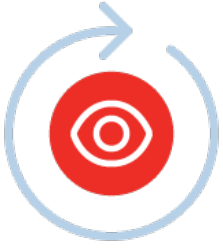
Normalization, Categorization & Enrichment* (performed automatically in the Qualys Cloud Platform)

Organize and Manage Assets (configure Asset Tags)

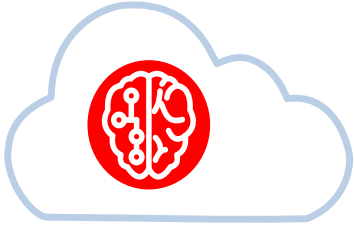


Qualys.

Comprehensive Asset & Software Inventory



Physical Scanner
Virtual Scanner
Cloud Connector
Container Sensor
Cloud Agent
Passive Sensor
API
Out-of-Band



CSAM Catalog: Categorize, Normalize and Enrich

OS/HW/SW
Support Stage
Manufacturer
Lifecycle Stage
License type
Category

Qualys CyberSecurity Asset Management (CSAM) aggregates data from all sensors.

Qualys.

Qualys Categorization, Normalization & Enrichment

Normalization & categorization

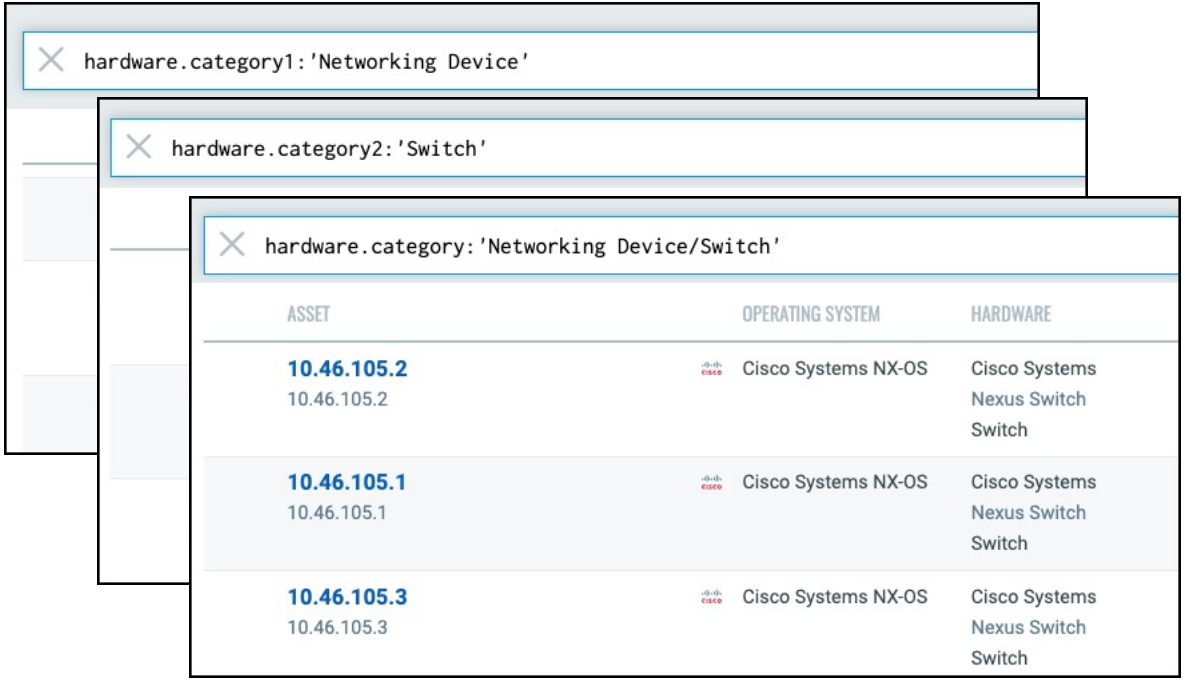
Advanced asset information

	Operating Systems	Hardware	Software
Raw Data	Base OS Runtime AIX: 06.01.0009.0300 EE	Dell, Inc. R510	mysql-community-server 5.6.35-2.el7.x86_64
Category	UNIX > Server	Computers > Server	Databases > RDBMS
Manufacturer	IBM	Dell	Sun Microsystems
Owner	IBM	Dell	Oracle
Product	AIX	PowerEdge	MySQL Server
Market Version / Model	6	R510	5
Edition	Enterprise	-	Community
Version	6.1	-	5.6
Update	TL9 SP3	-	35-2.el6
Architecture	64-Bit	-	64-Bit
Lifecycle Stage	EOL/EOS	OBS	EOL
End-of-Life	30-Apr-2015	1-Sep-2012	28-Feb-2018
End-of-Support	30-Apr-2017	1-Sep-2012	28-Feb-2021
Support Stage	Unsupported	Obsolete	Extended Support
License Type	Commercial	-	Open Source (GPL-2.0)

Search Hardware Categories

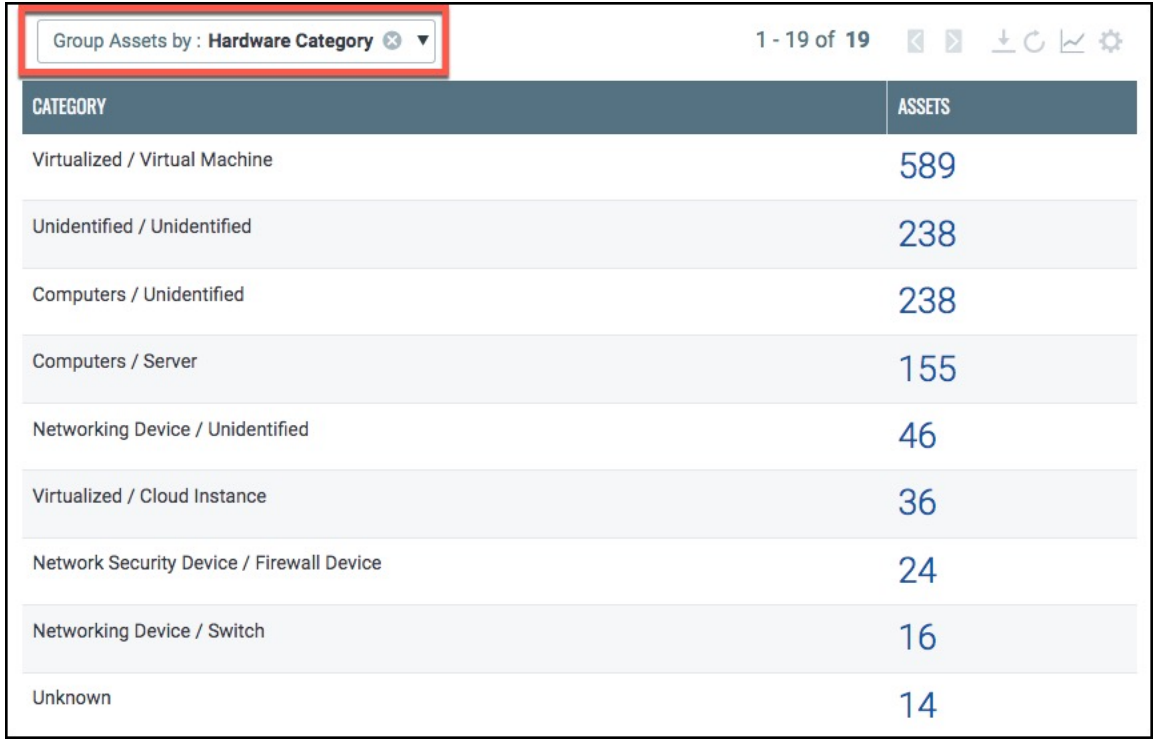
hardware.category1: value1
hardware.category2: value2
hardware.category: value1 / value2

hardware.category1: `Networking Device`
hardware.category2: `Switch`
hardware.category: `Networking Device / Switch`



Qualys.

Hardware Category List



CATEGORY	ASSETS
Virtualized / Virtual Machine	589
Unidentified / Unidentified	238
Computers / Unidentified	238
Computers / Server	155
Networking Device / Unidentified	46
Virtualized / Cloud Instance	36
Network Security Device / Firewall Device	24
Networking Device / Switch	16
Unknown	14

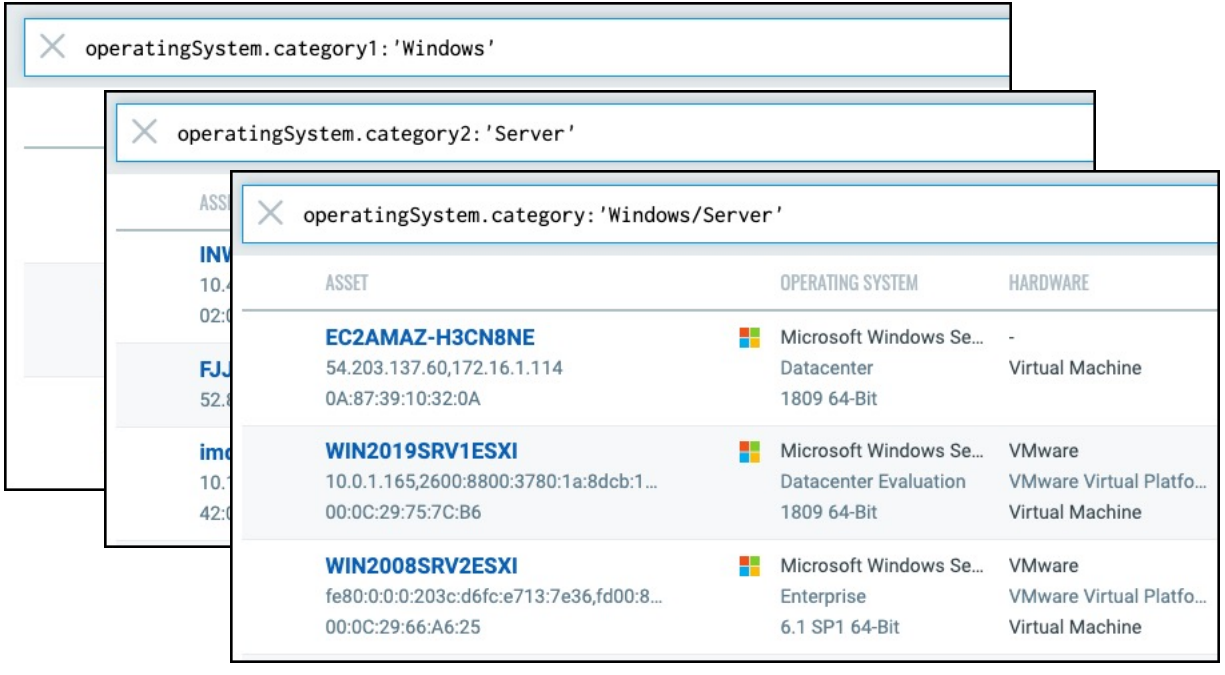
Group assets by Hardware Category to build a list of hardware category values in your account.

Qualys.

Search OS Categories

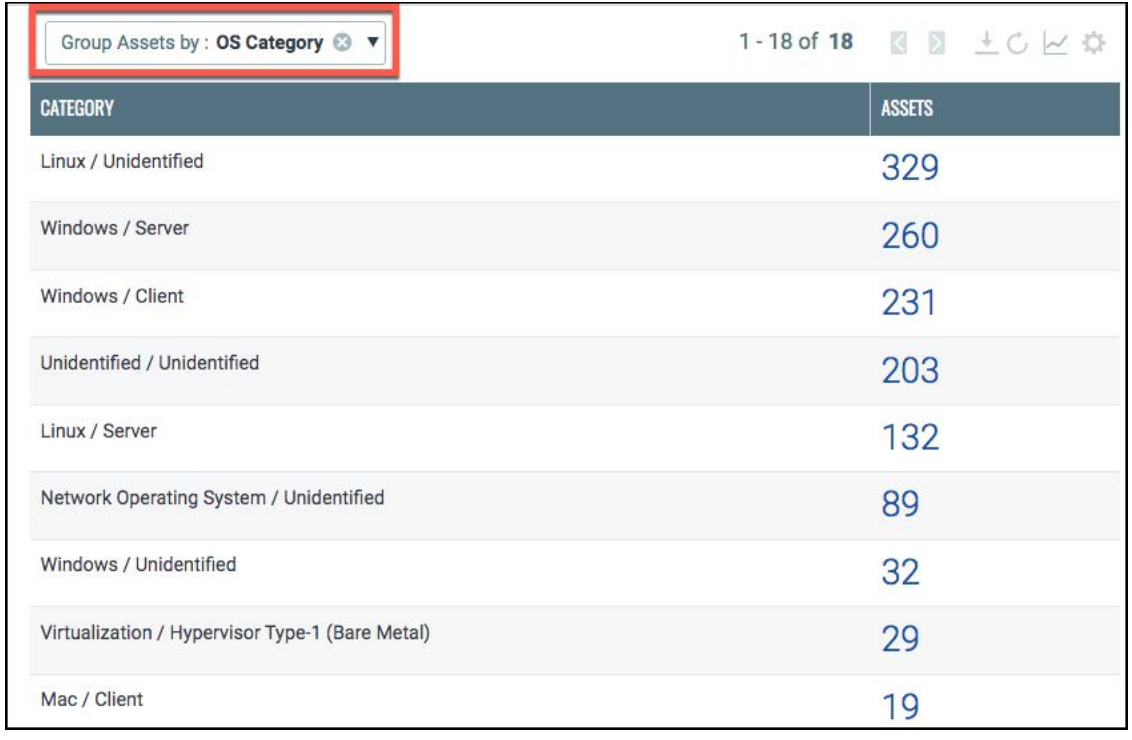
operatingSystem.category1: value1
operatingSystem.category2: value2
operatingSystem.category: value1 / value2

operatingSystem.category1: `Windows`
operatingSystem.category2: `Server`
operatingSystem.category: `Windows / Server`



Qualys.

OS Category List



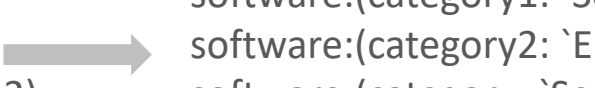
CATEGORY	ASSETS
Linux / Unidentified	329
Windows / Server	260
Windows / Client	231
Unidentified / Unidentified	203
Linux / Server	132
Network Operating System / Unidentified	89
Windows / Unidentified	32
Virtualization / Hypervisor Type-1 (Bare Metal)	29
Mac / Client	19

Group assets by OS Category to build a list of operating system category values in your account.

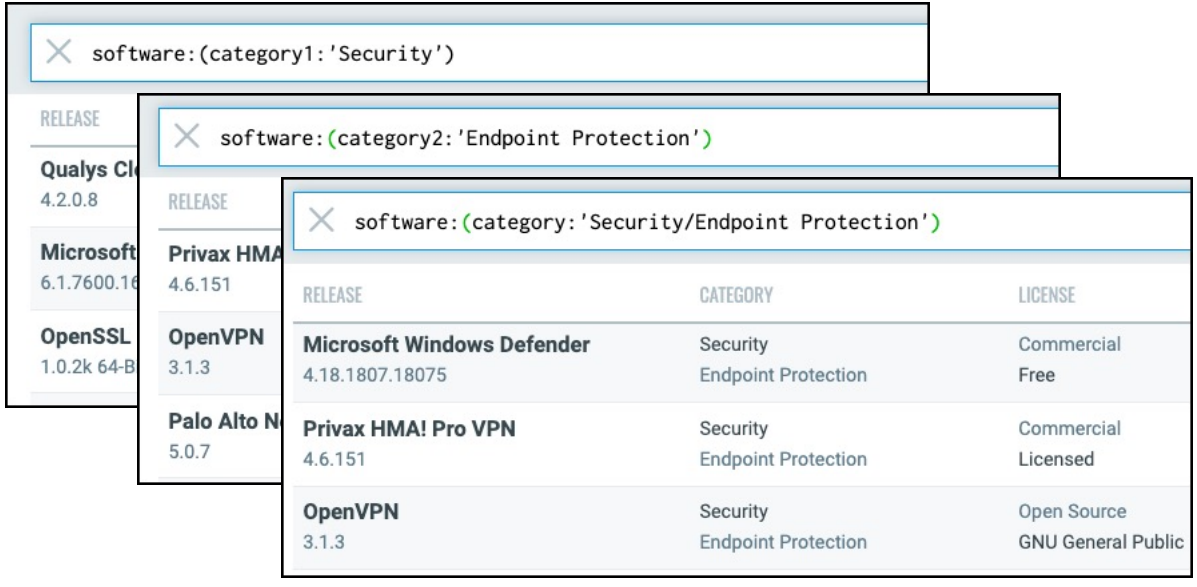
Qualys.

Search Software Categories

software:(category1: value1)
software:(category2: value2)
software:(category: value1 / value2)

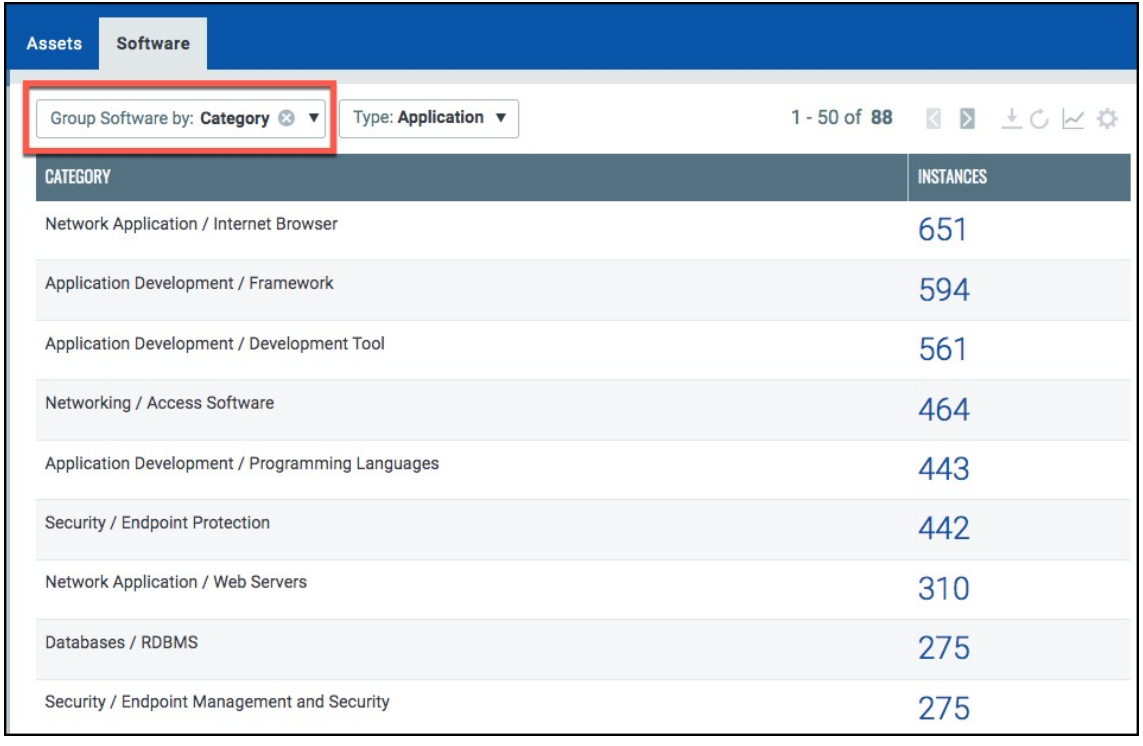


software:(category1: `Security`)
software:(category2: `Endpoint Protection`)
software:(category: `Security / Endpoint Protection`)



Qualys.

Software Category List



Group Software by Category to build a list of software category values in your account.

Qualys.

Lab 2 : Search Using Categories

Please consult pages 15 to 16 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 16.

Qualys.

Software License Category

Commercial – Supported by vendor.

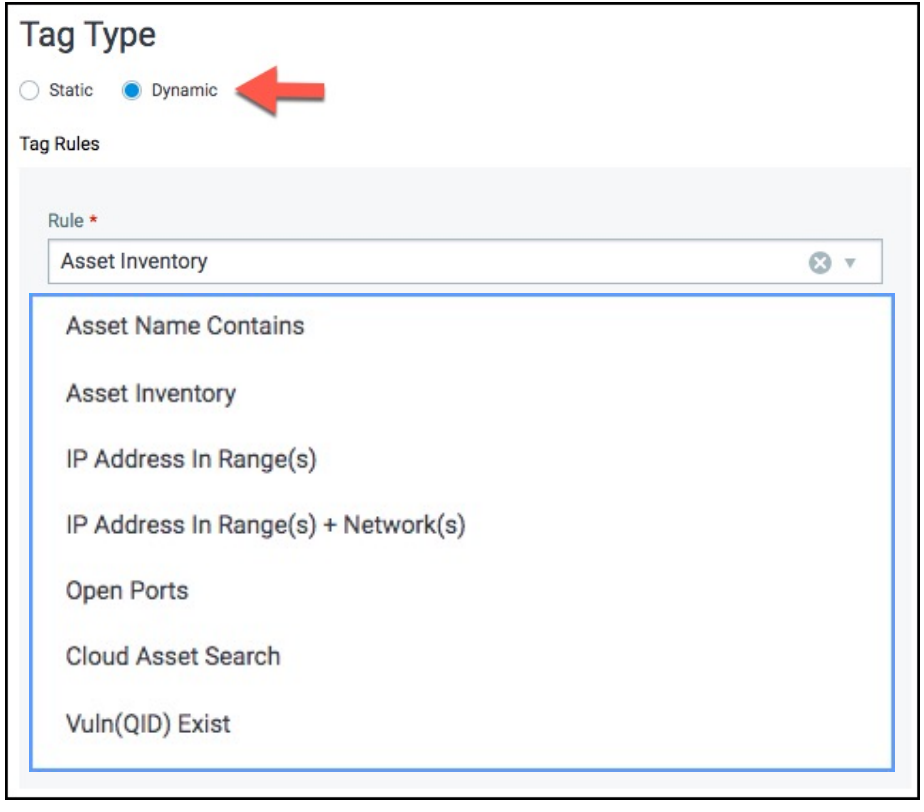
```
software:(license.category:`Commercial`)
```

Open Source – Free for public use.

```
software:(license.category:`Open Source`)
```

Qualys.

Dynamic Rule-Based Tags



- The “Asset Inventory” rule engine allows you to build tags using query tokens, including the Hardware, OS, and Software category tokens.
- Other “dynamic” rule engines are also available.

Qualys.

Lab 3 : Dynamic Rule-Based Tags

Please consult pages 17 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 17.

Qualys.

Unidentified vs. Unknown

Some OS and Hardware assets may appear as “unidentified” or “unknown.”

Unidentified

- Not enough data has been discovered/collected for Qualys to determine the asset’s hardware or operating system.

Unknown

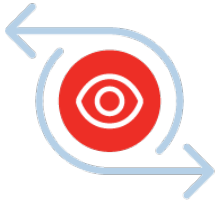
- Adequate data exists for Qualys to categorize the asset, but it has yet to be cataloged.

Qualys.

Network Passive Sensor

Qualys.

Passive Sensor Overview



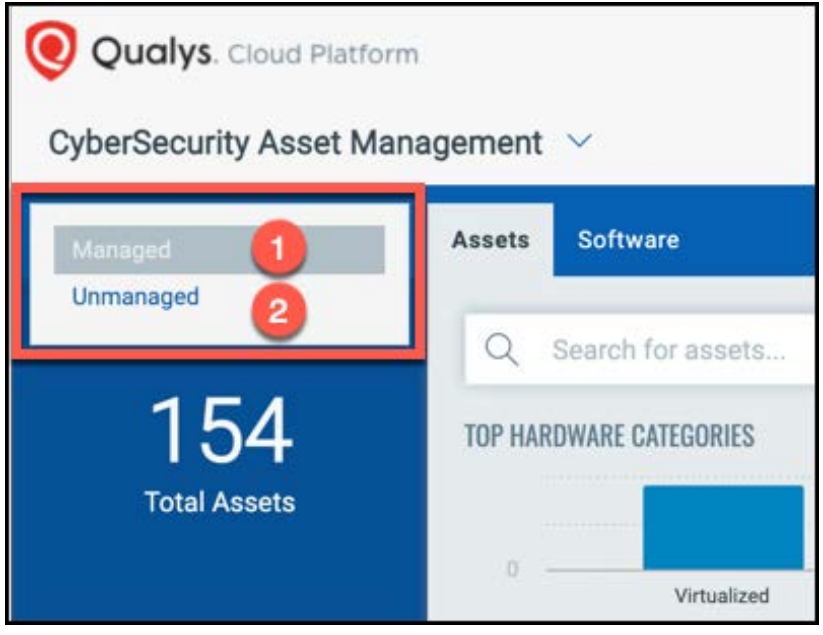
- Sniffs traffic via network TAP or the SPAN port of a network switch.
- Captured data and traffic is sent to the Qualys Platform for analysis and processing.

1. Discovered assets not in your account, are placed in the “Unmanaged” section of Qualys CSAM.
2. Enable “Traffic Analysis” to reveal communication between assets, including conversations between managed and unmanaged assets.

Qualys.

Managed vs. Unmanaged Assets

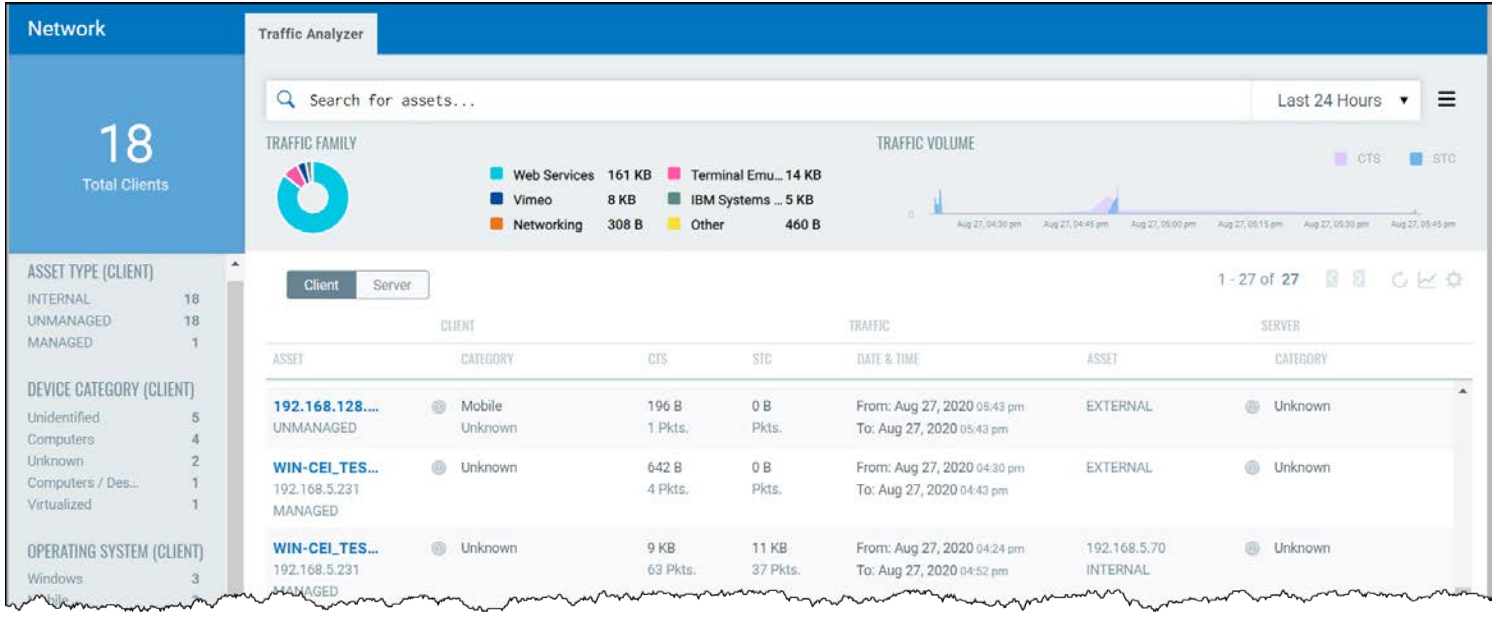
1. If discovered data is confirmed to match an asset already in your account, its information can be merged with the existing asset.
2. Discovered assets not in your account, are placed in the “Unmanaged” section of Qualys CSAM.



Qualys.

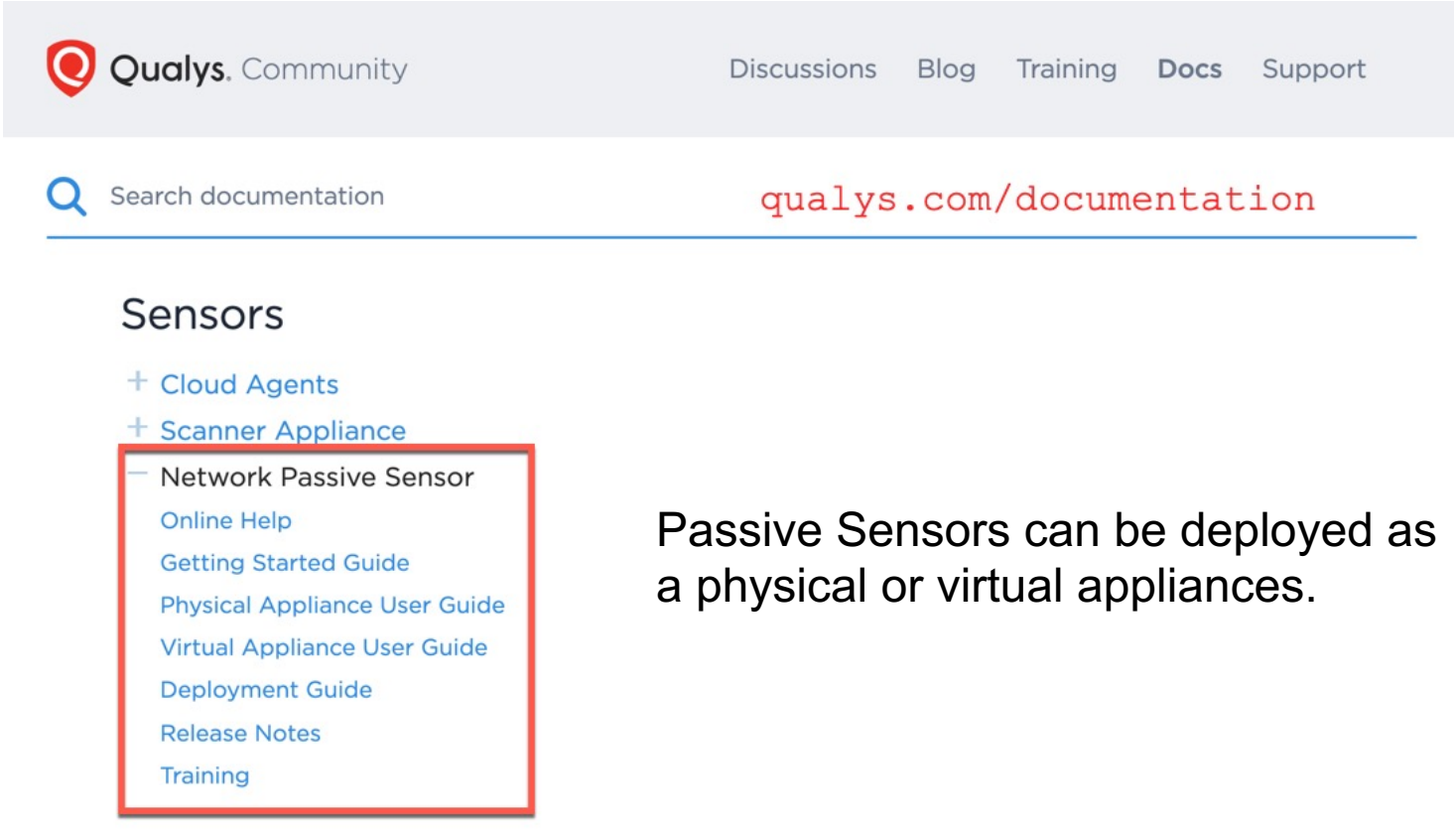
Network Traffic Analyzer

- Conversations between assets can offer new discoveries and insights.



Qualys.

Network Passive Sensor User Guides



Passive Sensors can be deployed as a physical or virtual appliances.

Qualys.

CMDB Sync

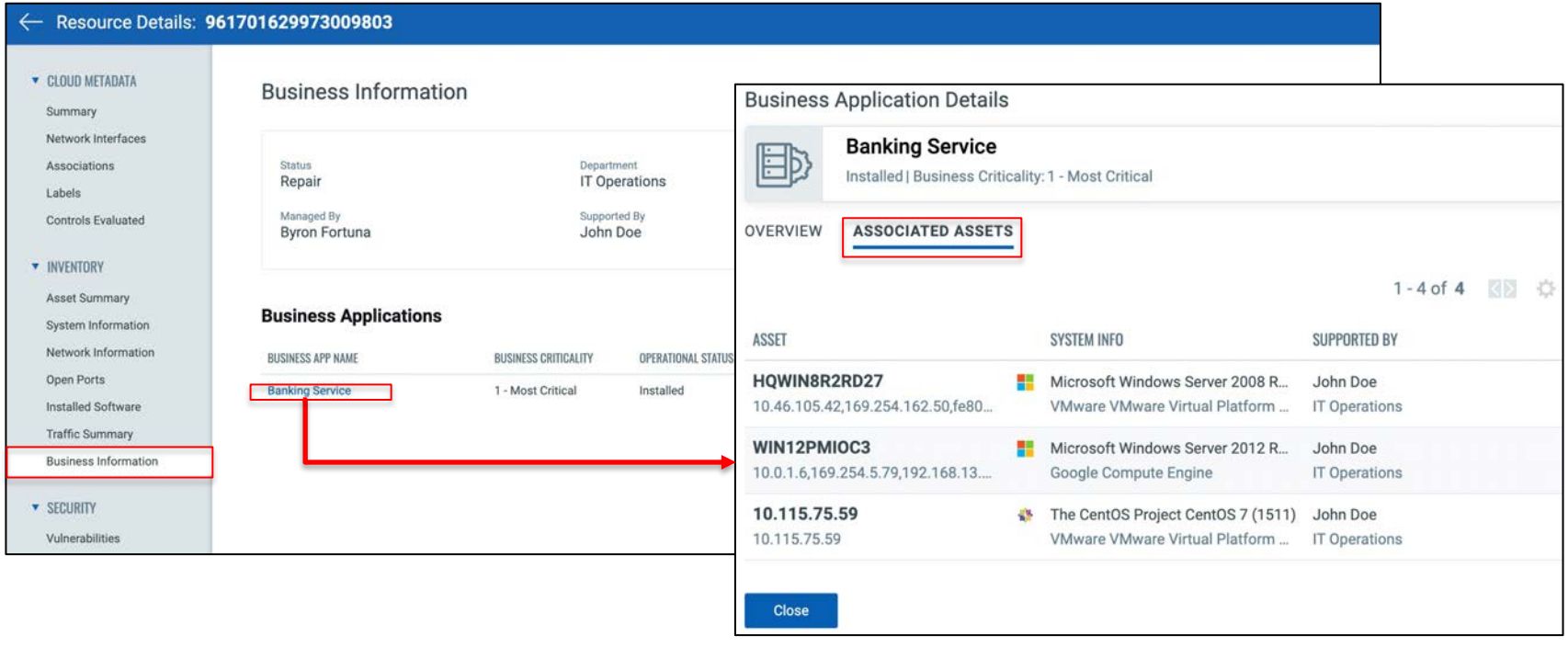
Qualys.

Certified ServiceNow CMDB Sync App

- Supports 2-way sync (Qualys to ServiceNow and ServiceNow to Qualys)
- Up-to-date, categorized, normalized, and enriched ServiceNow CMDB
- Enrich Qualys assets with key CMDB business data
- Synchronization schedules can be configured and saved.
- Asset metadata is only synchronized for assets that already exist in both Qualys and ServiceNow.
- Optionally, asset information is staged for user approval before being written to CMDB.

Qualys.

Import Business Attributes from ServiceNow CMDB



- Automatically import business application and business context attributes from ServiceNow CMDB
- Identify other assets associated with a business application

Qualys.

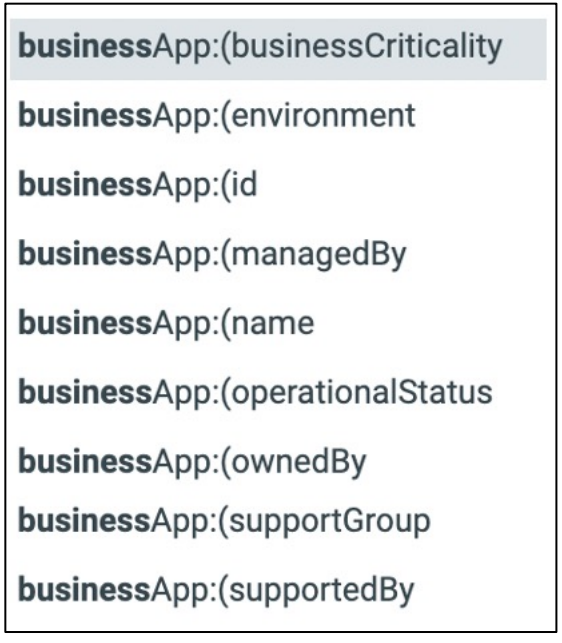
Lab 4 : CMDB Sync and Business Context

Please consult pages 19 to 20 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 19.

Qualys.

Use Business Attributes to Search for Assets



- Use any of the “businessApp” search tokens to single out assets, based on the business information and characteristics provided by ServiceNow.
- Queries using these tokens will impact assets already synchronized.

Qualys.

Integration with ServiceNow CMDB

To implement ServiceNow CMDB Integration, a Qualys subscription with API access is required, along with the following application modules:

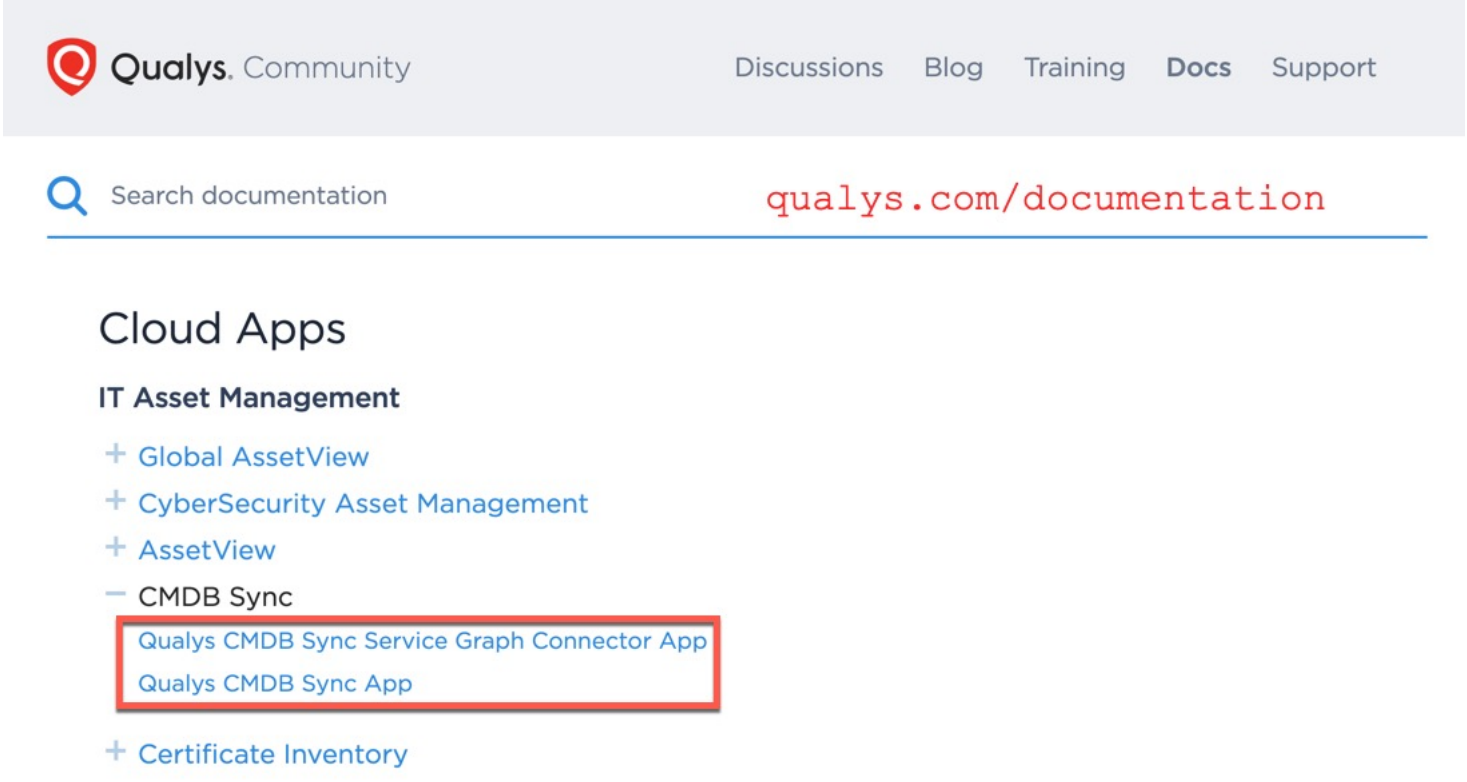
- CSAM
- Vulnerability Management

1. **Qualys CMDB Sync App**
   - Install the Qualys CMDB Sync App (available in ServiceNow Online Store)

2. **Qualys CMDB Sync Service Graph Connector App**
   - Install the Qualys Service Graph Connector App (available in ServiceNow Online Store)
   - ITOM Visibility license in ServiceNow

Qualys.

CMDB Sync App User Guides

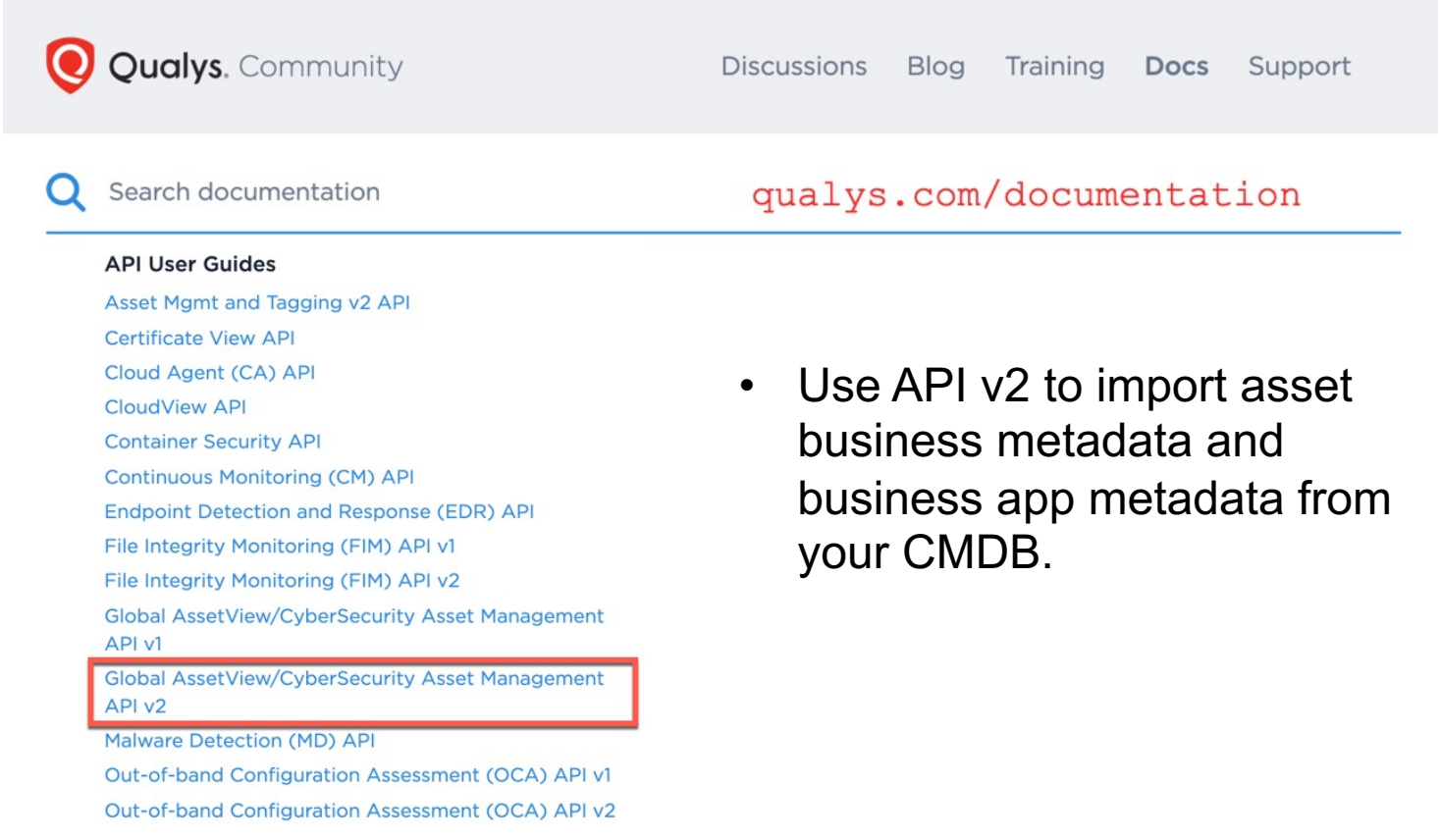


Qualys.

Public APIs for CMDB Sync

- CSAM now supports import of **Asset business metadata** and **Business app metadata** from your CMDB into your Qualys asset inventory (using v2 APIs).
- Imported business attributes are listed in the Asset Details page.
- User must have access to the CSAM module with API enabled for that role.
- Currently supports maximum 250 records for import in one API call for both Asset and Business app metadata.

API User Guide



- Use API v2 to import asset business metadata and business app metadata from your CMDB.

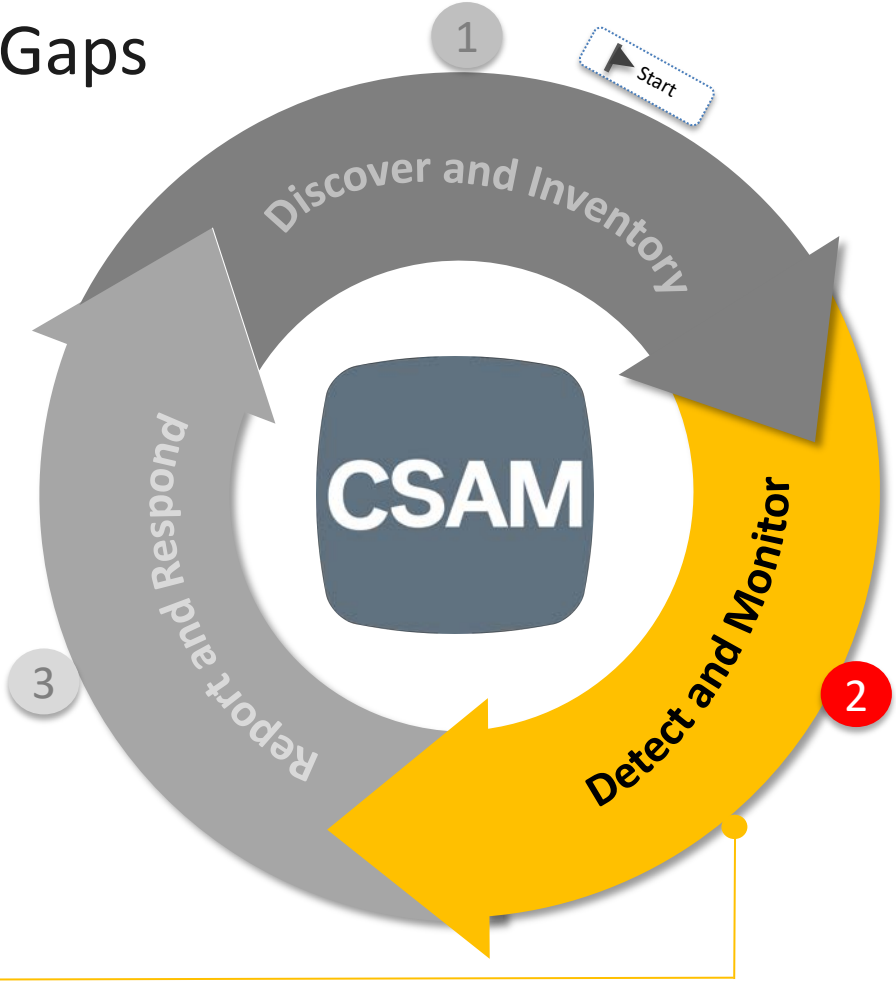
Qualys.

Detect and Monitor Security Gaps

Qualys.

Detect and Monitor Security Gaps

- **Asset Prioritization (**Define Asset Criticality Score)
- **Product Lifecycle Management*** (EOL/EOS/Obsolete hardware and software automatically identified through enrichment in QCP)
- **Software Authorization*** (configure rules to identify authorized/unauthorized software)

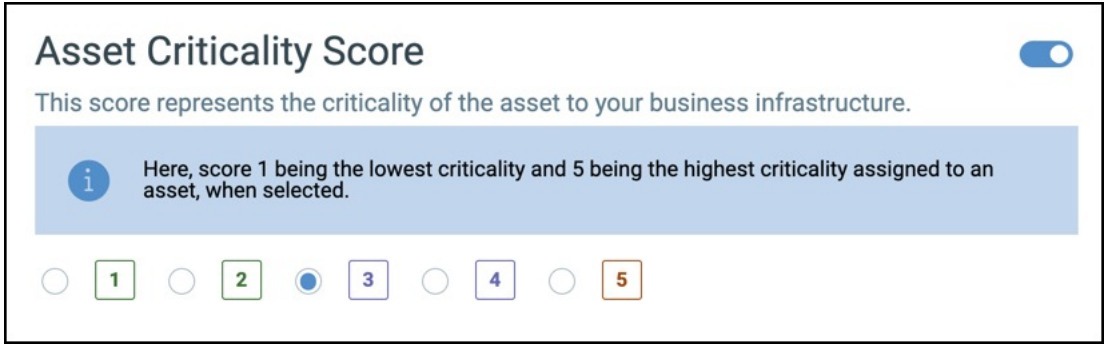


Qualys.

Asset Criticality Score

Qualys.

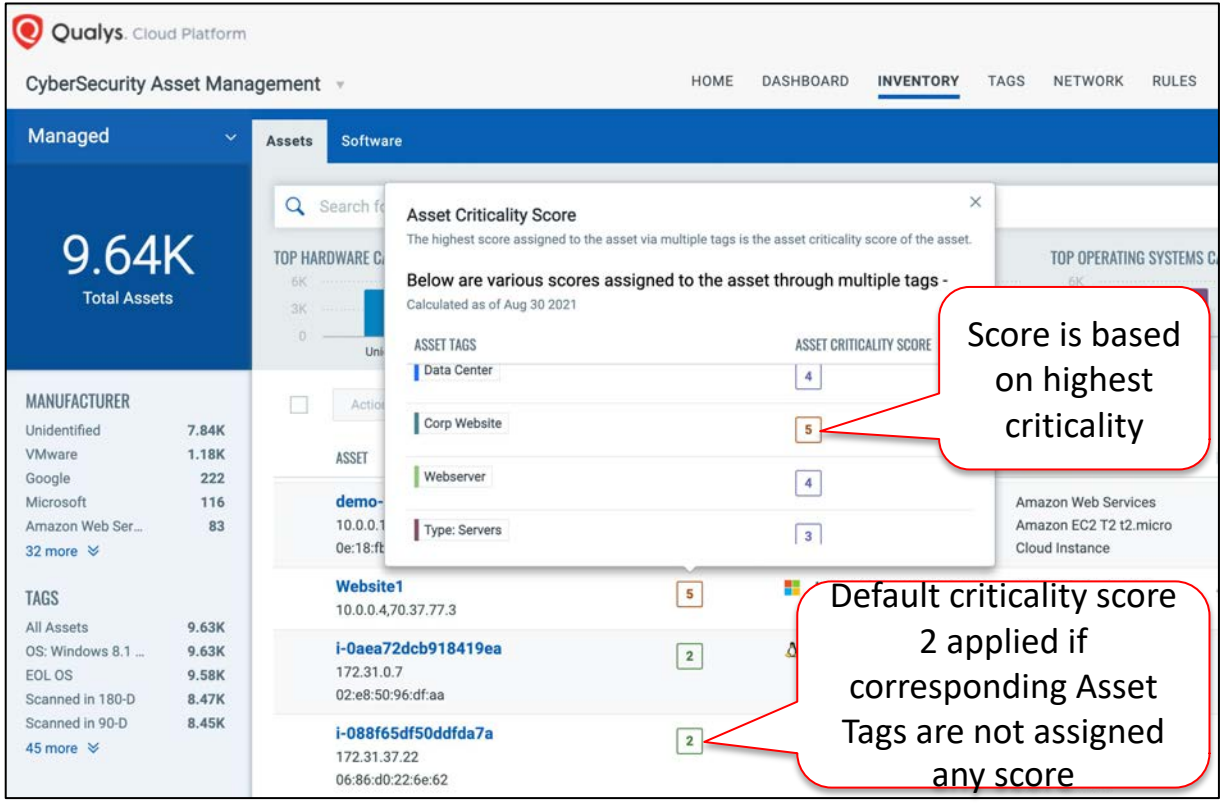
Asset Criticality Score



- User defined scores
- Configured and implemented through Asset Tags
- Scale of 1 to 5:
  - 5 = most critical
  - 1= least critical

Qualys.

Asset Criticality Score



- An asset is scored by its tag with the highest criticality.
- Assets without scored tags will receive a default score of two (2).

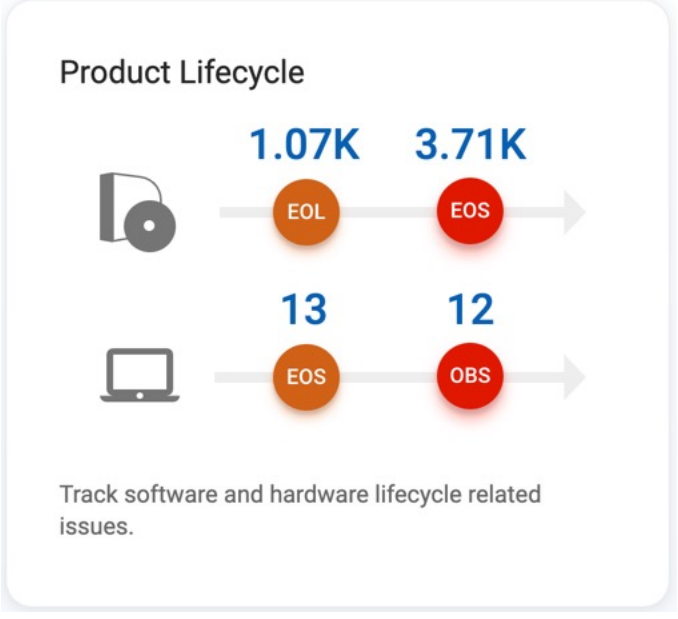
Qualys.

Product Lifecycle Management

Qualys.

Product Lifecycle Information

- Identify EOL/EOS software and hardware
- Secure your environment by eliminating unsupported software and hardware
- Plan hardware refresh and software upgrades

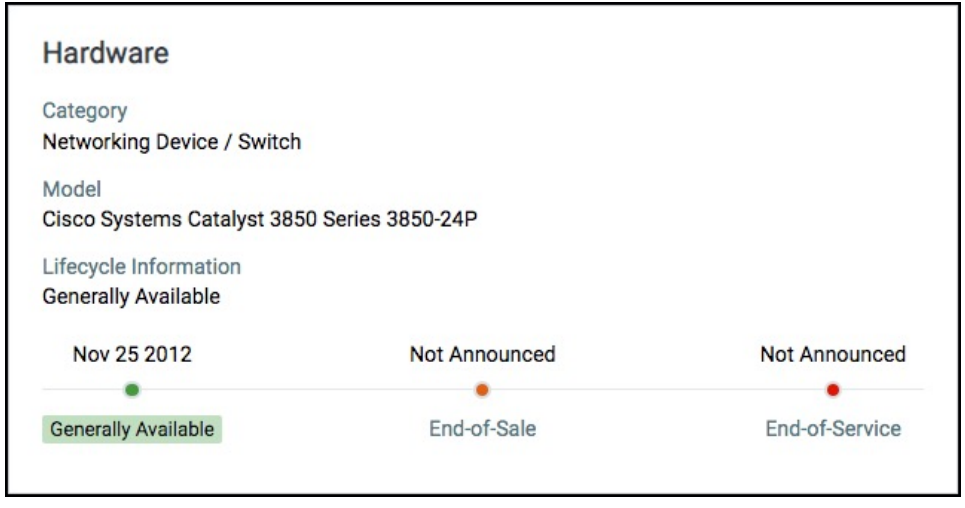


Qualys.

Hardware Lifecycle Stage

Search Token: `hardware.lifecycle.stage:`*`value`*

- **General Availability** (GA) - Hardware is in production, available for purchase, and supported
- **End of Sale** (EOS)- No longer being sold or by vendor
- **Obsolete** (OBS) - End-of-Service; no longer serviced via upgrades, patches, or maintenance



Qualys.

Hardware Lifecycle Search Tokens

Attribute	Examples	Search Token
lifecycle stage	"INTRO", "GA", "EOS", "OBS"	hardware.lifecycle.stage
Introduction date	Feb-2015	hardware.lifecycle.intro
General Availability date	Apr-21-2014	hardware.lifecycle.ga
End-of-Sale date	May-2016	hardware.lifecycle.eos
Obsolete date	Jun-2018	hardware.lifecycle.obs

- The ‘lifecycle.stage’ token is useful when searching for the present stage of an asset.
- Use the other ‘lifecycle’ tokens to search for future EOS, and OBS dates.

Qualys.

OS & Software Lifecycle Stages

Search Tokens:

`operatingSystem.lifecycle.stage:`*`value`*

`software:(lifecycle.stage:`*`value`*`)`

- **Generally Available** (GA) - When the product became available for purchase.
- **End-of-Life** (EOL) - No longer marketing, selling, building new features, or promoting product (Security patches may still be provided).
- **End-of-Service** (EOS) - No longer serviced via upgrades, patches, or maintenance.

Qualys.

OS Lifecycle Search Tokens

Attribute	Examples	Search Token
Lifecycle state	"GA", "EOL", "EOS"	operatingSystem.lifecycle.stage
Support Stage	"Premier", "Extended", "Obsolete"	
General Availability date	Feb-15-2008	operatingSystem.lifecycle.ga
End-of-Life date	Nov-23-2013	operatingSystem.lifecycle.eol
End-of-Support date	Jun-18-2015	operatingSystem.lifecycle.eos

- The ‘lifecycle.stage’ token is useful when searching for the present stage of an asset.
- Use the other ‘lifecycle’ tokens to search for future EOL and EOS dates.

Qualys.

Software Lifecycle Search Tokens

Attribute	Examples	Search Token
lifecycle stage	"Beta", "GA", "EOL", ”EOS"	software:(lifecycle.stage:
General Availability date	Apr-21-2014	software:(lifecycle.ga:
End-of-Life date	May-2016	software:(lifecycle.eol:
End-of-Support date	Jun-2018	software:(lifecycle.eos:

- The ‘lifecycle.stage’ token is useful when searching for the present stage of an asset.
- Use the other ‘lifecycle’ tokens to search for future EOL and EOS dates.

Qualys.

Lab 5 : Product Lifecycle Management

Please consult pages 23 to 24 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 23.

Qualys.

Authorized & Unauthorized Software

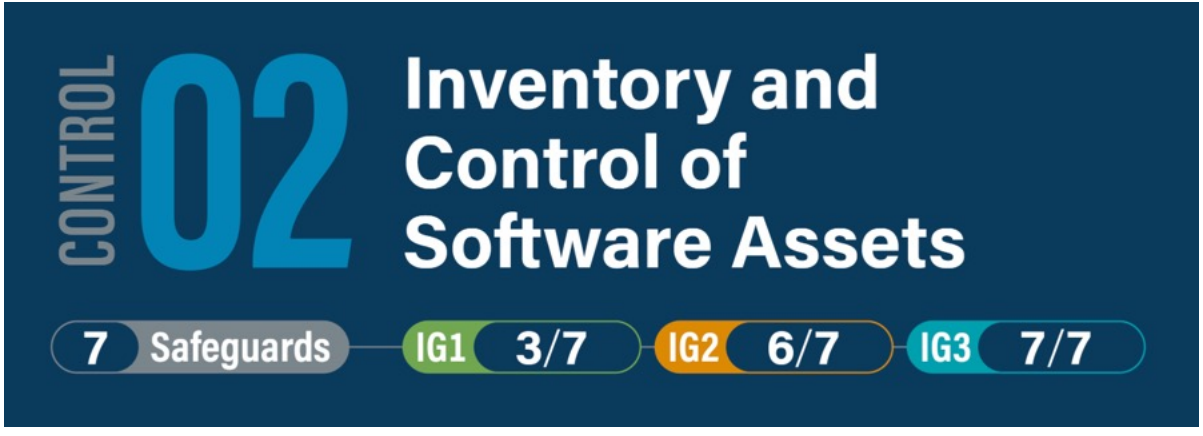
Qualys.

CIS Control 2: Inventory and Control of Software Assets

CIS Controls

Overview

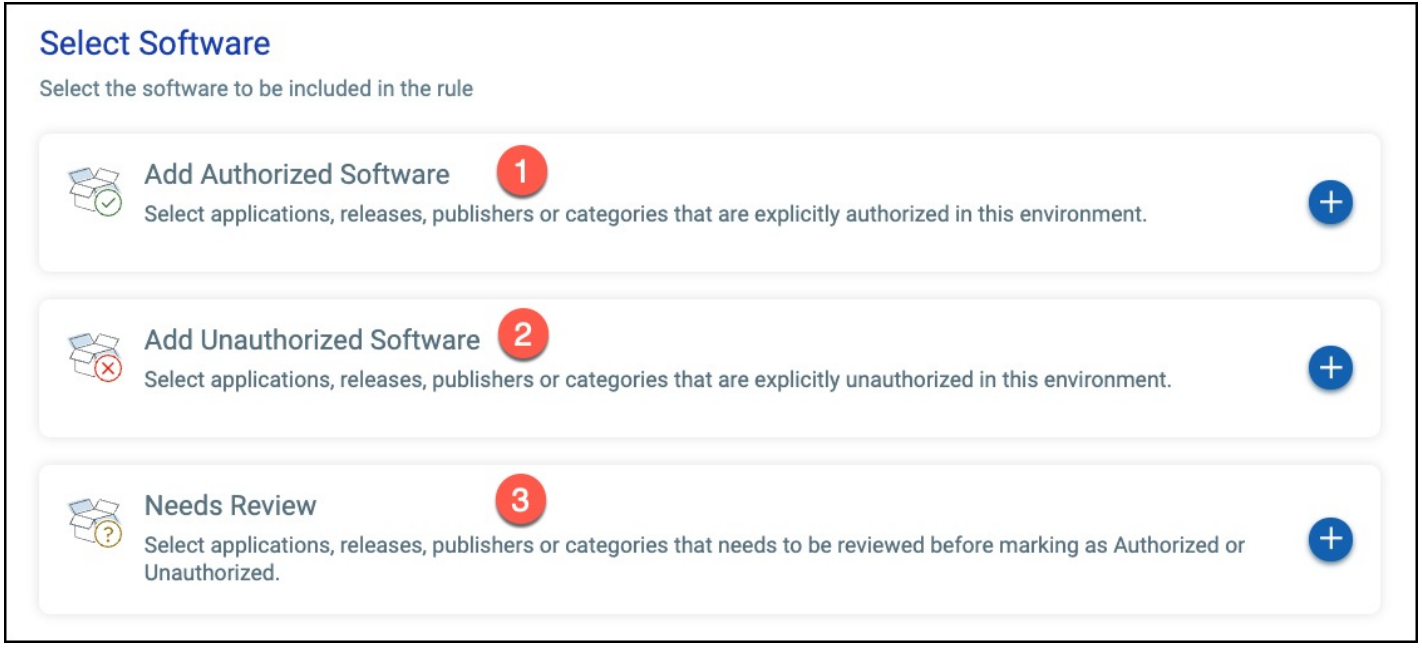
Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.



https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/

Qualys.

Software Rule Types



- Create rules for authorized/unauthorized software and software that needs to be reviewed.

Qualys.

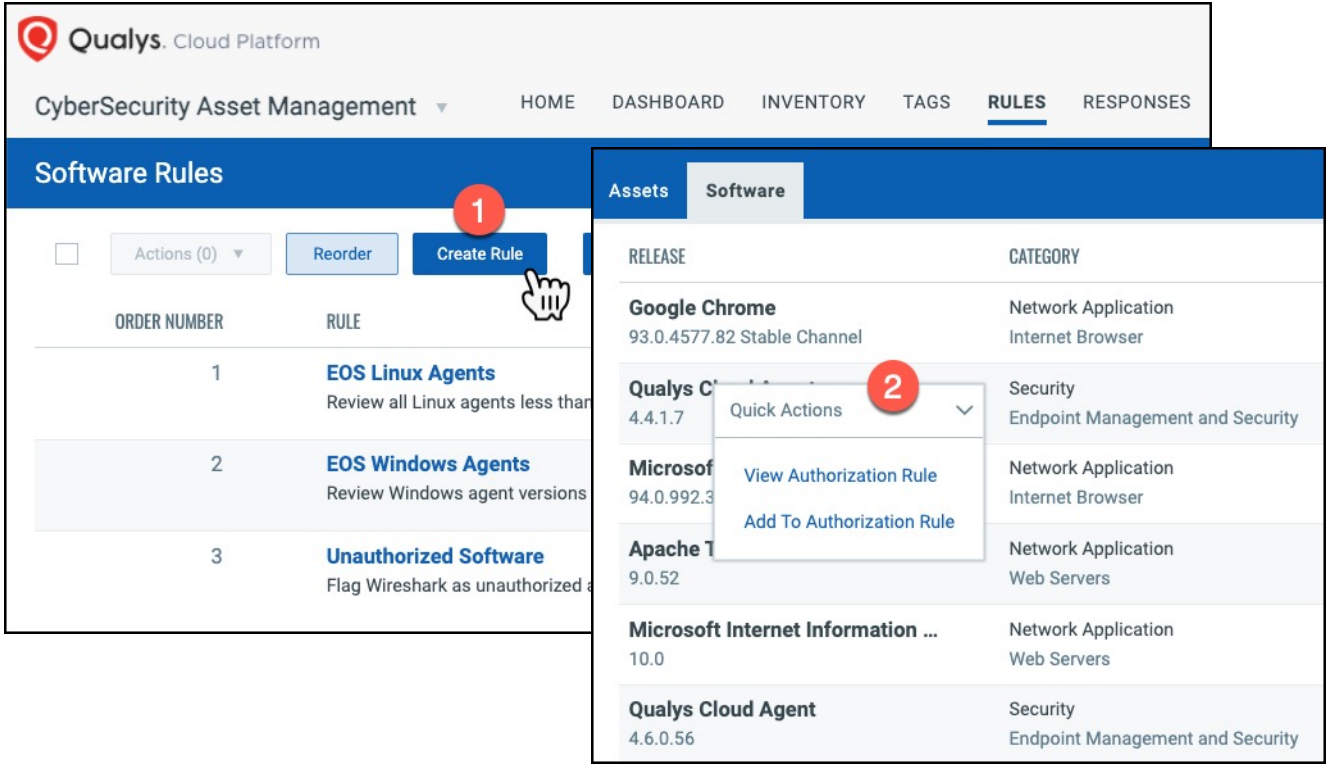
Lab 6: Software Authorization

Please consult pages 25 - 27 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 25.

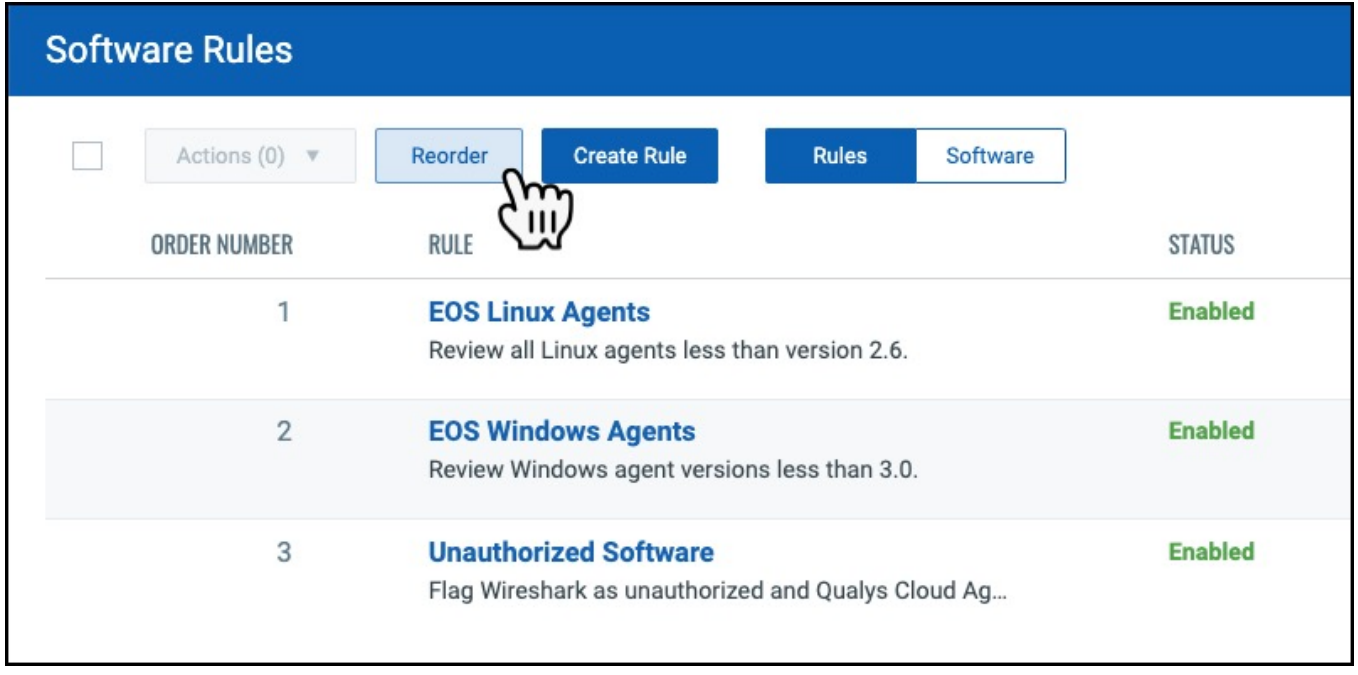
Qualys.

Create Software Rules



- View, create and modify rules from the RULES section or the “Software” tab under the INVENTORY section.

Rule Precedence

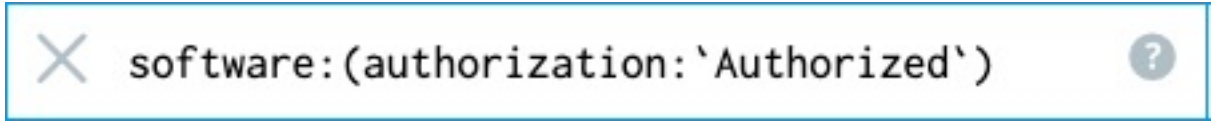


- Rules at the top of the list have precedence over the rules below.
- Click the “Reorder” button to move rules higher or lower.

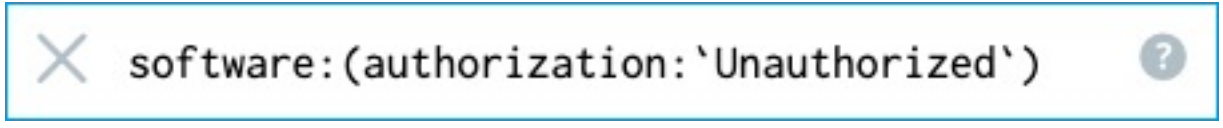
Qualys.

Software Authorization Tokens

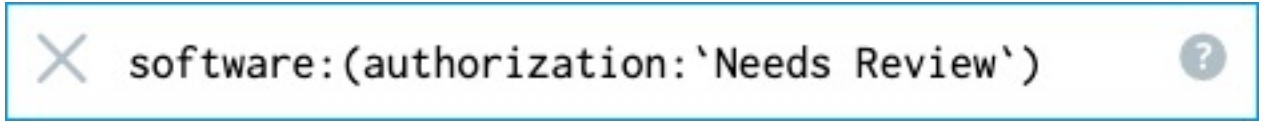
- **AUTHORIZED**



- **UNAUTHORIZED**



- **NEEDS REVIEW**



- After creating software authorization rules, software authorization tokens can be used to search and query.

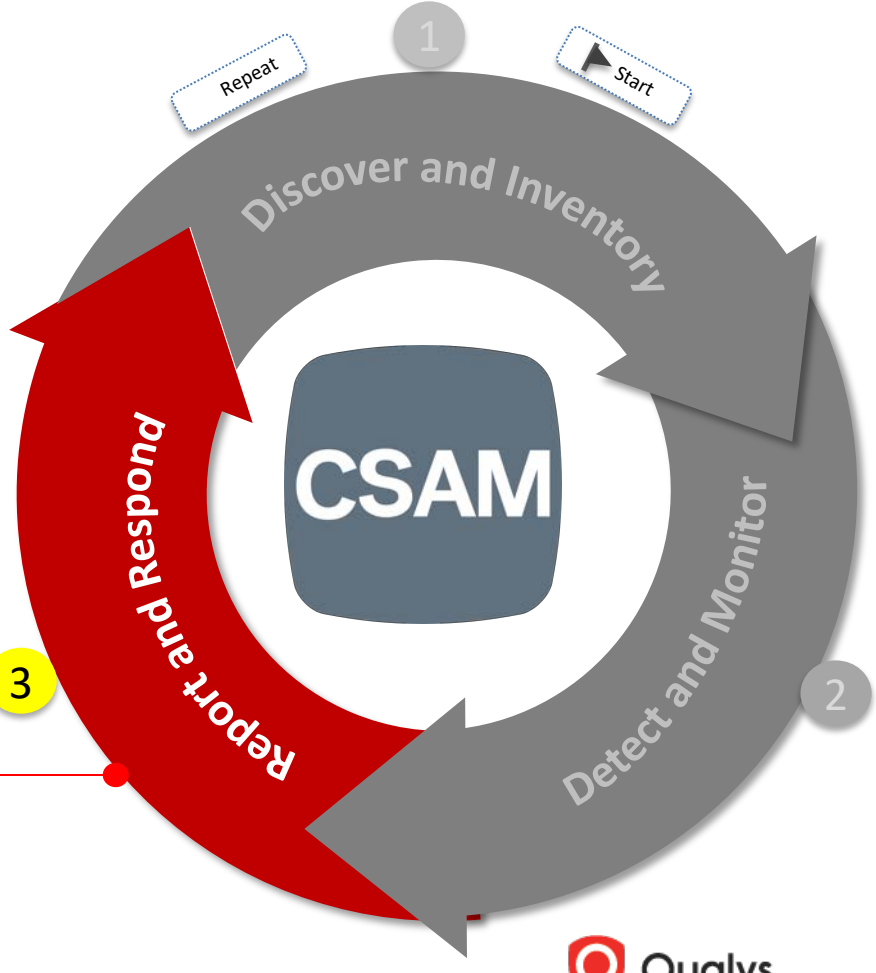
Qualys.

Report & Respond

Qualys.

Report and Respond

- **Visualize Data** (use dashboards to identify at risk assets)
- **Reports** (configure reports for IT and compliance requirements)*
- **Configure Rule-Based Alerts** (define criteria for alert notifications)*

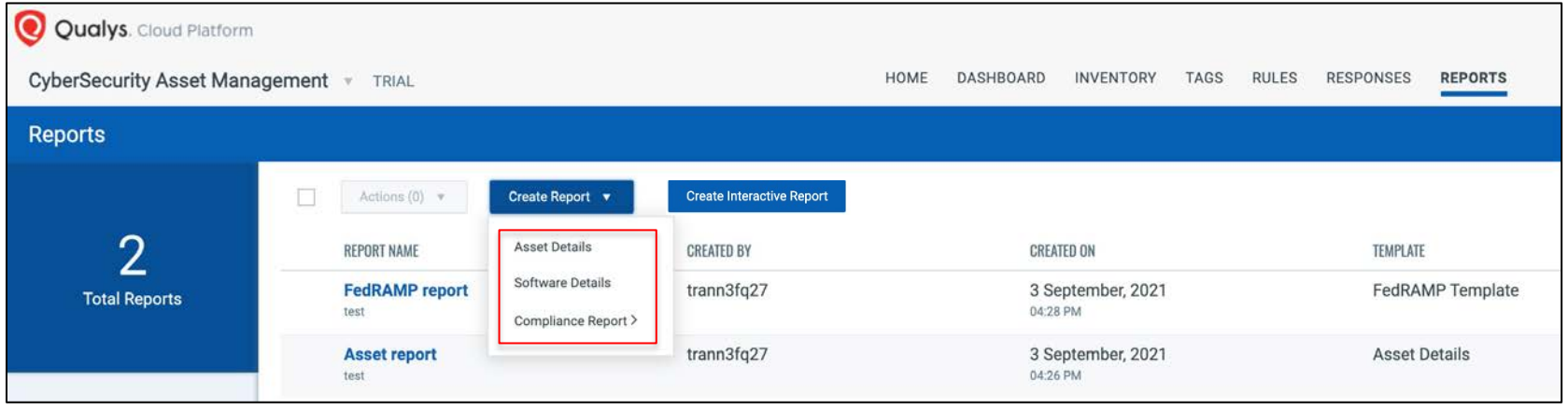


Qualys.

Reports

Qualys.

Asset, Software and Compliance Reports



- Custom Reports (.csv file format)
  - Asset Details *(host information)*
  - Software Details *(host and software information)*
  - FedRAMP Compliance *(host and software information as required by RedRAMP)*

Qualys.

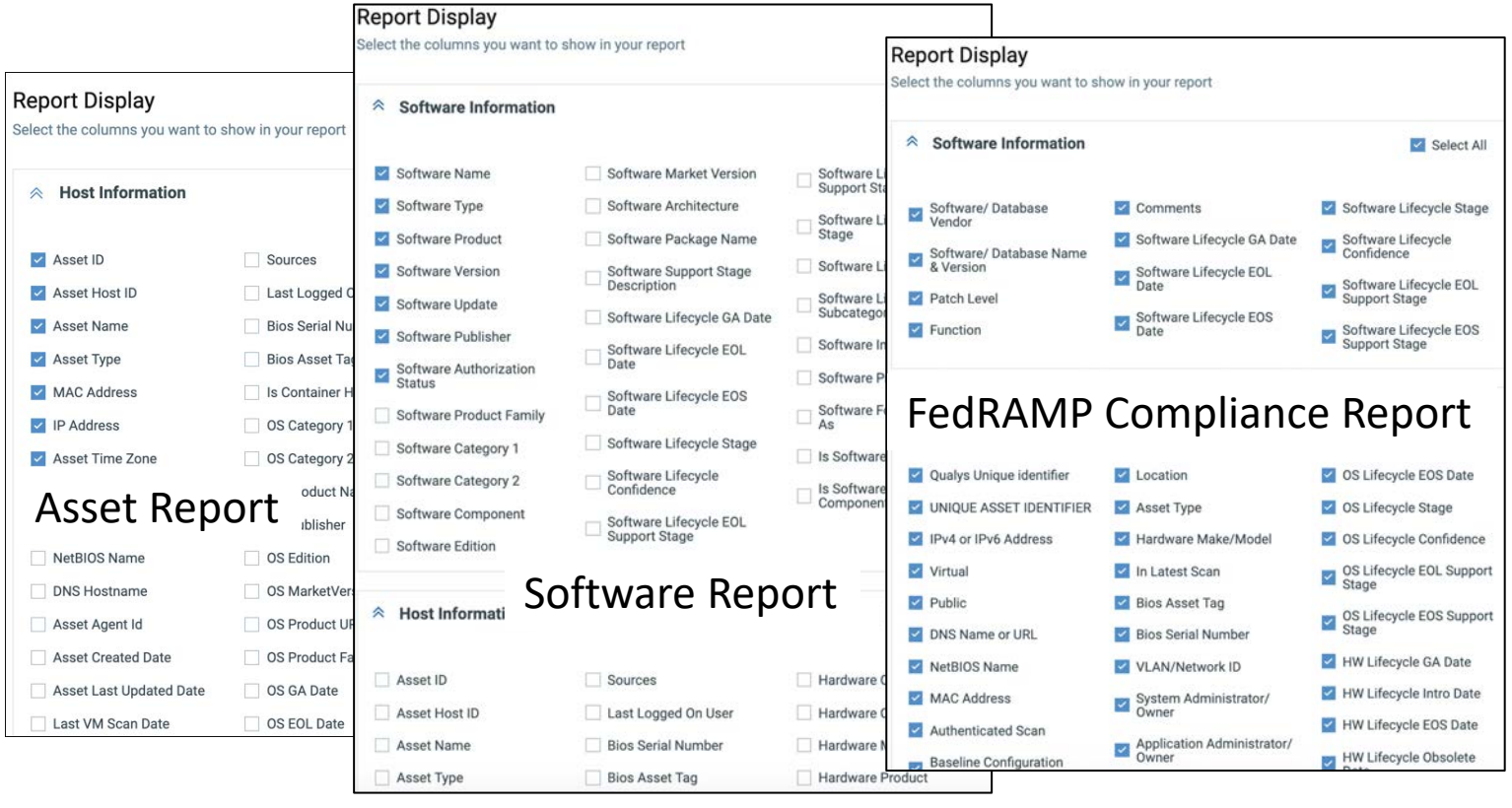
Lab 7 : Asset, Software, and Compliance Reports

Please consult pages 28 to 30 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 28.

Qualys.

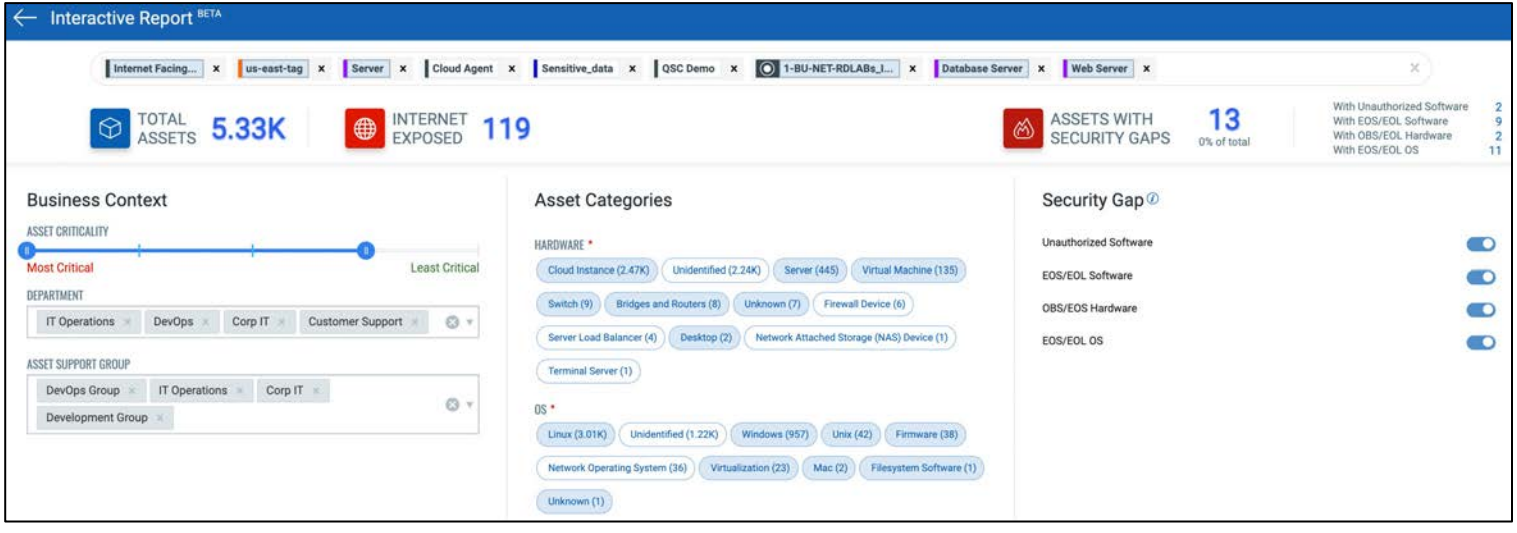
Display Options



Selected attributes will be column headers in the report

Qualys.

Interactive Report



- Includes an interactive workflow to identify and list issues and security gaps (obsolete hardware, EOL/EOS software, unauthorized software, etc.).

Qualys.

Lab 8 : Interactive Reports

Please consult pages 31 to 33 in the lab tutorial supplement for details.

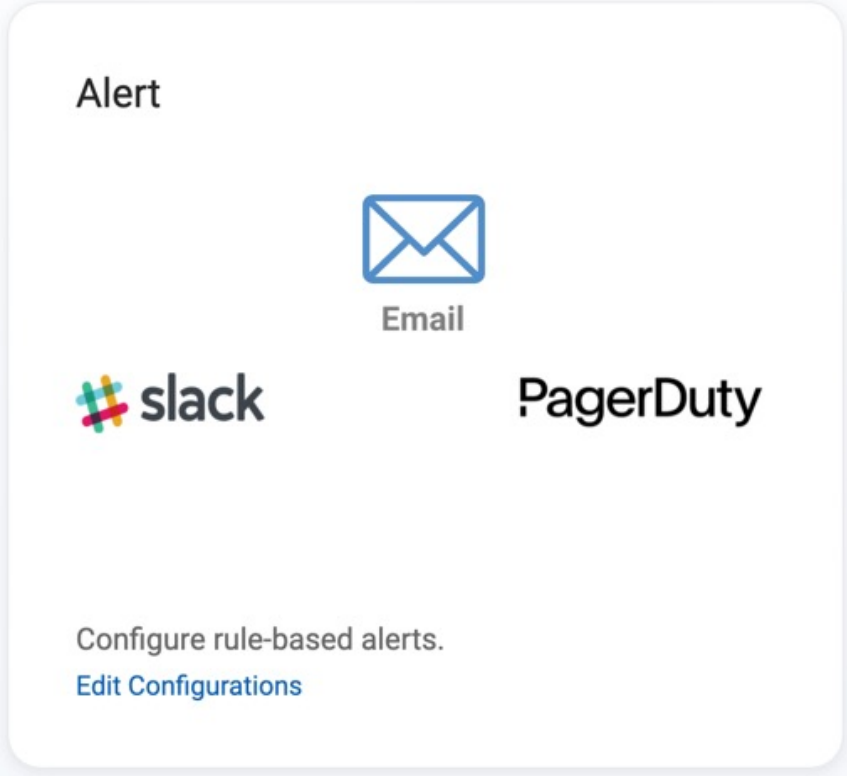
PLAY Tutorial begins on page 31.

Qualys.

Rule-Based Alerts

Qualys.

Alert Actions



- Receive alert notifications via Email, Slack, and PagerDuty.
- Alert Rules are evaluated when host inventory is updated.
- One or more actions must be defined prior to creating Alert Rules.

Qualys.

Lab 9 : Rule-Based Alerts

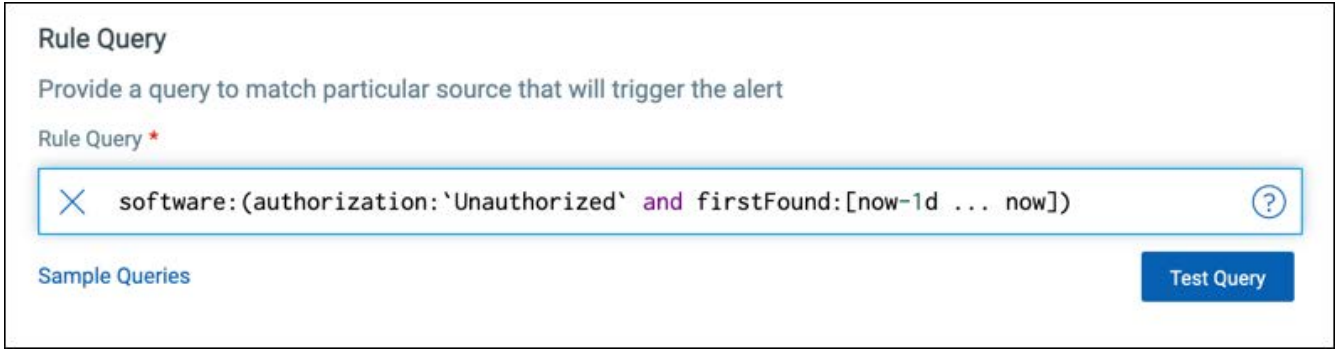
Please consult pages 34 to 37 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 34.

Qualys.

Rule Query

- The Rule Query specifies the criteria for triggering an alert action.



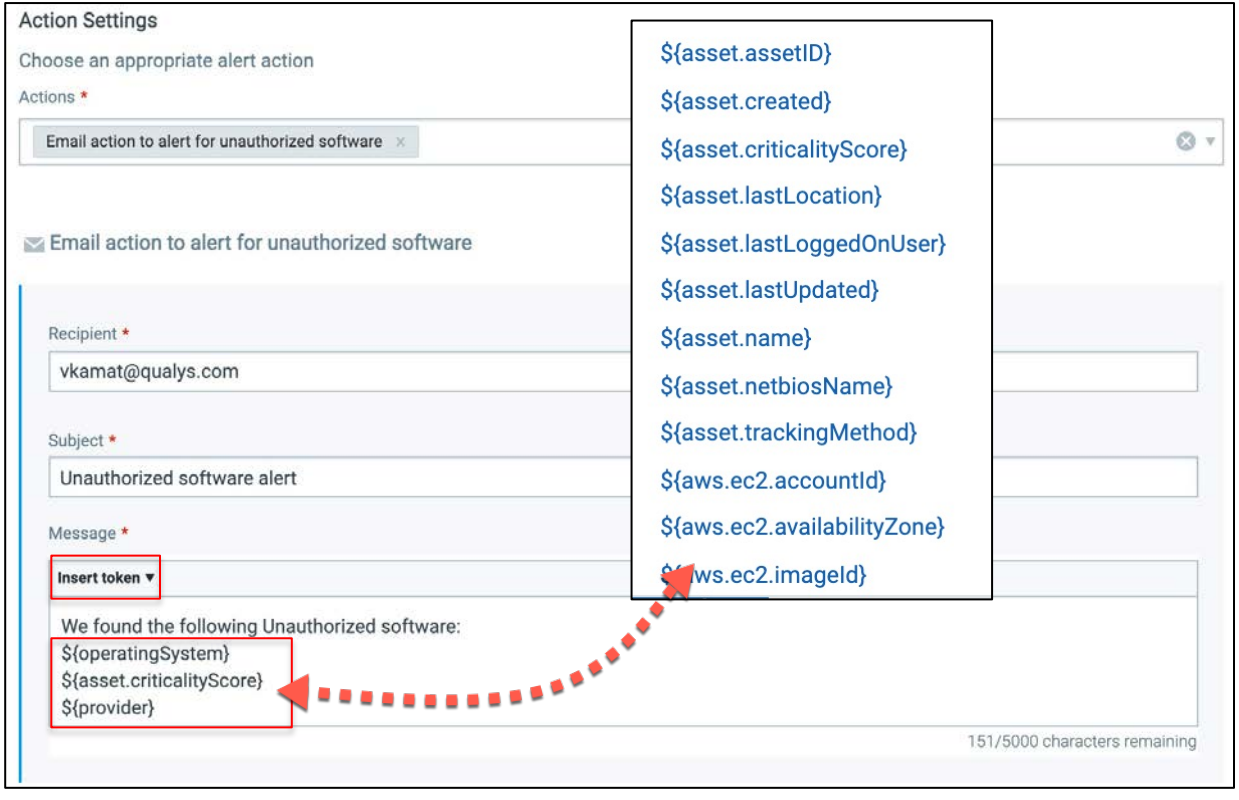
- Sample queries are provided to get you started.
- Immediately notify your operational teams when critical or suspicious events are monitored:
  - Unauthorized software discovered
  - Assets reaching EOS dates
  - Insufficient storage space on host
  - Malicious software discovered
  - and more...

Qualys.

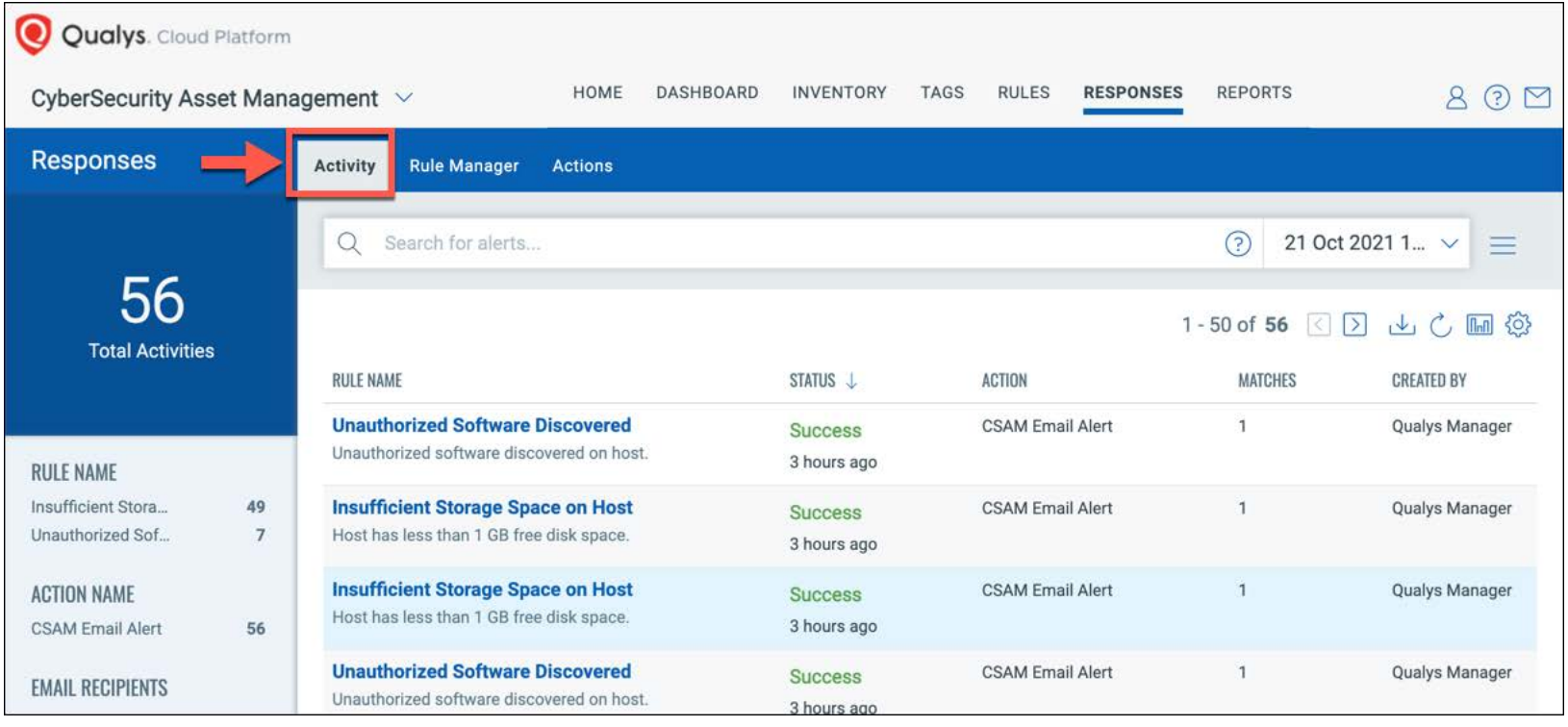
Insert Tokens

Insert tokens into the message body to include useful asset information and details in the alert:

- Asset Criticality Score
- Last Logged On User
- AWS, Azure, and GCP metadata
- Hardware and OS categories
- and more...



Alert Activity



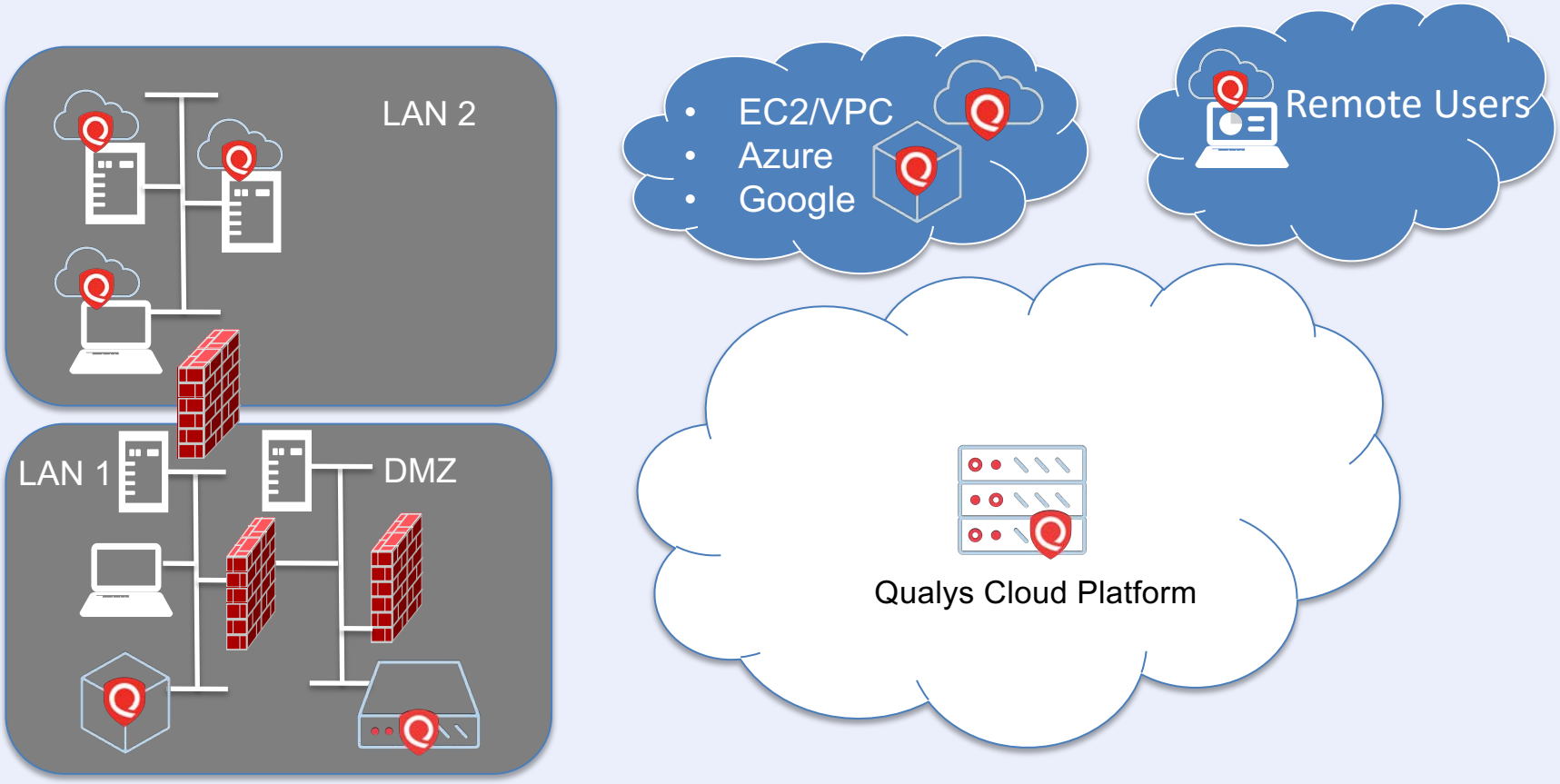
- Monitor alert activity under the “Activity” tab.

Qualys.

Vulnerability Management

Qualys.

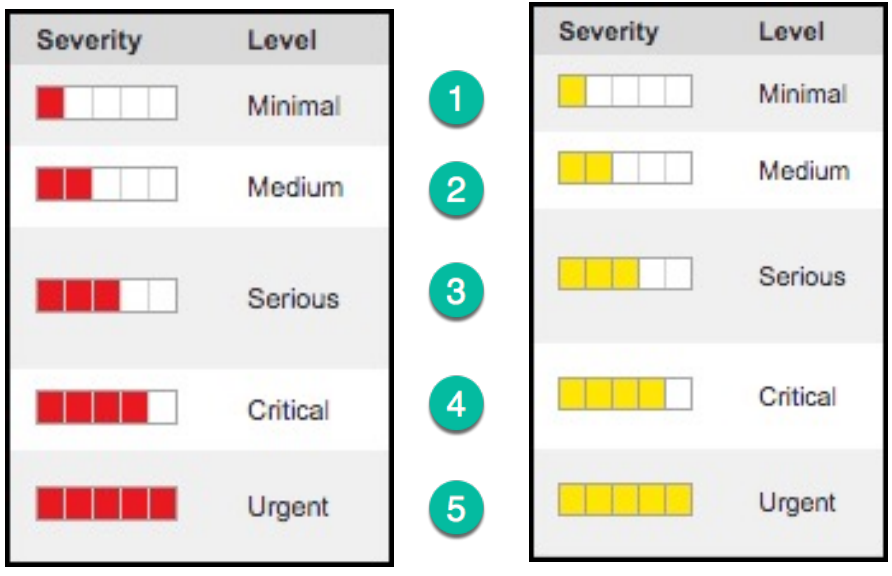
VM Sensors



Qualys.

Vulnerability Findings

- Industry-leading vulnerability KnowledgeBase with tens-of-thousands of vulnerability signatures.
- Each vulnerability is ranked and associated with:
  - Qualys Severity Level
  - CVSS Score
  - CVE & Bugtraq IDs
  - Available Patches
  - Known Threats
  - Associated Malware
  - and more...



- An unlimited number of ways to identify, prioritize, and patch vulnerabilities.

Qualys.

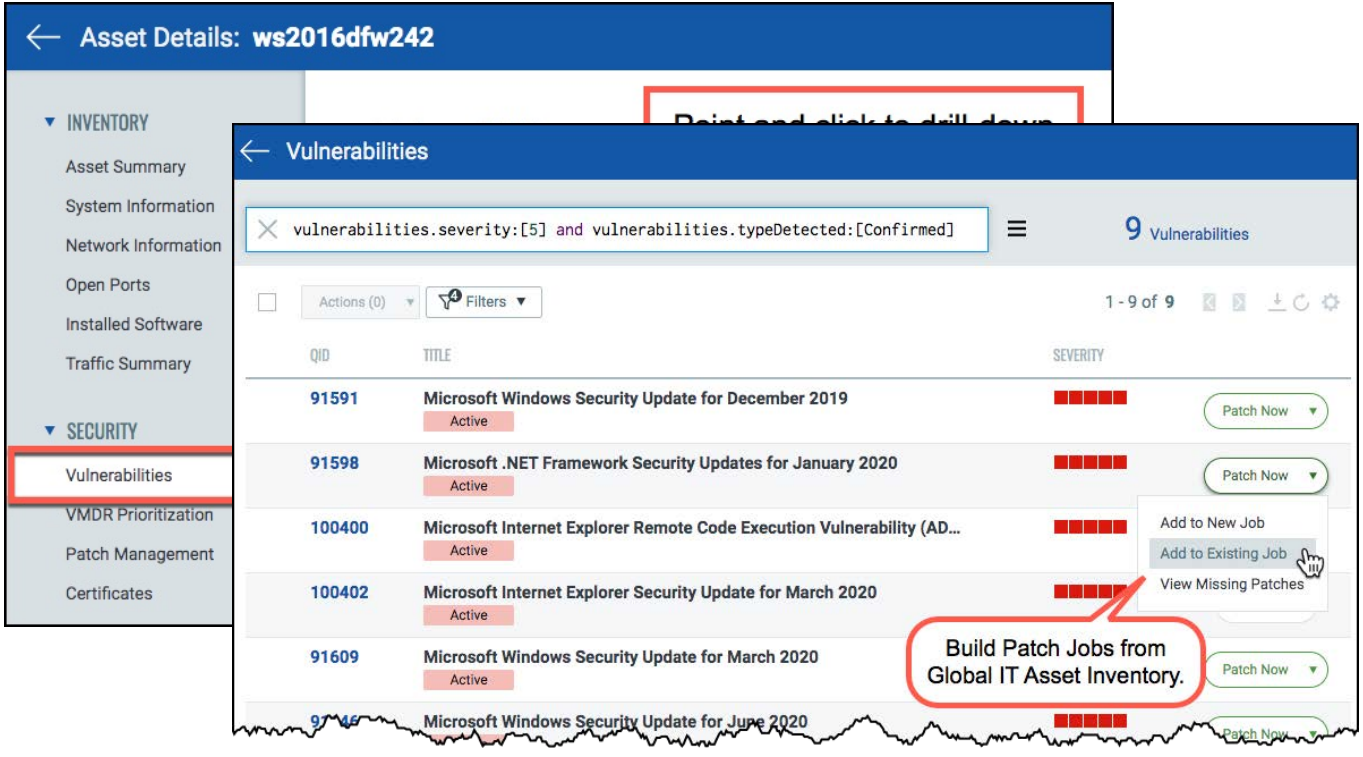
Lab 10 : Vulnerability Findings

Please consult pages 38 to 40 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 39.

Qualys.

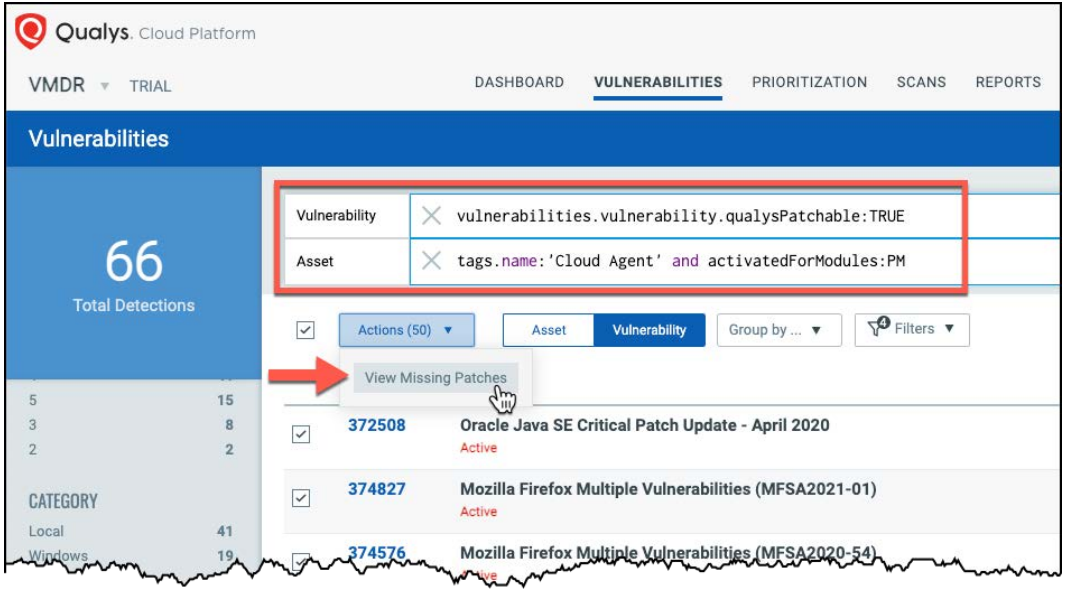
Vulnerability Findings In CSAM



- View and patch vulnerability findings from within CyberSecurity Asset Management (on a per asset basis).

Qualys.

Vulnerability Findings in VMDR



Which ones are patchable?

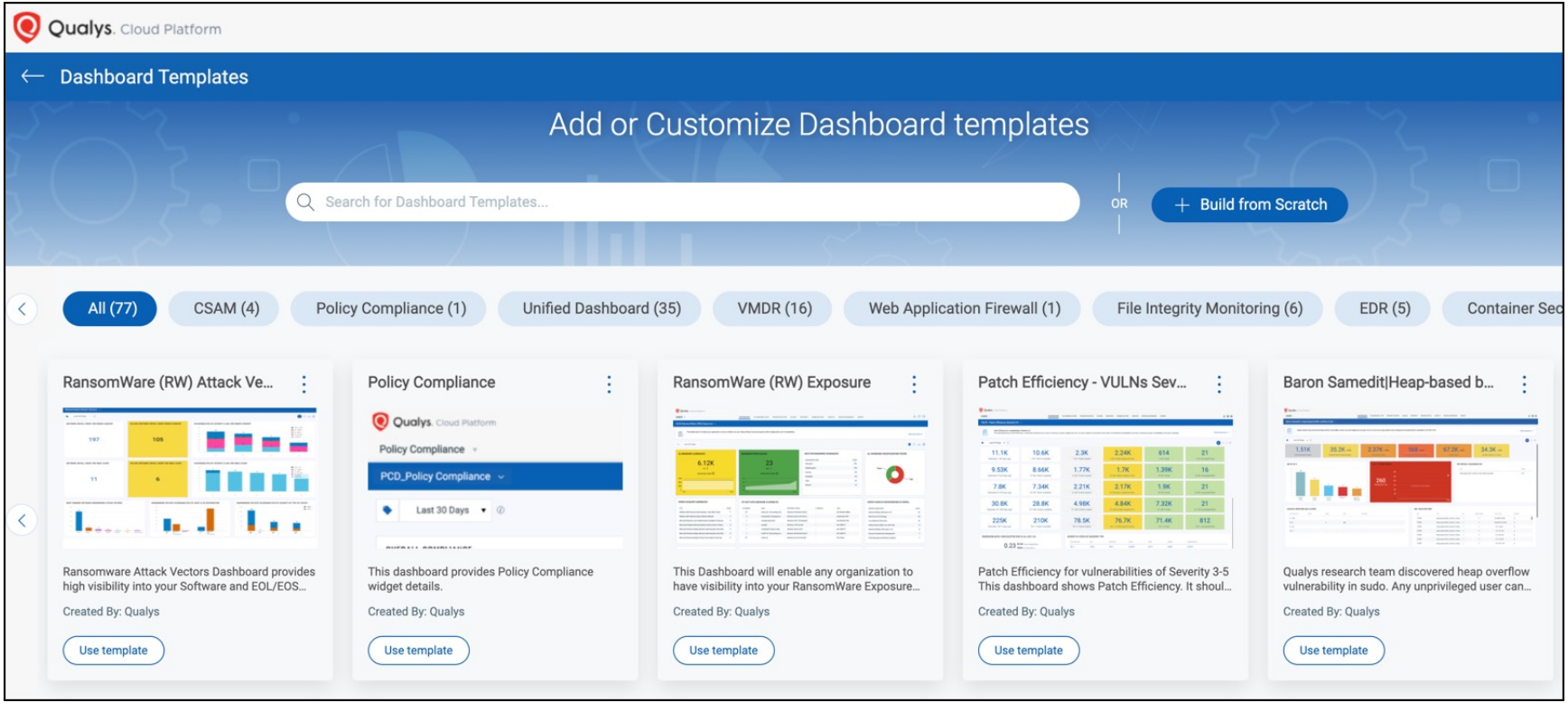
1. Detected vulnerabilities must be associated with one or more patches found in the Qualys Patch Catalog
2. Detection Host must be running the Qualys Cloud Agent
3. Cloud Agent must have the PM module activated

Qualys.

Dashboards & Widgets

Qualys.

Out-of-Box Dashboard Templates



Qualys.

Widget Types

Dashboard widgets can be designed to display query results as counts, tables, columns, or pie charts.

Qualys.

Lab 11 : Dashboards & Widgets

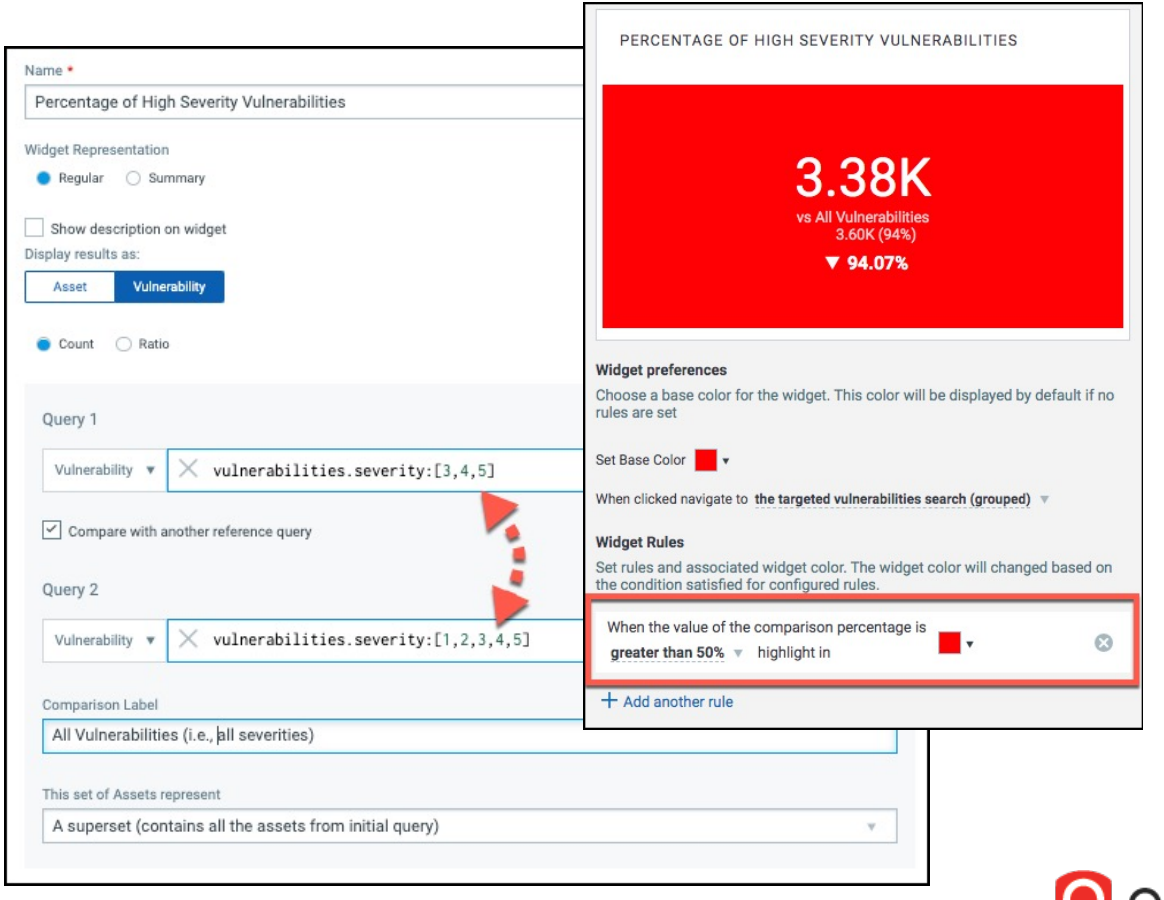
Please consult pages 41 to 44 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 41.

Qualys.

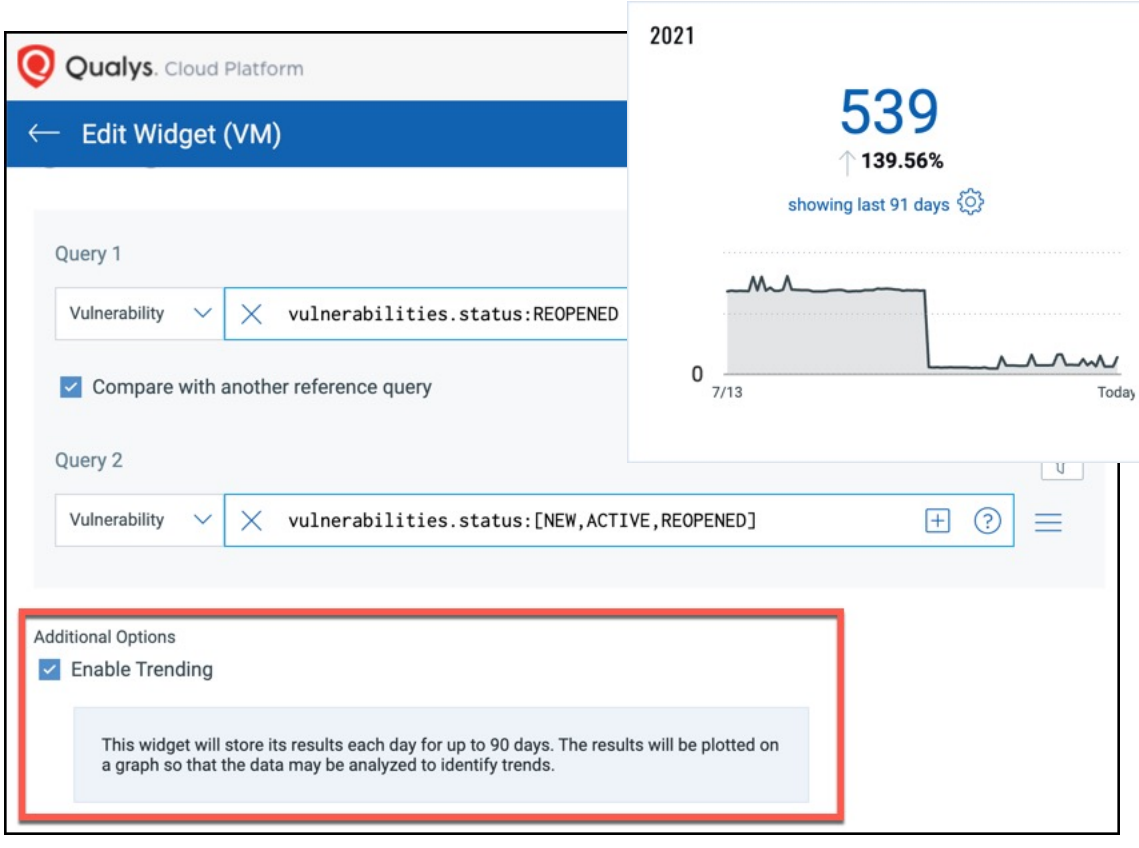
Count Widget

- The “Count Widget” can be configured to automatically change color, when specific conditions or thresholds are met.



Qualys.

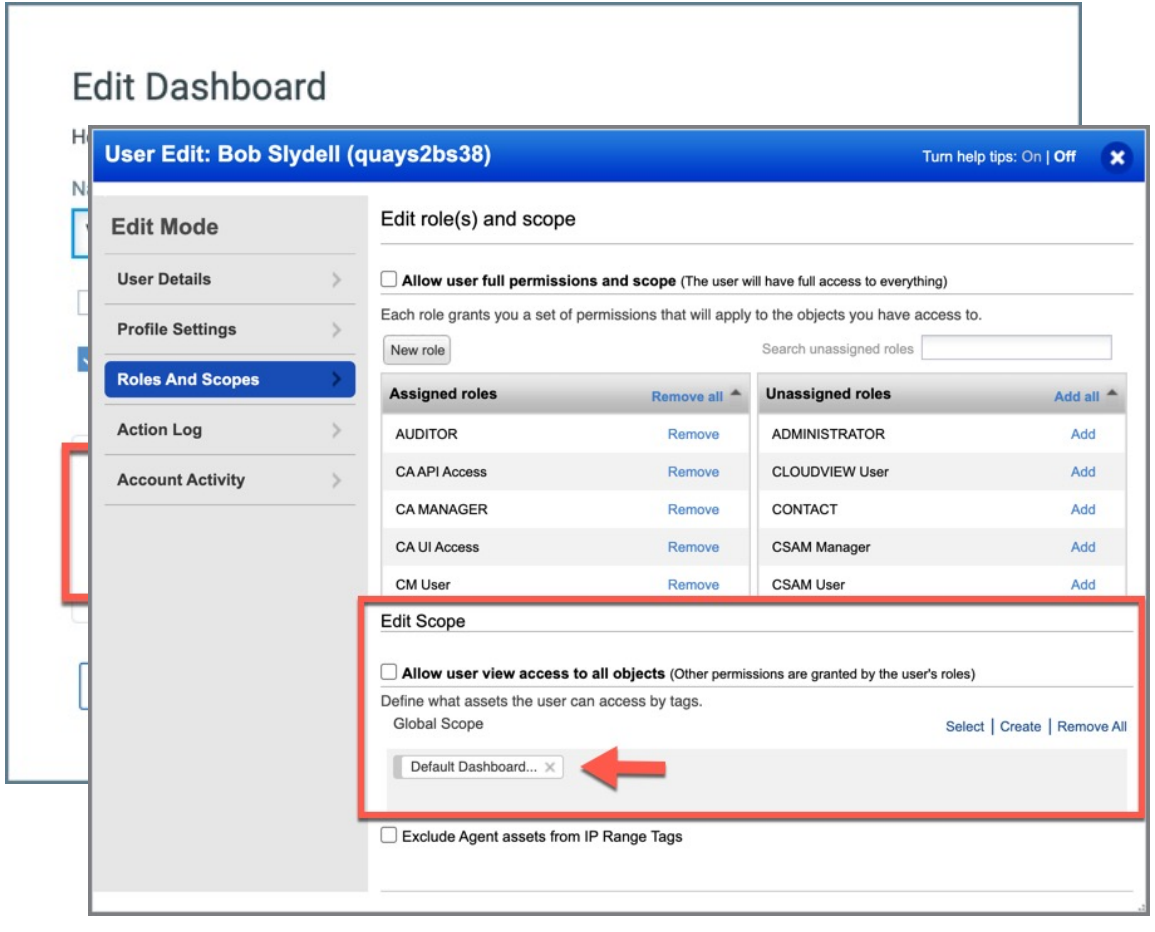
Enable Trending in Widgets



- Visualize changes or swings in momentum or progress.
- When enabled, widgets can store trend data for up to 90 days.
- Trend lines plotted on a graph are added to the widget.

Qualys.

Dashboard Tags



- Add one or more Asset Tags through the Dashboard Editor.
- The “Default Dashboard Access Tag” is created by Qualys.

Default Dashboard Access Tag

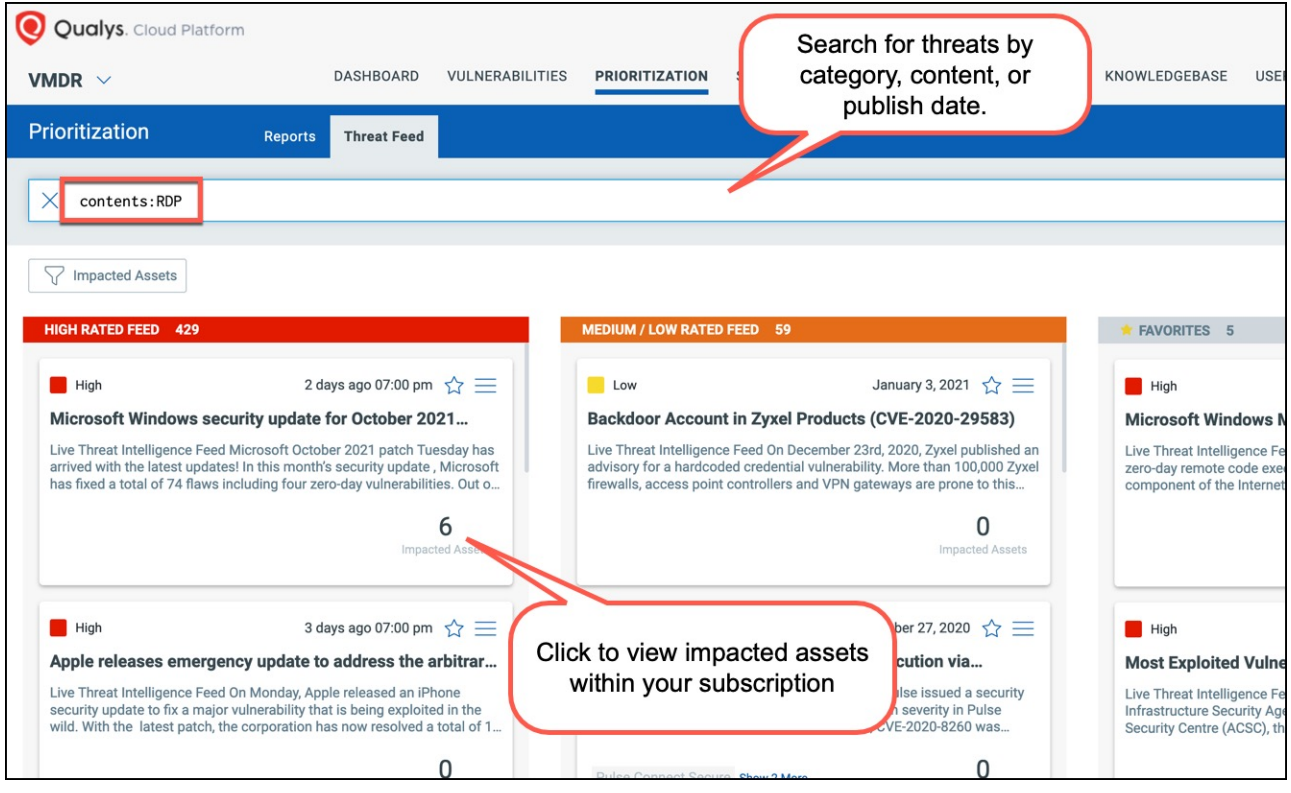
- Share dashboards with other Qualys users by assigning “dashboard” tag(s) to their accounts.

Qualys.

Threat Detection & Prioritization

Qualys.

VMDR Threat Feed



Search for threats by content, category or publish date and click to view impacted assets.

Qualys.

Threat Feed Sources

Exploit Sources

Source Type	Data Type
Core Security	PoC Exploits mapped to CVEs
Exploit-DB	PoC Exploits mapped to CVEs
Metasploit	PoC Exploits mapped to CVEs
Contagio Dump	Exploit Kits mapped to CVEs
Immunity - Agora - Dsquare - Enable Security - White Phosporus	PoC Exploits mapped to CVEs
Google Project Zero	Zero-Days mapped to CVEs

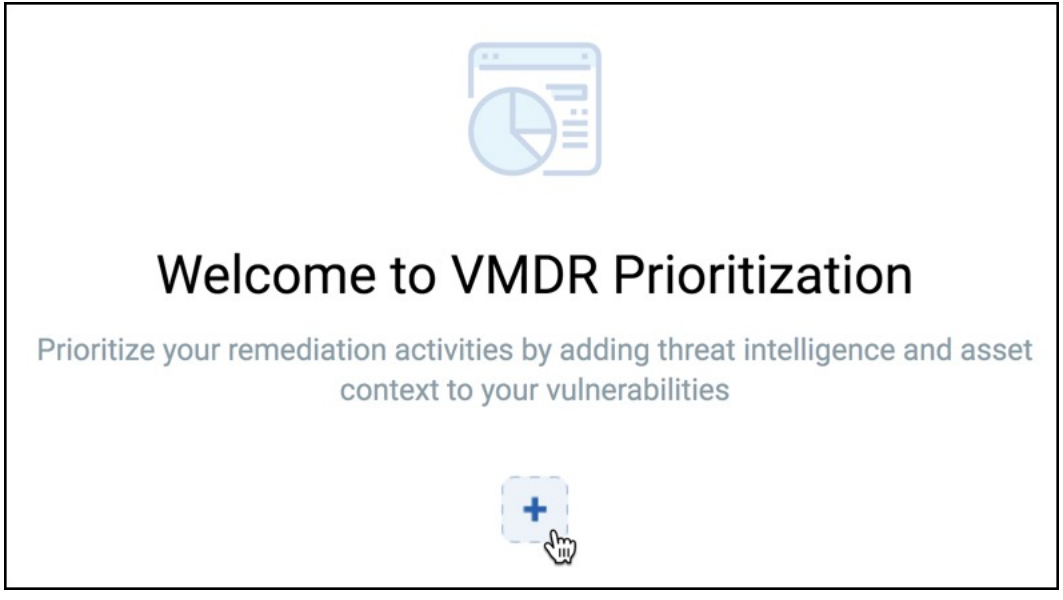
Malware Sources

Source Type	Data Type
Reversing Labs	CVEs associated with malware
Trend Micro	Malware names associated with CVEs
McAfee	Ransomware mapped to CVEs

- The Qualys Threat and Malware research team leverages exploit and malware data from multiple sources.

Qualys.

VMDR Prioritization Report



Prioritize vulnerabilities by:

- Asset Context
- Vulnerability Age
- Threat Intelligence
- Attack Surface

Qualys.

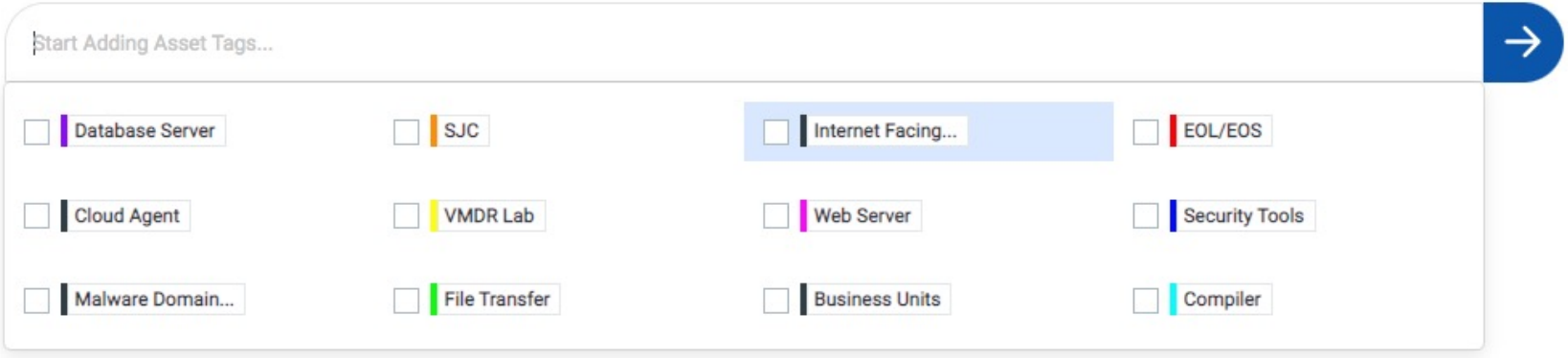
Lab 12: VMDR Prioritization Report

Please consult pages 46 to 51 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 46.

Qualys.

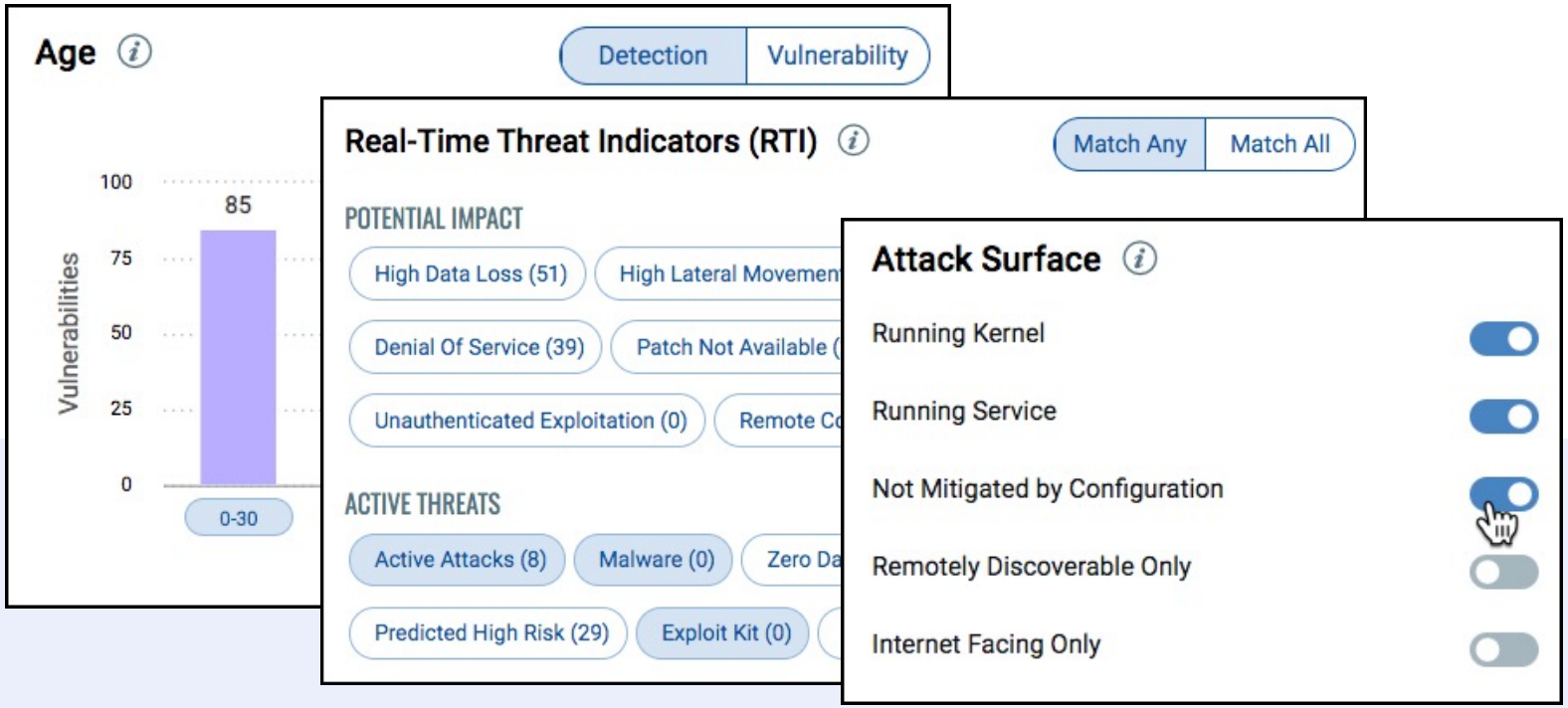
Asset Tags Add Context



- Design and build Asset Tags that help to distinguish the “context” of your assets.
- Leverage tags that use the “Asset Inventory” rule engine, along with 1) hardware, 2) software, and 3) OS categories.

Qualys.

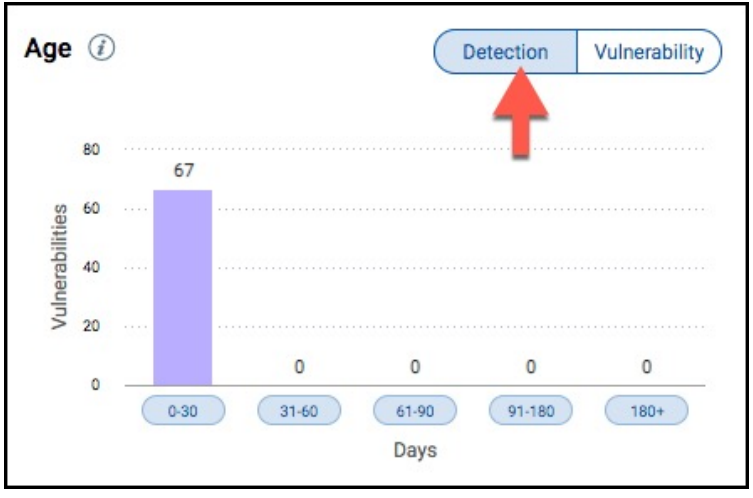
Priority Options

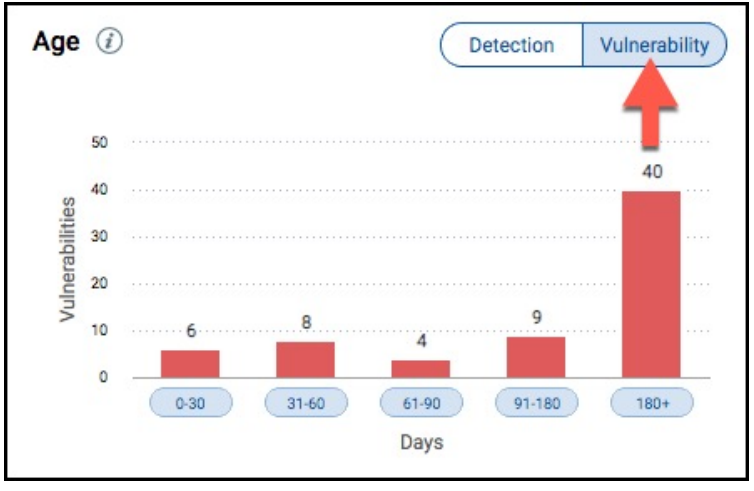


Prioritize discovered vulnerabilities by Age, RTIs, and Attack Surface.

Qualys.

Age

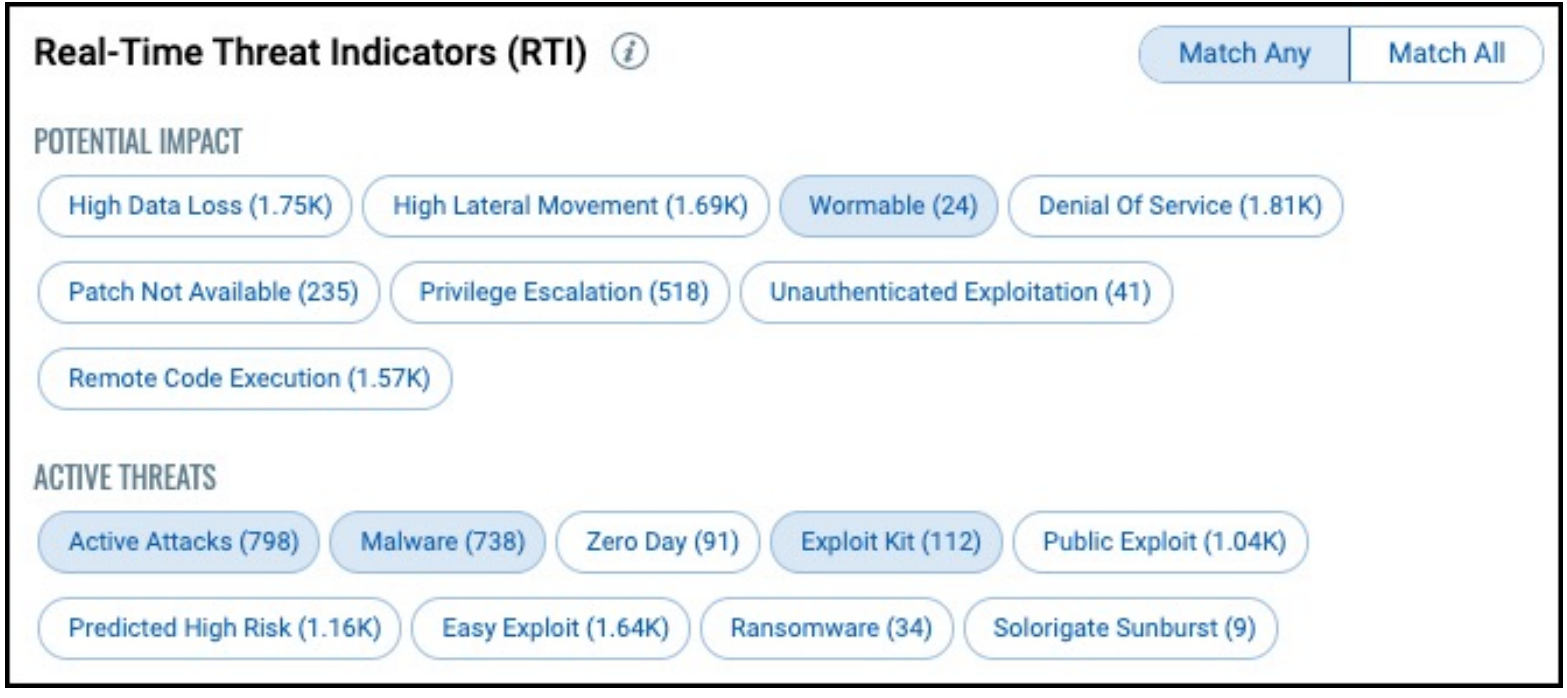




- **Detection Age** – reflects the number of days since you first detected the vulnerability (e.g., by Qualys scanner or Cloud Agent).
- **Vulnerability Age** – (i.e., real age) reflects the number days since Qualys published the vulnerability to our KnowledgeBase.

Qualys.

Real-Time Threat Indicators (RTI)



- Provided by VMDR Threat Feed.

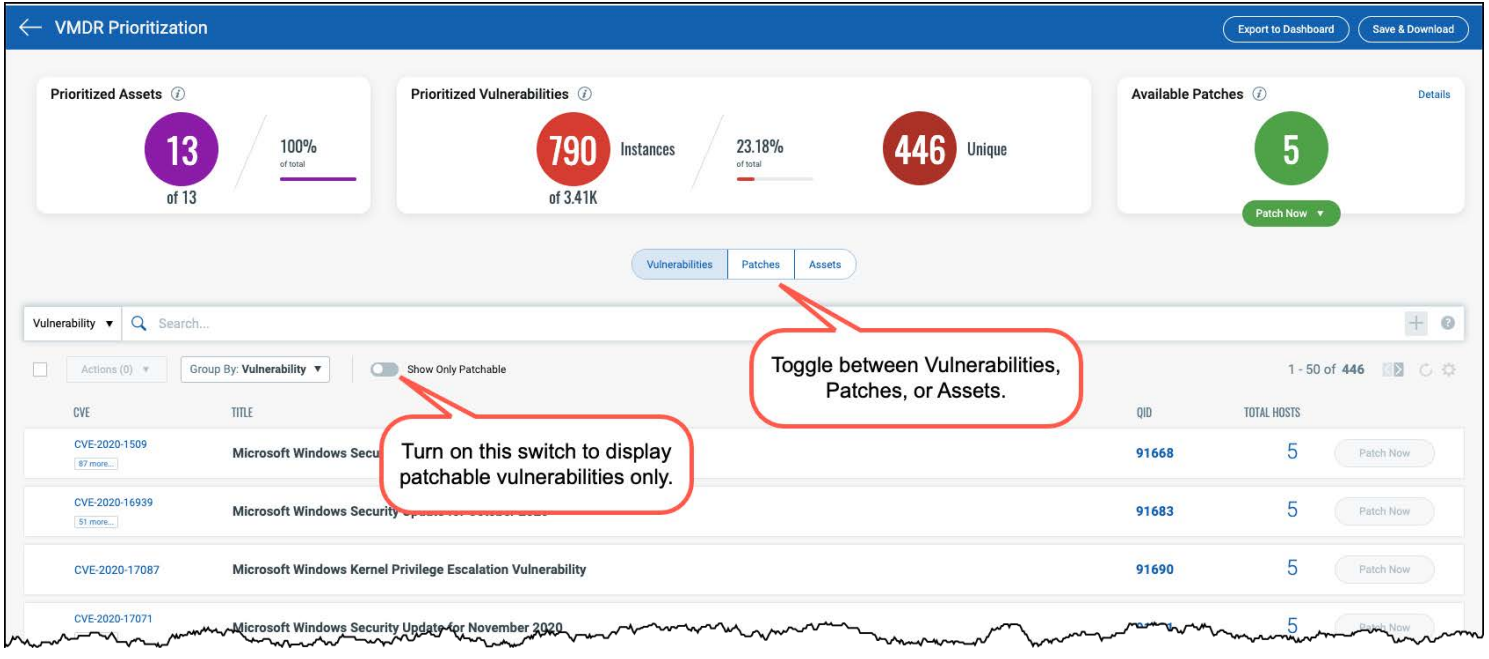
Qualys.

Attack Surface

Continue to define asset context with “Attack Surface” options.

Qualys.

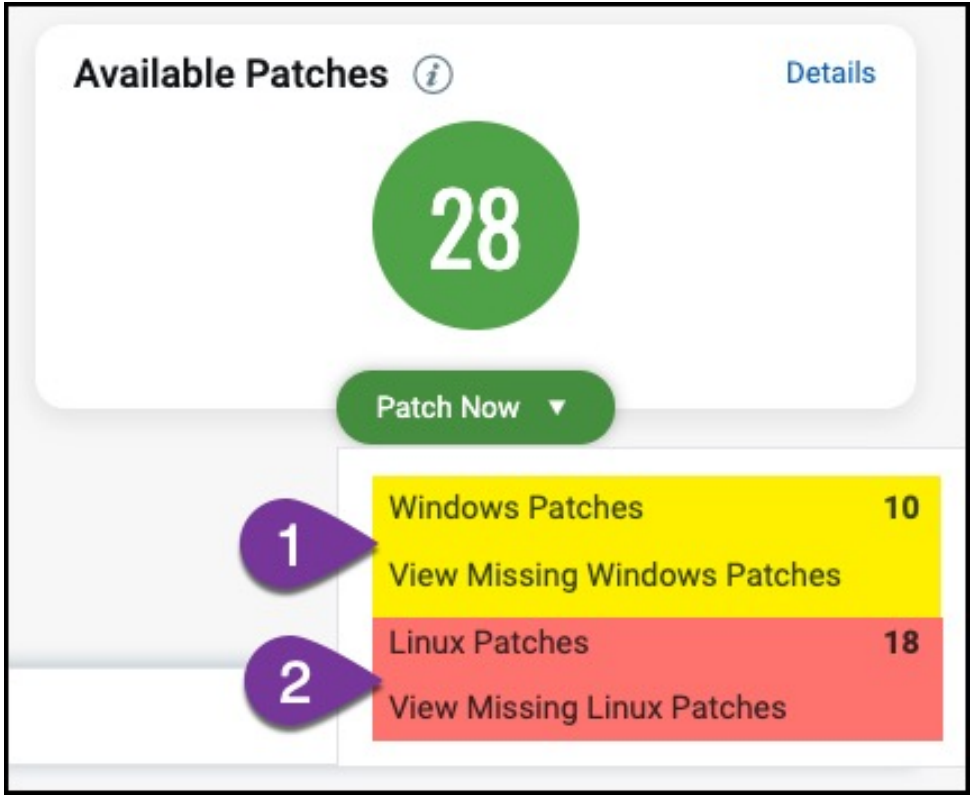
Deploy Priority Patches



Patchable assets have Cloud Agent installed and Patch Management activated.

Qualys.

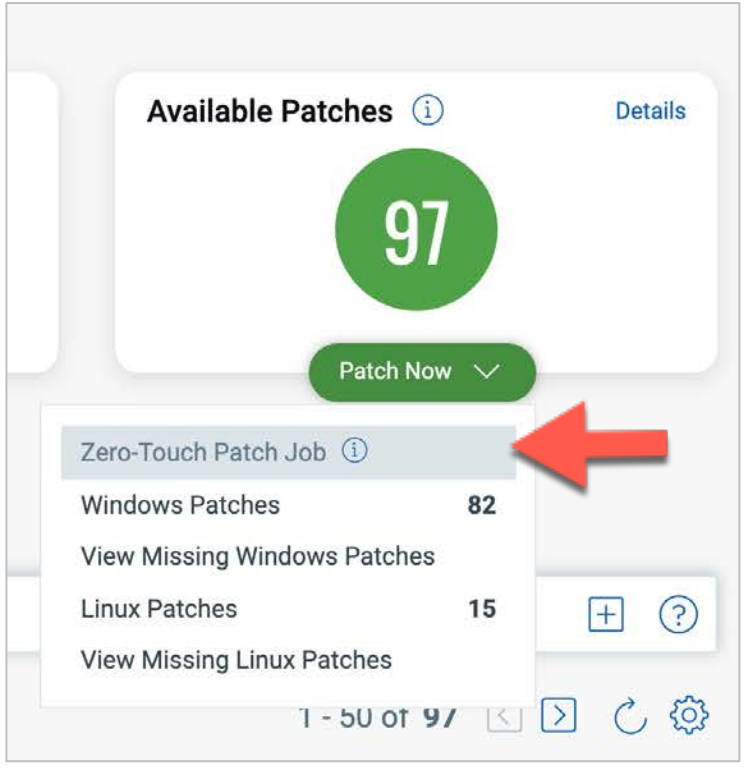
Windows & Linux Patches



1. Available patches provided for Windows hosts.
2. Available patches provide for Linux hosts.

Qualys.

Zero-Touch Patch Job



- Select the “Zero-Touch Patch Job” option from the VMDR Prioritization Report.
- Patches are not selected individually, but instead are targeted using a query.
- Schedule patch jobs to recur daily, weekly, or monthly.
- Specific patching use-cases are ideal for ”Zero-Touch” patching.

Qualys.

Lab 13 : Zero-Touch Patch Job

Please consult page 50 in the lab tutorial supplement for details.

PLAY Tutorials begins on page 50.

Qualys.

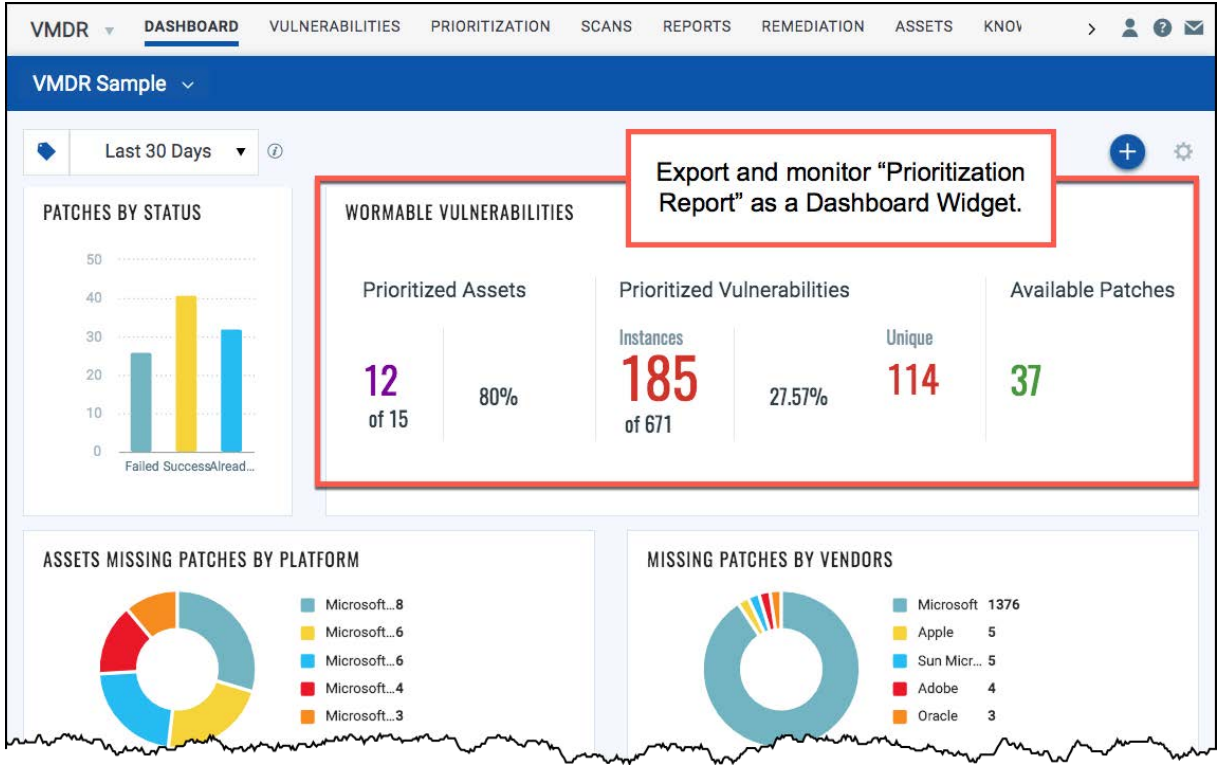
Automated Patch Selection

Patches that meet the query condition are added to the deployment job, automatically.

- The query is generated from the options (Age, RTIs, and Attack Surface) selected in the Prioritization Report.

Qualys.

Export to Dashboard



Results will be continuously updated within the Dashboard Widget.

Qualys.

Patch Management

Qualys.

Patch Management Overview

- Automatically correlates discovered vulnerabilities with their required patches
- Leverage existing Qualys Cloud Agents to deploy and uninstall patches
- Provides OS and Application patches, including patches from third-party software vendors (e.g., Adobe, Java, Google, Mozilla, Microsoft, etc...)

Qualys.

Patch Management Overview (cont.)

- Available for Windows, CentOS 6/7, and RHEL 6/7/8
- Provides patching just about anywhere an Internet connection is available (e.g., airports, coffee shops, remote offices, etc...)
- Qualys Agents determine which patches are missing or required and can identify superseded patches
- Build patch jobs that target specific vulnerabilities, severity levels, and known threats

Qualys.

Patch Sources

OS and Application Patches come from:

- Vendor Global CDNs (e.g., Oracle, Adobe, Microsoft, Apache, Google, etc...)
- YUM repositories (Linux)
- Local repository (i.e., Qualys Gateway Server)
  - Patch downloads requested by one agent, are cached on QGS and made available “locally” for other agents that need the same patch.
  - QGS also provides a cache for manifests and agent binaries

Qualys.

Qualys PM Workflow

CA 1. Install Cloud Agent on target host.

CA 2. Assign target agent host to a CA Configuration Profile that has PM configuration enabled.

CA 3. Activate PM module on target agent host.

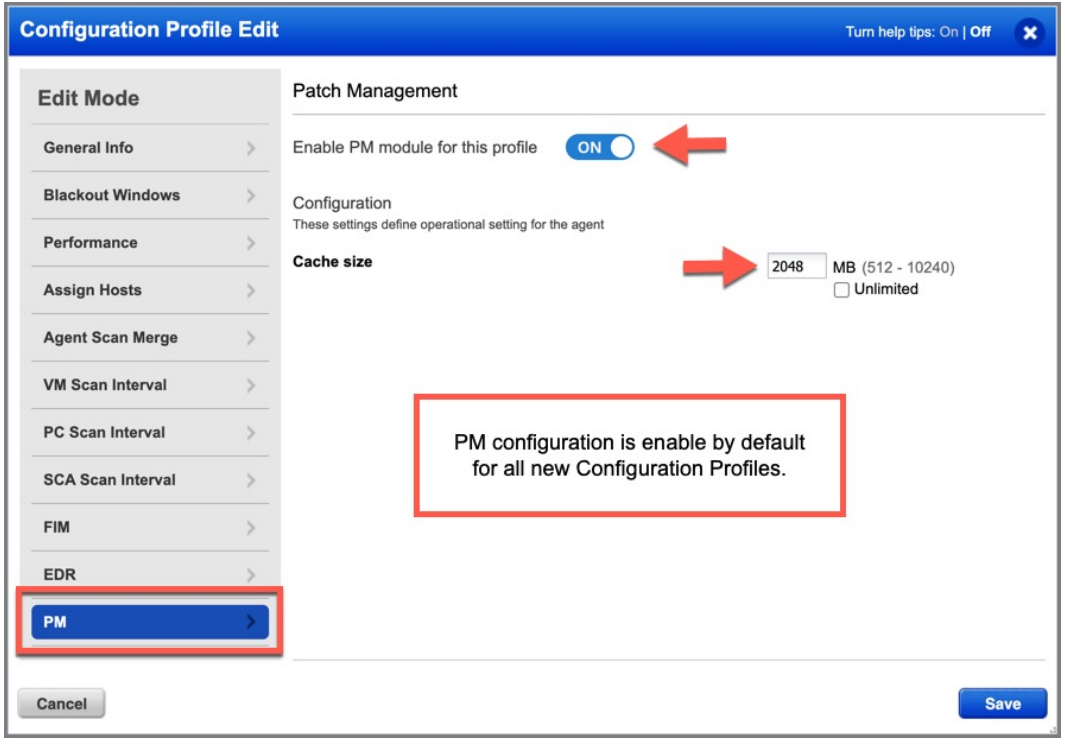
PM 4. Assign target agent host to an enabled Assessment Profile.

PM 5. Allocate patching licenses.

PM 6. Create Patch Jobs.

Qualys.

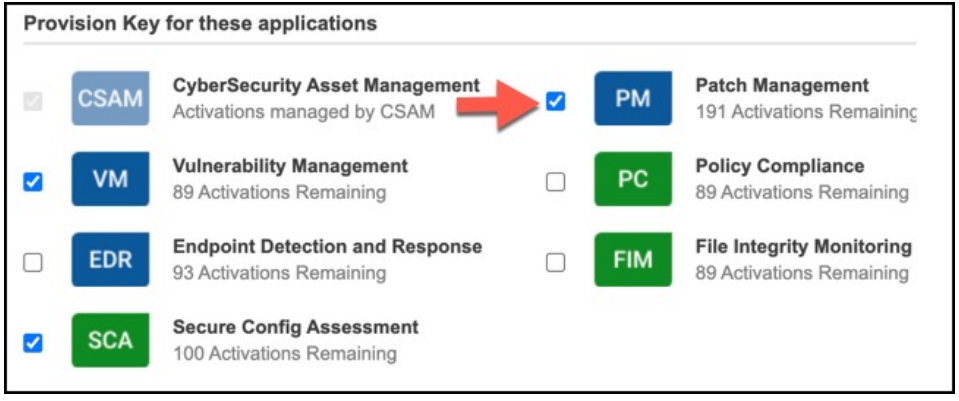
Configuration Profile



- Presently, PM has one agent configuration setting.
- Set “Cache size” to at least 2048 MB, to accommodate Windows Updates.

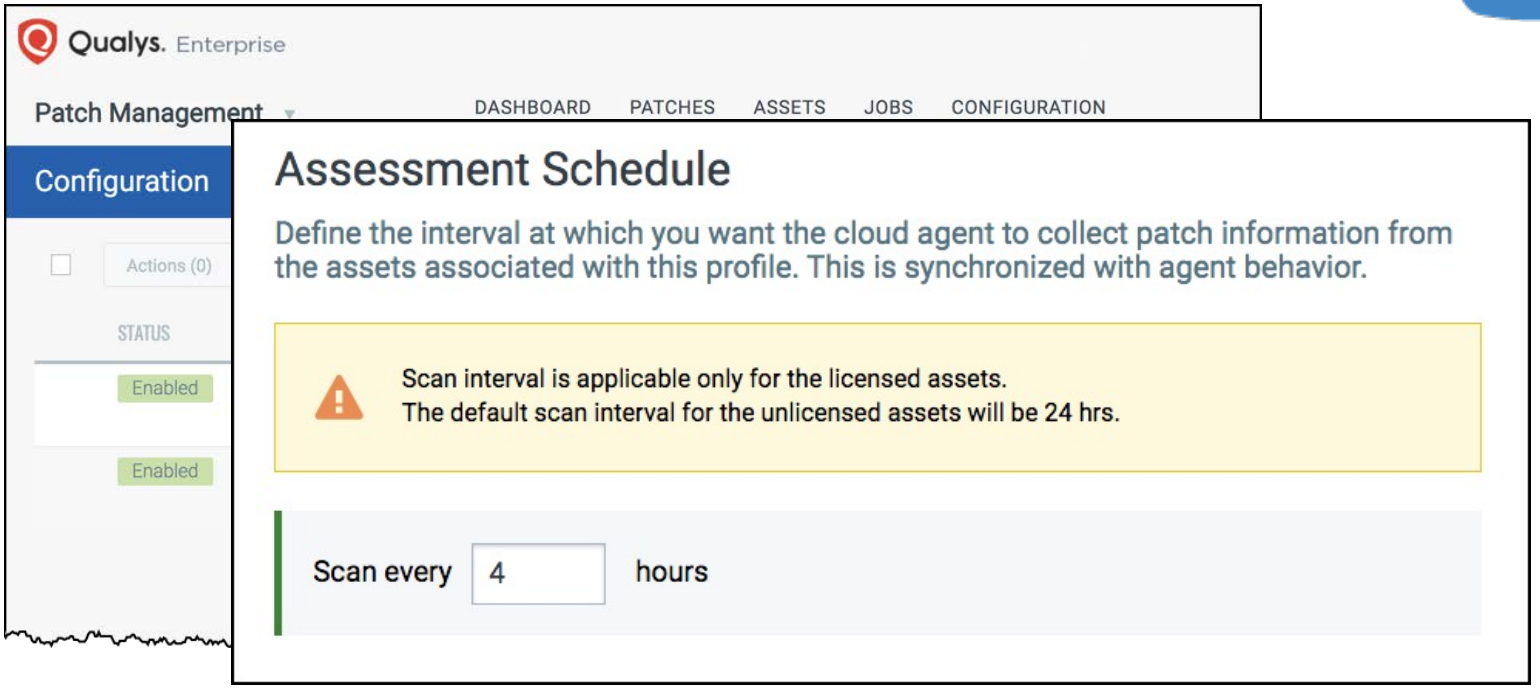
Activate PM Module for Target Host

- Select the PM module in the Agent Activation Key, before and after agent deployment.



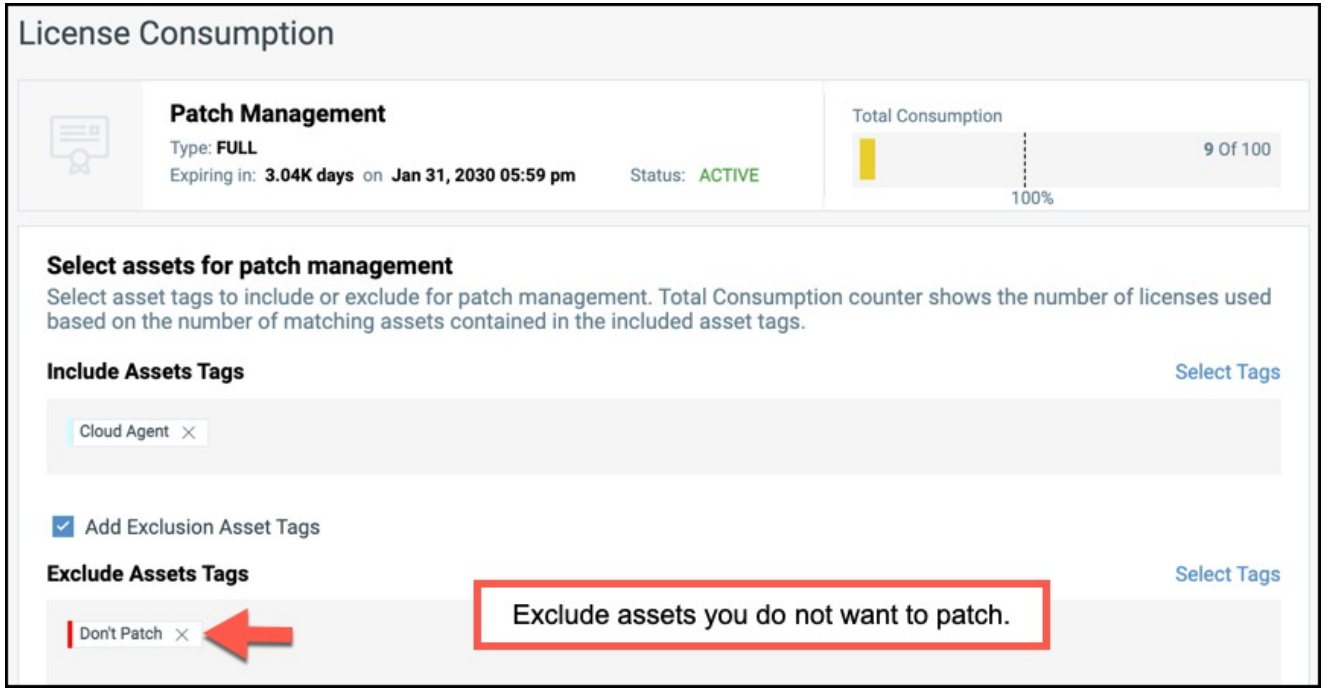
- Use the “Quick Actions” menu to activate PM for any agent host or use the Qualys Cloud Agent API.

Assessment Profile



- Specifies frequency of patch assessment scans.
- System Profile will be used by default.

License Consumption



- Use Asset Tags to specify hosts for patching and to exclude others.
- Only agent host assets will consume a patch license.

Patch Deployment Job

Qualys.

Deployment Job Wizard

- Build patch jobs step-by-step.
- Select assets and patches.
- Configure scheduling option or run on-demand.
- Configure communication and reboot options.
- Assign access to a job.

Qualys.

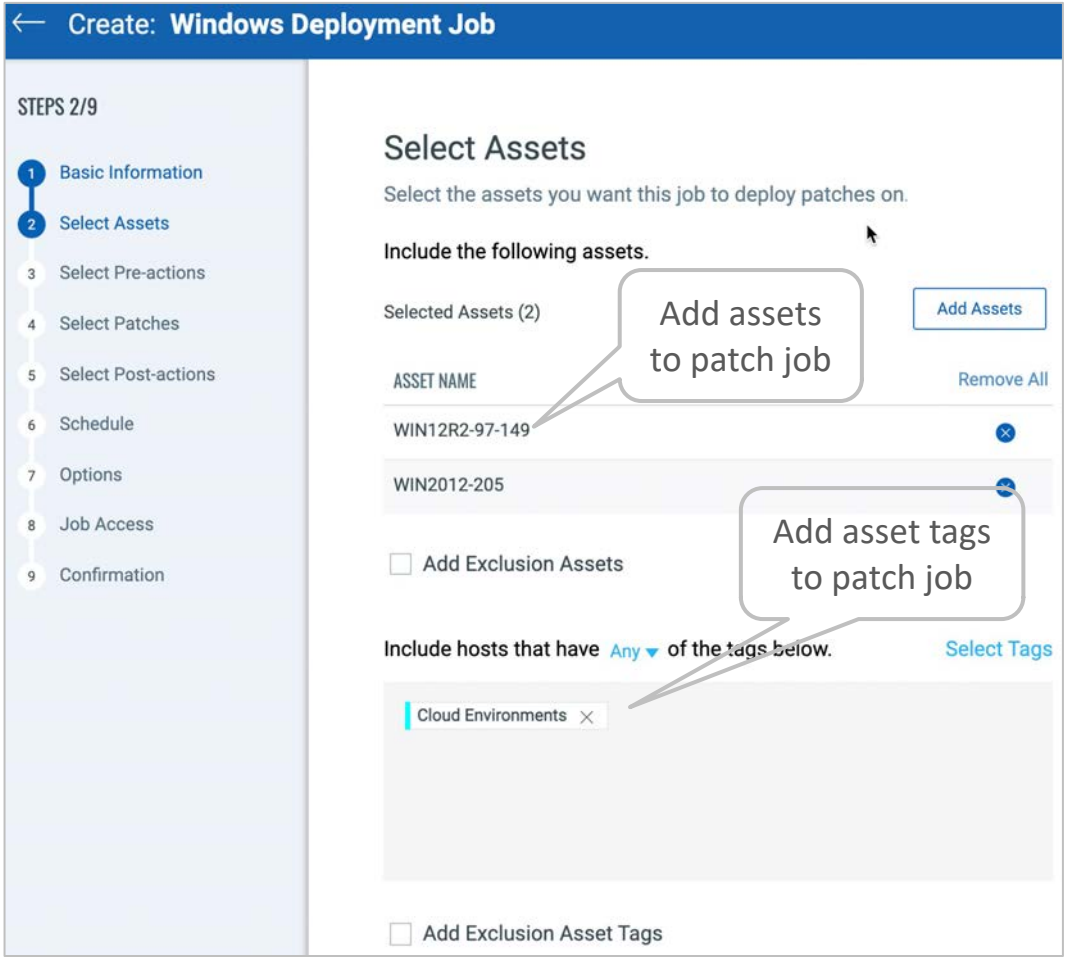
Lab 14 : Patch Deployment

Please consult pages 52 to 57 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 52.

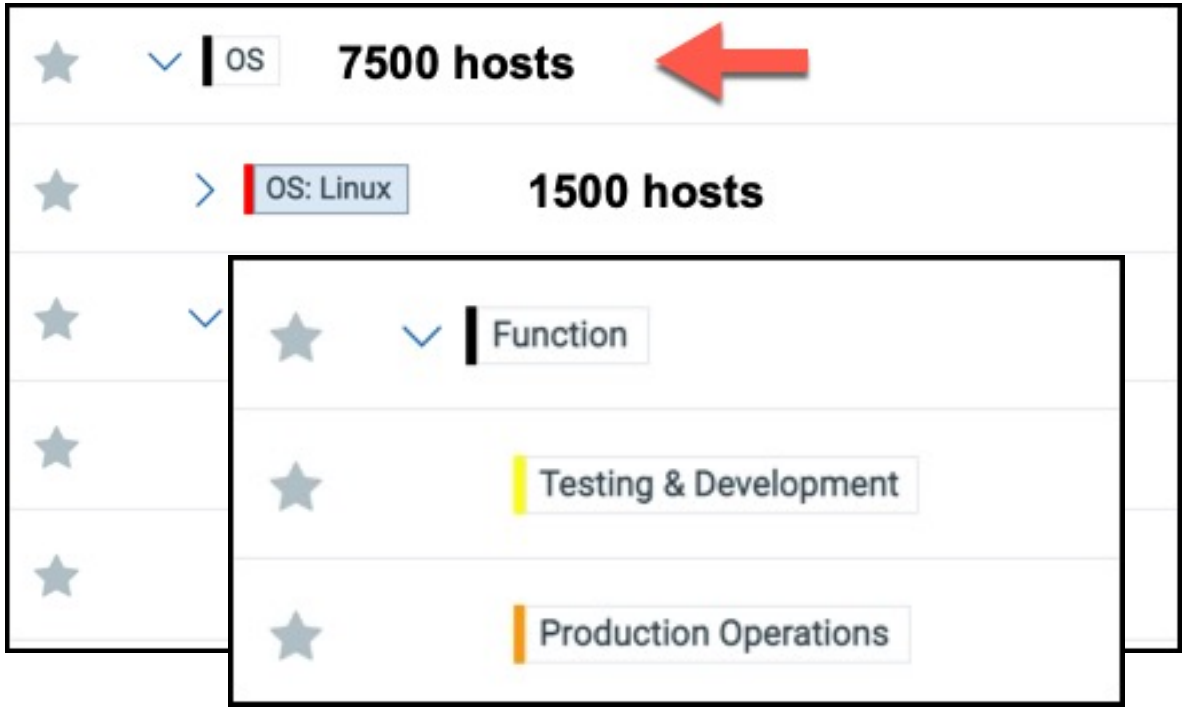
Qualys.

Select Assets



Qualys.

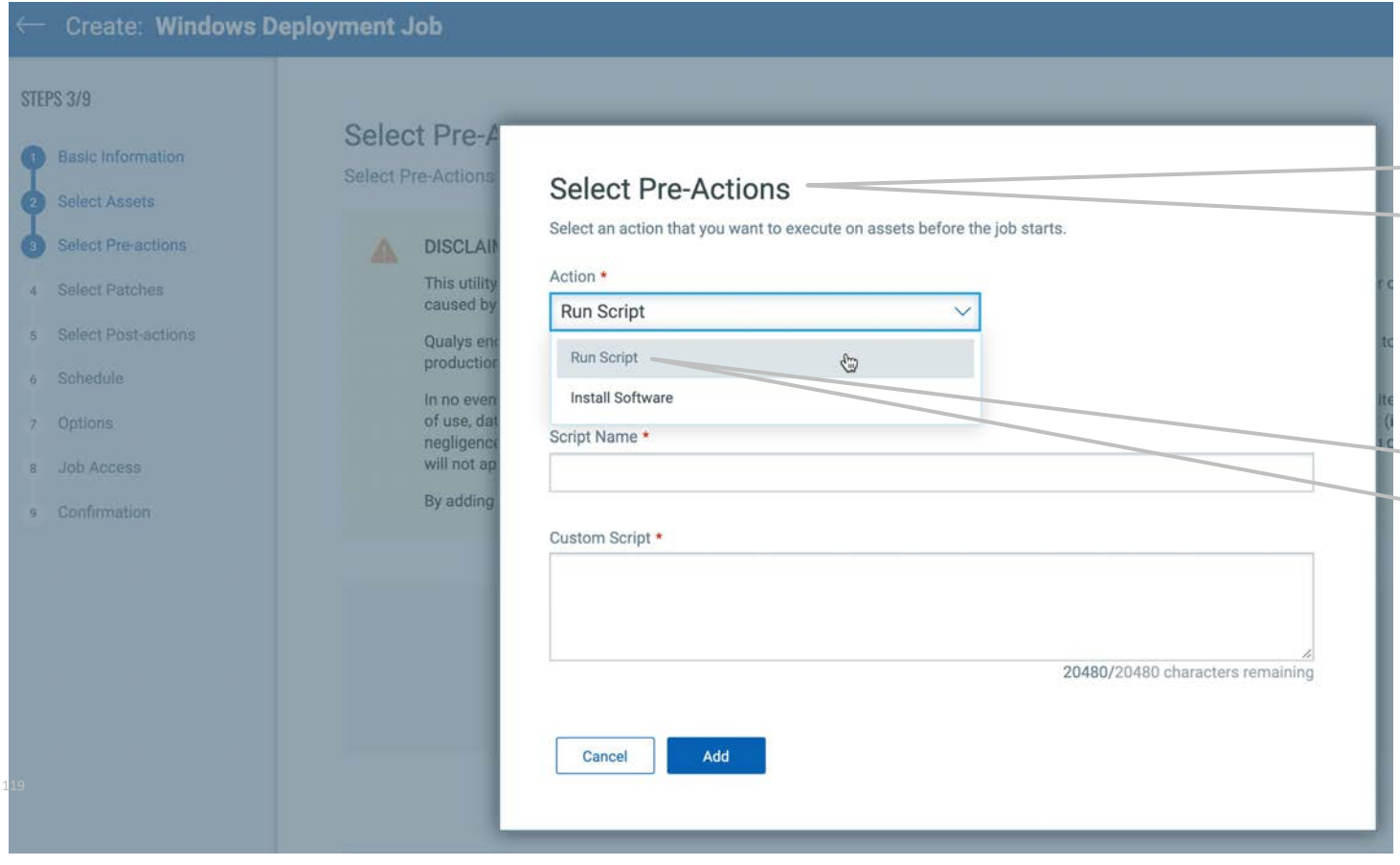
Asset Tag Tips



- Design Asset Tag hierarchies with nested structures.
- Selecting a “parent” tag as a patching target, includes its “child” tags automatically.
- Use tags to distinguish between production and testing assets.

Qualys.

Pre and Post Actions

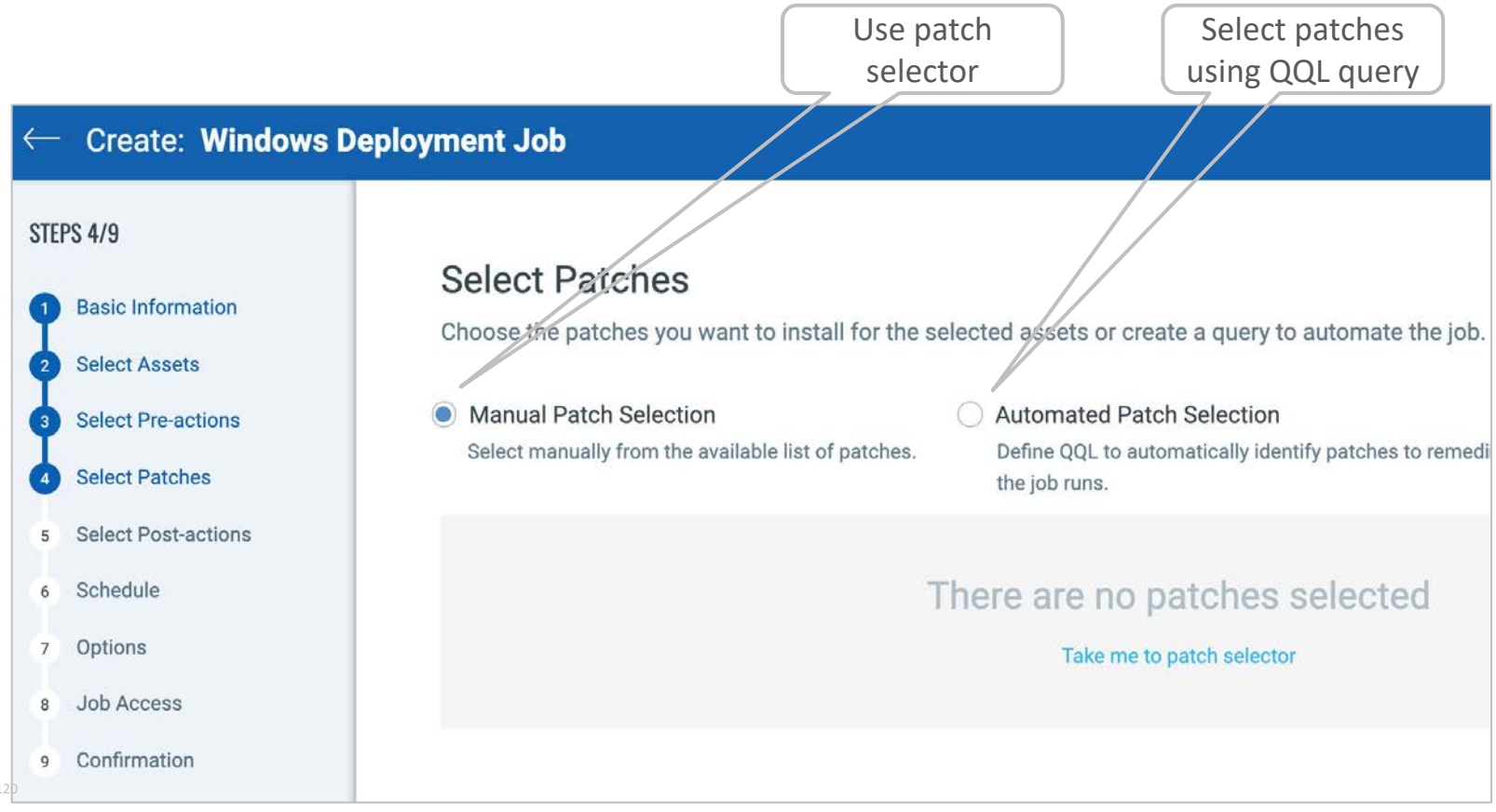


Configure action to execute before job starts

Run a PowerShell script or install software

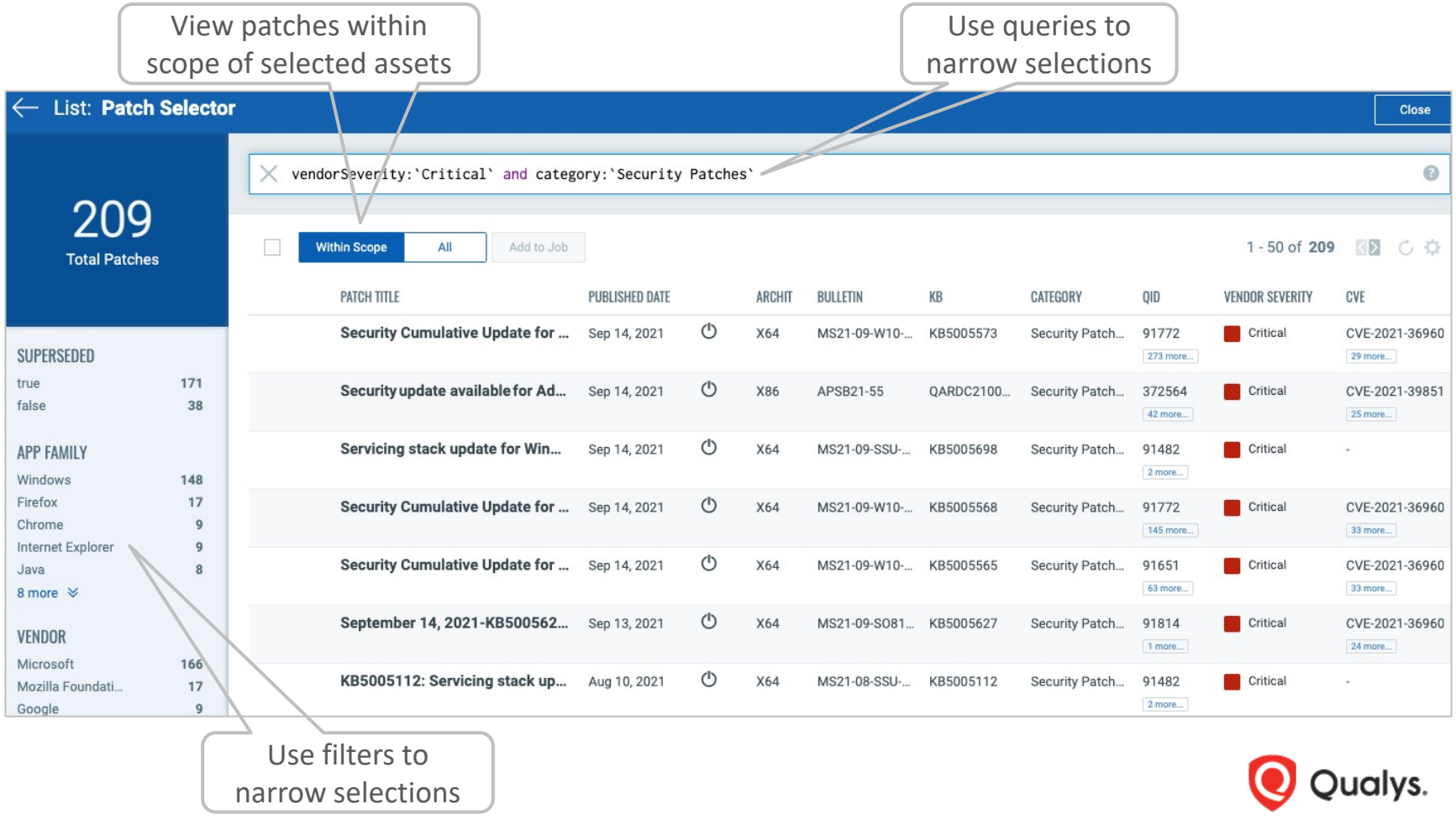
Qualys.

Select Patches



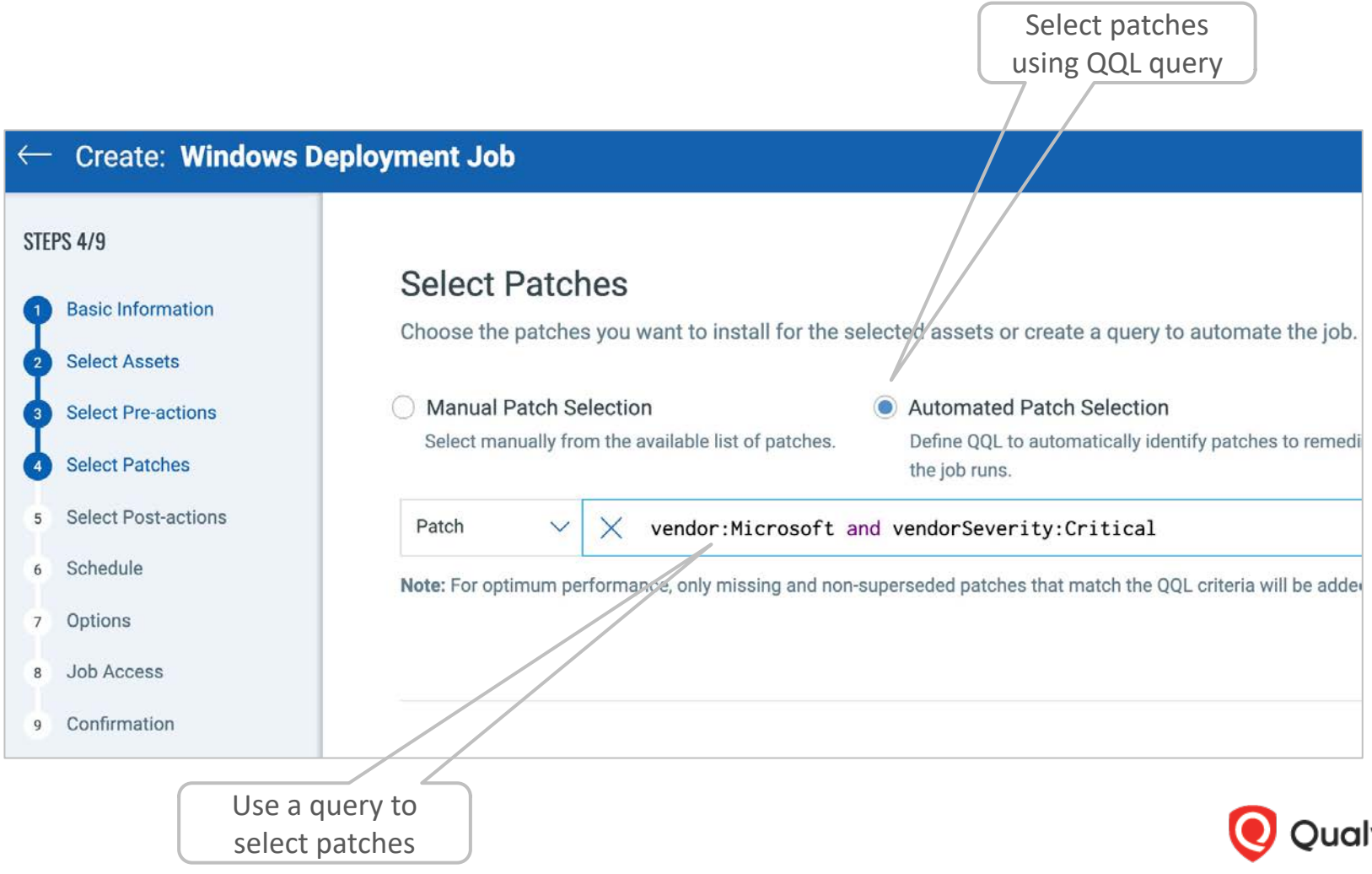
Qualys.

Manual Patch Selection



Qualys.

Automated Patch Selection



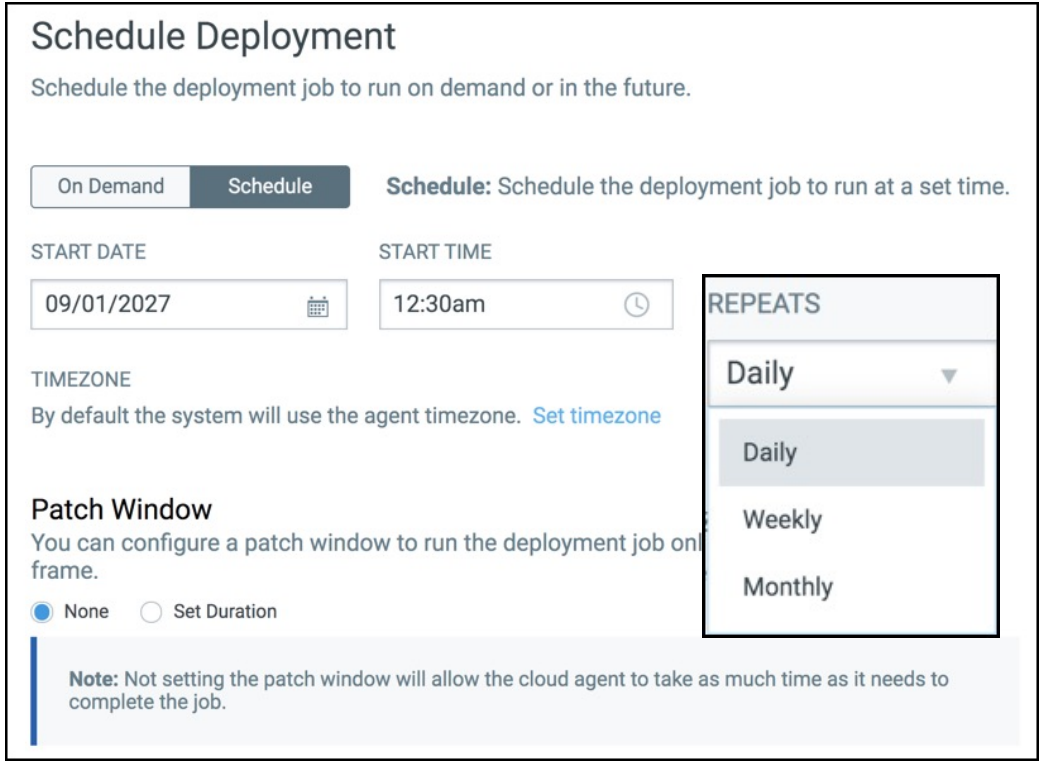
Qualys.

“Within Scope” Patch

“Within Scope” only includes patches needed by your targeted host assets.

Qualys.

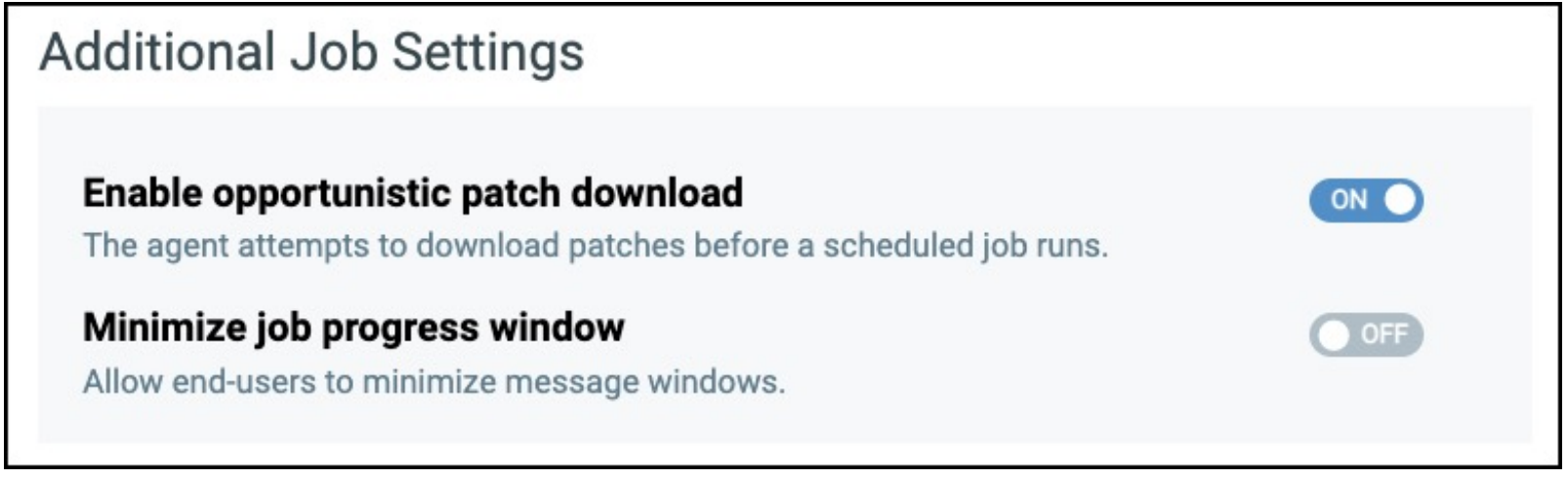
Schedule Deployment



Run jobs ”on demand” or schedule them to run at regular frequencies.

Qualys.

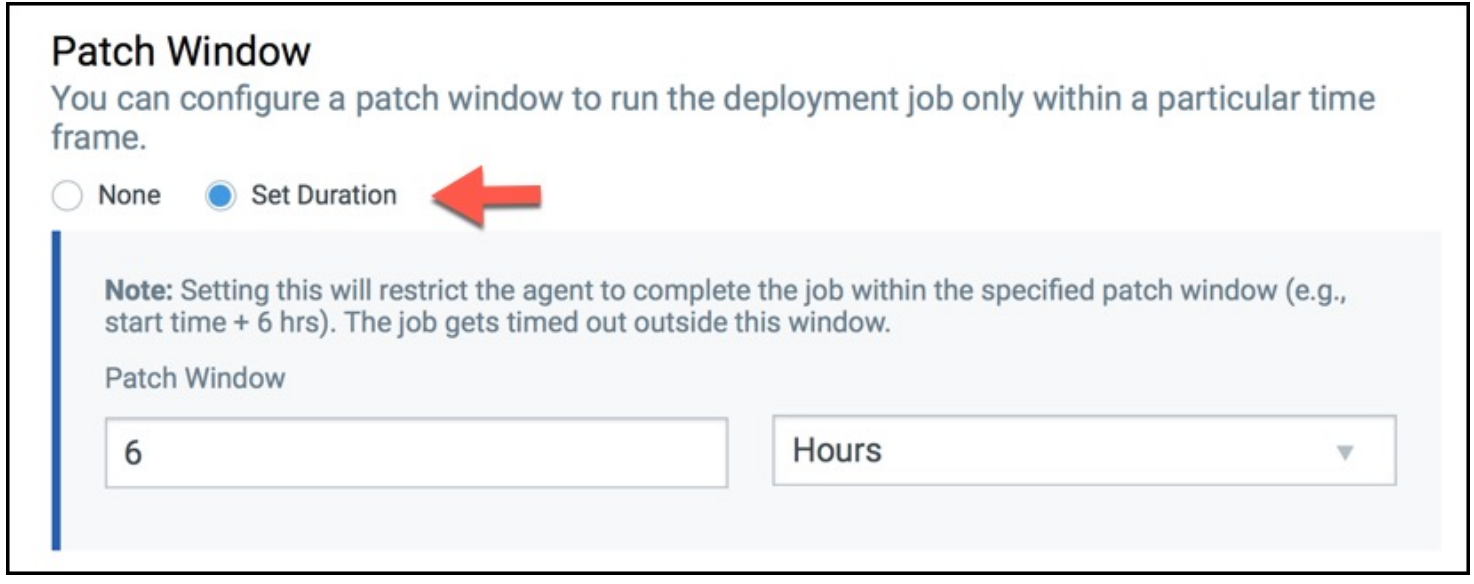
Opportunistic Patch Download



You can “Enable opportunistic patch download,” to allow agents to download required patches prior to the start of a scheduled job.

Qualys.

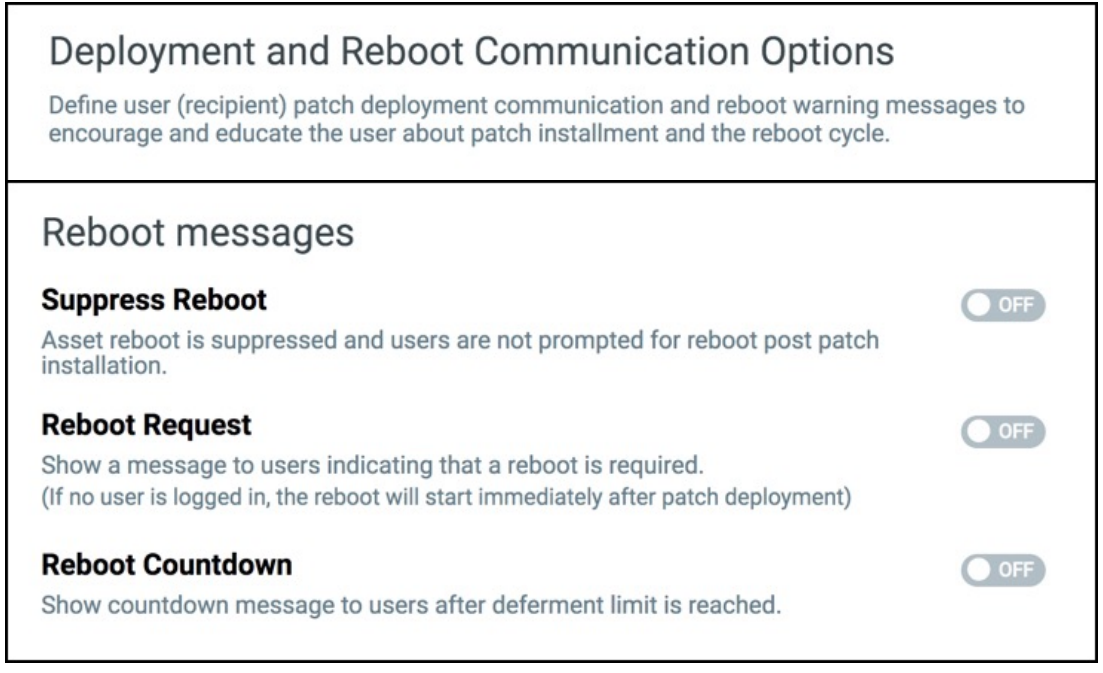
Patch Window



- A host will display the “Timed out” status, if the patch installation does not start within a specified patch window.
- Select the “None” option to give agents an unlimited amount of time.

Qualys.

Windows Communication Options

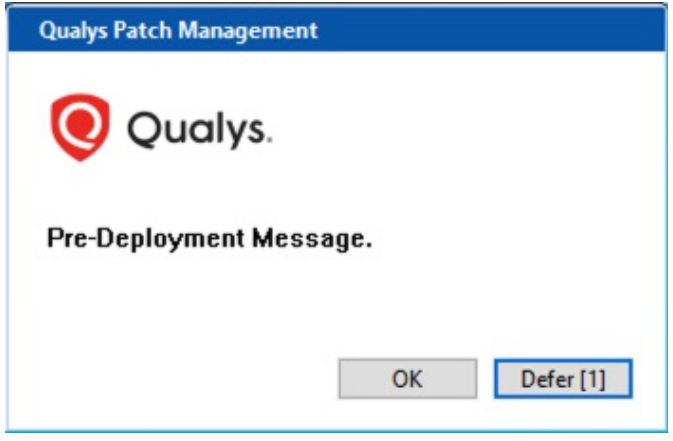


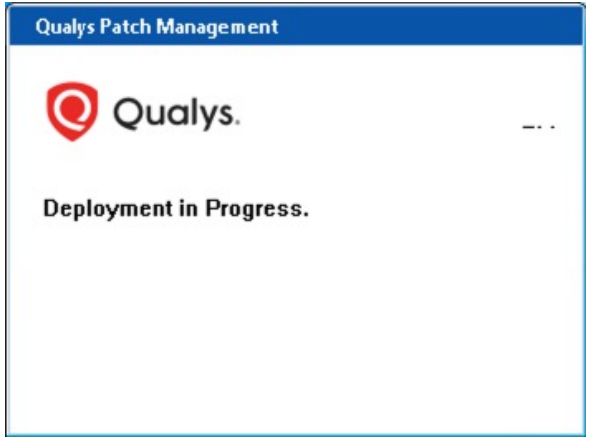
Choose the type of “Deployment and Reboot Communication Options” for each Deployment Job.

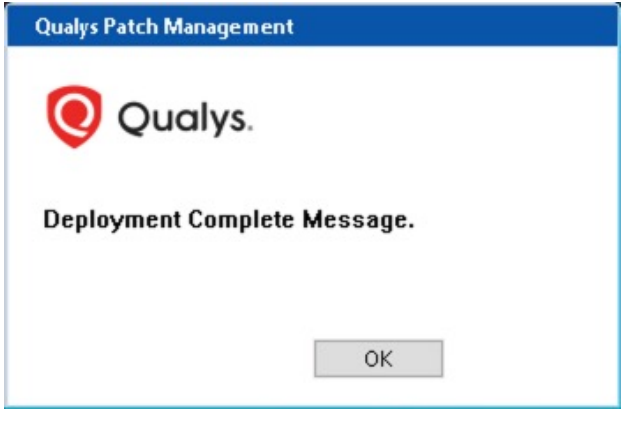
Qualys.

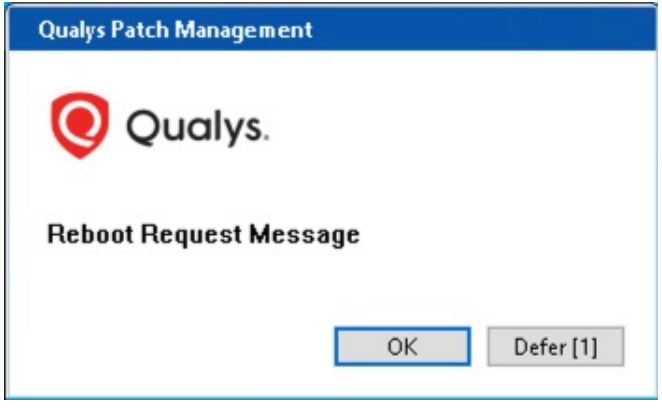
Host “Pop-Up” Messages

“Pre-Deployment and “Reboot Request messages can be configured with deferment options.



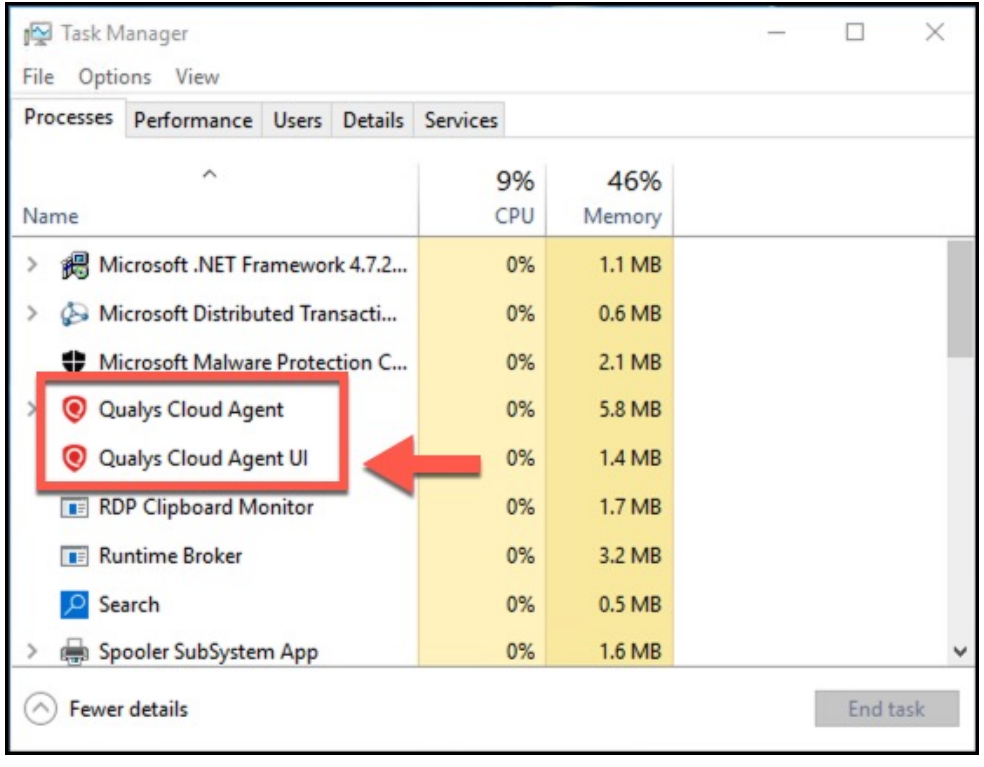






Qualys.

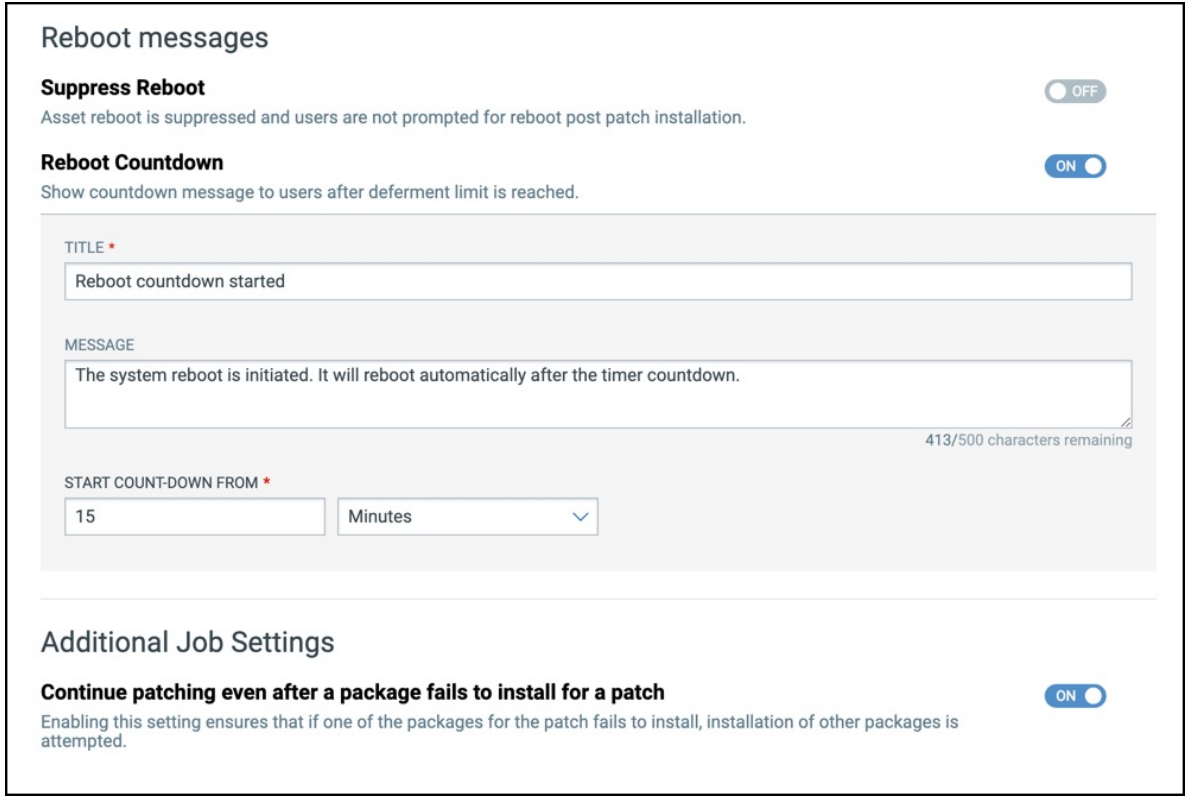
PM Processes & Executables



- When patching is active on a Windows host, patching messages and notifications are managed by the “Qualys Cloud Agent UI” process (QualysAgentUI.exe)
- ‘stdeploy.exe’ is the name of the patching executable.

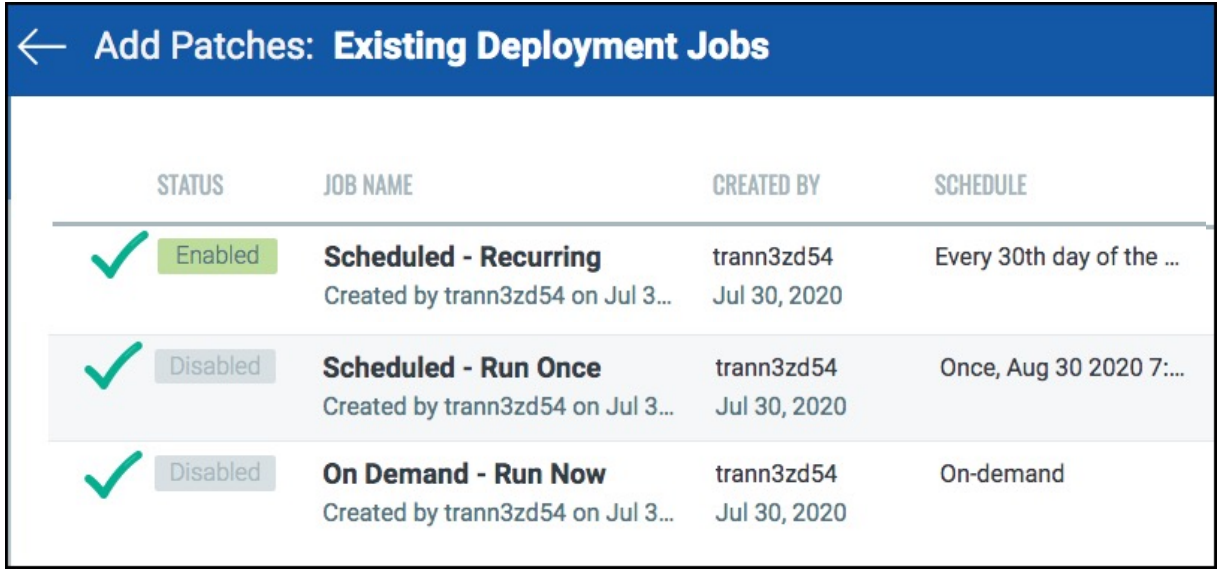
Qualys.

Linux Communication Options



Qualys.

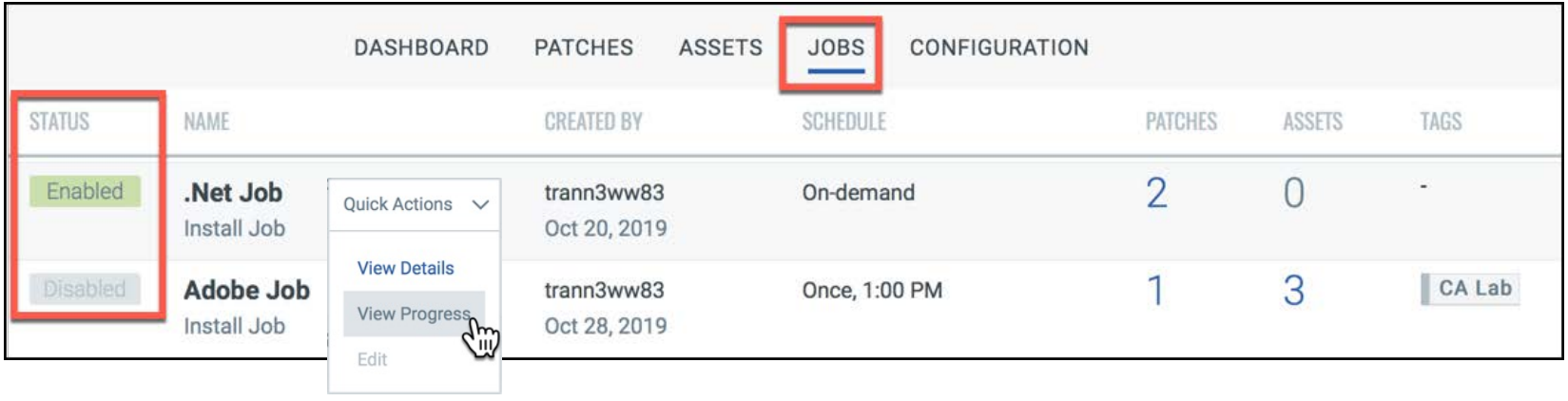
Add to Existing Job?



- Patches and assets can be added to any deployment job, before it is enabled
- Patches and assets can be added to a “recurring” job, both before and after it is enabled.

Qualys.

Job Status



View Job Status:

- **Enabled** – Job is presently active.
- **Disabled** – Job is presently inactive.
- **Completed** – Job has completed.

Qualys.

View Job Progress

STATUS	ASSET NAME	OS	PATCHES		
			INSTALLED	FAILED	SKIPPED
Pending Oct 28, 2019	**WS2016DFW242** fe80:0:0:0:d42d:825a:8140:153, 192.168....	Microsoft Windows Server 2016 Stand...	—	—	—
Completed Oct 28, 2019	**WS2012EVAL206** fe80:0:0:0:383a:fada:a31b:e92c, 192.168...	Microsoft Windows Server 2012 R2 Sta...	0	0	1
Completed Oct 28, 2019	**WS2016DFW251** fe80:0:0:0:fd21:1c55:3da9:ba53, 192.168...	Microsoft Windows Server 2016 Stand...	0	0	1

Pending → Job Sent → Downloaded → Patching → Pendir → Completed

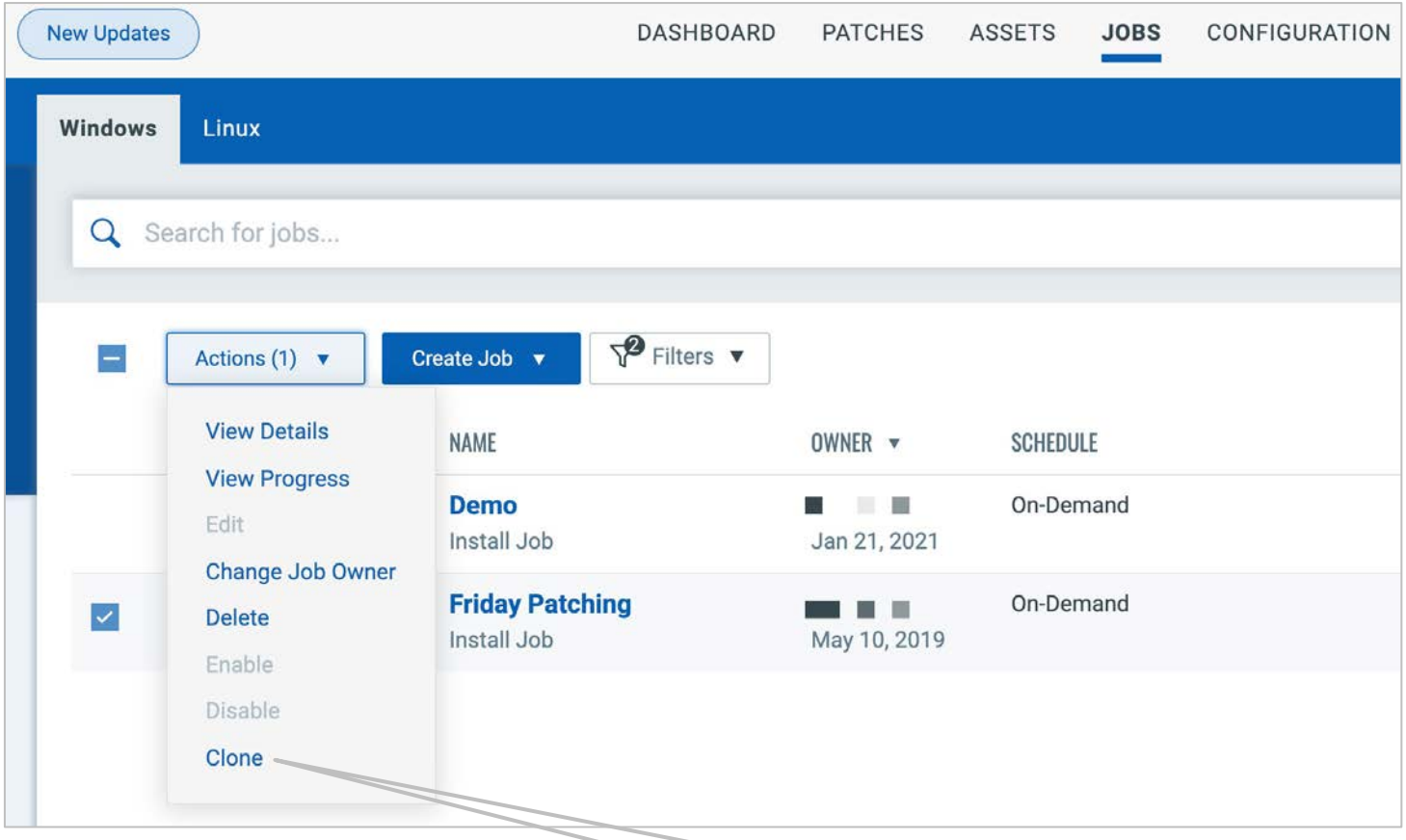
Qualys.

Best Practices

- Use Asset Tags as targets for patch deployment jobs.
- Deploy patches to test hosts, first (create Asset Tags that distinguish between test and production assets).
- Once test deployments are verified, **clone the deployment job** and include production asset tags

Qualys.

Clone job



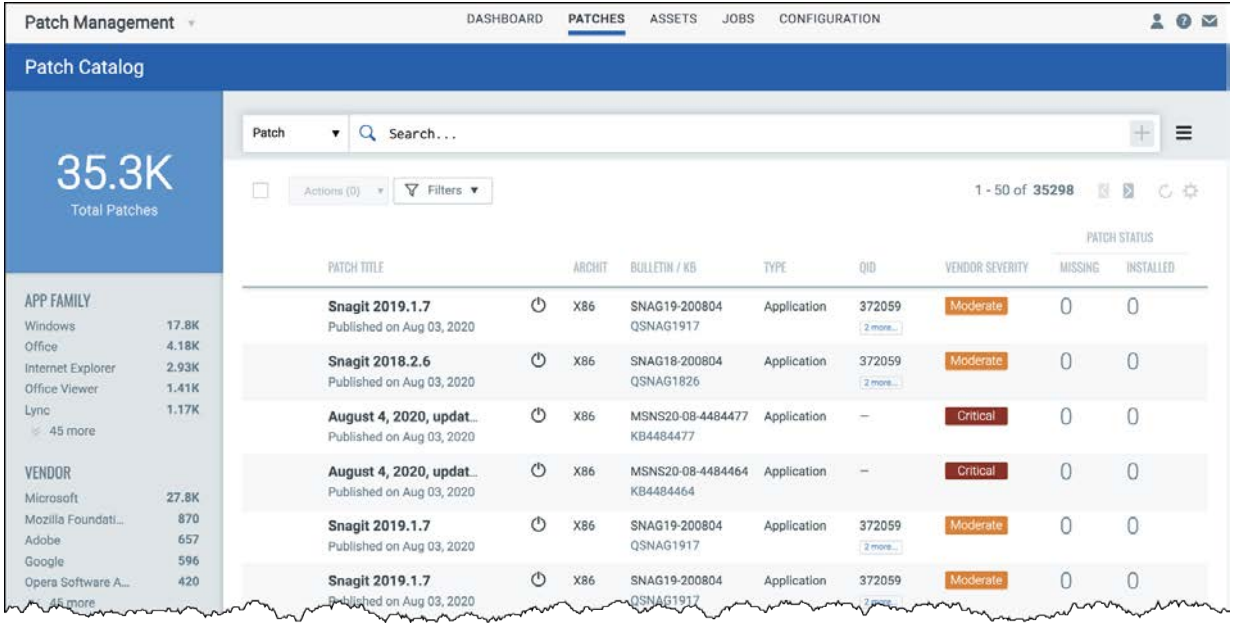
Clone an existing job

Qualys.

Patch Catalog

Qualys.

Patches



- The Patch Catalog contains tens of thousands of OS and application patches.
- Presently, you can add up to 2000 patches to a single job.

Qualys.

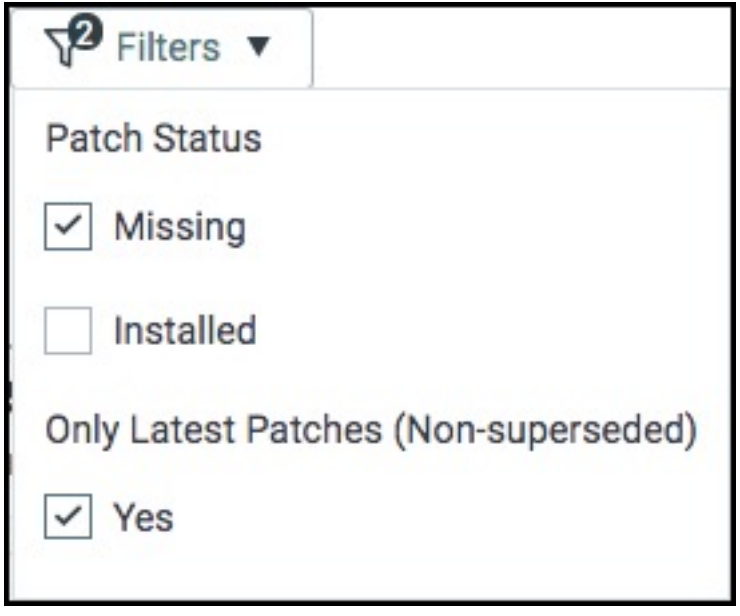
Lab 15 : Patch Catalog

Please consult pages 58 to 61 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 58.

Qualys.

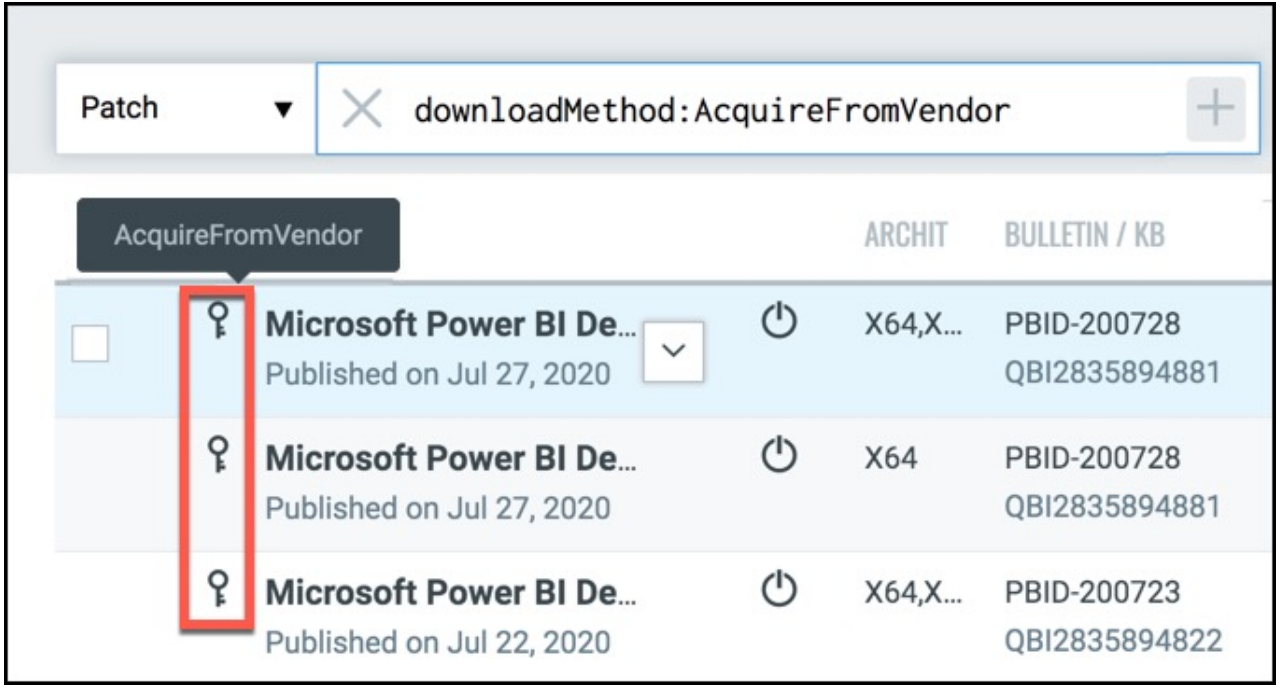
Catalog's Default Display Filters



The default filters in the Patch Catalog, display patches that are missing and only the latest patches (non-superseded).

Qualys.

Acquire From Vendor



Patches identified with the “key-shaped” icon, cannot be downloaded by Qualys’ Cloud Agent.

Qualys.

Prioritized Products

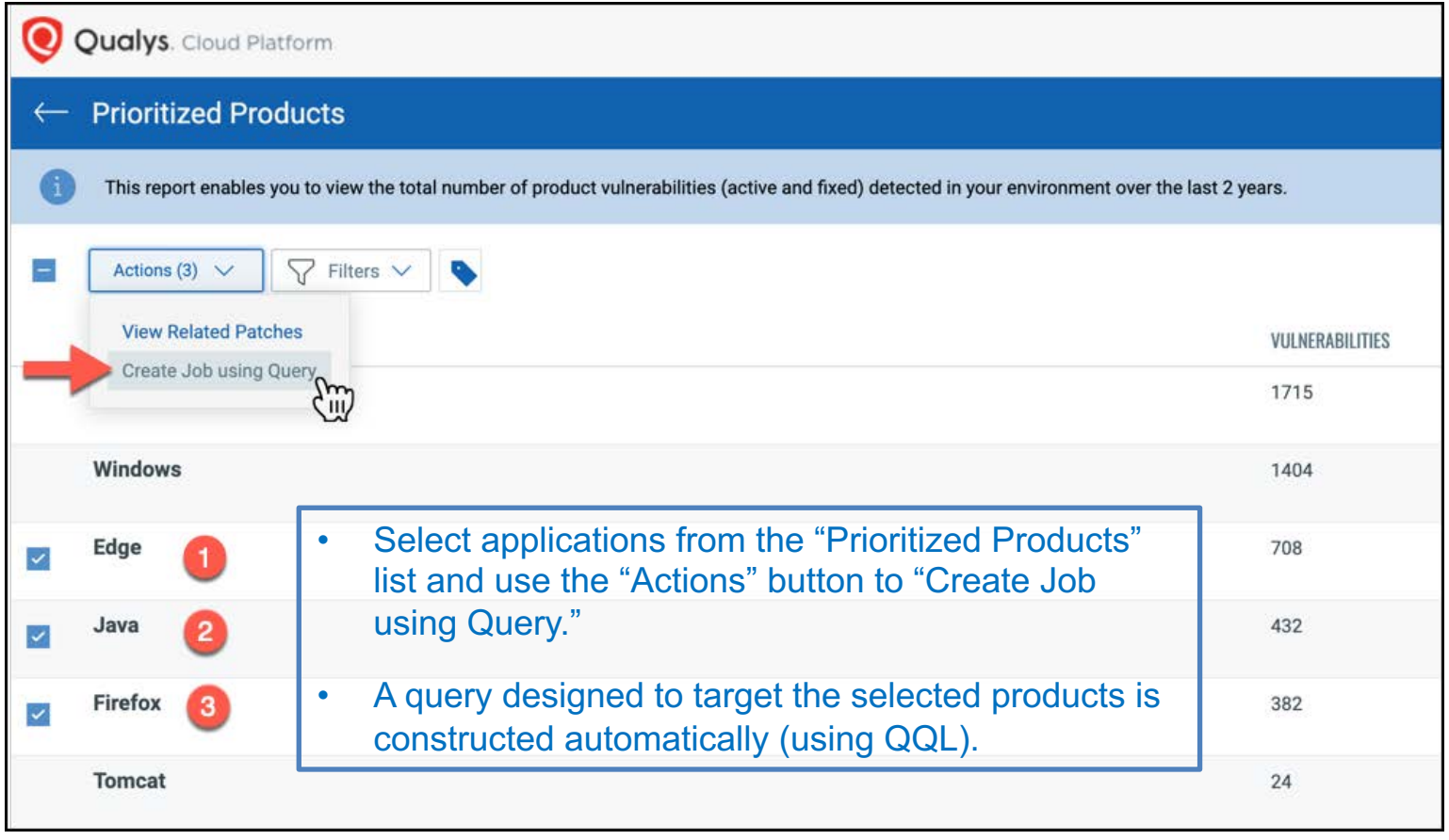
Qualys.

Prioritized Products

- Focus on products in your environment that are important to patch on a regular basis
- Prioritizes products that have introduced the most vulnerabilities (over the last 2 years)
- Create a “zero-touch” patch job targeting products with most vulnerabilities
  1. Patches are selected using QQL
  2. Selected patches are included in recuring deployment jobs (daily, weekly, monthly)
- Click the “Prioritize Products” button from the Patch Catalog.

Qualys.

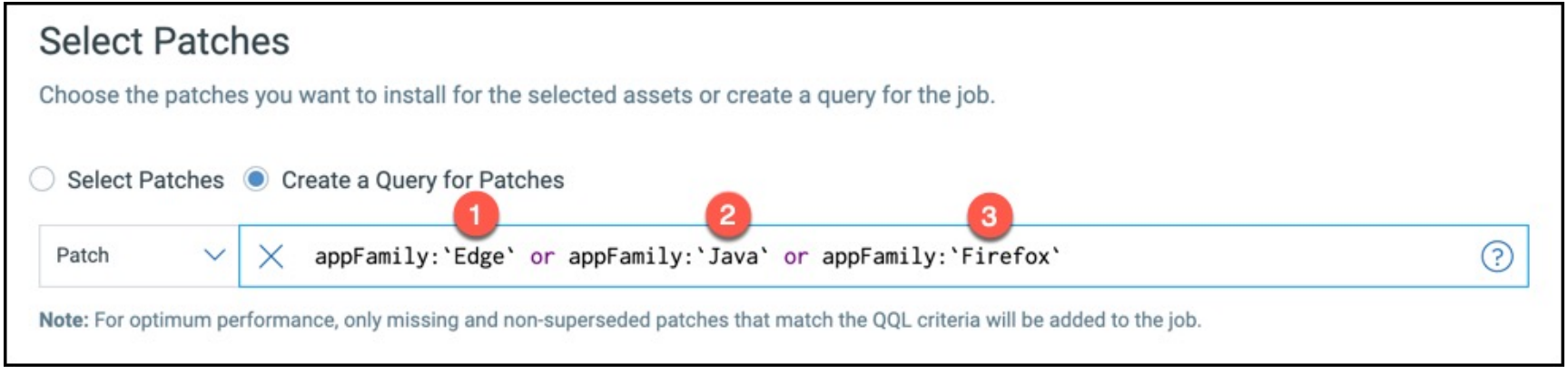
Create Job Using Query



- Select applications from the “Prioritized Products” list and use the “Actions” button to “Create Job using Query.”
- A query designed to target the selected products is constructed automatically (using QQL).

Qualys.

Create a Query for Patches



- The generated query condition(s) will specify the criteria for selecting patches each time the job runs:
  - daily
  - weekly
  - monthly

Qualys.

Course Resources

VMDR Certification Exam

https://gm1.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?&id=22511237827

VMDR Trial Account

https://www.qualys.com/forms/vmdr/

You will find the exam link and trial account link at the back of the VMDR Lab Tutorial Supplement.

Qualys.

Qualys®

Continuous Security

Thank You

training@qualys.com