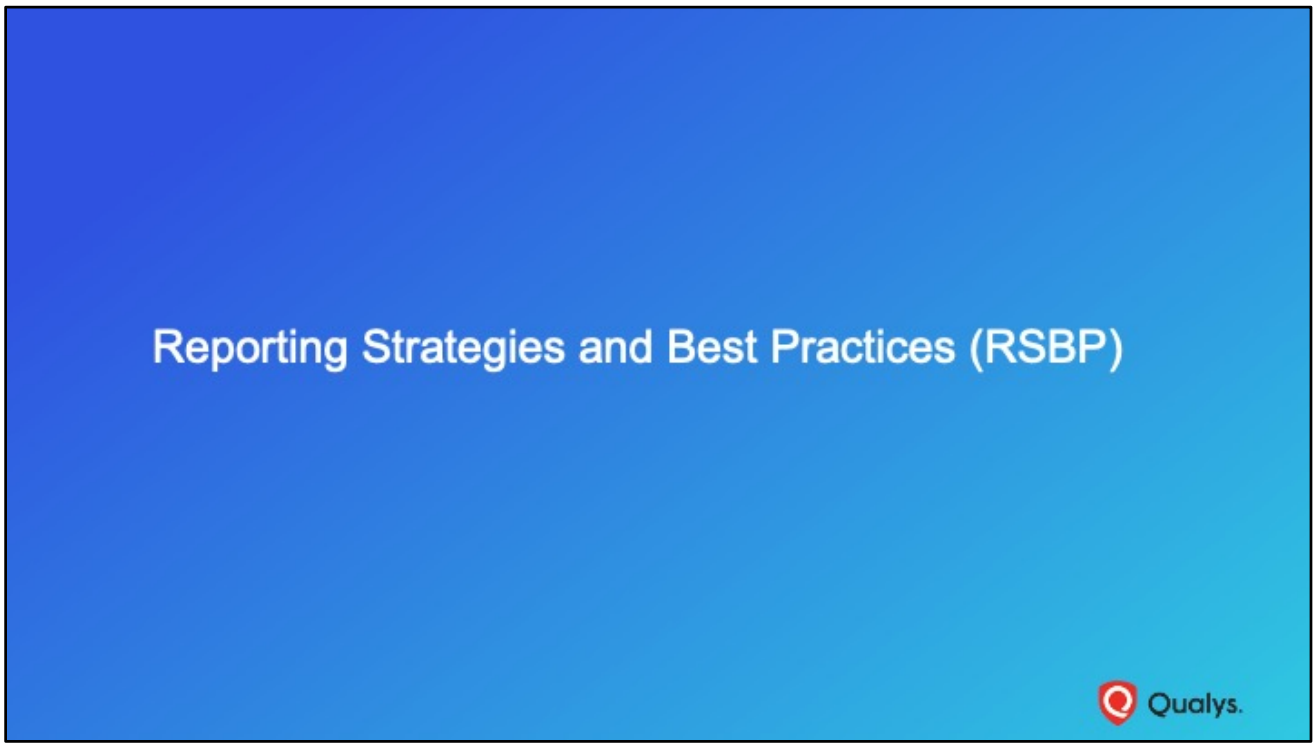
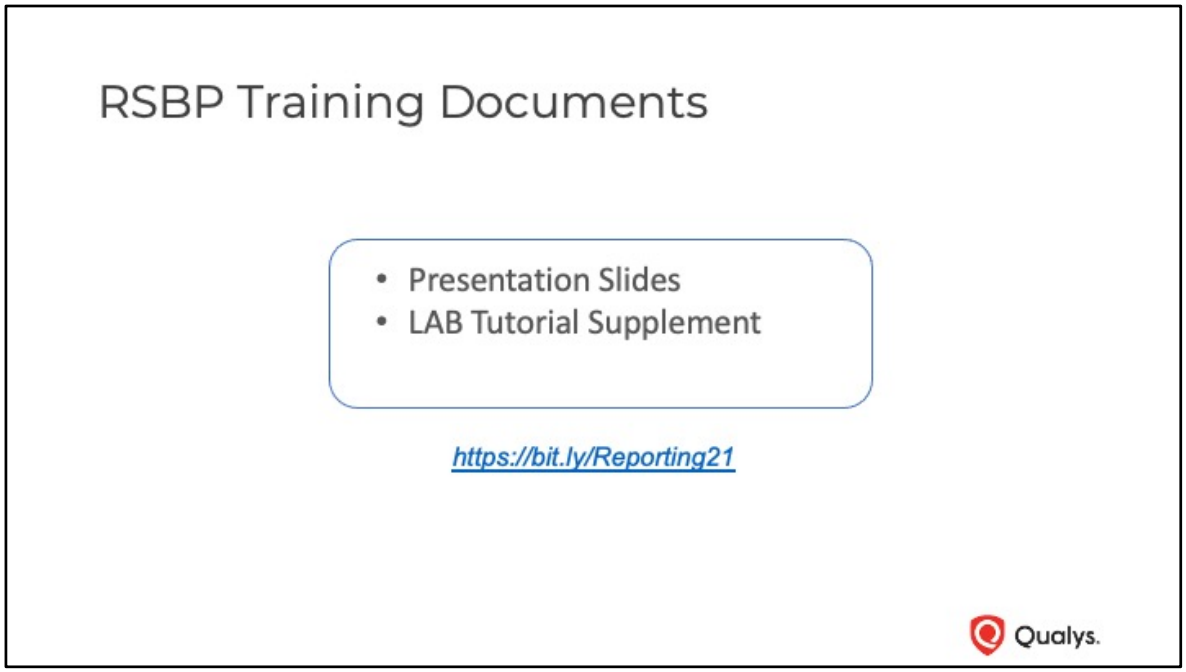


Welcome to the Qualys Reporting Strategies and Best Practices (RSBP) training.

In this course, we will discuss the different strategies and tools that can be used to produce various types of reports for different stakeholders in your organization.

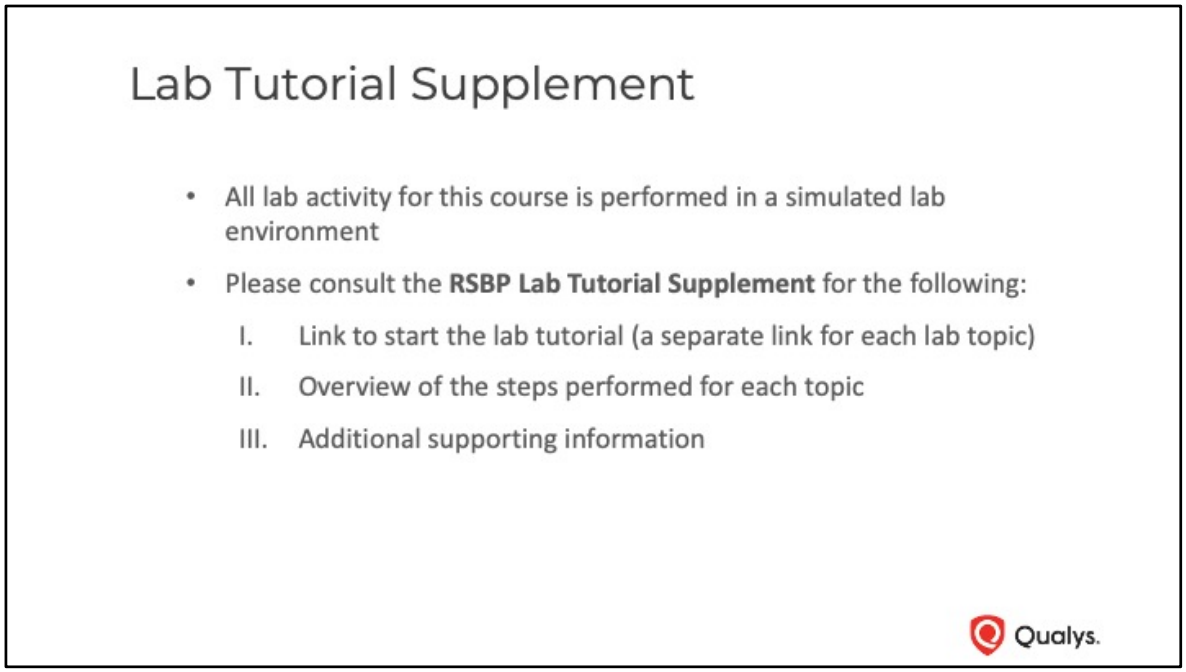


We'll begin this training class with a quick overview of the items needed to complete the RSBP training course, namely the lab tutorial supplement and presentation slides.

You will find the training documents for this course on our learning portal qualys.com/learning.

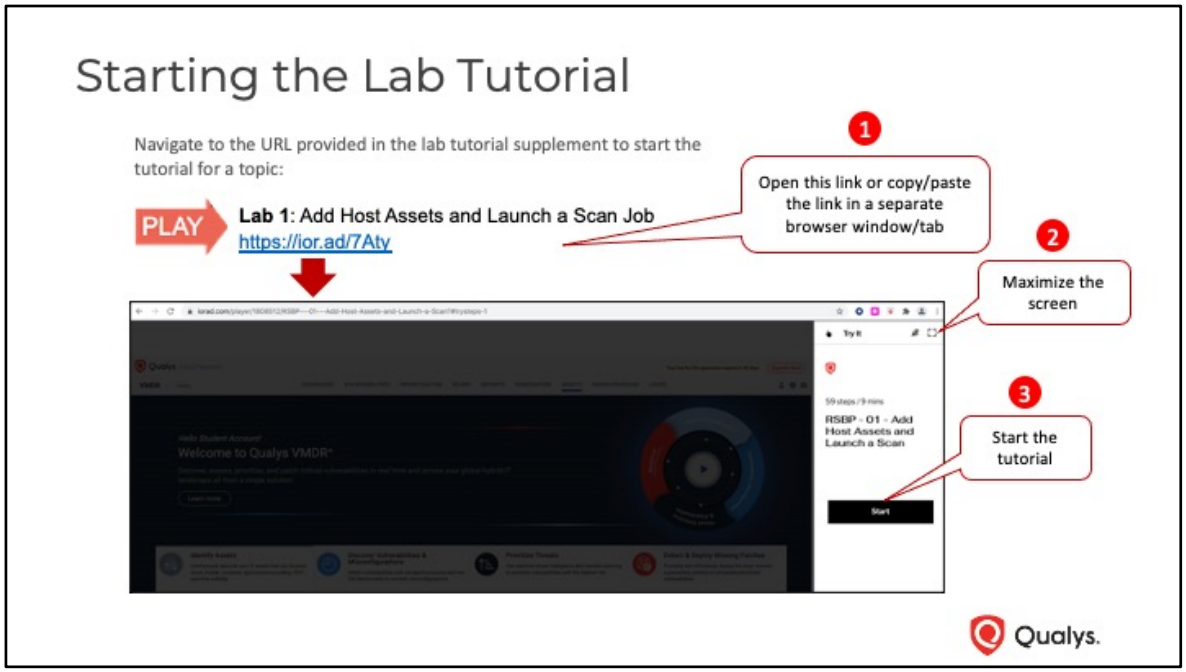
If you have not downloaded these documents, please do so now.

Note that you will need a PDF reader like Adobe Acrobat to view these files.

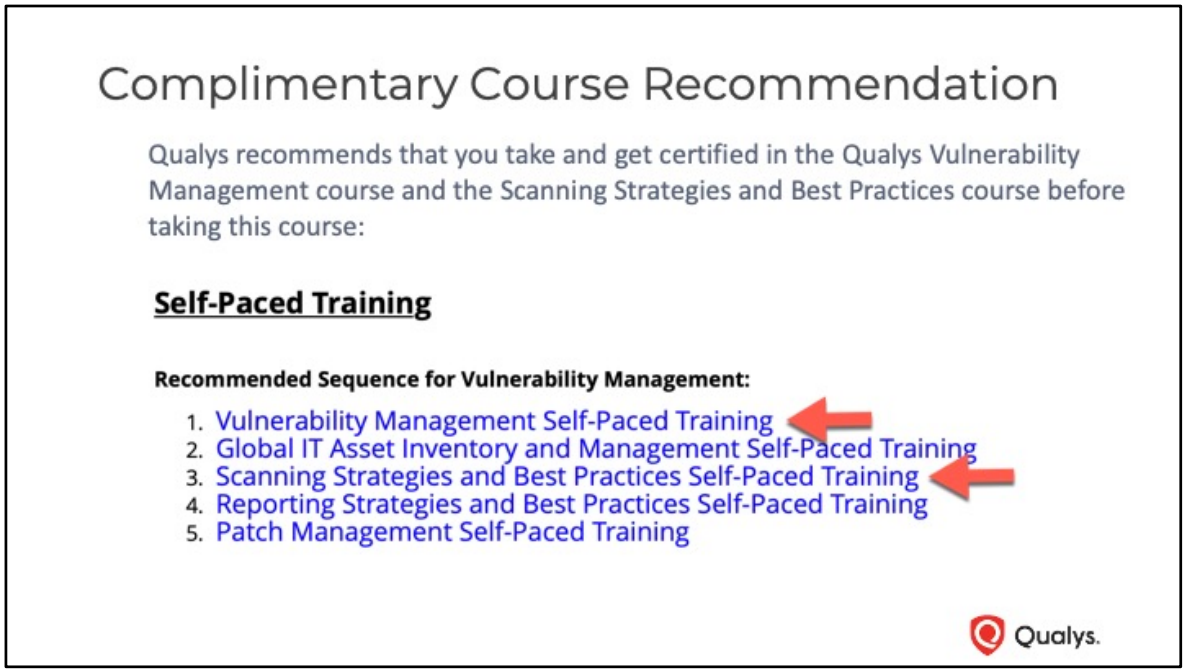


Participants will perform all lab activity for this training in a simulated lab environment. Please consult the RSBP Lab Tutorial Supplement document for further instructions.

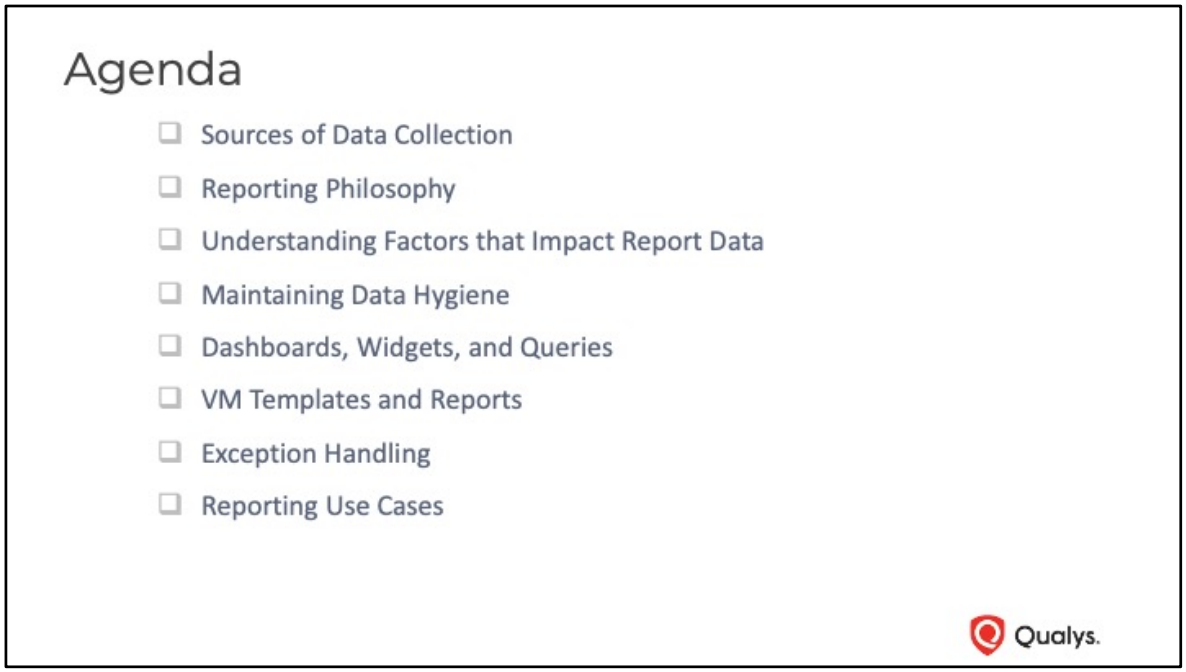
For a trial account where you can experiment and go off-script, you can request a 30-day account at: https://qualys.com/free-trial.



Scroll down in your Lab tutorial supplement to the specific topic to find the lab tutorial link. Open the link in a separate browser tab or window and start the lab tutorial.
Collapse the lab window when done and read through the lab tutorial supplement for further instructions.



We recommend that learners be familiar with the Vulnerability Management application before taking this course. You can meet this recommendation by successfully completing the Qualys Vulnerability Management and Scanning Strategies and Best Practices training courses.



We will start the course with a discussion on the different sensors that are used by Qualys to collect data from your infrastructure.

We will then talk about the different approaches to reporting and look at a use case where an organization's custom severity ranking can be translated to a configuration within Qualys.

Next, we will understand the various factors that impact report data which include authentication, configuration changes and other environment specific factors.

In the following topic we will discuss the best practices and recommendations for getting clean data for reporting by using appropriate house keeping options and maintaining good purging practice to remove stale data from the environment.

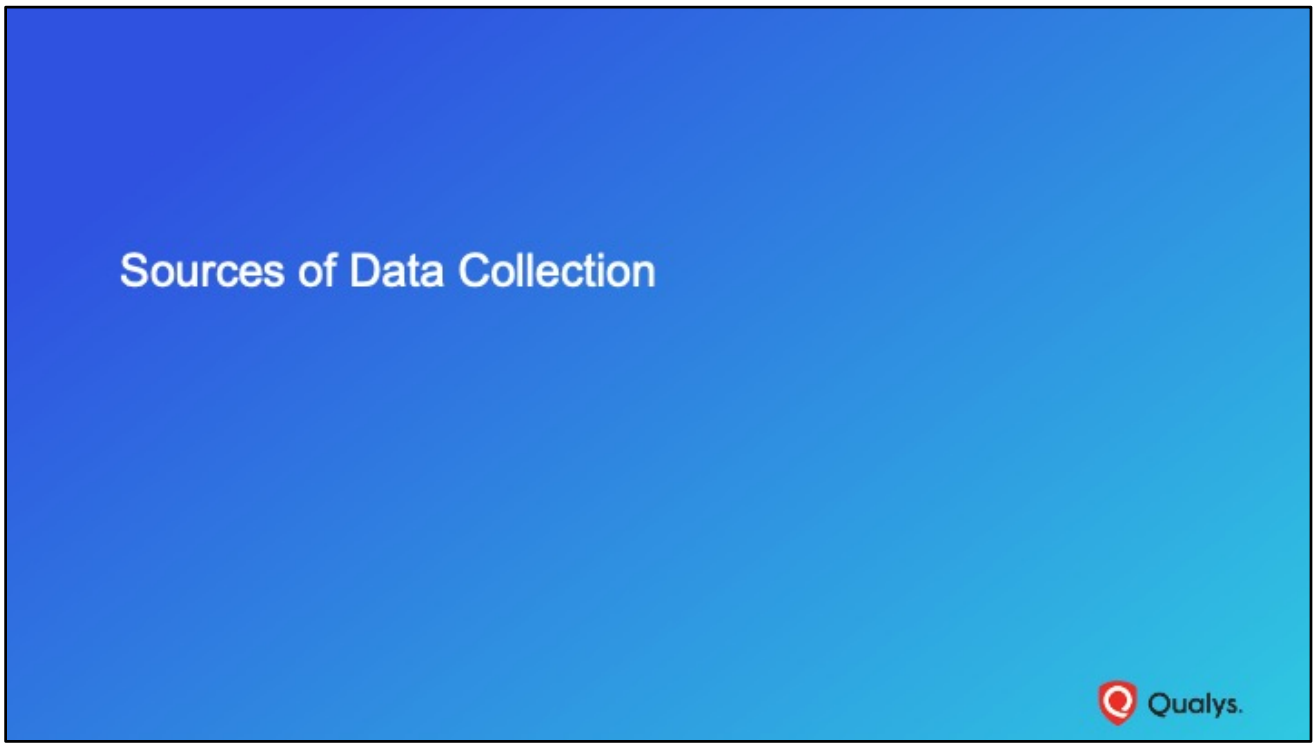
Moving further, we will talk about the use cases and best practices concerning interactive reporting tools such as dashboards, widgets and queries with an emphasis on the VM/VMDR dashboard, Unified dashboard (UD) and the Qualys threat protection application.

Next, we will talk about the best practices applicable to UI based vulnerability reporting. Then we will discuss how to configure VM report templates, the different types of findings that can be included in a template and the different options and filters that can be configured in a template to tweak the output that is shown in a report. Further we will discuss some of the available report types such as Authentication report, Patch report and Scorecard report and understand how to distribute reports to different users.

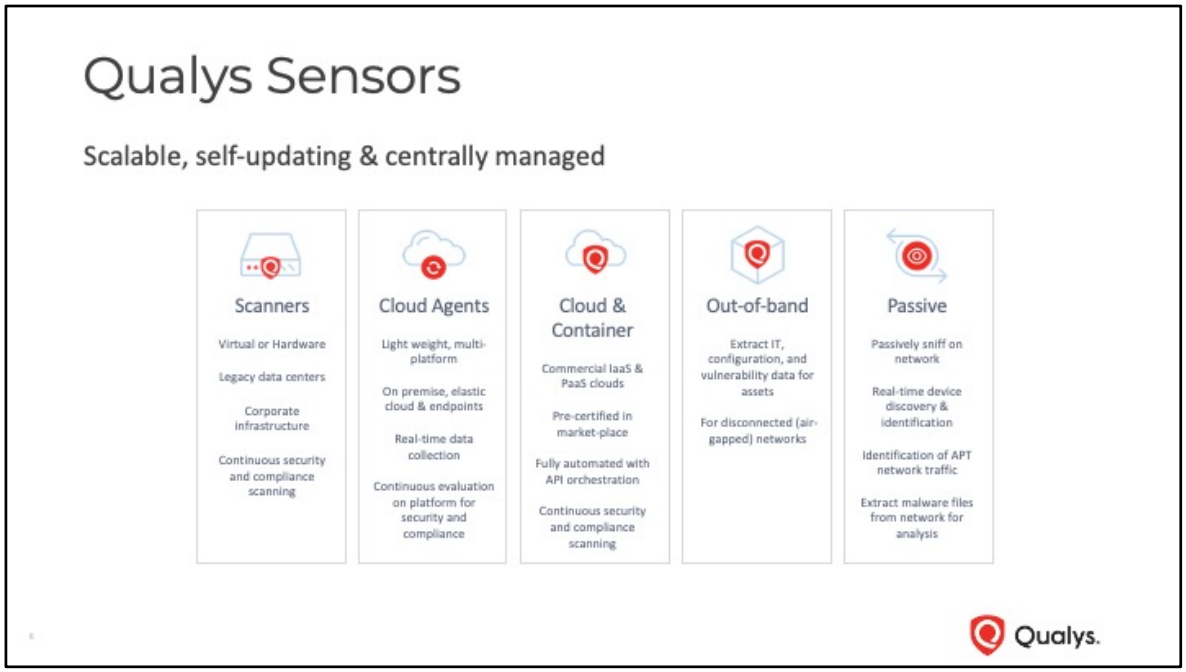
Next, we will talk about managing exceptions using remediation policies in vulnerability management.

We will then consider a few scenarios where you can apply some of the concepts covered in this training to generate appropriate reports.

Finally, we'll finish the course with a checklist or a summary of all key points that you need to consider for an effective reporting strategy.



This section covers the different data collection mechanisms used by Qualys.

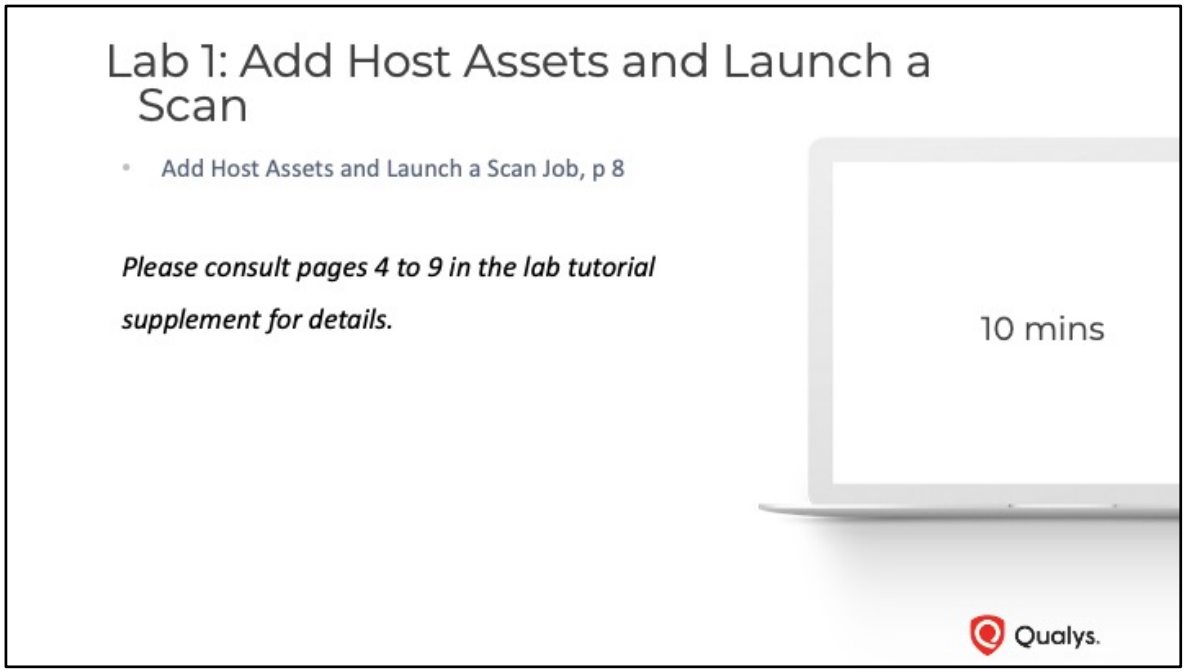


Qualys has various sensor types that collect data for you.

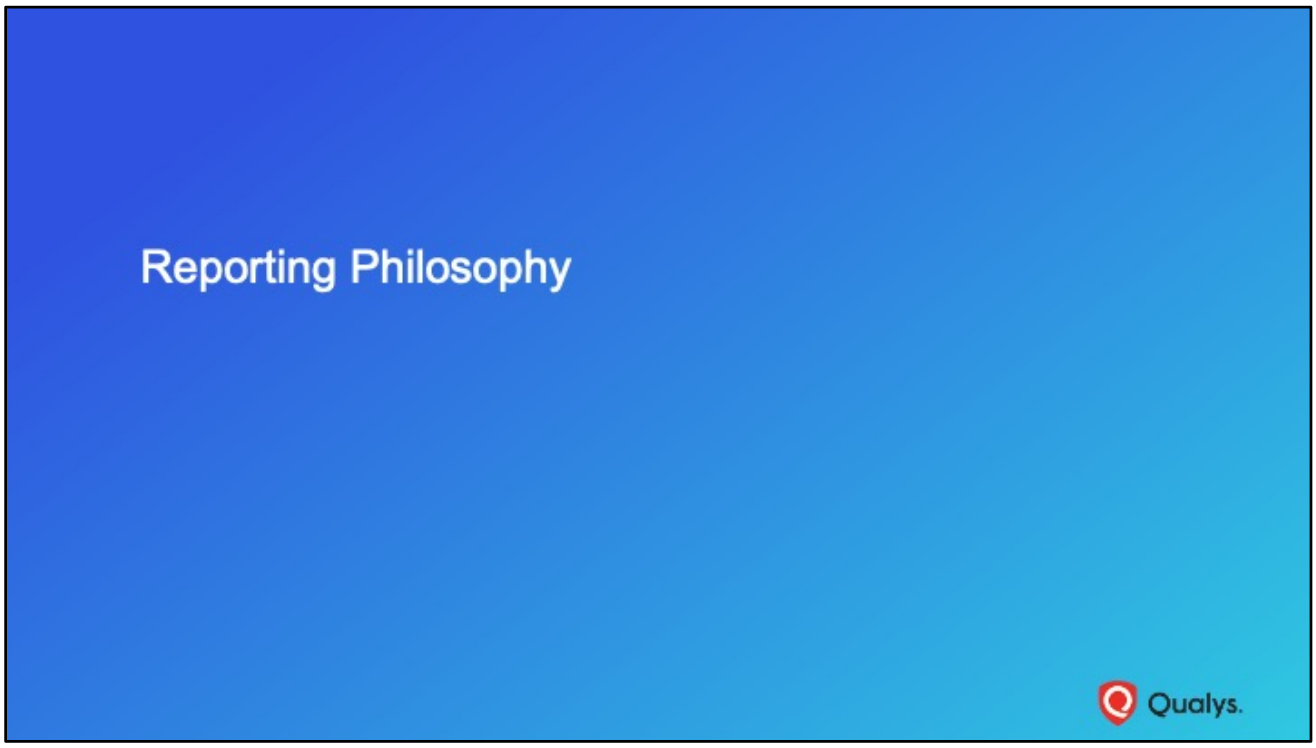
Scanner Appliances: Intranet and internal scanners, physical or virtual, used to scan on-prem or cloud assets.
Cloud Agent: lightweight agents that can be installed on clients and servers for real-time visibility. Ideal for assets with dynamic IP, remote/roaming users, ephemeral cloud instances, and systems sensitive to external scanning.
Cloud Connectors: collect metadata from cloud platforms such as Amazon Web Services, Microsoft Azure and Google Cloud Platform.
Passive Sensor: Available as physical or virtual appliance, continuously monitors all network traffic, profiles devices and flags any asset activity.
Container Sensor: Available as an image for Docker-based containers, designed to discover, track and continuously secure containers – from build to runtime.
Out-of-band Sensor: Out-of-band configuration assessment helps you extract IT, configuration, and vulnerability data for assets deployed on disconnected (air-gapped) networks.

The Qualys Sensors are all populating the the platform with your inventory, vulnerability, threat, compliance, cloud, and web app data. This gives you your data in one place.

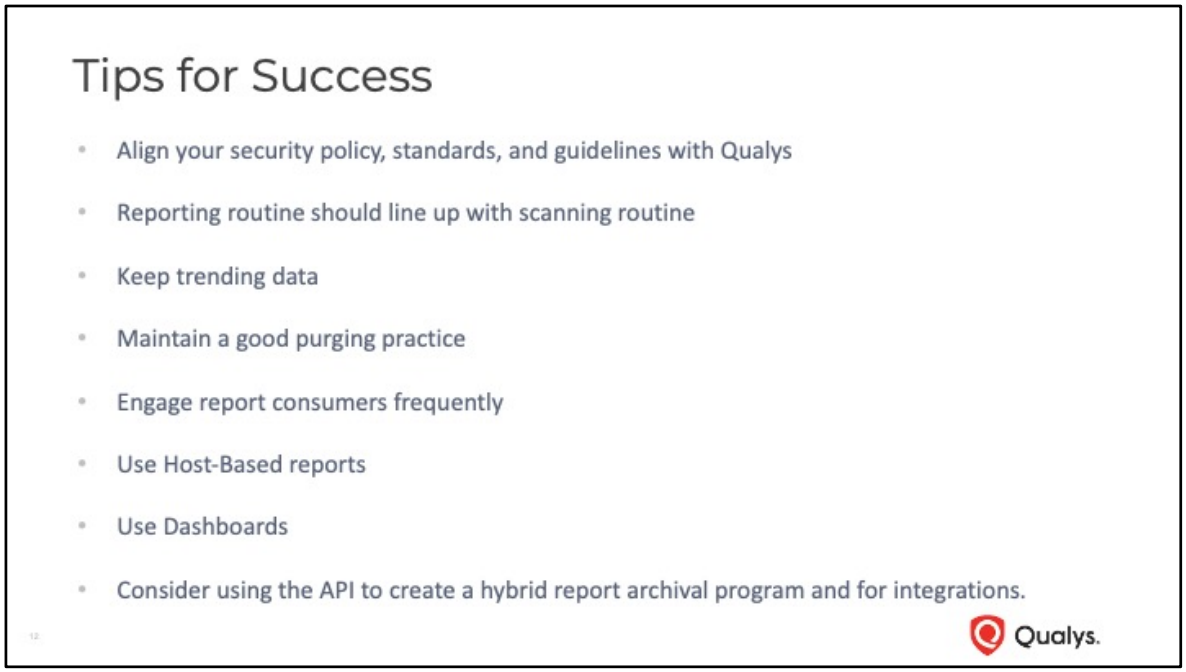
This is where the conversation on reporting starts. We are taking data that is already in the Qualys platform, and we are viewing it in different ways.



- You will add assets to your Qualys account, create Asset Groups, setup Authentication Records, and perform an authenticated scan.
- Nice review of the VM course and it serves as the foundation for Reporting that this course needs.
- Follow narrator closely if you haven't taken the VM course.
- To build reports you need to get assessment data first.
- This can be from scanning hosts or deploying Cloud Agents.
- Cannot get to reporting or building dashboards-widgets until you have some data to work with.

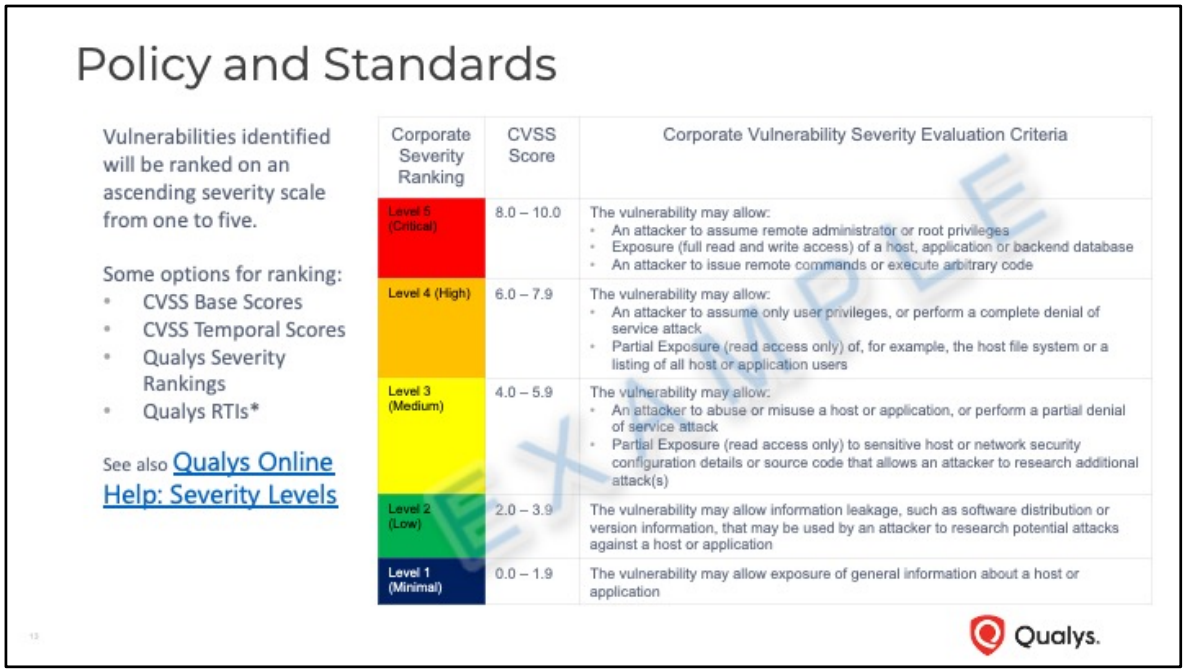


This section provides an overview of the basic concepts and components needed to build custom reports in the Qualys Vulnerability Management application.



Some tips for setting up reporting:

1. Make sure your Qualys report setup is aligned with what is defined in your organization's security policy. For example, Confirmed, Severity 5 Vulnerabilities in External (Public Facing) and DMZ (serving public assets) subnets must be remediated in 5 business days vs. Confirmed, Severity 5 Vulnerabilities in Internal server subnets must be remediated in 10 business days.
2. Scheduling – Your report frequency should align with your scanning routine. For instance, if you scan weekly, report weekly.
3. Try to keep a reporting practice that is ongoing for good trending data. If you change often, this will be hard to measure.
4. Purging – More on this later. If you aren't purging, you have stale data.
5. Keep engaged with your audience – Talk to consumers of reports so you know they are getting what they need.
6. Focused Host Based reports are much more efficient than Scan Based reports.
7. Use dashboards - Dashboards are interactive reports…so there's no need to change the approach between traditional reporting and dashboarding schemas.
8. API – Use API for having a report archive program.

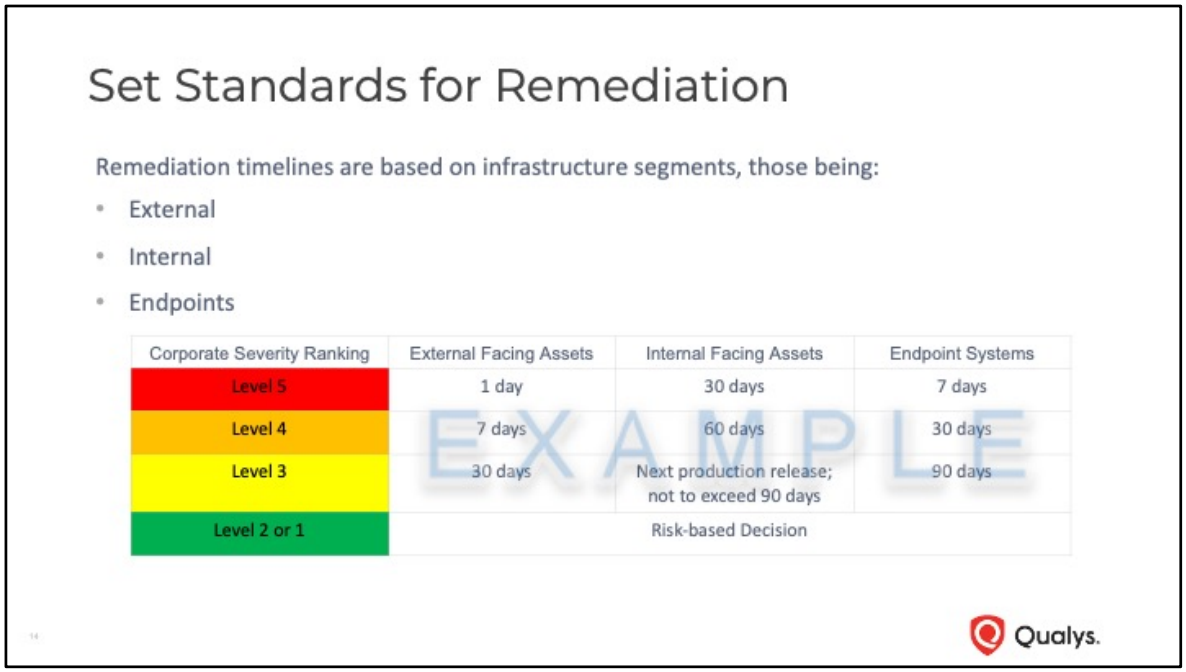


Qualys services a plethora of business types, Federal, Medical, Energy, Consumer Packaging, etc., meaning different lines of business are subject to different regulatory requirements. Qualys Severity and Detection Type is proprietary and meant to help those businesses that may not have a mature program to get something up and running.

There are various other ways by which vulnerabilities may be ranked and prioritized. This includes CVSS scores, Real-time Threat Indicators (aka RTI's),etc.

It is important that you align your corporate severity ranking mechanism to one of these methods. This will allow you to have a consistent, org-wide security policy for dealing with vulns.
One way to do this is by using CVSS scores.
For example, CVSS score 8.0 and above may be classified as Level 5 (Critical).
Similarly, Levels 4 (High), 3 (Medium) , 2 (Low) and 1 (Minimal) are mapped to the corresponding CVSS scores, as shown in the slide.
Qualys supports CVSS Version 2 and CVSS Version 3. Please consult https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/knowledgebase/cvss.htm for more information on CVSS scores.

Alternatively, you may also map your corporate severity rankings to Qualys severity ratings.
For example, Qualys Severity rating 4 and 5 corresponds to High, 3 corresponds to Medium, and1 and 2 corresponds to Low.



It's important that organizations set standards for driving remediation.

Severity and threats to organization, play a part. Remediation for certain types of vulnerabilities should be prioritized. This is based on highest attack surface and severity.

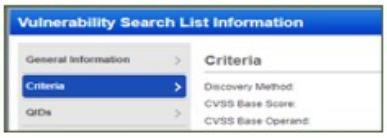
It's equally important to consider the asset context when prioritizing remediation. For instance, your external assets with high severity vulnerabilities are going to have a high priority. We are using Level 5 here as the highest severity, but this could also include your threat protection RTIs.

Your endpoint systems may also have a high priority as they can be "on an island all by themselves."

Aligning with Corporate Policies and Standards

Question: How do I select specific types of vulnerabilities based on corporate severity rankings?
Answer: Qualys Search List

Corporate Severity Ranking	CVSS Score	Corporate Vulnerability Severity Evaluation Criteria
Level 5 (Critical)	8.0 – 10.0	The vulnerability may allow: • An attacker to assume remote administrator or root privileges • Exposure (full read and write access) of a host, application or backend database
Level 4 (High)	6.0 – 7.9	The vulnerability may allow: • An attacker to assume only user privileges, or perform a complete denial of service attack
Level 3 (Medium)	4.0 – 5.9	The vulnerability may allow: • An attacker to abuse or misuse a host or application, or perform a partial denial of service attack

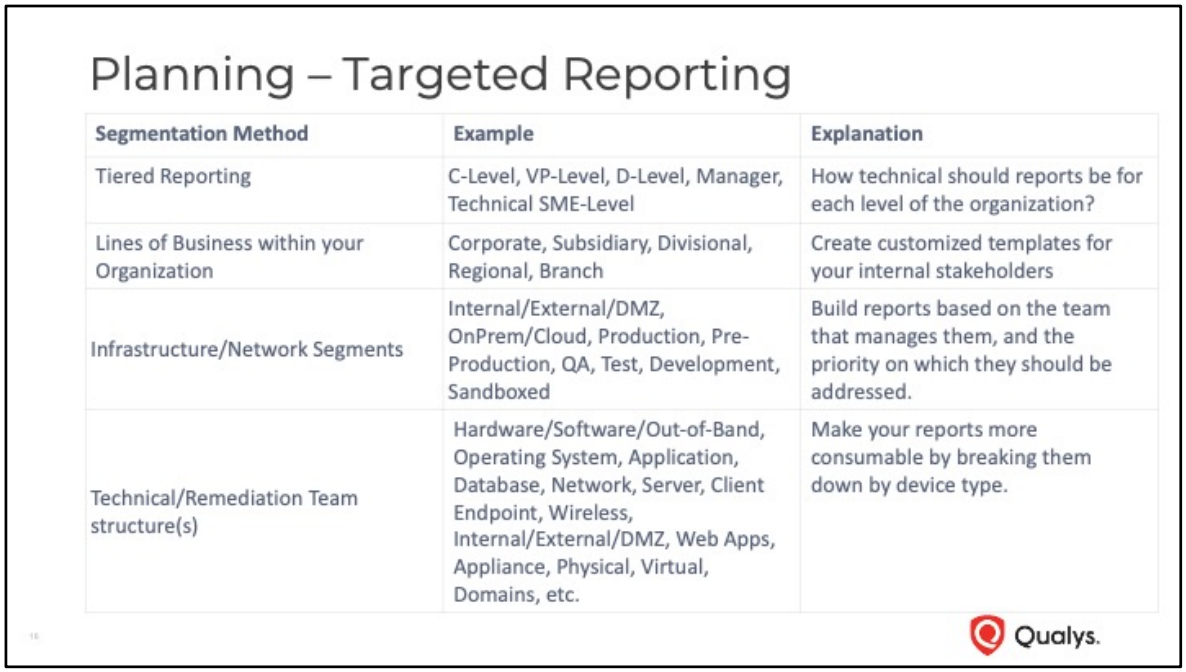


Qualys.

You want to align your Corporate Policy with what you are doing in Qualys.

In the example above, let's say you are ranking your vulnerabilities by severity and CVSS. Maybe you are using base scores for external and temporal scores for internal because they depend on environment. You then want to build your search lists that are relevant for the types of reports you are creating for each type of asset, internal vs external vs endpoint.

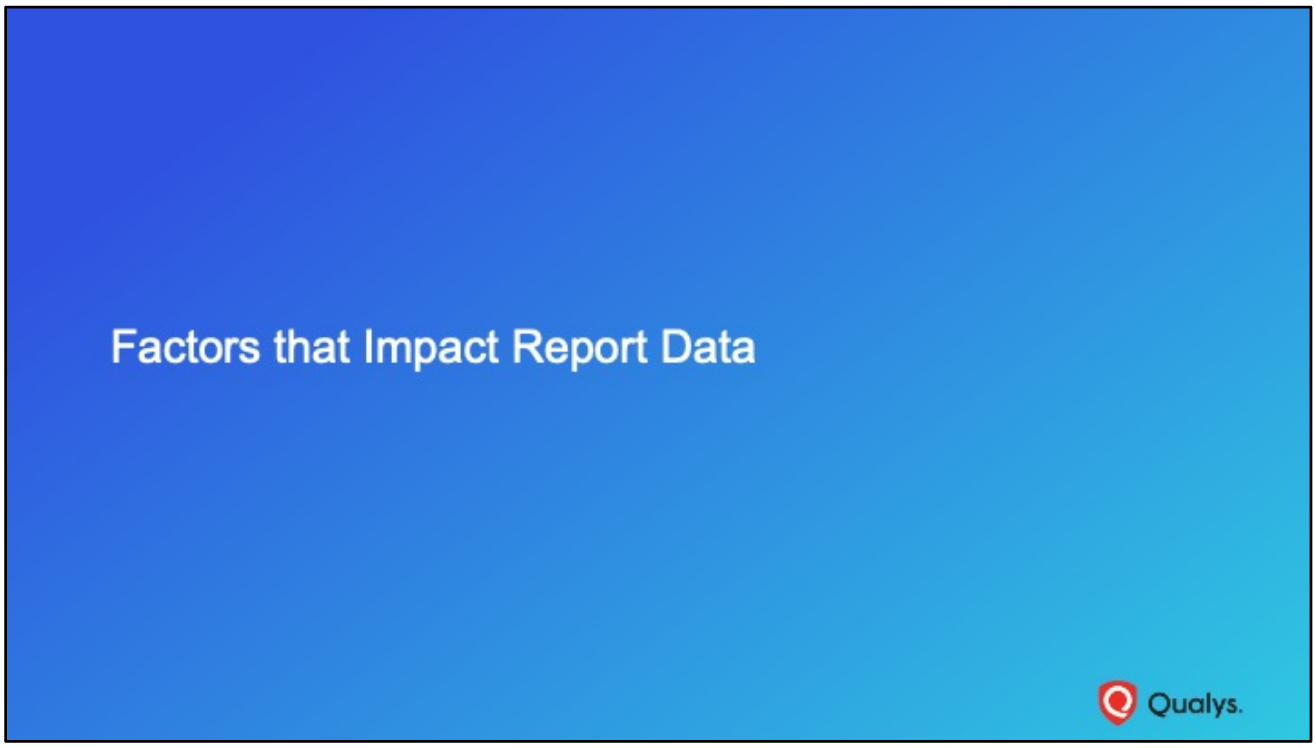
You could also do this using Threat Protection RTIs.



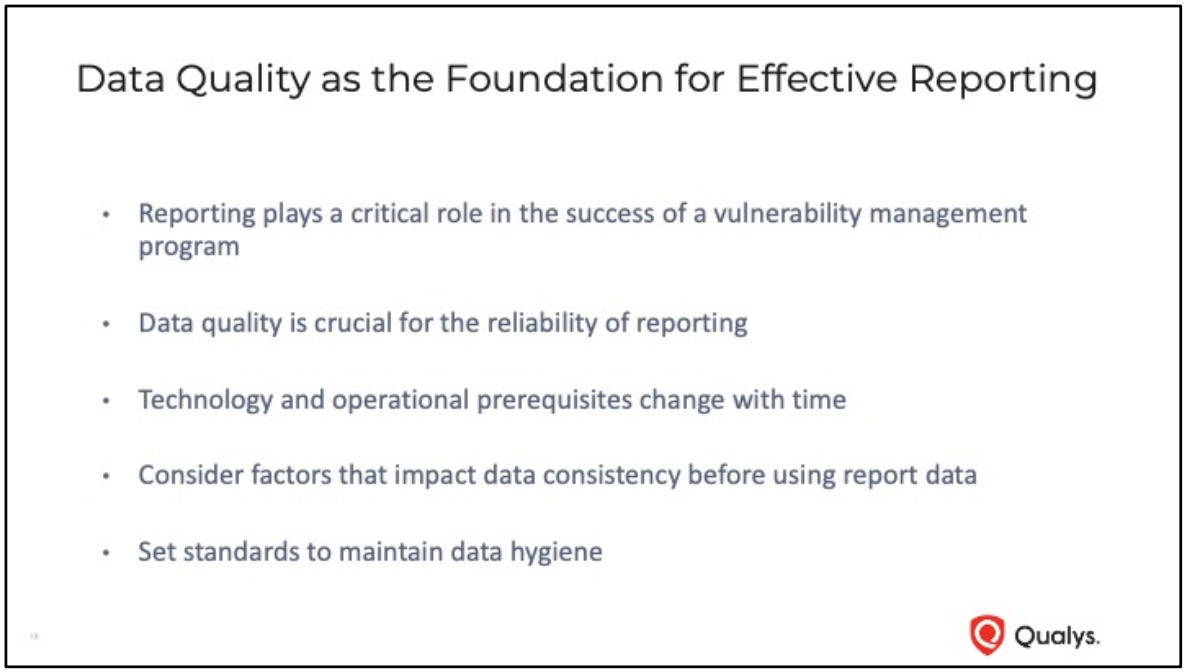
When planning your reports in Qualys VM/VMDR, first make sure you understand which levels of the organization need to see reports and what they need to see. For example, does a C-level need to see the specific patch needed for all of your Windows workstations? Or do they want to better understand the overall risk posture.

Next, consider lines of business. Should they have their own separate reports?

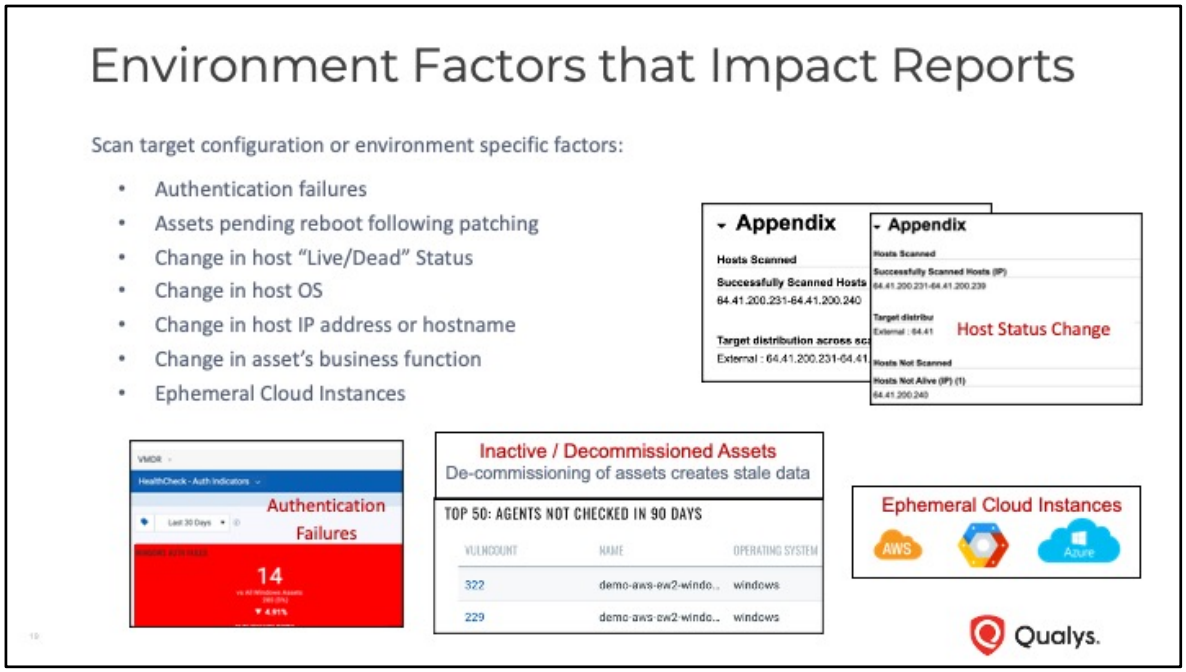
Infrastructure/Network Segments: Separate Cloud assets from On-Prem assets. You might also separate by device type to gain an understand how a certain type of asset has a risk associate with it.



This section outlines some of the factors that impact report data, and which must be considered before using report data for analysis and decision making.

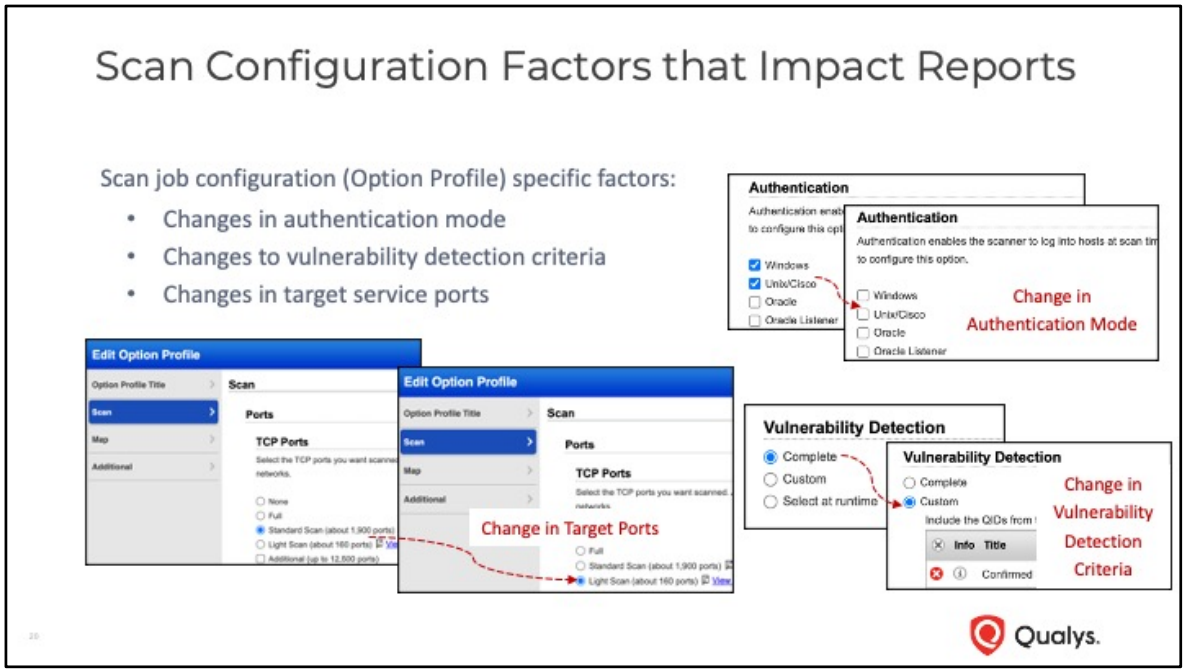


Reporting is a critical aspect of any VM program as it drives decision making and strategy building. And Data quality is crucial to the reliability of business analytics / reporting. Technology and operational requirements change over time and these factors impact report data in different ways. So, it is important to understand these factors and set appropriate processes and standards in place to maintain data hygiene.

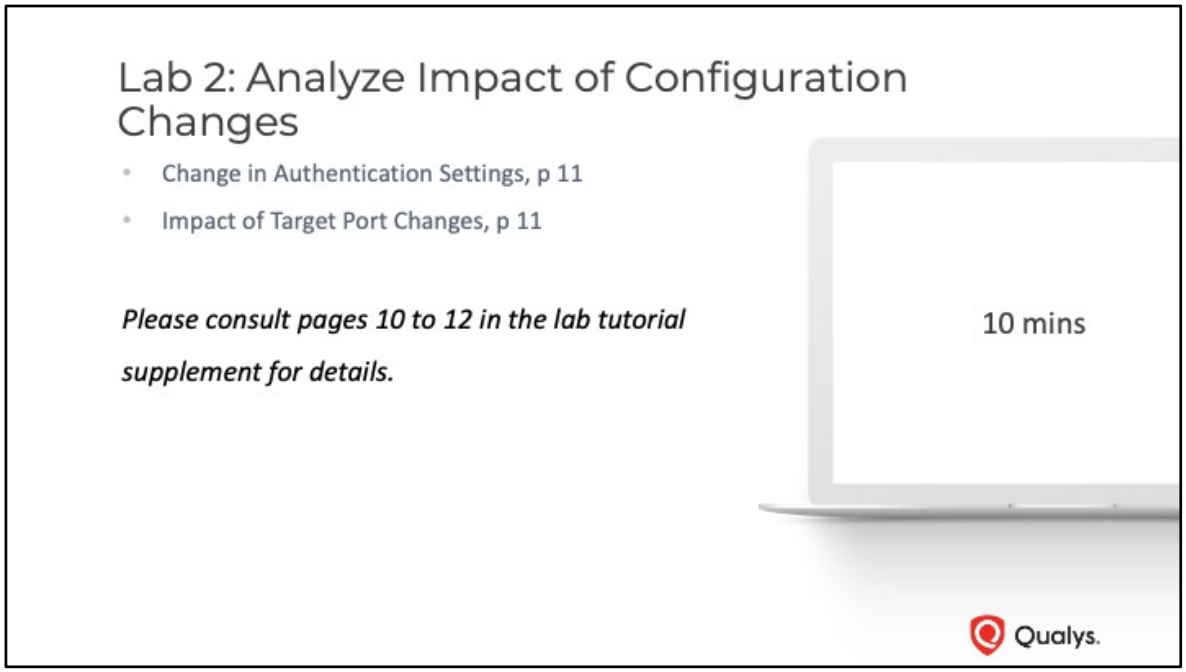


This slide outlines some of the factors that impact report data. Changes to host IP address and/or hostname are common. And then there may be changes to the authentication setup or other environment issues that may impact existing authenticated scans. Also Assets are decommissioned at the end of their asset lifecycle or used in a completely new role. These changes can result in stale and inconsistent vulnerability data in your account. And sometimes the asset may be pending reboot following a security patching exercise. In this case the vulnerability continues to be flagged as open or active even though it has been fixed as the changes will only take effect after a reboot.

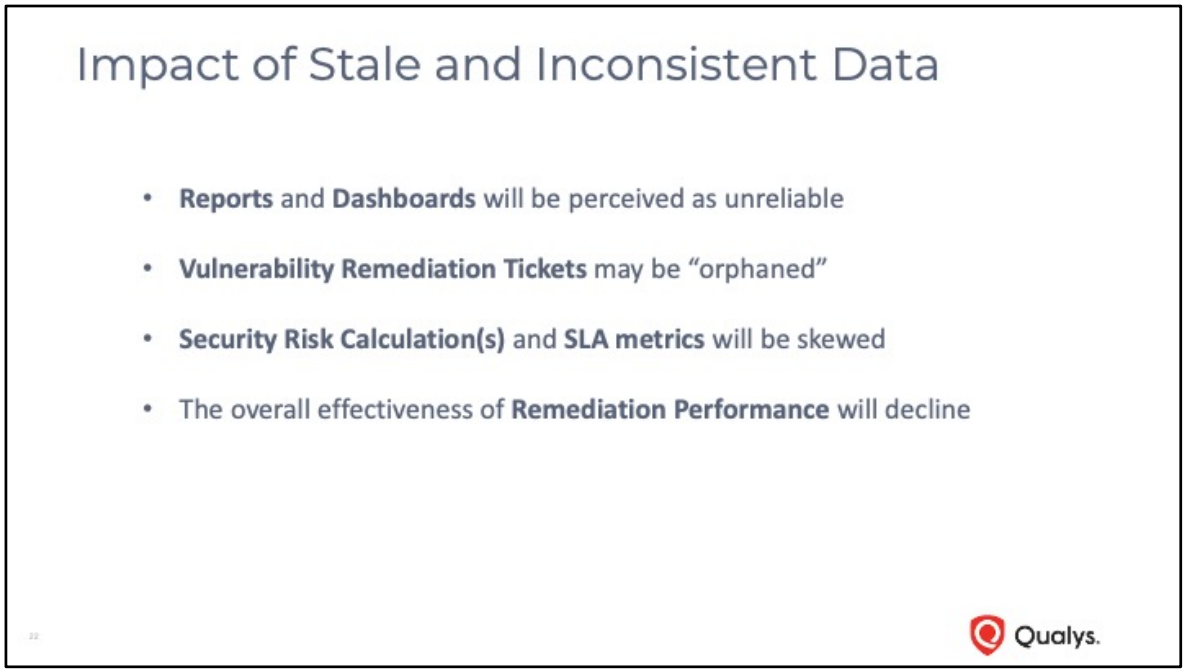
Lastly, the ephemeral nature of assets deployed in the cloud can generate lot of stale vulnerability data in your Qualys account.



In addition to environmental changes, frequent scan job configuration changes also impact data consistency. Changes to authentication mode, target ports for scanning and vulnerability detection criteria can all lead to data inconsistency issues. Vulnerabilities that are no longer targeted due to change in authentication settings, target ports or vulnerability detection criteria will continue to remain open forever thus impacting remediation SLAs and also the overall reporting strategy.



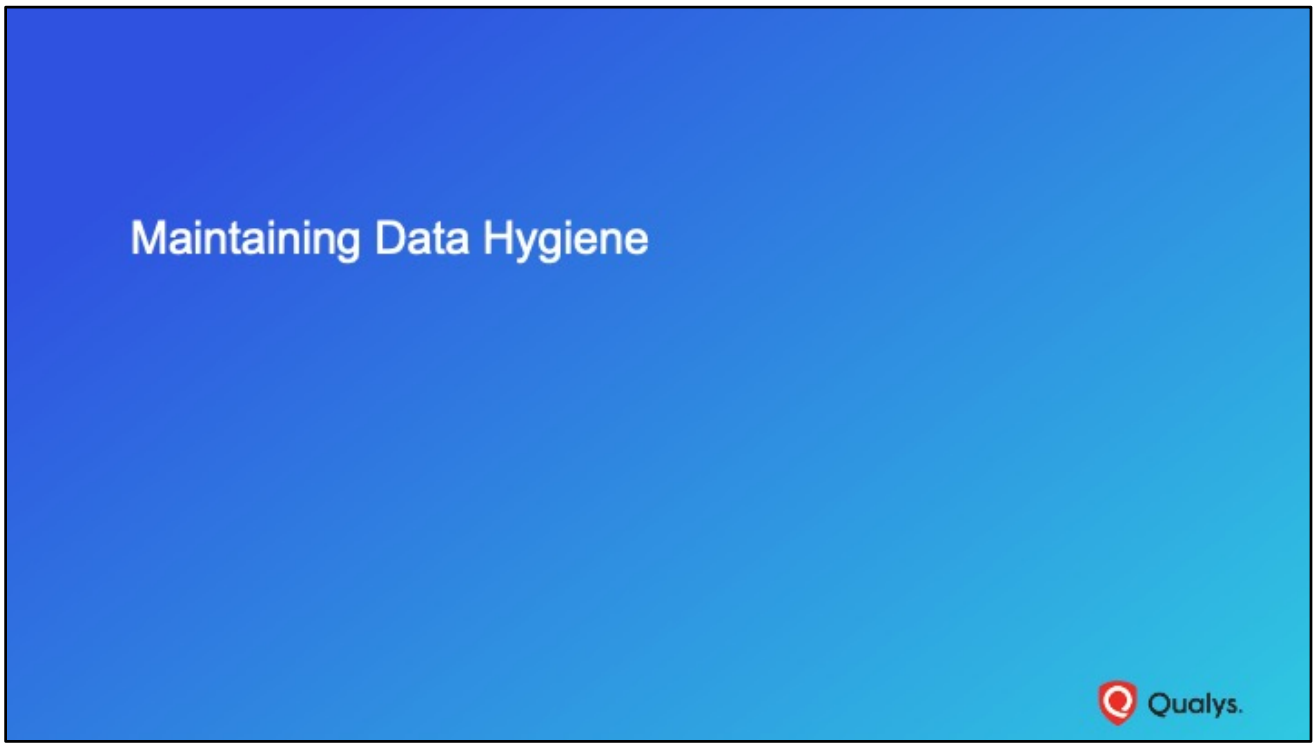
- 2 activities in this lab.
- Activity 1, it shows a specific QID that needs a trusted scan to discover. Then it will show what happens if you run a scan without authentication.
- It could be the case that authentication changes scan-to-scan. This can lead Qualys to report vulnerability data that is not complete.
- In activity 1 the QID could have been patched just before the untrusted scan and you wouldn't know it.
- Activity 2, a vulnerability gets discovered on port 8443.
- In that second scan, 8443 is not in the Option Profile which also shows that inconsistencies can occur scan-to-scan.



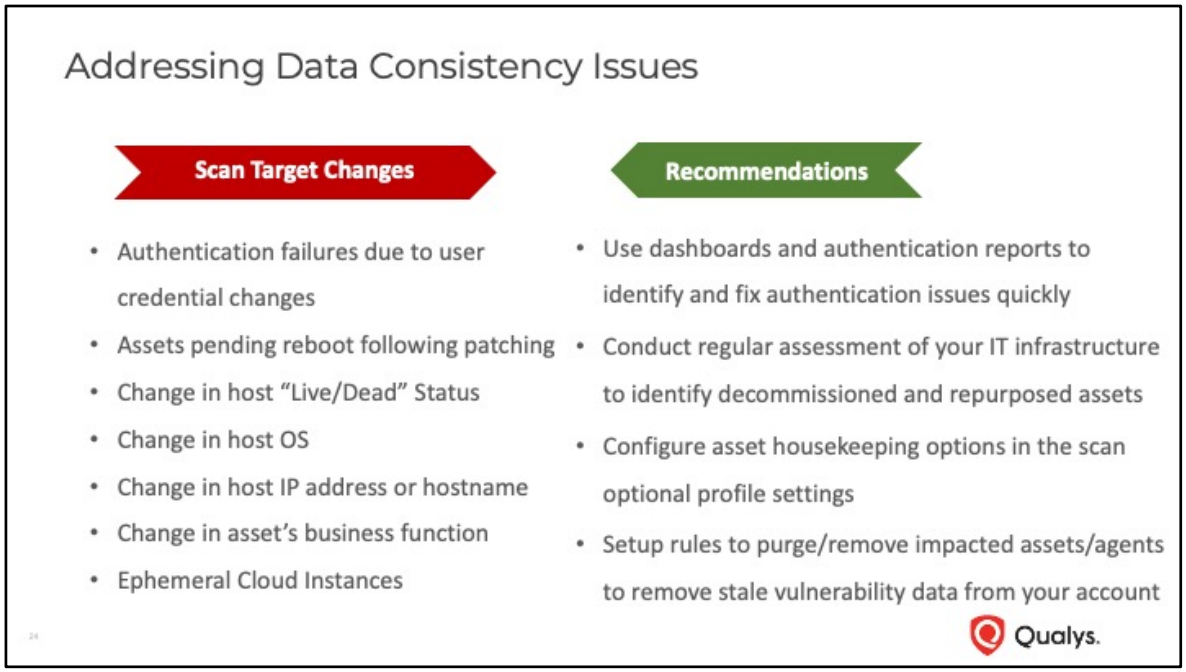
So, it is clear that Without proper asset housekeeping processes in place, you will have stale and inconsistent data in your account that will impact dashboards and reports.

Moreover, if the stale asset continues to remain in your subscription and the associated IP/hostname has been assigned to another asset, when new findings come in, it will result in inconsistent scan reports.

Vulnerability tickets of the stale asset will continue to remain open affecting your risk calculation and SLA metrics. Remediation performance will be impacted too.



This section provides some recommendations to maintain data hygiene in your environment to generate consistent and reliable reports.



As discussed in the previous topic, authentication failures, assets pending reboot, change in hosts' live dead status or change in IP address or hostname, etc. impact report data. So it is important to assess these factors and take appropriate measures to maintain data hygiene. "

Dashboards and authentication reports can help you identify and fix authentication issues. You can also use dashboards to identify assets pending reboot.

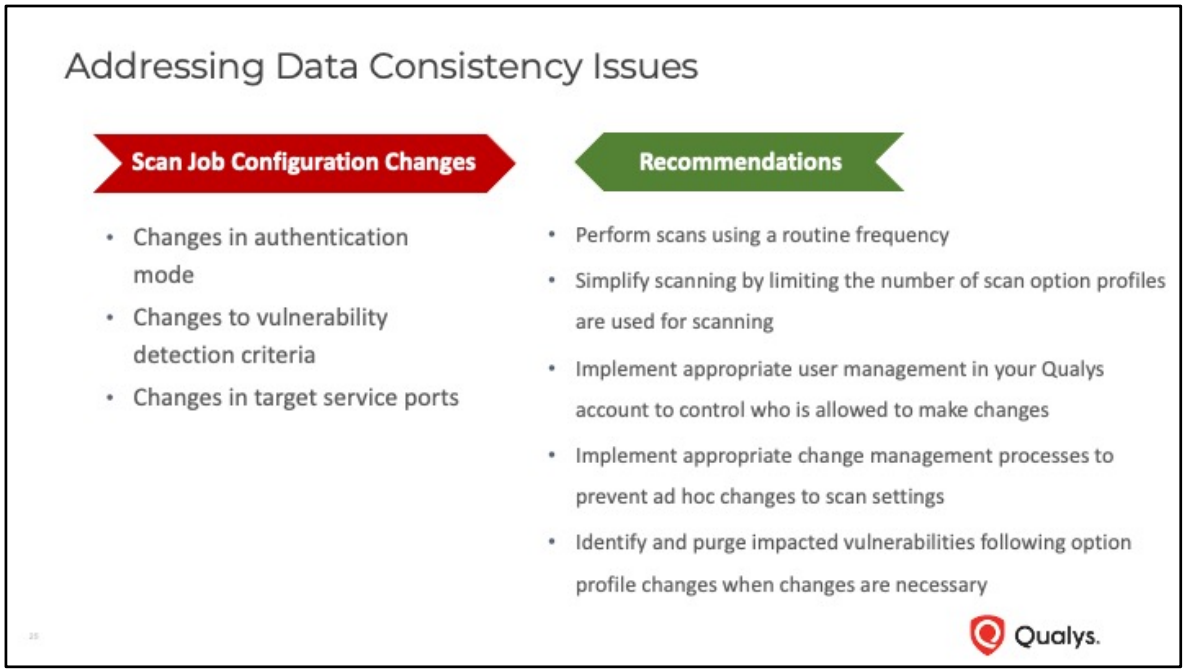
It's recommended that you track and classify assets throughout their lifecycle. Conduct regular assessment of your IT infrastructure to identify decommissioned, inactive and repurposed assets. Consider the use of Qualys asset tagging feature to automate this classification where applicable.

Qualys also provides asset housekeeping options within the scan option profile to manage stale data from "dead" or inactive assets and assets with major changes to their OS. Consider using these options where applicable.

In all scenarios where automatically deployed assets are spun up, you must also consider the automated process of purging or removing them from your Qualys

account. You can setup purging rules to automatically identify stale and inactive assets and remove stale data from your account.

Being proactive in addressing factors that cause data inconsistency will save you time, resources and hassle in the long run.



Again, as discussed previously, scan job configuration changes such as changes to authentication mode, or vulnerability detection criteria or target service ports, also impact report data. So, maintaining good data hygiene is also about implementing the right scanning strategies and best practices. It's important that your scanning configuration is aligned to your organization's standards and policies.

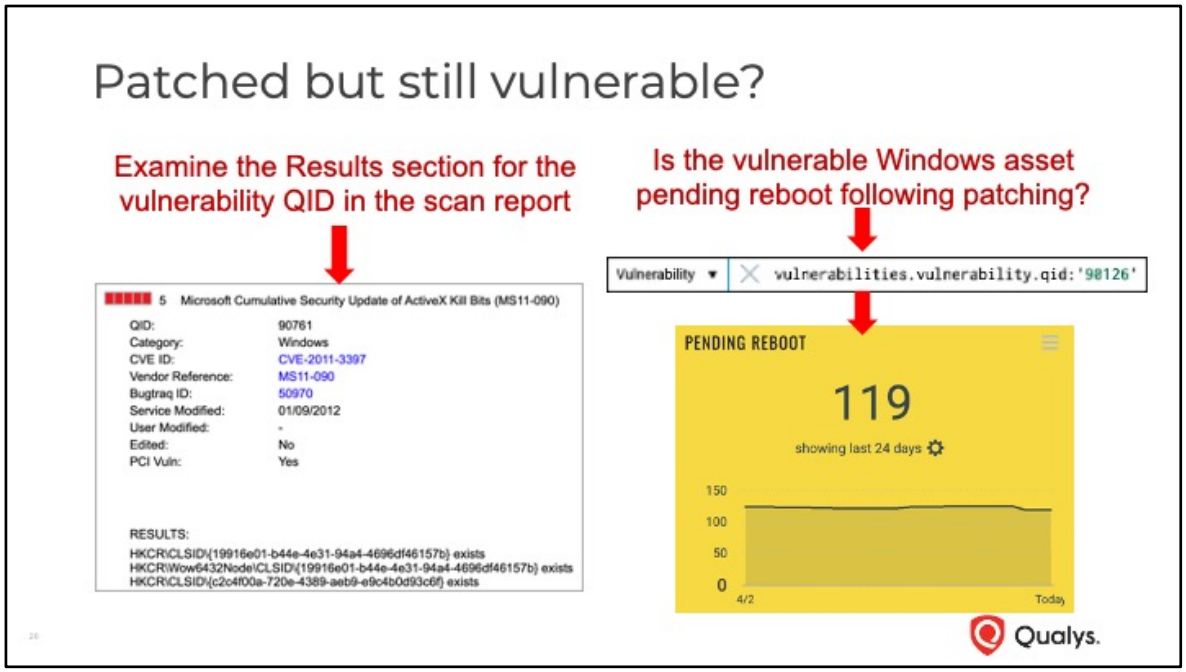
We recommend that you scan regularly to get a more up to date and consistent vulnerability posture of your assets.

Also simplify scanning by limiting the number of option profiles configured in your account.

We recommend that you setup appropriate user roles in your Qualys account to restrict who is allowed to make changes to the option profile settings. It is also important to apply appropriate change management policies to your scan job configuration to prevent ad hoc configuration changes.

When scan configuration changes cannot be avoided due to change in corporate stance on vulnerability assessment, you need to identify impacted vulnerabilities and

consider purging s such vulnerabilities.

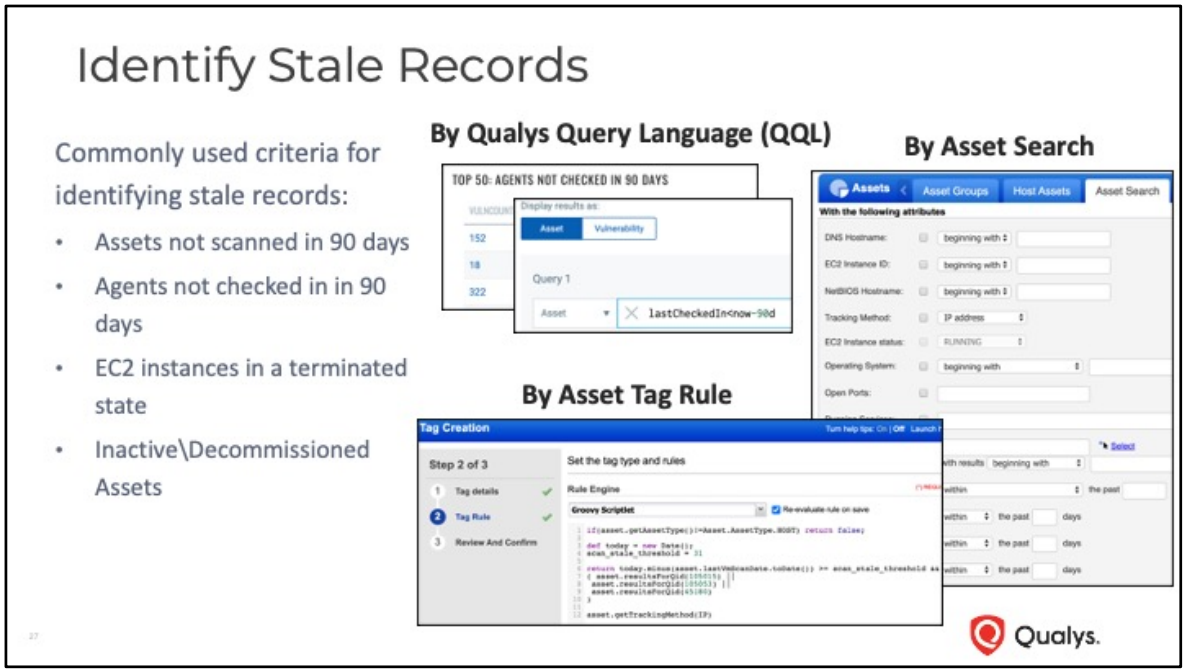


At times, you'll find patched vulnerabilities still appearing in your scan results and reports. This happens for various reasons, like old registry keys, DLL or temp files, pending reboot etc.

To investigate why the vulnerability is still being flagged, open your Scan Results, and look at the Results section of the QID in the scan results or report.

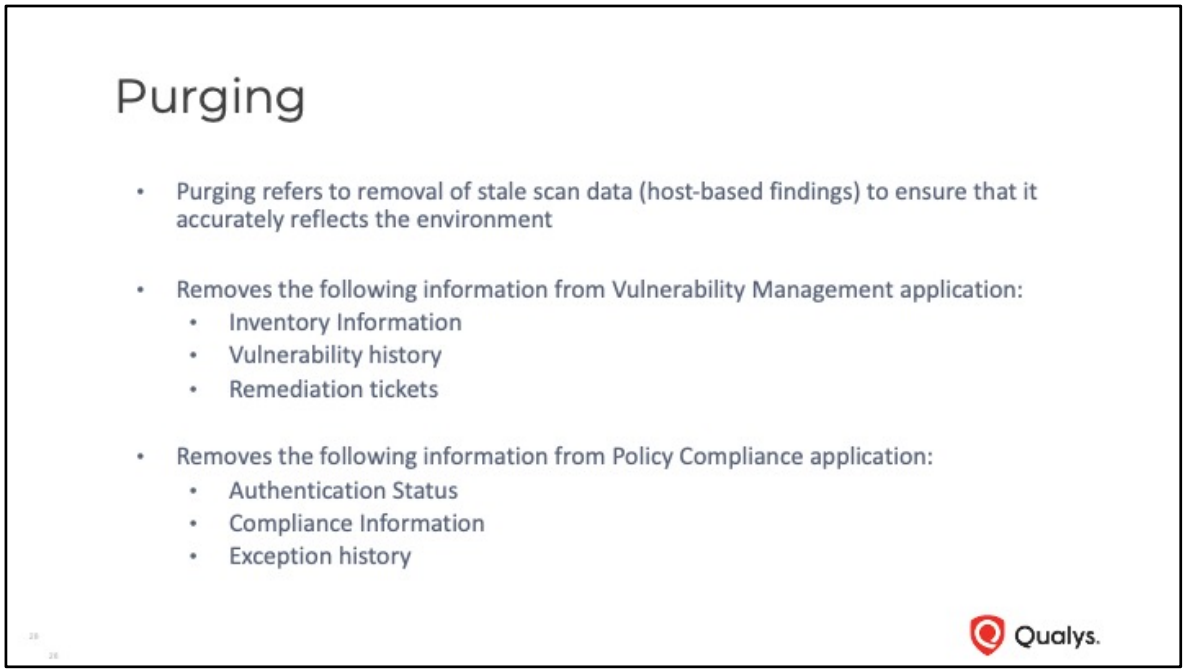
Also identify if such hosts are pending reboot following patching. QID 90126 can be used to build a dashboard widget or added to a Search List as a filter to identify such assets pending reboot. Note that you must perform authenticated scans to accurately identify hosts that are pending reboot using this QID.

Lastly, keep in-mind that discrepancies in your vulnerability findings can be resolved by performing an additional scan. When analyzing such discrepancies, compare the "last detected" date of the suspect finding to the date of your report. Wide gaps between the last detected date and the report date could be an indicator that an additional scan is required.



There could be several criterial used to identify stale records. Common ones include assets that haven't been scanned for a certain no of days, AWS EC2 instances in a terminated state, inactive or decommissioned assets, etc. Once assets are identified and validated, you can purge such assets via the Qualys UI or API.

You can search for such assets using Asset Search in the VM/VMDR application . You can also use search queries to search for required assets or build dashboard widgets to identify assets for purging. You can also build widgets using search queries to automatically identify assets for purging. Lastly, you can also use asset tag rules to automatically identify and tag assets for purging.



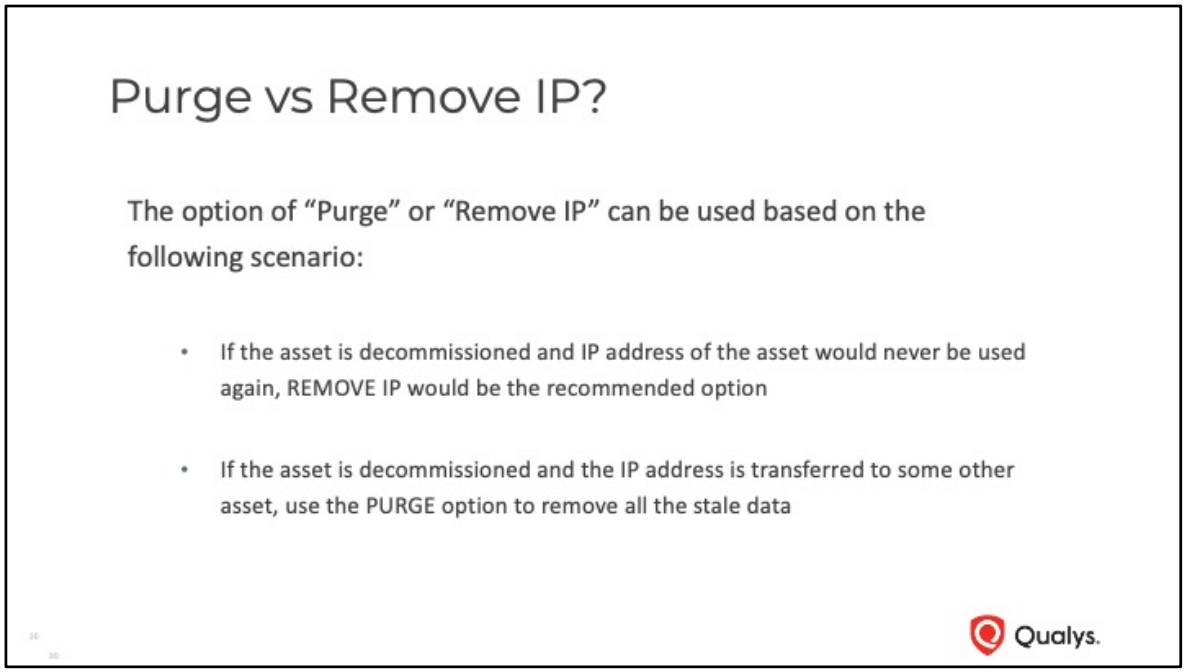
Purging refers to the removal of stale asset data from your Qualys account. Purging is required when a host is decommissioned or used in a completely new role - new operating system, new applications, new purpose. Purging becomes very important in highly dynamic and ephemeral environments where assets are replaced or deleted very frequently such as in Cloud provider environments.

When a host is purged in the Vulnerability Management application, it causes asset inventory, vulnerability, and remediation information to be removed.

When a host is purged in the Policy Compliance application, it causes authentication, compliance and exception history information to be removed.

Purging: What, why, when, how, what happens to the data?
https://success.qualys.com/discussions/s/article/000006221

- Activity 1 you are going to Purge for single and multiple hosts.
- The asset remains in your subscription, but the data for it is removed.
- This is irreversible because you are clearing the host-based bucket that Qualys maintains.
- The data will have to be rebuilt from future scanning.
- Activity 2, you are going to Remove the host asset from your subscription.
- It will remove the host from authentication records as well as the host-based findings data (like purge).



While purging allows you to retain the IP in your subscription and delete the associated data from your subscription, removing the IP causes the IP and associated data to be deleted from your subscription.

Purging is recommended when the IP has been reassigned to another asset or the asset has been assigned to another role.

Removing is recommended when you no longer to the scan the IP. In practice, removing an IP is seldom used, as in most cases the same IP is reused and assigned to another asset. So, purging the IP is better suited for most scenarios. This way when a new asset is assigned the IP of a decommissioned asset, you don't need to add the asset again to your Qualys account to scan it.

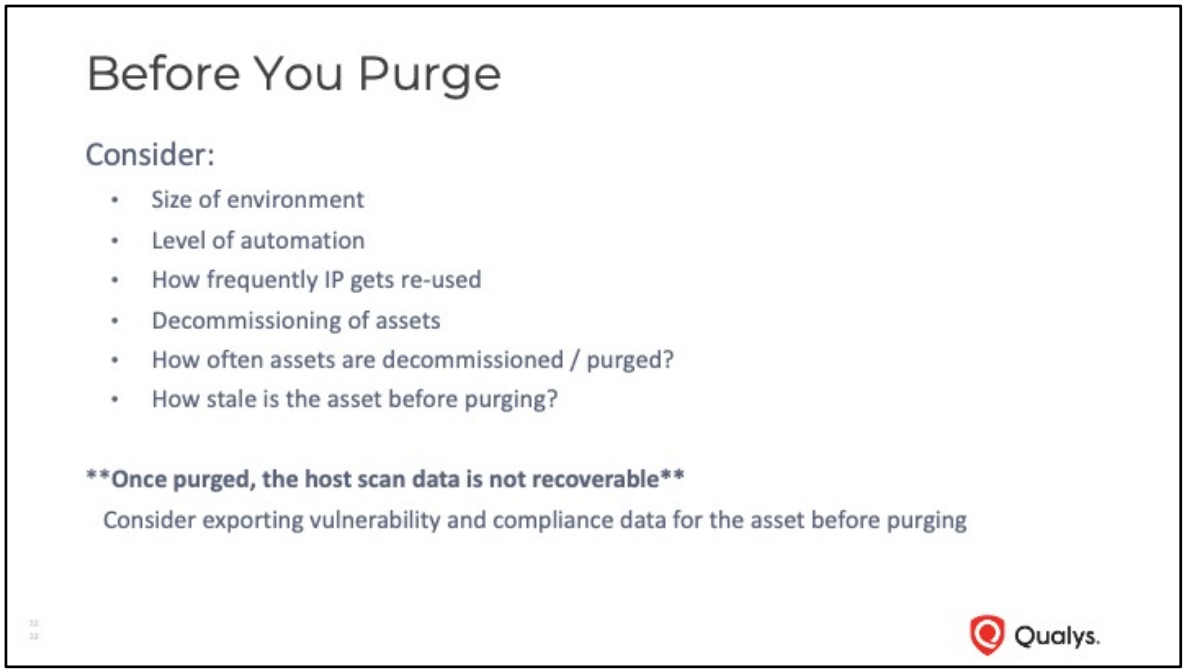
Impact of Purging vs Removing an Asset

Impacted Entity	Purge	Remove
Inventory Information	Deleted	Deleted
Vulnerability History	Deleted	Deleted
Remediation Tickets	Deleted	Deleted
Comments	No change	Deleted
Host Assets	No change	Deleted
Asset Groups	No change	Deleted
Authentication Records	No change	Deleted
Scan Findings	No change	Deleted
Scheduled Scans / Reports	No change	No change
Global Exclusion List	No change	No change

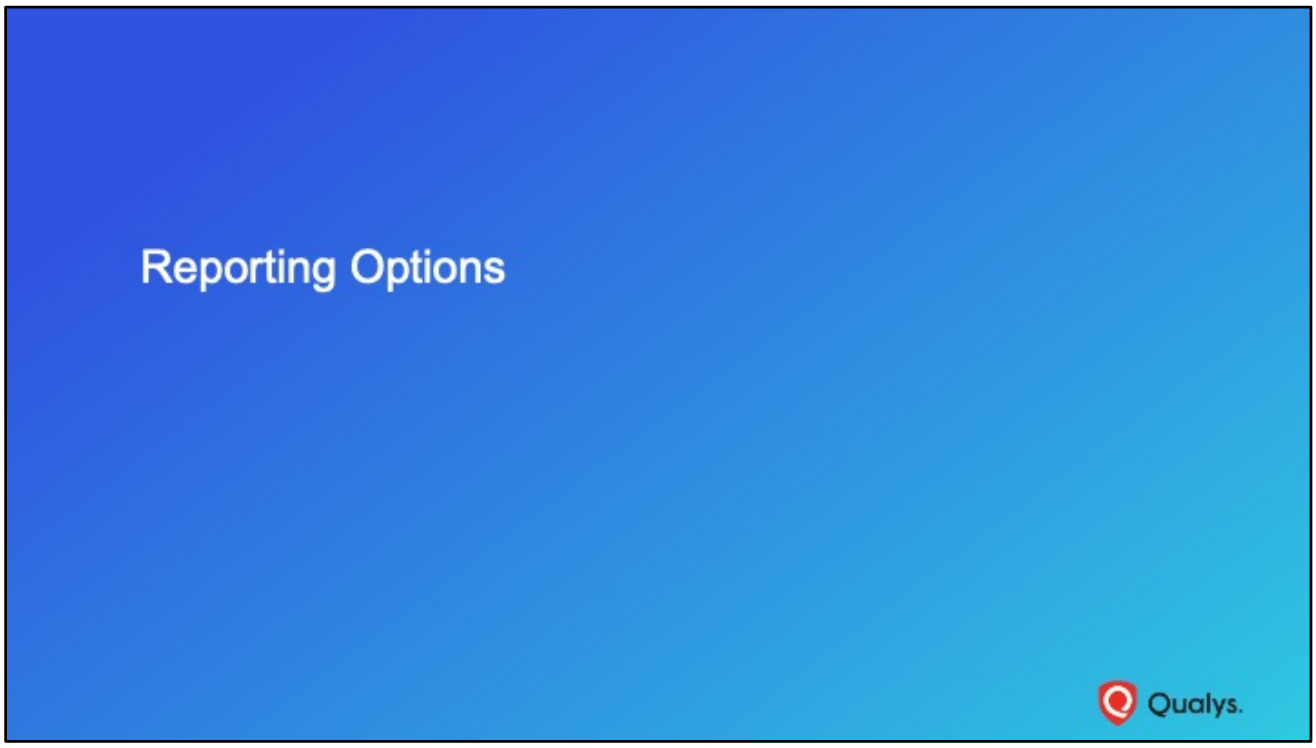
Qualys.

When a host is purged, it causes inventory, vulnerability and remediation ticket information to be deleted. All other information is retained.

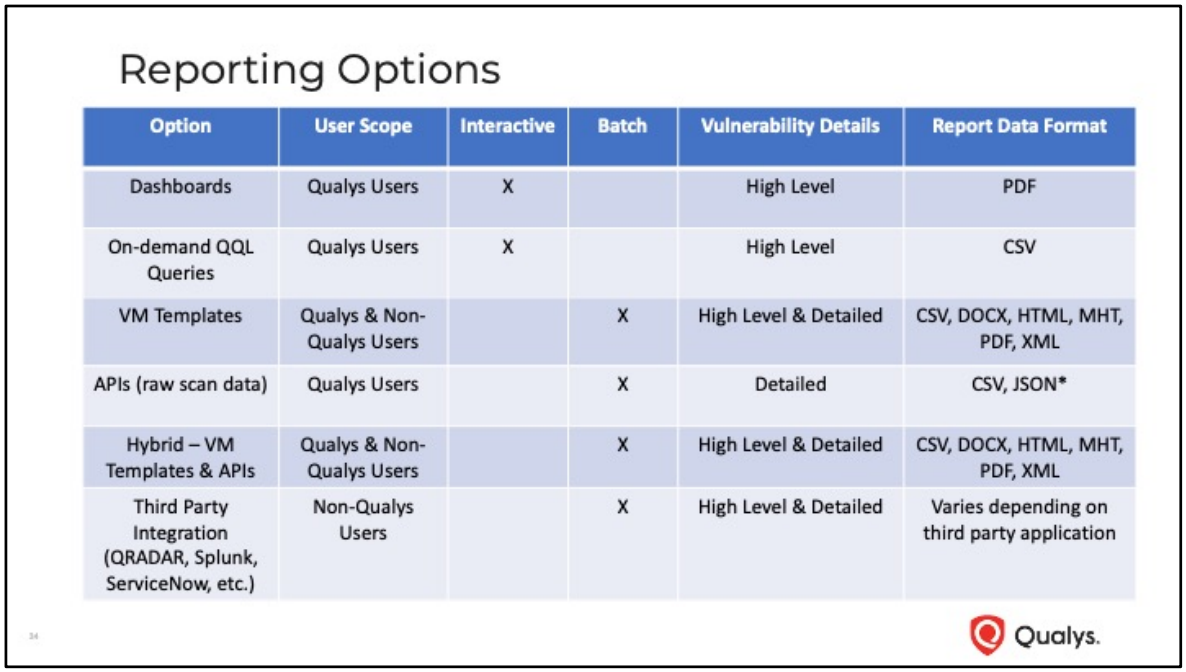
When a host is removed, it causes scheduled scans and reports to be retained and the IP continues to remain in the Global Exclusion list. All other information is deleted.



Before you start purging, consider the size of your environment and how many IP's you intend to purge. Purging a large number of IP's can take time. If you need to purge on a regular basis, it's a good idea to automate this using APIs.
Also note that once you purge an asset, all host scan data (findings) for the asset is removed from your Qualys account, and this action is irreversible. So, consider exporting host scan data for the concerned asset before purging. We recommend using Qualys APIs for exporting this data as APIs are better suited for bulk data export operations.



This section provides an overview of the options that can be used for vulnerability reporting.



Reporting Options

Option	User Scope	Interactive	Batch	Vulnerability Details	Report Data Format
Dashboards	Qualys Users	X		High Level	PDF
On-demand QQL Queries	Qualys Users	X		High Level	CSV
VM Templates	Qualys & Non-Qualys Users		X	High Level & Detailed	CSV, DOCX, HTML, MHT, PDF, XML
APIs (raw scan data)	Qualys Users		X	Detailed	CSV, JSON*
Hybrid – VM Templates & APIs	Qualys & Non-Qualys Users		X	High Level & Detailed	CSV, DOCX, HTML, MHT, PDF, XML
Third Party Integration (QRADAR, Splunk, ServiceNow, etc.)	Non-Qualys Users		X	High Level & Detailed	Varies depending on third party application

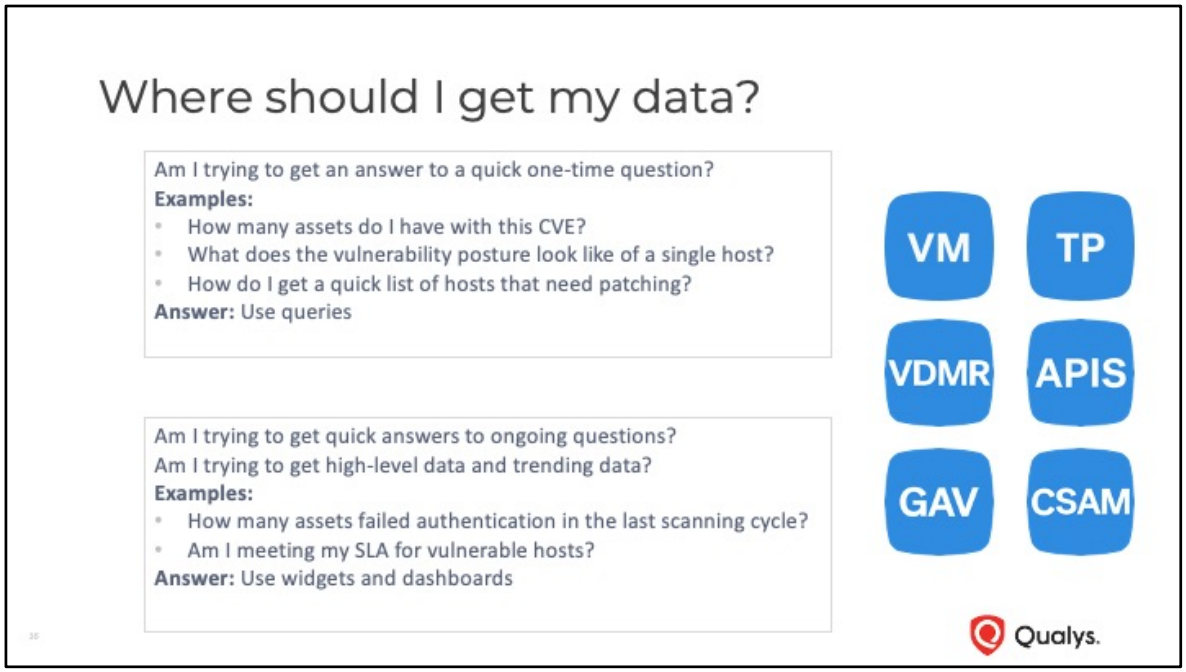
Qualys.

There are multiple ways to get data with Qualys – queries, widgets and dashboards, VM reports, and API. The table in this slide indicates the various options that can be used for reporting. Some of the factors that decide the choice of a particular option include accessibility by Qualys\non-Qualys users, interactivity, level of details that can be included in the report and report data format. Reporting using Dashboards, QQL queries and VM templates are covered in this course.

On-Demand QQL Queries are interactive in so far as you can refocus the view until you reach the format most meaningful to you.

VM Templates are Batch vs. Interactive.

**When using APIs for exporting data from your Qualys account note that not all API extracts support JSON. Please consult the API guides for specifics.*
Please subscribe to the **Qualys API Fundamentals Self-Paced Course** for more information on using APIs for reporting.

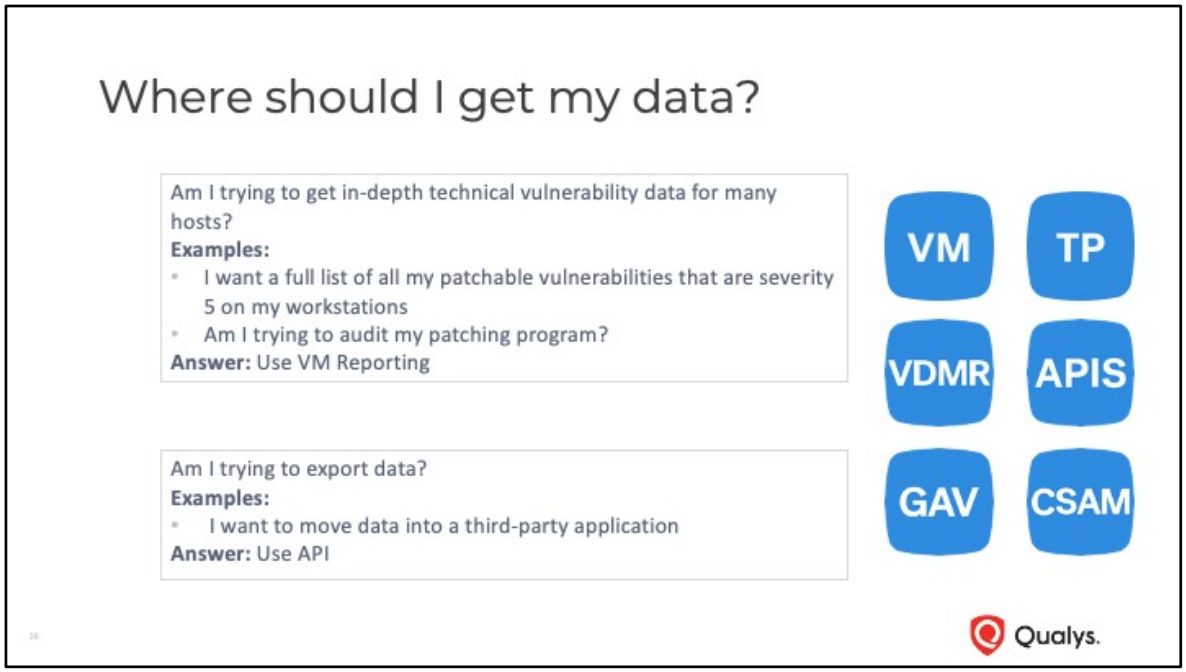


Queries – this is the fastest way to get data and is best-suited when you're looking for quick answers, typically to one-time questions. Examples include – how many of my assets are vuln to a specific QID, how many vulns of severity 5 exist, how many hosts have not been scanned in the past 30 days, how many hosts with a specific operating system or software exist.

Widgets and dashboards – this allows for visual representation of data. This includes count, bar, table and pie graph widgets. Use widgets for data needs to be constantly monitored. Examples include – assets taking long to scan, assets not rebooted, count of vulns, distributions of operating systems etc.

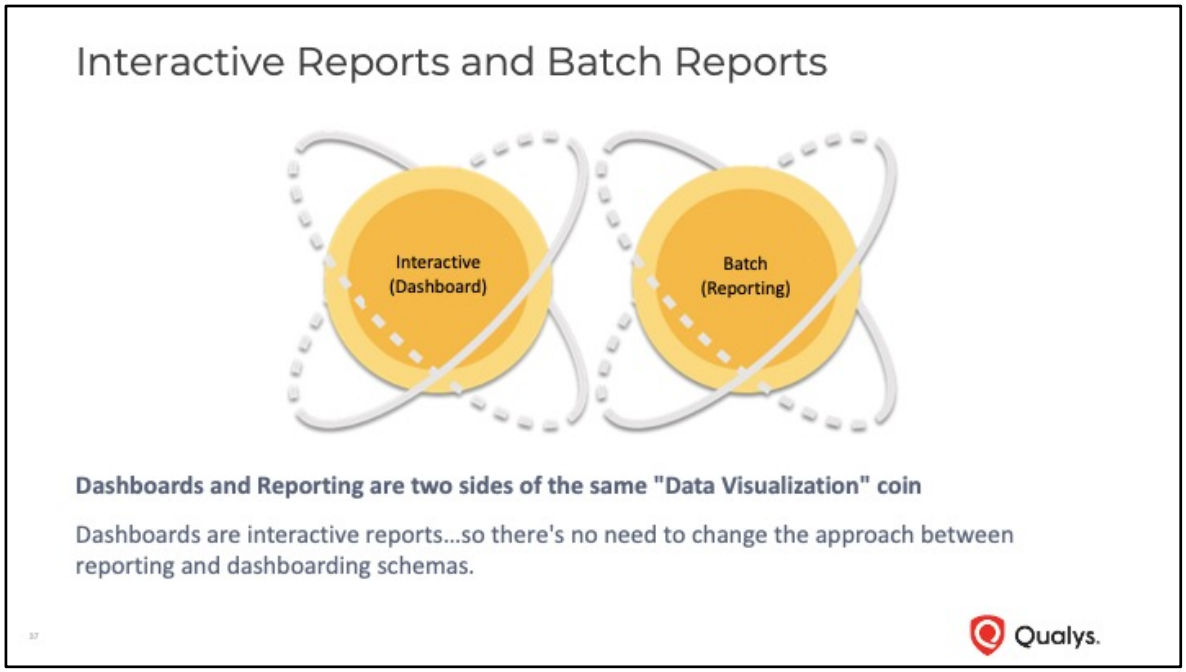
Qualys APIs, VM/VMDR, Threat Protection (TP) and CyberSecurity Asset Management (CSAM) / Global AssetView (GAV) are commonly used for fetching asset and vulnerability data for reporting.

While AssetView is also widely used, it has reached its end-of-life (EOL) stage and will go away soon. Please contact your Qualys TAM for more information on AssetView EOL.



VM/VMDR Reports – this should be used when you want detailed technical reports. These reports can be customized to show only specific data such as patches, malware, threat, compliance etc. and can be shared with other teams. This should also be used when you want to automate reports.

Qualys APIs – use this when you want to download large amounts of data. APIs are also used when you're trying to integrate Qualys with third-party applications like Splunk, ServiceNow, etc.



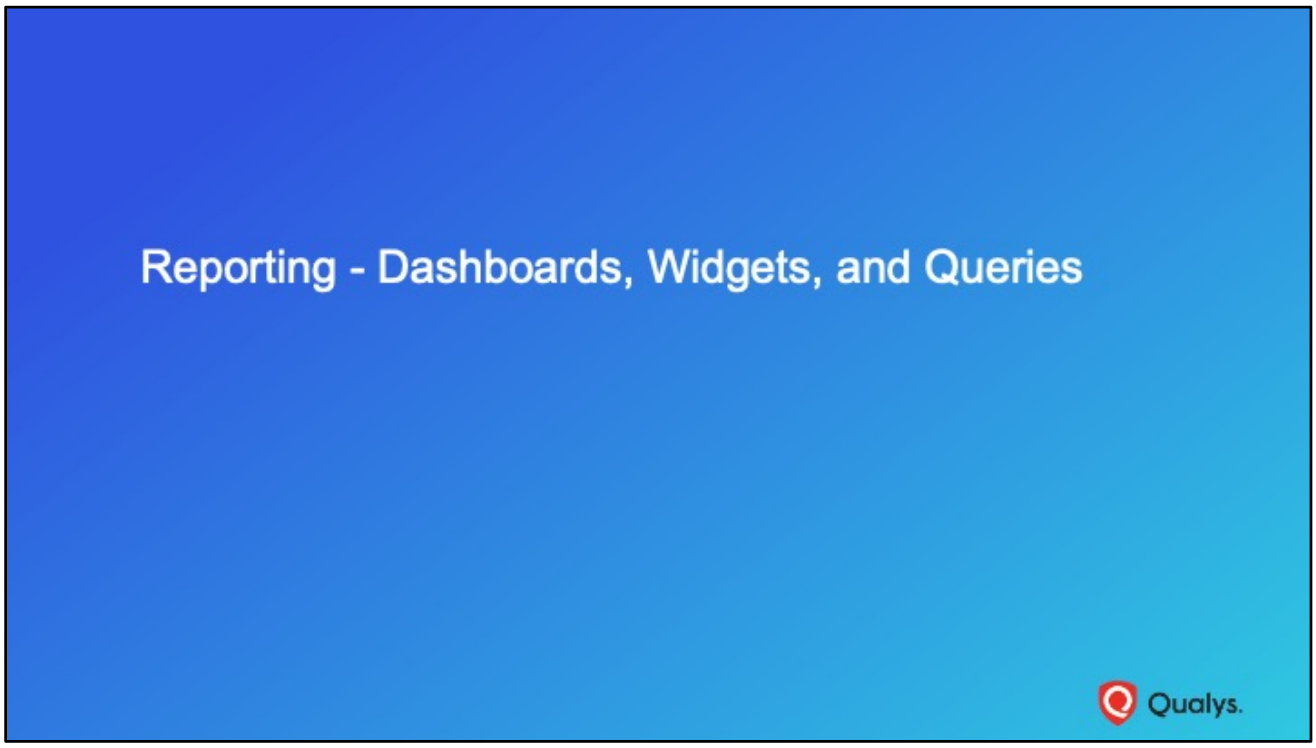
Comparing dashboarding and reporting data is not as cut and dry as you might think. In-depth understanding of your detection data, proper query formatting and proper template/search list selections is/are required.

Some considerations...

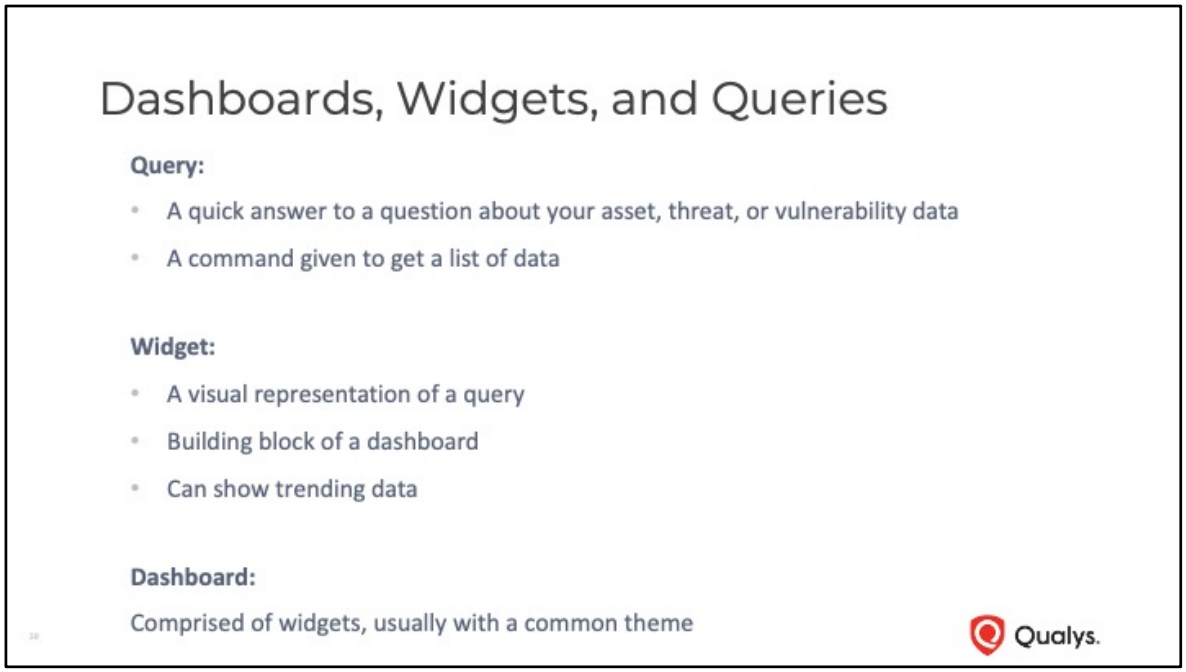
•All dashboards are not created equal

•To process historical data properly, be sure to specify date/time in queries: lastVmScanDate, lastPcScanDate, lastCheckedIn, firstFound, lastFound.

Also, dashboard trend graphs are not meant to be an audit-ready method of tracking data over time. The data is too volatile for that, as it can easily be wiped with a widget change. It is designed to be a visual indicator that something changed, so a major change in the widget count can be noticed. It only provides context for the count, because without it, you only have a current-state number.



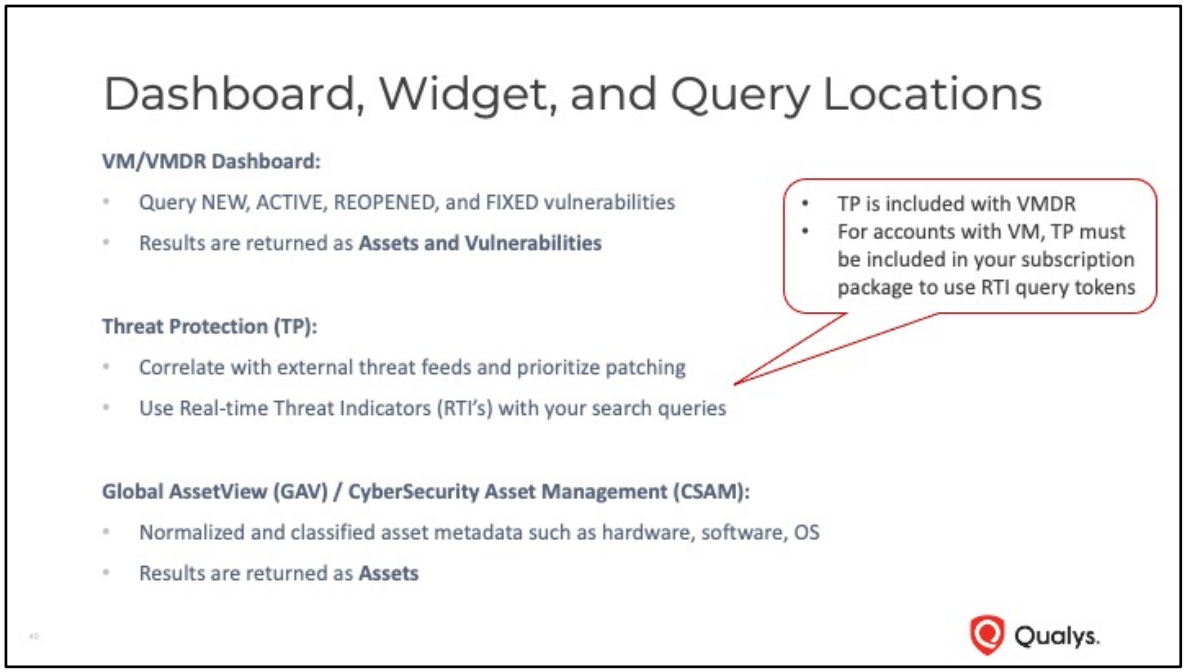
This section provides an overview of the considerations for using interactive reporting options such as dashboards, widgets and queries for vulnerability and asset tracking.



If you're looking for an answer to a quick question, use a Query. This includes examples like – how many devices have a specific port open, how many devices have an SSL vulnerability, how many devices have a zero-day vulnerability etc.

If you'd like to visually represent a query, use a Widget. Widgets can be pinned on dashboards and tracked over a period of time.

Dashboards are made up of multiple widgets. Widgets having a common theme are placed in a single dashboard. For example, a dashboard for SSL/TLS, a dashboard for Cloud Agent health, a dashboard for WannaCry vulnerabilities etc.



Queries, widgets and dashboards can be used across multiple apps in Qualys. Knowing which app to use will help you get the required data fast.

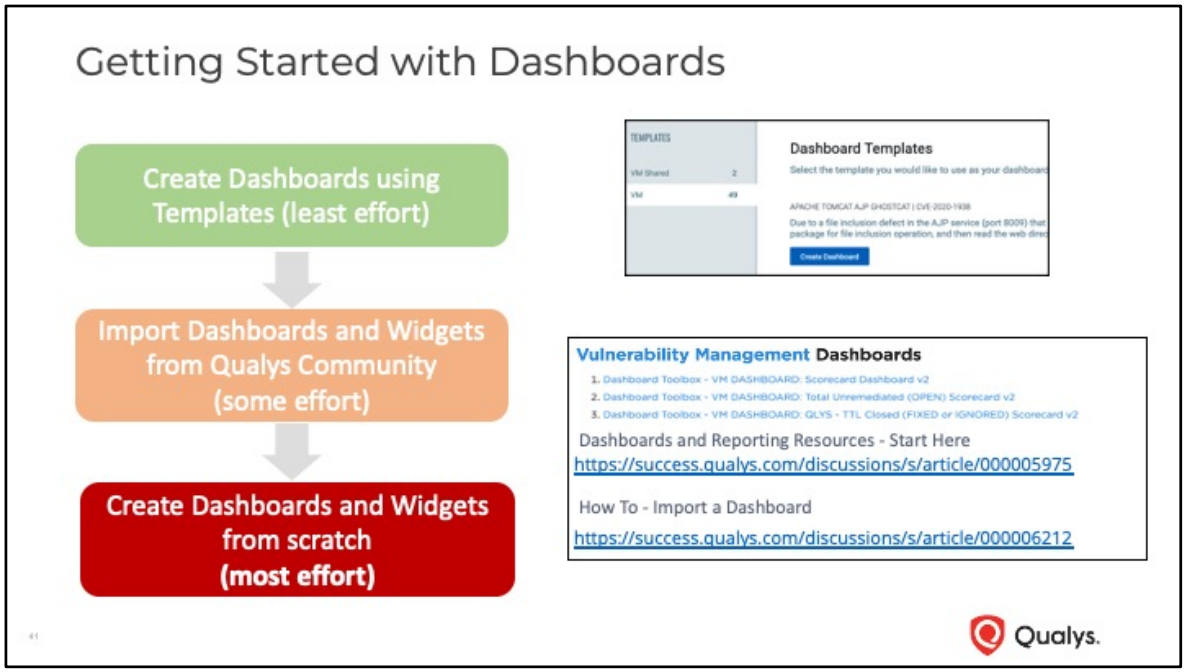
VM/VMDR Dashboard – this has more powerful and flexible search options. It is designed to give you a list of asses AND list of vulns matching your search query. It includes NEW, ACTIVE, REOPENED, and FIXED vulnerabilities.

Threat Protection (TP) – designed as an extension of AssetView, use this to search assets matching specific threats. You can use Real-Time Threat Indicators (RTIs) with your vulnerability search queries in VMDR. For accounts with a VM subscription, Threat Protection must be added to the subscription to use RTI search query tokens. Please contact your Qualys TAM for more information.

Threat Protection is included with VMDR and provides RTIs to the VMDR Prioritization Report, that will help you identify the potential impact of discovered vulnerabilities, as well as vulnerabilities that have known or existing threats.

Global AssetView (GAV) / CyberSecurity Asset Management (CSAM) - use this to get a more granular picture of your assets. This includes standard asset data collected in

AssetView plus details such as manufacturer name, product name, software version, hardware and software product release dates, end-of-life dates and license categories.



You can create your own dashboard using existing widget templates that we provide, customize existing widgets or create your own widgets to suit your need.

Creating Dashboards Using Template

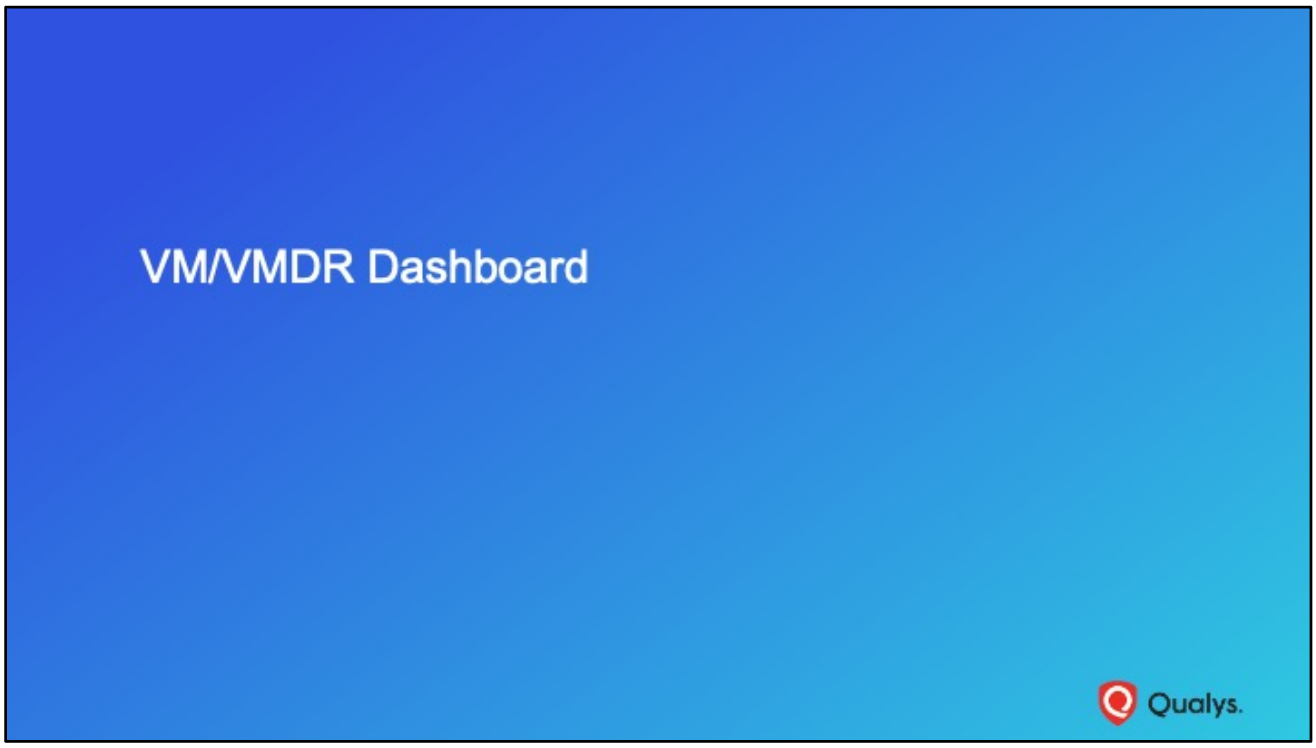
Qualys provides ready to use templates for dashboards that you could quickly add to your list of dashboards and start monitoring your assets. Amongst the templates, choose the one that suits your need of data population for your assets and create a dashboard. Your dashboard is ready to use. You could add more widgets to dashboard, edit existing widgets, change the layout of widgets and many more things in your dashboard. New templates are regularly added to the template library in your Qualys account as and when these are published.

Importing Dashboards and Widgets from Qualys Community

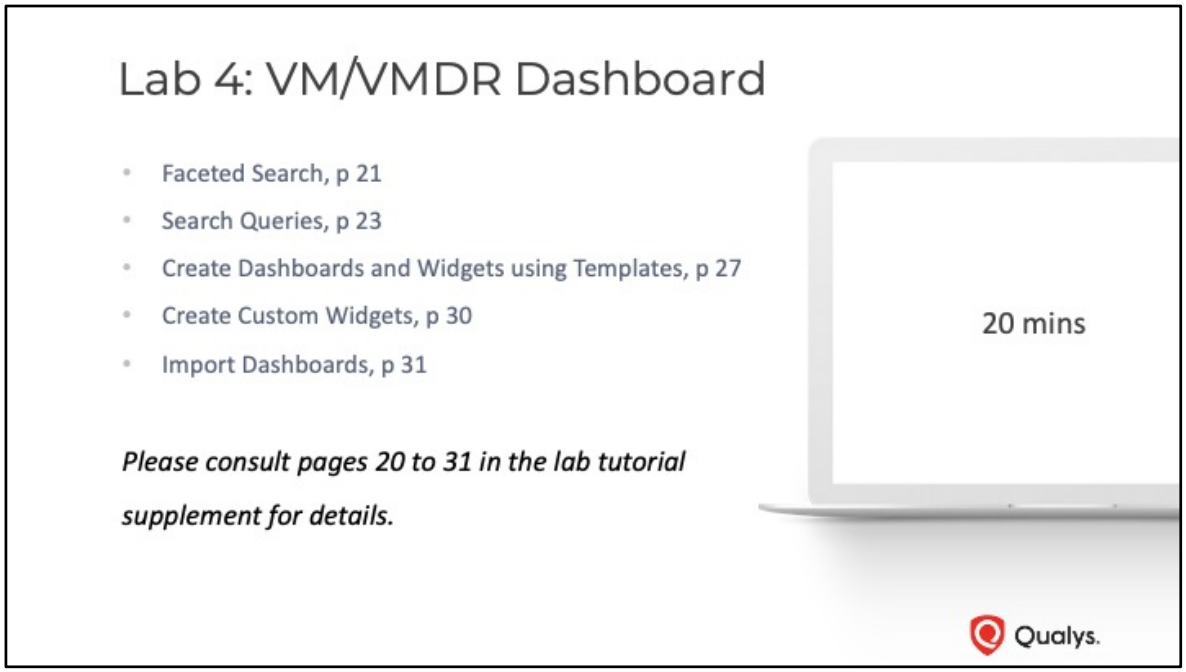
In addition to using templates for building dashboards, you can also import dashboards available on Qualys community into your Qualys account. You'll find links for ready-to-import VM/VMDR dashboards on https://success.qualys.com/discussions/s/article/000005975. Please consult https://success.qualys.com/discussions/s/article/000006212 to know more about importing dashboard JSON files into your Qualys account.

Creating Dashboards From Scratch

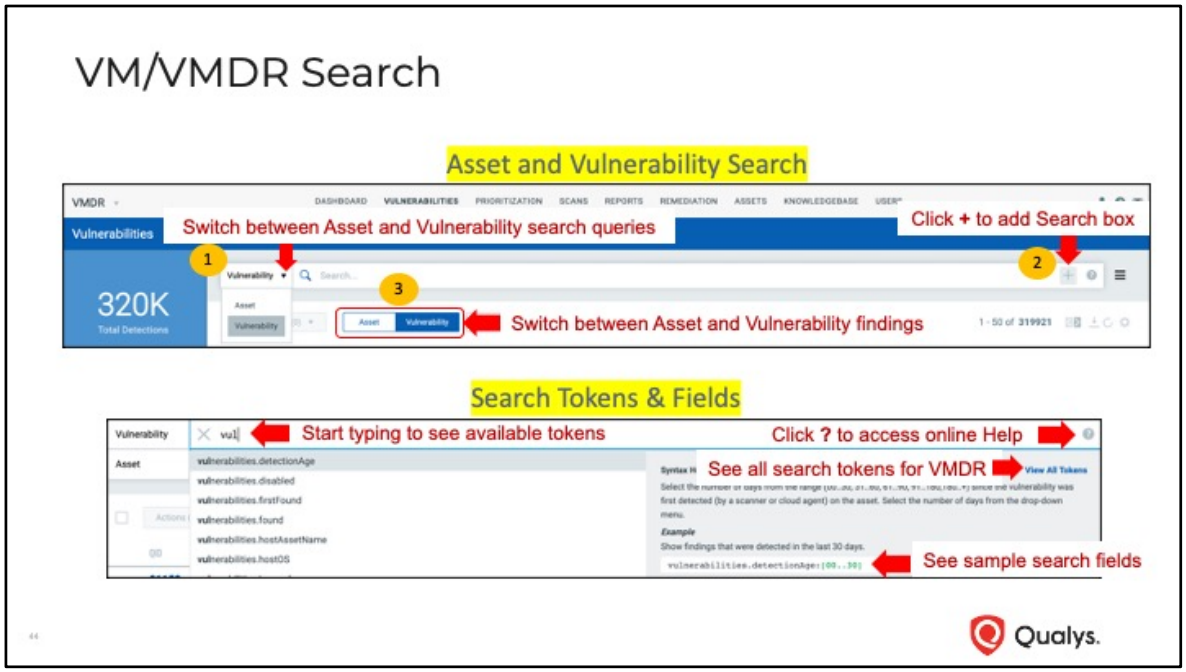
This involves the most effort as you will need to create your own widgets using search queries. A good understanding of query tokens and query formatting requirements and best practices are a prerequisite to using this approach to build your own custom dashboards and widgets.



This section outlines features of the VM/VMDR Dashboard at a high level.



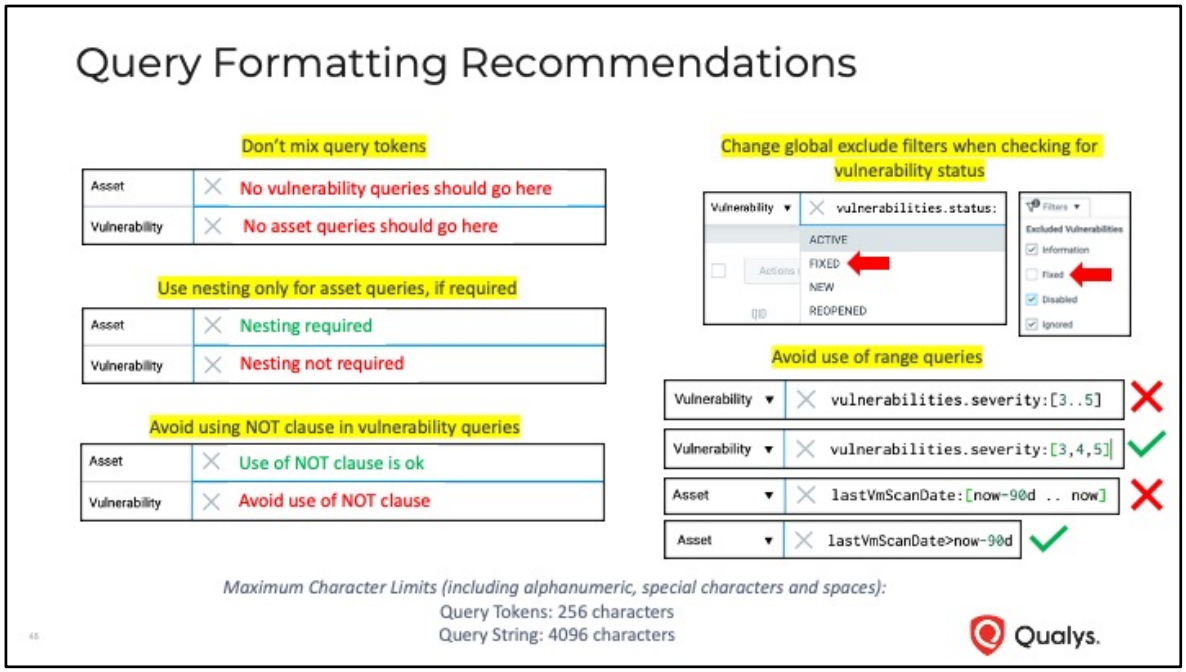
- Activity 1, will show you how to use faceted search to filter down vulnerability information.
- Watch how it builds the query in the Search bar as you click on the faceted search.
- You will also see the Online Help and where to go for syntax help on the QQL. Toward the end you will see examples of tokens that will query the when was the last time an asset checked in.
- Activity 2, shows how to filter search query results.
- Activity 3, shows you how to create a dashboard (from template and scratch).
- There is a test and preview feature you want to be aware of to use beyond this course.
- Activity 4, you will create a widget that compares 2 queries and enable trending.
- Activity 5, shows you how to import a dashboard from the Qualys Community.



The Vulnerabilities tab gives you an integrated, incremental search and browse experience to help you find all about your assets.
Choose Vulnerability to display vulnerability data or Asset for asset data. From there you can easily browse the data list and explore details.

How to Search
https://qualysguard.qg2.apps.qualys.com/portal-help/en/assetview/assets/asset_search_samples.htm

Search tokens for asset and vulnerability search in Vulnerabilities tab
https://qualysguard.qg2.apps.qualys.com/portal-help/en/vm/index.htm#t=search_tips%2Fsearch_ui.htm



Here we have outlines some of the query formatting recommendations and suggestions for improved query performance.

When you are working on a dashboard that contains more than one data source query box as indicated by the plus sign on the right of the query search box, make absolutely certain that you only include the tokens applicable to the data source indicated on the left of the query search box. In other words, do not enter asset tokens in the vulnerability box, and vice-versa. Doing so will produce invalid results.

Next, when working in the VM/VMDR dashboard, note that nesting within a query is only required for ASSET, not for VULNERABILITY type of queries.

Also avoid the use of NOT clause within vulnerability queries and opt instead to using **explicit includes** vs **excludes** to improve accuracy.

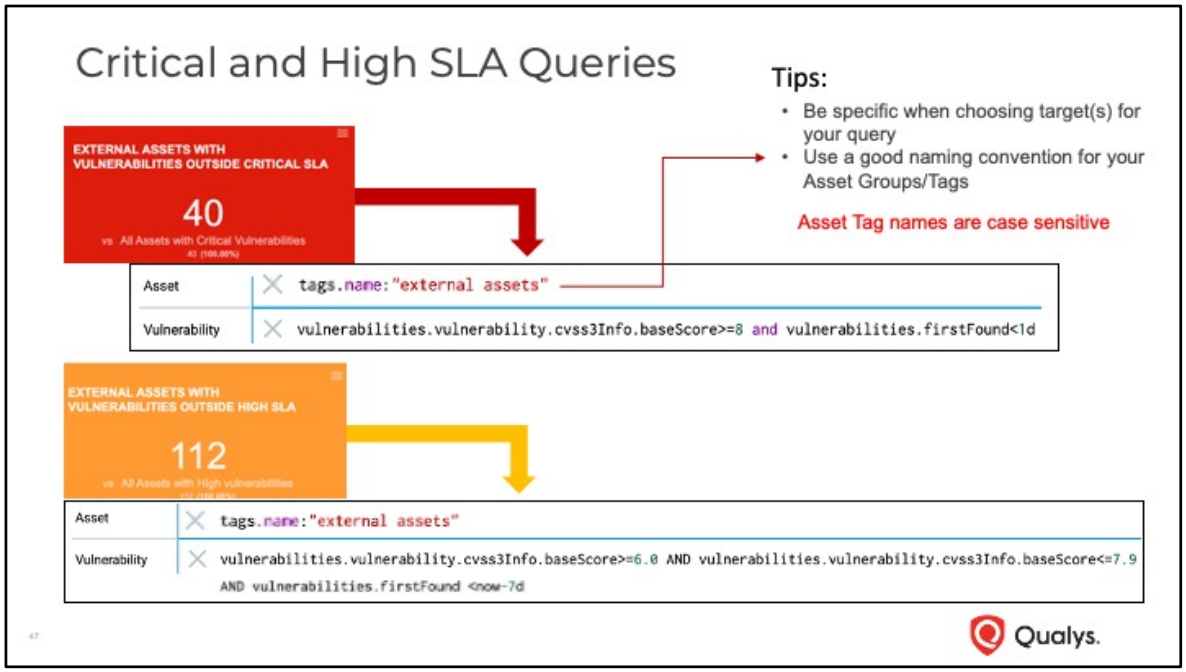
Next, note that by default, Information QIDs and Fixed, Disabled and Ignored vulnerabilities are not included in the search results. So when using the query tokens to list vulnerabilities by their status ,you need to UNCHECK the appropriate checkbox under Filters to list all vulnerabilities including FIXED or Disabled or Ignored

vulnerabilities and Information gathering QIDs.

We also recommend that you try to reduce the use of range queries, where possible to improve query performance. The checked queries indicate the most performant queries.

Lastly note the Maximum Character Limits for using queries. For Query Tokens this is limited to 256 characters and for Query String it is 4096 characters. *Note that these limits are inclusive of any alphanumeric characters, special characters and spaces used in the search query.*

This is an example of how you can represent your corporate remediation SLA within your VM/VMDR dashboard using custom widgets.



This slide illustrates some of the queries used to build the custom dashboard widgets illustrated in the previous slide.

The first query looks for all external facing assets that have vulnerabilities with CVSSv3 Base score of 8 and above and which have been first found more than 1 day ago:
tags.name:"External Assets" **AND**
vulnerabilities.vulnerability.cvss3Info.baseScore>=8.0 **AND**
vulnerabilities.firstFound<now-1d

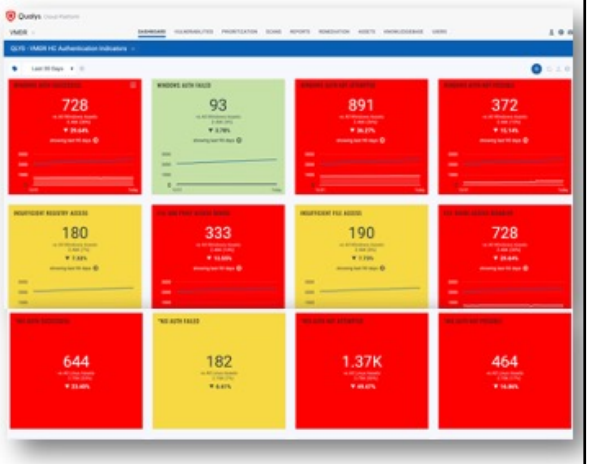
The second query looks for all external facing assets that have vulnerabilities with CVSSv3 Base score of 6 and above but less than or equal tp 7.9 and which have been first found more than 7 day ago:
tags.name: "External Assets" **AND**
vulnerabilities.vulnerability.cvss3Info.baseScore>=6.0 **AND**
vulnerabilities.vulnerability.cvss3Info.baseScore<=7.9 **AND** vulnerabilities.firstFound <now-7d

Qualys recommends using a good naming convention when using Asset Groups

and/or Asset Tags for organizing and managing the IT assets in your Qualys account. We also recommend being specific when choosing a target(s) for reporting. Also note that asset tag names are case sensitive.
Please consult
https://qualysguard.qualys.com/qwebhelp/fo_portal/host_assets/tags_asset_tagging.htm for more information on getting started with Asset Tags.

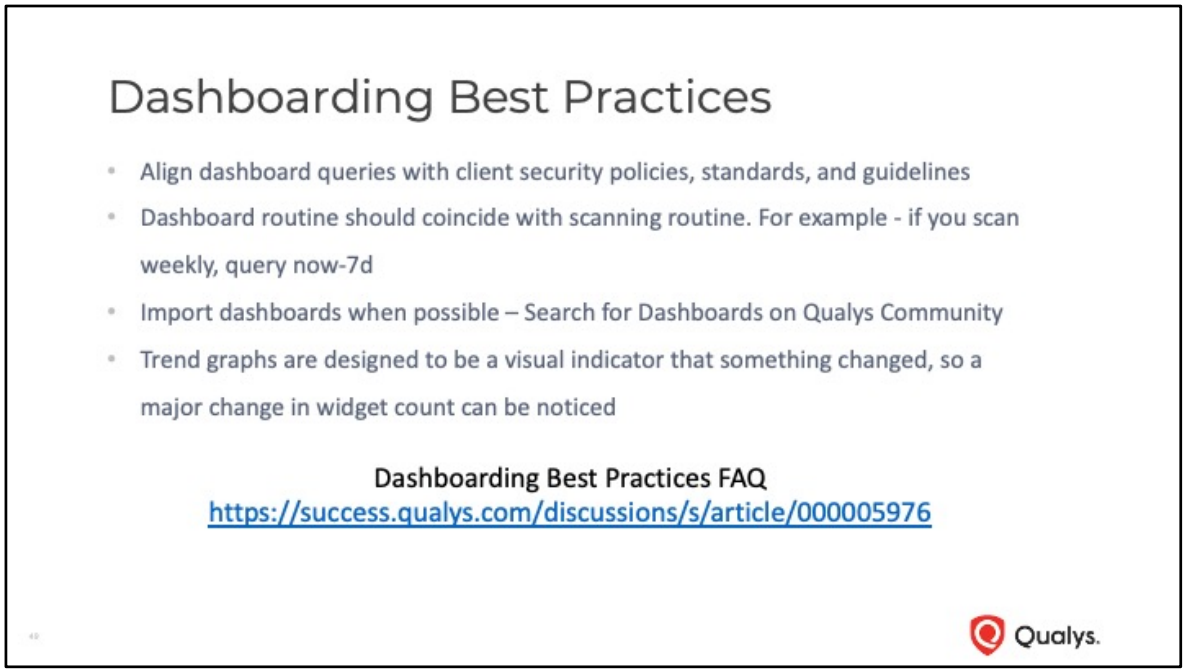
Authentication Dashboard

- Dashboards enable you to be more pro-active in your authentication management of Qualys Scans
- Get a quick, easy glance at KPIs for authentication successes and failures across different technologies.
- Authentication dashboards:
  - Allow to drill down into details
  - Updated automatically
  - Provide more details regarding authentication failures compared to authentication reports
- Authentication dashboards and Authentication Reports complement each other



Qualys.

Pre-built VM/VMDR dashboard JSON files for Windows Authentication Management are available on the following link:
https://success.qualys.com/discussions/s/article/000006159

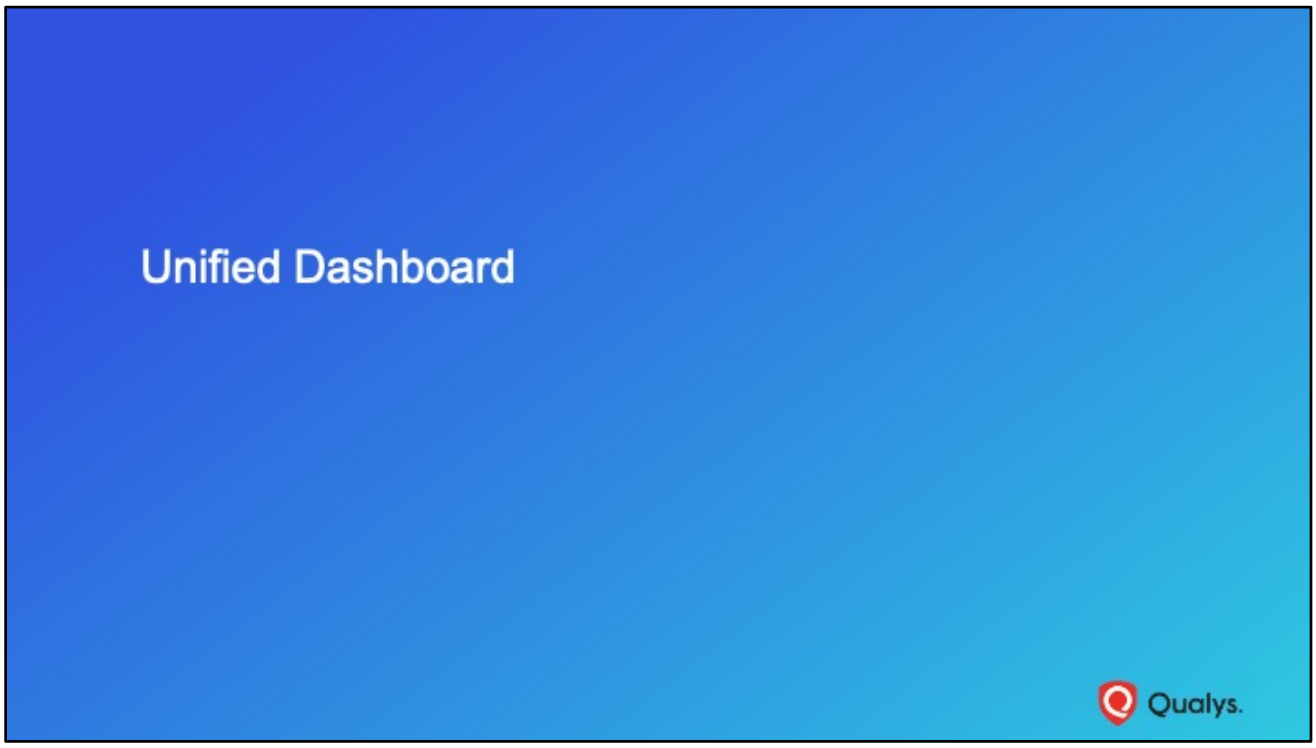


The queries used to populate your dashboards should align with your security policies and your scanning routines. For example, if you're scanning every week, use now-7d in your queries. For example, vulnerabilities.firstFound: now-7d.

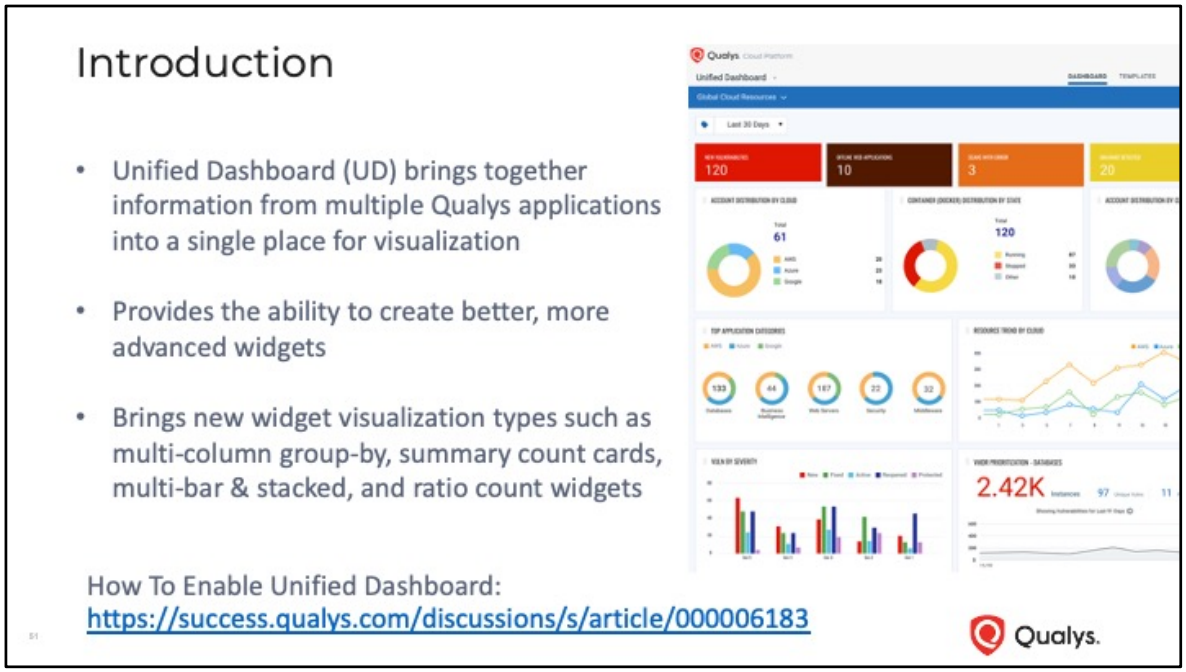
The Qualys Community has several ready-to-import dashboards available. To get these, visit community.qualys.com. Note that dashboards and widgets posted in/on the community are Qualys application modules specific and are not interchangeable between application modules. AssetView, Global Asset Inventory, Threat Protection, Cloud Agent, VM/VMDR, etc. dashboards are all independent of the other.

Trend graphs should be used when you need to monitor the variance of a specific metric, such as, assets not scanned in the last 30 days, total vulns fixed in the last 7 days etc.

For more information on dashboarding best practices please consult the FAQ on https://success.qualys.com/discussions/s/article/000005976



This section outlines the features and benefits of the Unified Dashboard (UD).



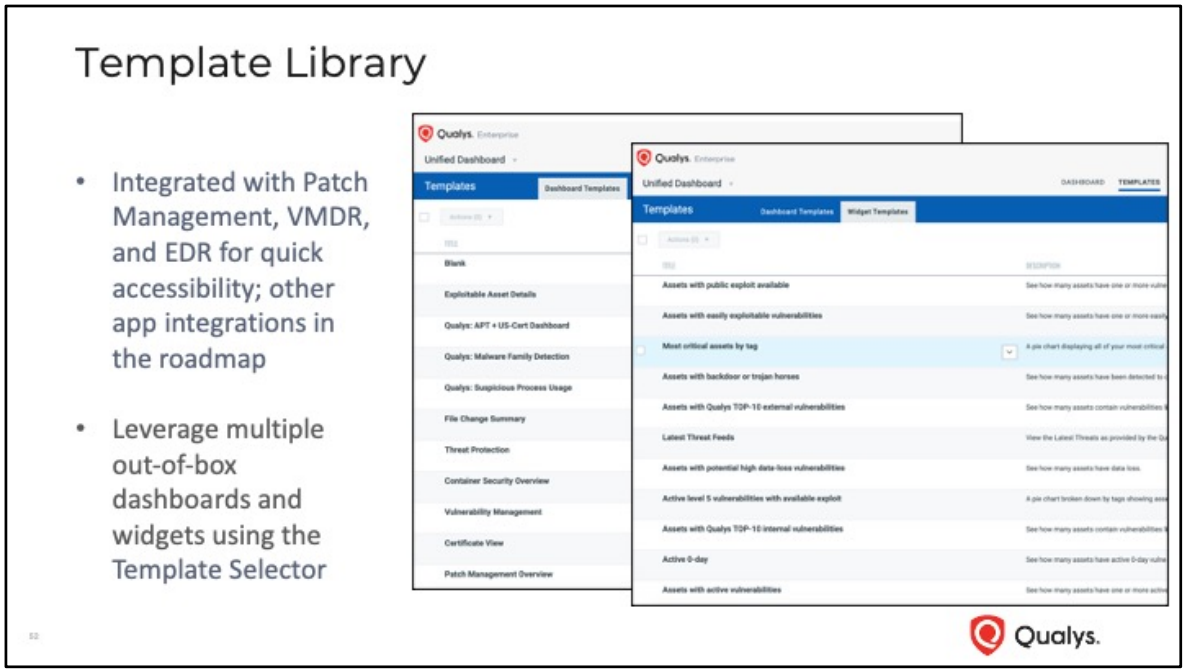
Unified Dashboard (UD) brings information from all Qualys applications into a single place for visualization. UD provides a powerful new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities. You can use widget builder and improvise dashboards to make it uniform across all products.

Qualys Unified Dashboard has the following features:

- Ease of use for visualizing data and creating / managing dashboards
- Widget creation from different modules for cross-data visualization
- Ability to save, manage, view, and create a widget from recent queries
- Easy duplication of widgets
- Complete full-width use of the entire screen
- Easy pivot from widget to another application
- Easy pivot from a dashboard to another dashboard
- Responsive UI for all types of devices
- Ability to provide more enhanced descriptive text to the widgets and dashboard
- Additional group-by's
- Multi-column support

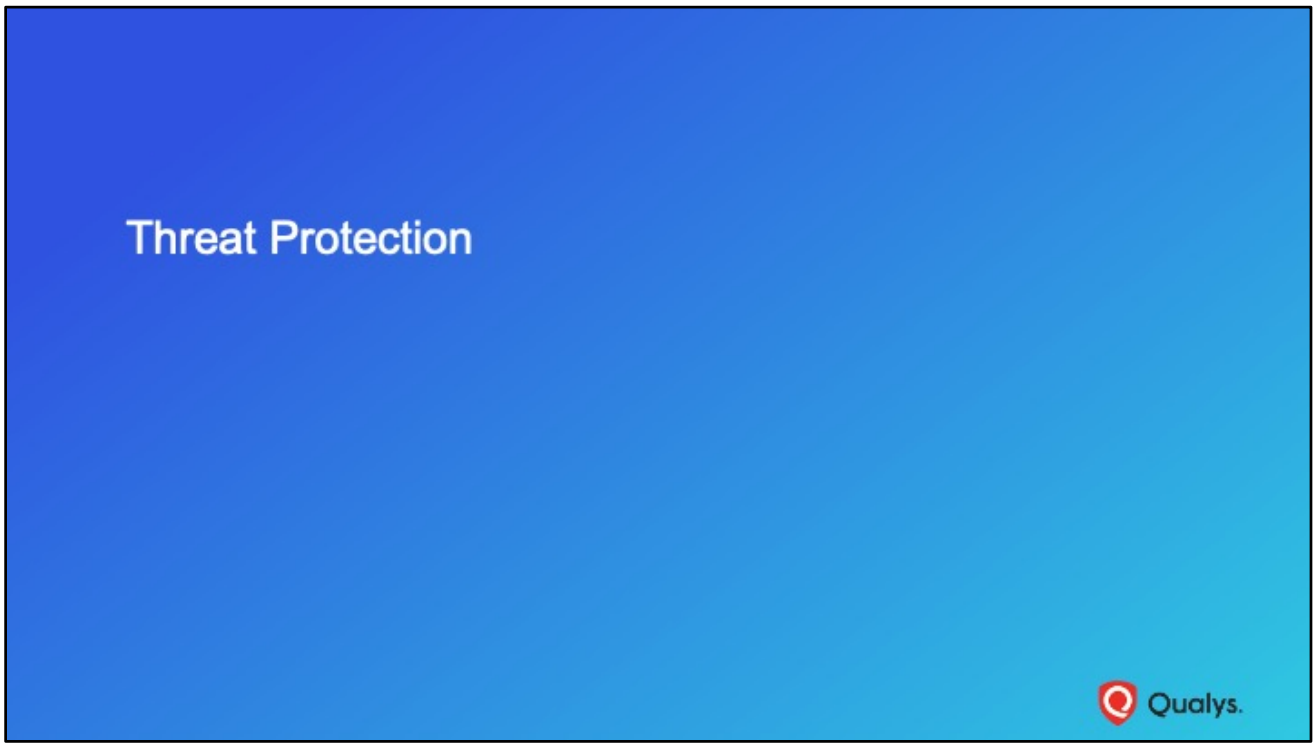
- Multi-dimensional group-by
- *more to come…*

Please consult the following document to know how to enable the Unified Dashboard in your Qualys account:
https://success.qualys.com/discussions/s/article/000006183



UD enables security teams can see their IT asset inventory along with vulnerability and the current patch posture breakdown for their organization in one place. UD can cohesively and dynamically work with Global IT Asset Inventory, EDR, Vulnerability Management, Patch Management, and many more widgets to give a single view of your enterprise.

Dashboard and Widget Template Selector shows multiple applications to choose templates from for cross-data visualization.

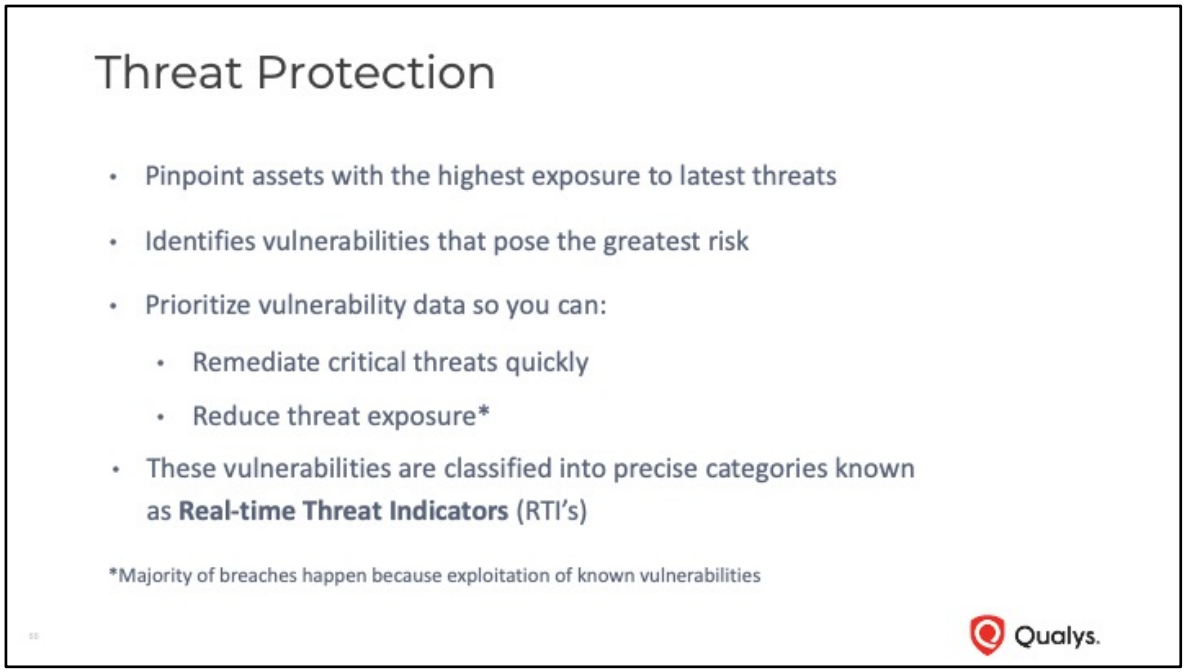


This section explains how Threat Protection can be used to prioritize vulnerabilities for remediation. Threat Protection datasheet - https://www.qualys.com/docs/threatprotect-datasheet.pdf

There are several parameters that you can use to determine which vulns to fix first.

A common way of doing this is to use the Qualys severity ratings and start with the high priority ones. This includes severity 4 and 5 vulns. You may also include other factors such as an exploit being available, a malware associated with the vulnerability, how important is the asset and whether it affects your overall compliance posture. Another way to prioritize is to look at CVSS scores.

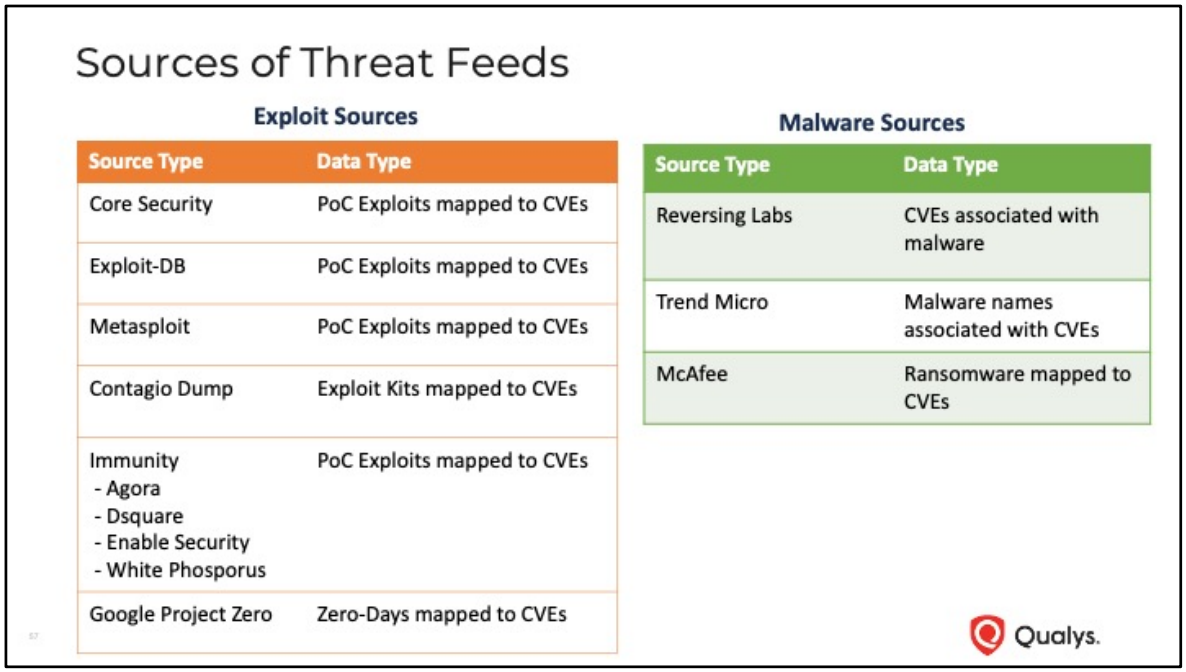
Qualys Threat Protection provides real-time threat indicators that can also be used to prioritize remediation. These RTI's correlate your vulnerabilities to external threat vectors such as zero-day, denial of service attacks, etc.



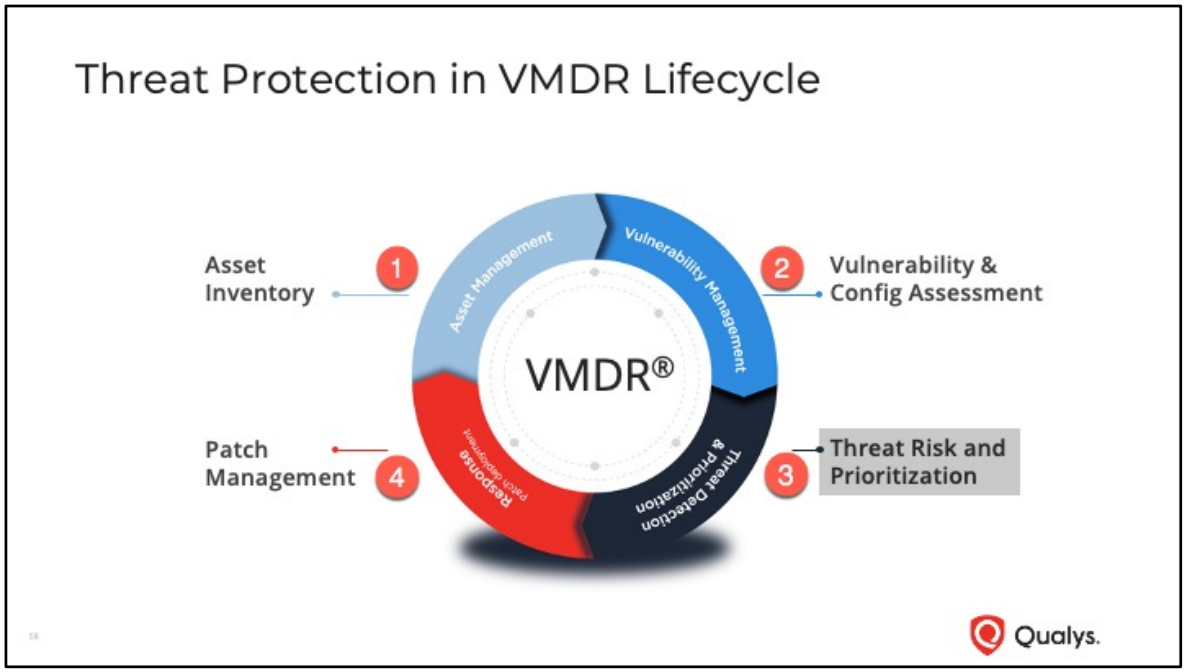
The severity level of a vulnerability identifies the impact if the vulnerability is exploited. Severity is not equal to threat.
For example, if a high severity vulnerability has a known threat associated with it, then it is an immediate threat and needs to be fixed asap.
Threat Protection includes a live feed of known threats and correlates these to your assets.

Threat Protection allows you to identify assets associated with threats, not just having vulnerabilities. This way you can prioritize those assets that have a higher risk and that have multiple threats associated with them.

- Activity 1, shows you the VMDR prioritization report and how useful RTIs are in prioritization efforts.



The table on this slide lists threat data subscriptions used by Threat Protection.



Here's a quick review of the Qualys Vulnerability Management Detection and Response (VMDR) lifecycle model and where threat protection fits in.

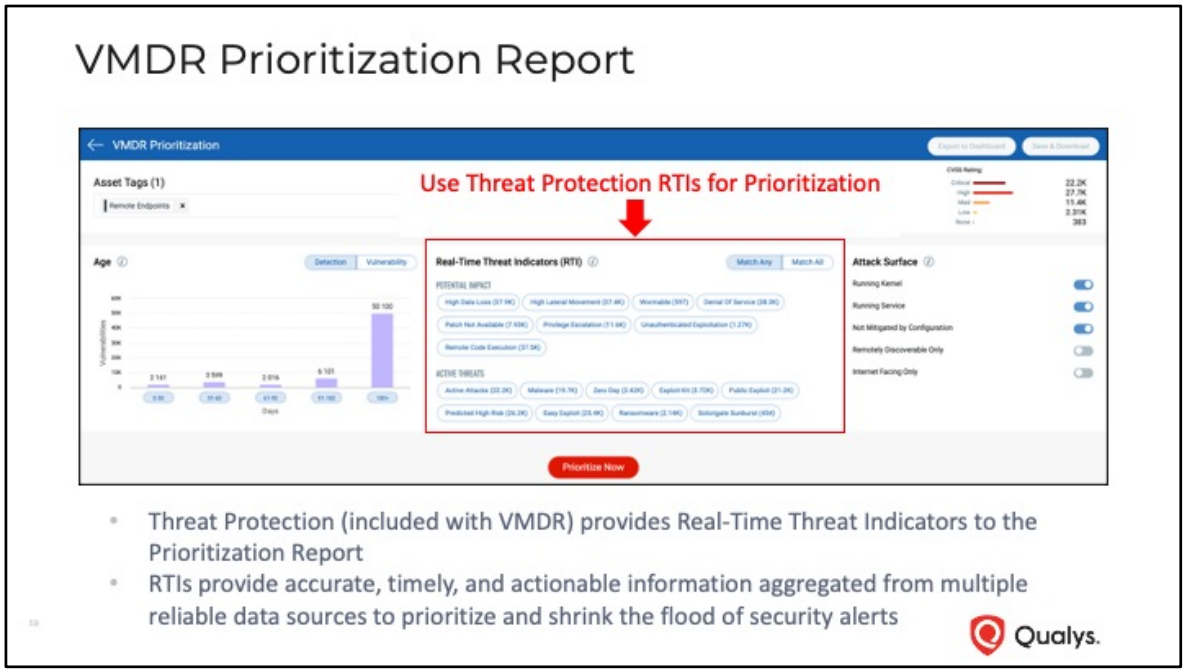
The VMDR Lifecycle, begins (step 1) by identifying and managing all assets throughout your business or enterprise architecture.

Once your assets have been discovered, the next step is to scan them for vulnerabilities and configuration gaps and report on the findings.

Next step is to identify vulnerabilities associated with different threats and prioritize them based on the threat perception. When you have lots of assets that need to be patched, or lots of patches that need to be applied, it
becomes important to prioritize. Which asset to patch first and which patch to deploy? Threat Protection allows you focus on vulnerabilities that have threats associated with them. Examples include zero-day, denial of service,
actively attacked vulns etc.

In the final step of the VMDR Lifecycle (step 4), Qualys Patch Management (PM) then allows you to respond to detected vulnerabilities and threats, within days or even

hours, rather than weeks or months.



The VMDR Prioritization Report is designed to help you prioritize and patch vulnerabilities, using multiple factors, including: Asset Context, Vulnerability Age, Threat Intelligence, and Attack Surface dynamics.

The Qualys Threat Protection application (which is part of VMDR) provides Real-Time Threat Indicators to the Prioritization Report, that will help you identify the potential impact of discovered vulnerabilities, as well as
vulnerabilities that have known or existing threats.

Simply select the threat indicators you want to use to prioritize vulnerabilities. If you select multiple threat indicators, be sure to select the appropriate logical operator, in the upper-right corner.
Match Any == OR
Match All == AND

Real-time Threat Indicators are data points collected per vulnerability. It is accurate, timely and actionable information aggregated from multiple reliable data sources to prioritize and shrink flood of security alerts.
Current Real-time Threat Indicators are categorized into 2 types:

Potential Impact Real-Time Threat Indicators:

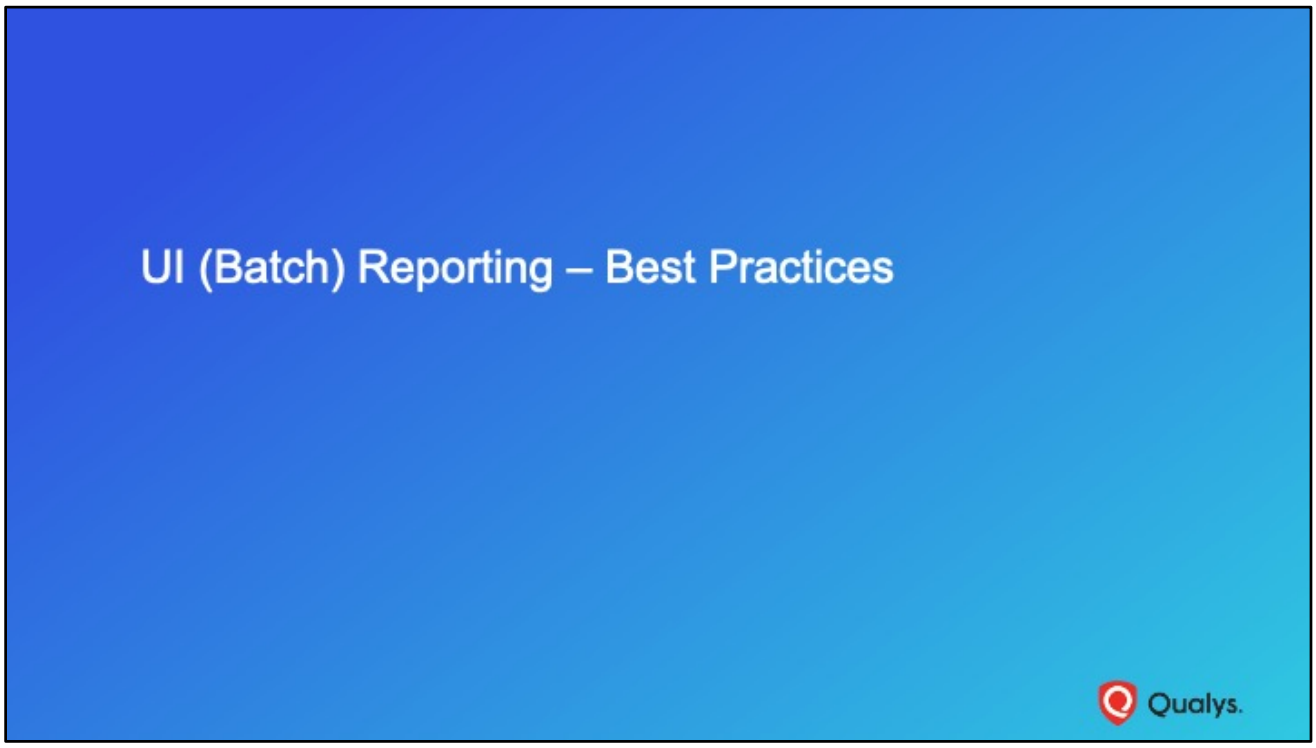
1. High Data Loss
2. High Lateral Movement
3. Wormable
4. Denial of Service
5. Patch Not Available
6. Privilege Escalation
7. Unauthenticated Exploitation
8. Remote Code Execution

Active Threat Real-Time Threat Indicators:

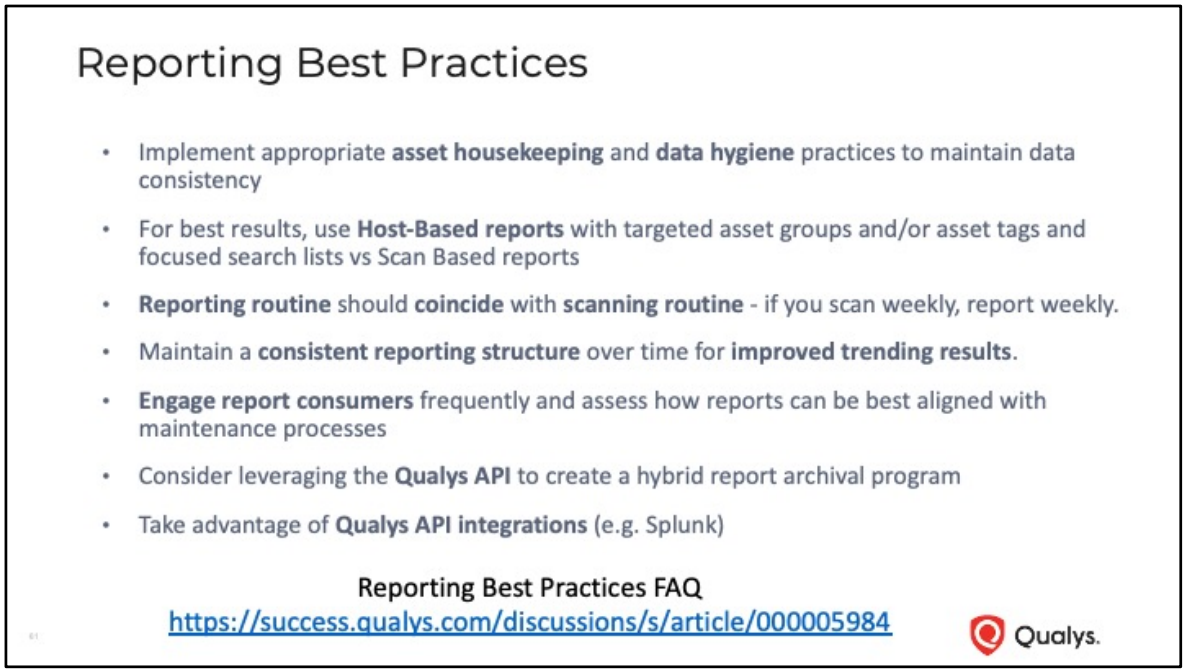
1. Active Attacks
2. Malware
3. Zero Day = Actively Attacked + Patch Not Available
4. Public Exploit
5. Predicted High Risk
6. Easy Exploit
7. Exploit Kit

Please consult https://qualysguard.qg2.apps.qualys.com/portal-help/en/vm/threat/rti_info.htm for more information on TP RTIs.

Please subscribe to the VMDR training course to learn more about the VMDR prioritization report.



This section provides an overview of Qualys UI reporting related best practices and philosophy.



Remember:
Qualys UI Reporting is intended to generate reports that are easy to read, understand and prioritize, not for exporting every vulnerability from a subscription. **Qualys UI Reporting is not designed for large scale data exports**. Qualys provides APIs for large data exports e.g. exporting every vulnerability from a subscription.

Some best practices to consider..

Implement appropriate asset housekeeping and data hygiene practices to maintain data consistency in your environment. These recommendations were covered in a previous topic in this course.

For best results, use Host-Based reports with targeted asset groups and/or asset tags and focused search lists vs Scan Based reports.
Please consult https://qualys-secure.force.com/discussions/s/article/000006215 for focused search lists that make it possible to track, and quickly spot or check, relevant indicators in your environment.

Reporting routine should coincide with scanning routine - if you scan weekly, report weekly.

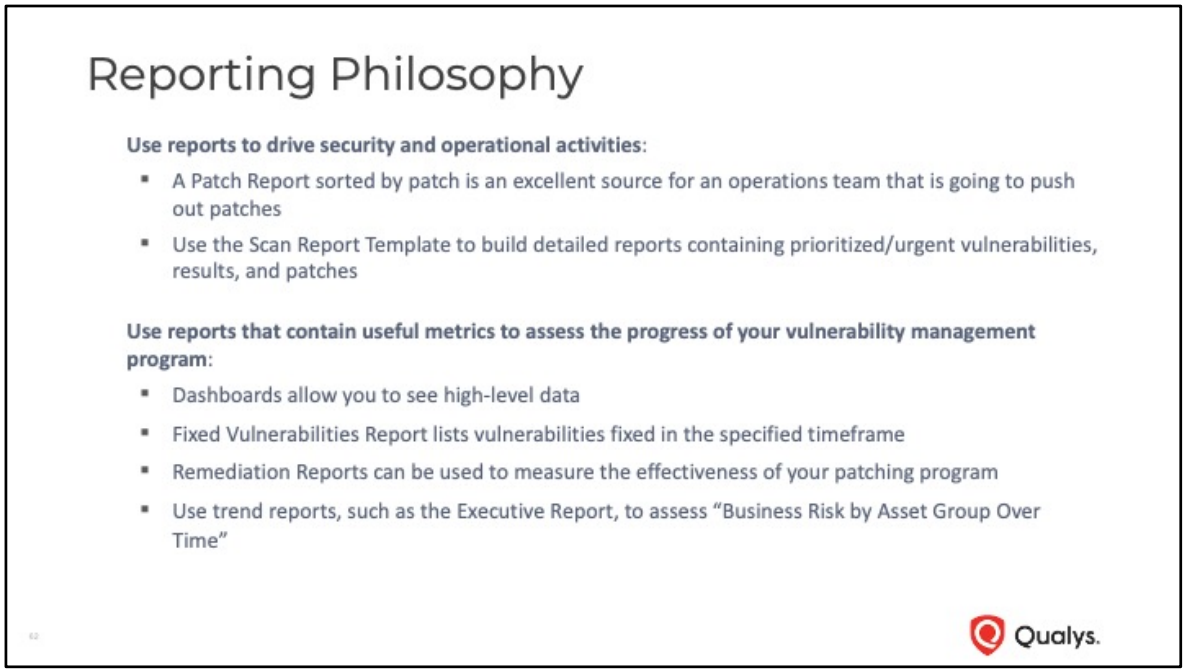
Maintain a consistent reporting structure over time for improved trending results.

Engage report consumers frequently and assess how reports can be best aligned with maintenance processes.

Qualys provides APIs for large data exports e.g. exporting every vulnerability from a subscription to create a hybrid report archival program.

You can also take advantage of Qualys API integrations with third party applications. E.g. the Qualys App for Splunk Enterprise pulls (via the TA-QualysCloudPlatform) vulnerability and compliance detection data from your Qualys account and puts it in Splunk for easier searching and reporting.

Reporting Best Practices FAQ:
https://success.qualys.com/discussions/s/article/000005984



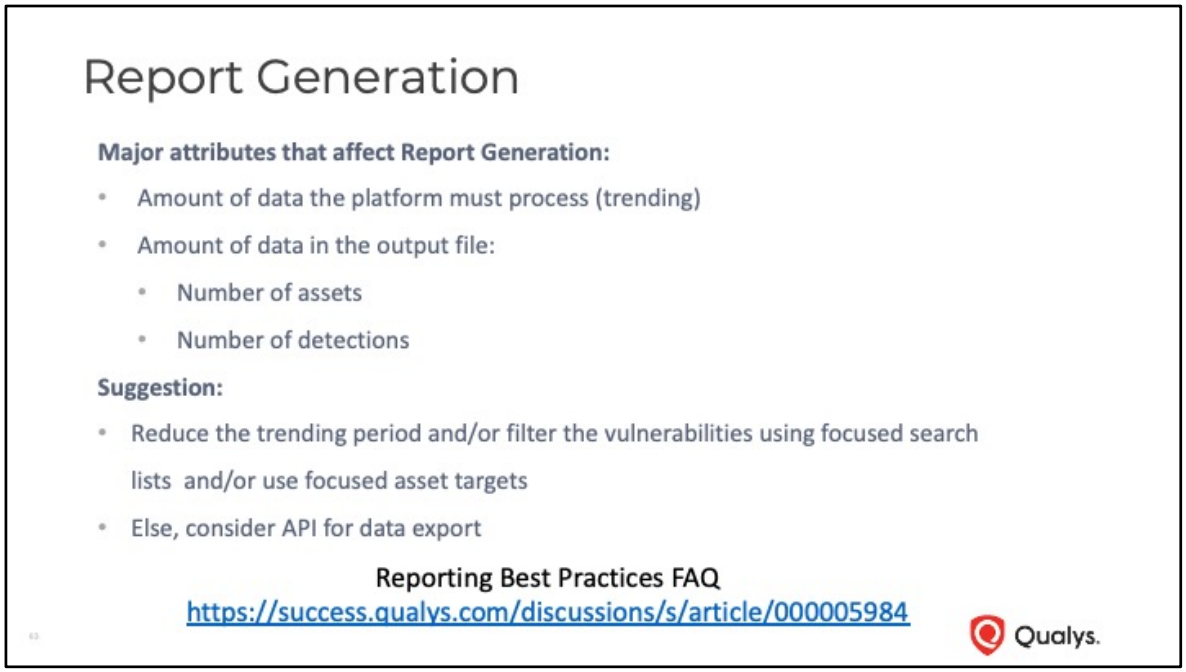
Reports can be used to either drive remediation in your environment or used as an audit of your patching program to see how well things are going. The Scan report template is the most popular report because it offers the most flexibility for sorting the technical data it can include, and prioritization.

You can also build a patch report to show the necessary patches required in your environment. Best practice is to sort by patch.

Using dashboards, you can see high level data on assets and vulnerabilities you want to track. They also allow you to query your data quickly.

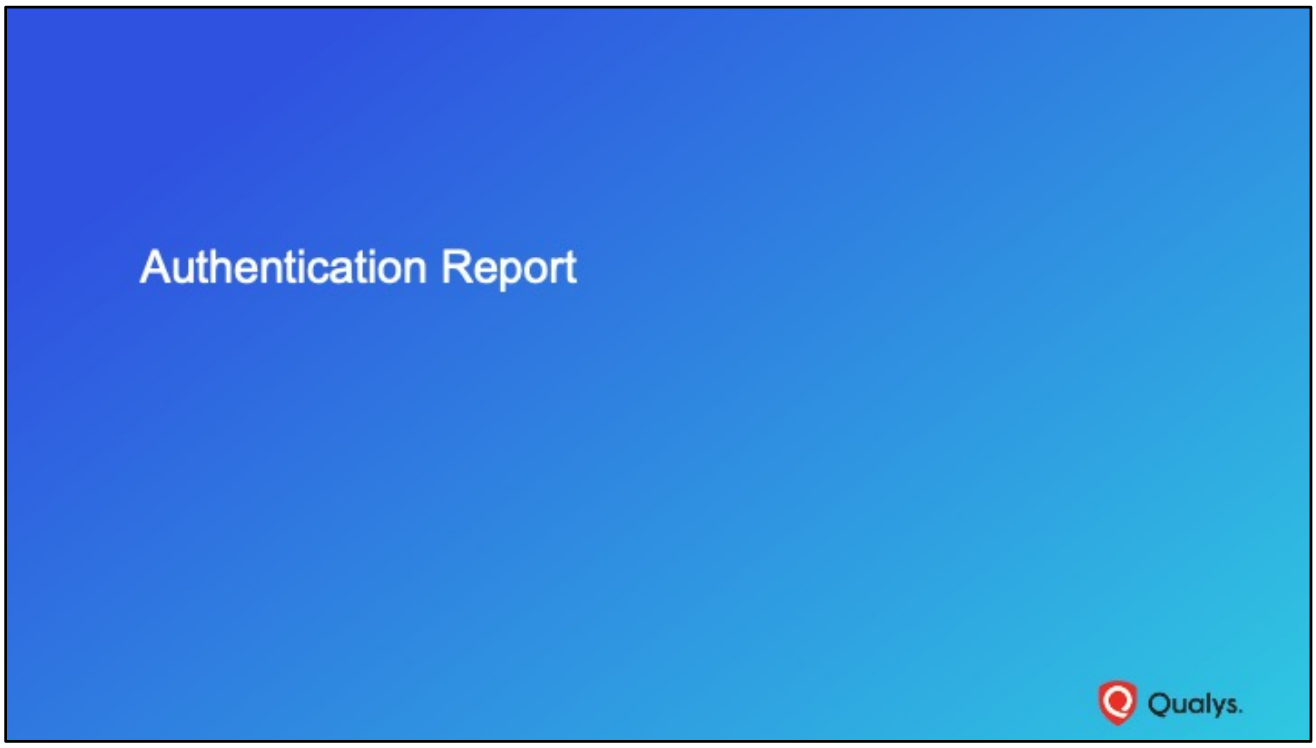
Run a fixed Vulnerabilities report. There is an importable template already available to you in the report templates section. Remediation reports can help you measure open tickets and how long they've been open. You can use trend reports in your scan report template to see Business risk by asset group over time.

Vulnerability Scorecard reports can help you define a goal for remediation and see how you are doing it.

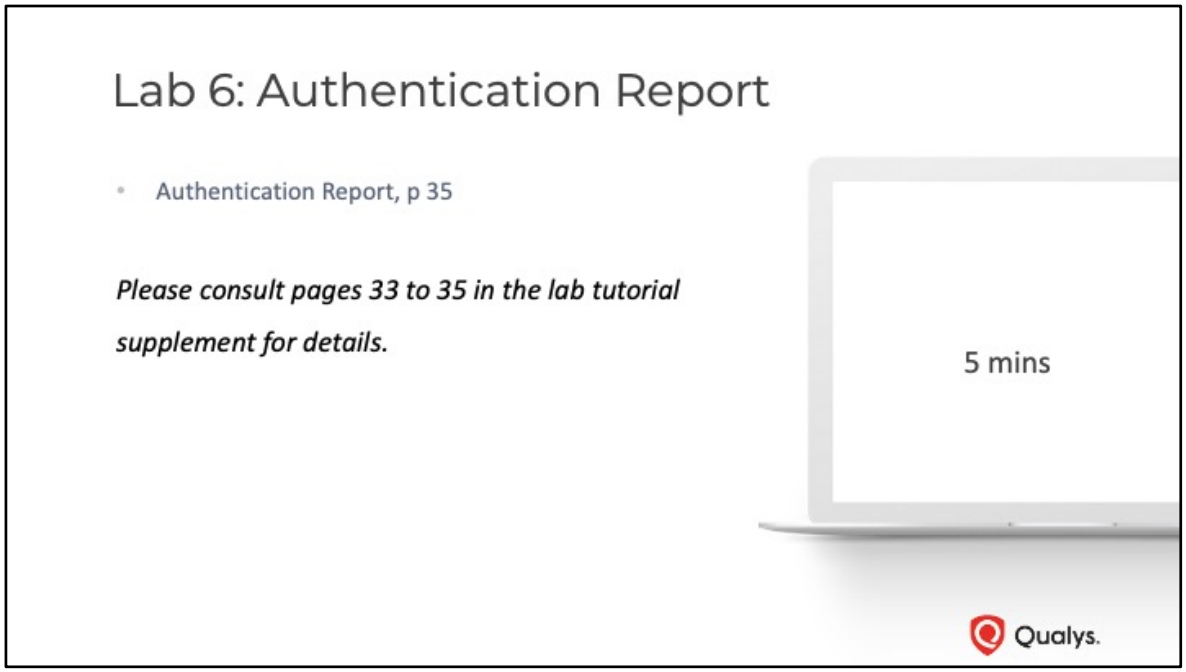


Let's consider this report example:
Say you'd like to create a Report including a Trending Graph. The graph in the report does not increase the size of the output file by much, but the amount of transitional data for each detection for each asset the Qualys platform must process to build that Trending Graph increases by many folds. Further, if detections have a long history with high volume of transitions, the Qualys platform now has to process a lot more data for the same number of detections. This could severely impact the success rate for report generation.

Suggestion: Reduce the trending period and/or apply vulnerability filtering and/or apply asset filtering. All these actions will reduce the data the Qualys platform has to process and increase the success rate.



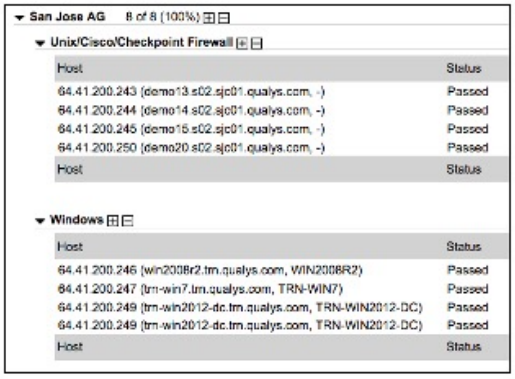
This section describes the Authentication report.



- You will build an Authentication Report and see what the result looks like.

Report Generation

- The Authentication Report shows the authentication status for each scanned host:
  - Passed
  - Failed
  - Passed with insufficient privileges
  - Not Attempted
- Run this report after performing an authenticated scan.

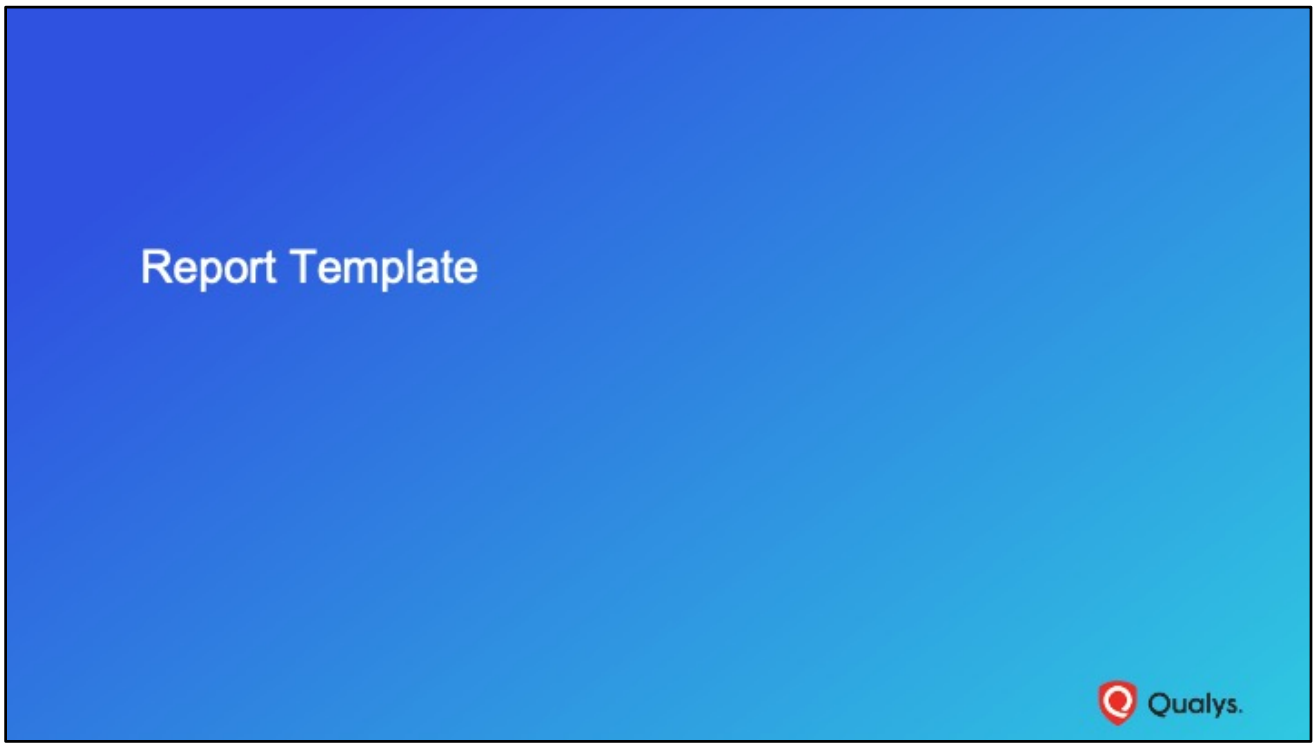


Qualys.

When running an authentication report, you must first define the report format. The PDF file format is commonly used, with "scheduled" authentication reports. Other options include: HTML, CSV, and XML.

Next, select the assets to report on. This can be either Business Units, Asset Groups, IP, or Asset Tags. The option you select here determines how the report data will be grouped.

Host assets from the target you select will be listed along with the status (PASS/FAIL) of the last authentication attempt.



This section outlines the steps to create a vulnerability report and the two types of findings that can be included in a report.

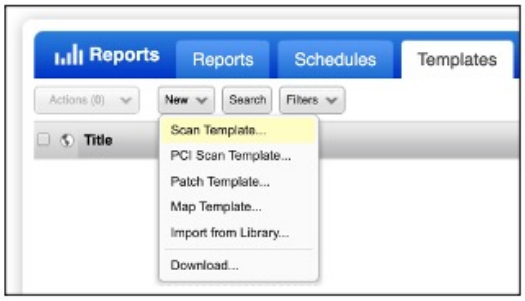
Steps to Create a Vulnerability Report

1. Perform host assessment:
   - Qualys Scanner Appliance
   - Qualys Cloud Agent

2. Run report using a Report Template:
   - Use a pre-defined report template

   OR

   - Create a custom report template



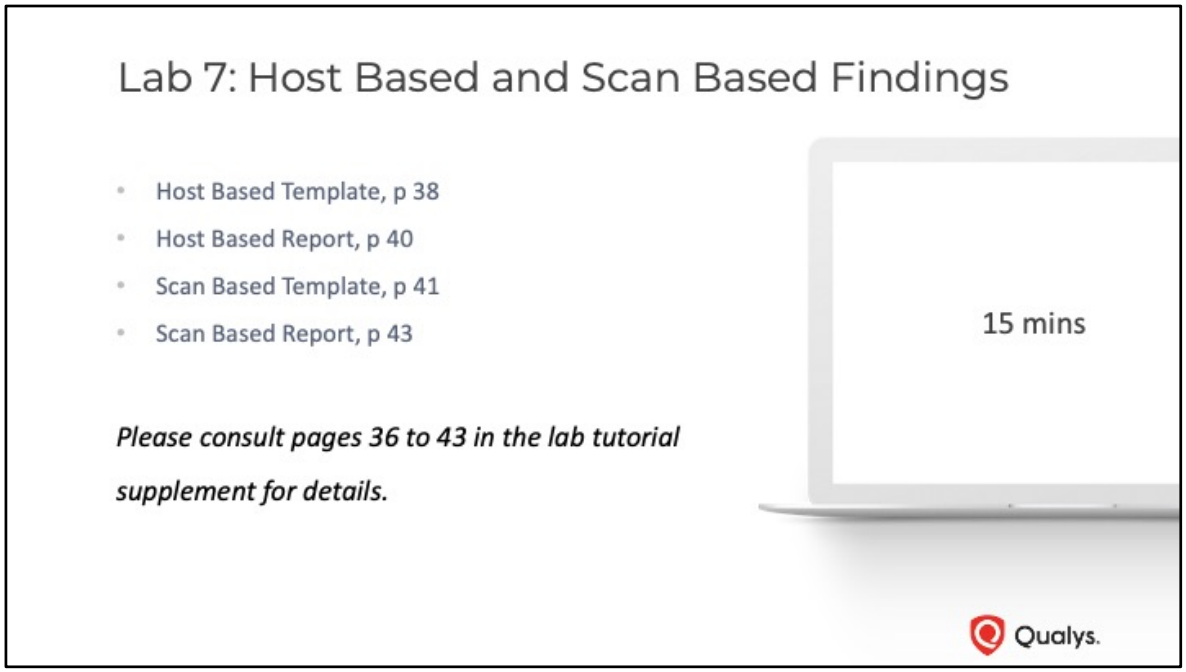
Qualys.

Before you can create a custom vulnerability report, you'll first need to perform an assessment of targeted host assets, to collect the host data that will ultimately produce various findings. Presently, Qualys provides two different ways for you to perform a host assessment: You can launch a scan using a Qualys Scanner Appliance or you can deploy Qualys Cloud Agent directly onto your host assets.

Once you have used scanners or agents to collect your host data, you'll then build or create a Report Template that contains your custom reporting preferences.

When you have a Report Template that satisfies your needs, you'll use it to generate a report for host assets you target.

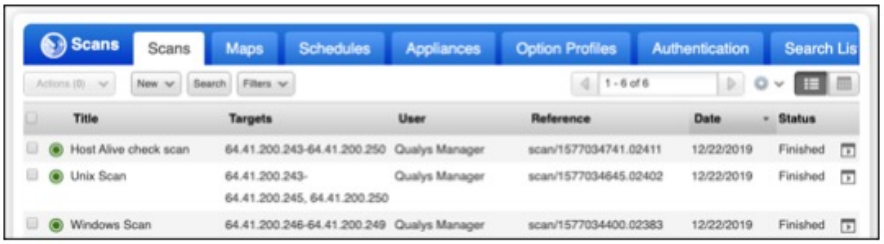
It's important to note that data collection via scanner appliance or agent must be completed first before generating a report.



- Host-based vs Scan-based findings is covered in this one lab.
- Activity 1, you will make a host-based template.
- Activity 2, you will run a report off the host-based template and see what the report looks like.
- Activity 3, you will make a scan-based template. As you build it under the Display section of the template watch how those settings are filtering what results you see in the report.
- Activity 4, you will run a report off the scan-based template and at the end you will see this report has more depth of information (because you filtered less than the host-based activity).

Scan Based Findings

- Scan Based findings (or “raw” scan reports) are found under the “Scans” tab
- Scan Based findings are ideal for “snapshot” reports that target a specific point in time

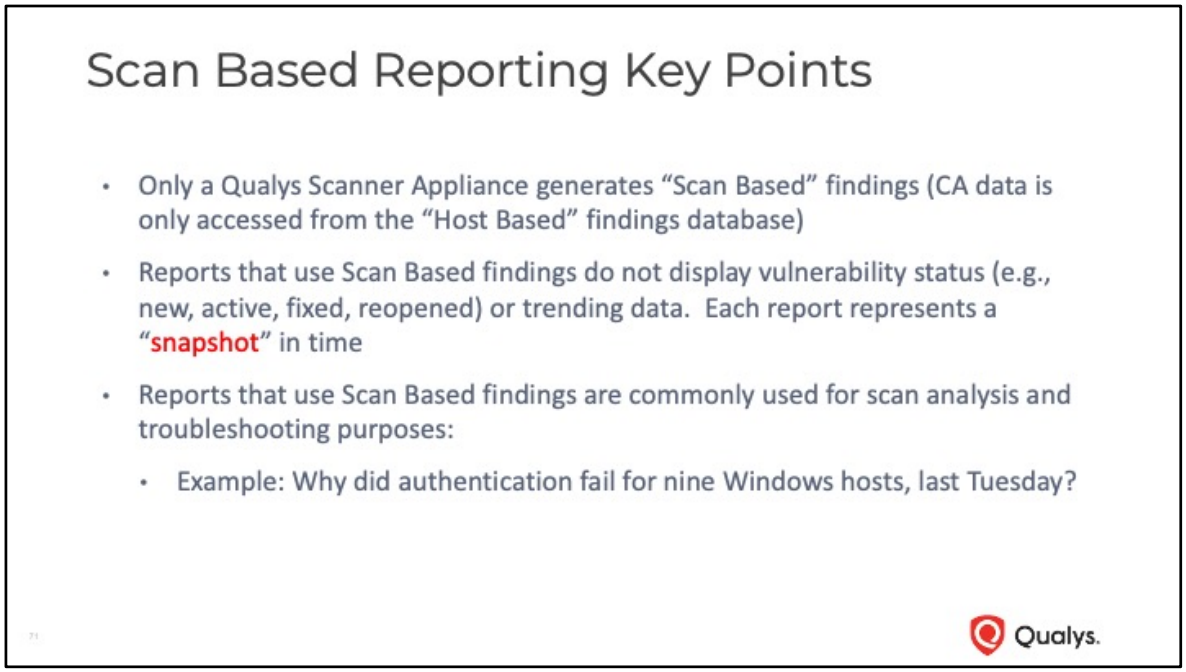


Qualys.

You can view all of your SCAN data within the Vulnerability Management application by clicking the "Scans" menu, followed by the "Scans" tab. These are your Scan Based findings.

Every vulnerability scan performed within your Qualys account is listed here; not counting, of course, any scans that have been deleted.

If you want to create a report that focuses on data and findings collected at a specific time--on a specific date--your report should use Scan Based findings.

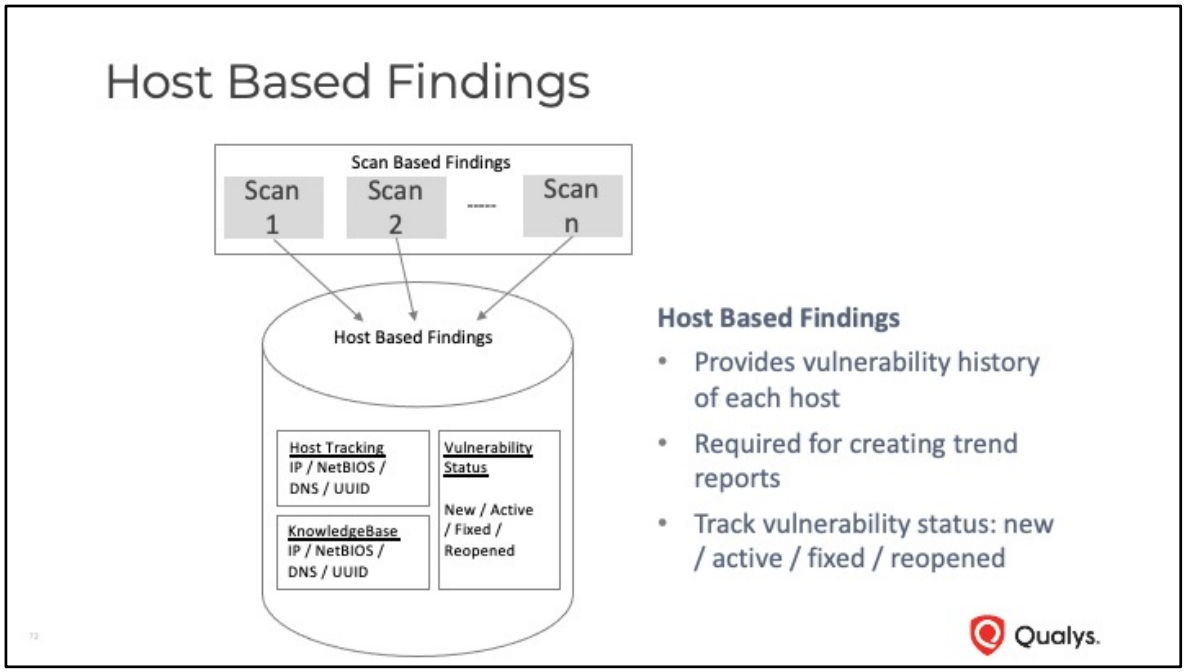


Scan Based findings are only generated for assets that have been scanned with the Qualys scanner appliance. Since the Qualys Cloud Agent is in an automated continuous scan mode, it only generates Host Based findings.

Scan Based findings include point in time snapshots of the assets. As a result, vulnerability status is not displayed.

Most of the time you'll be using Host Based findings – this focusses on the latest posture of the asset.

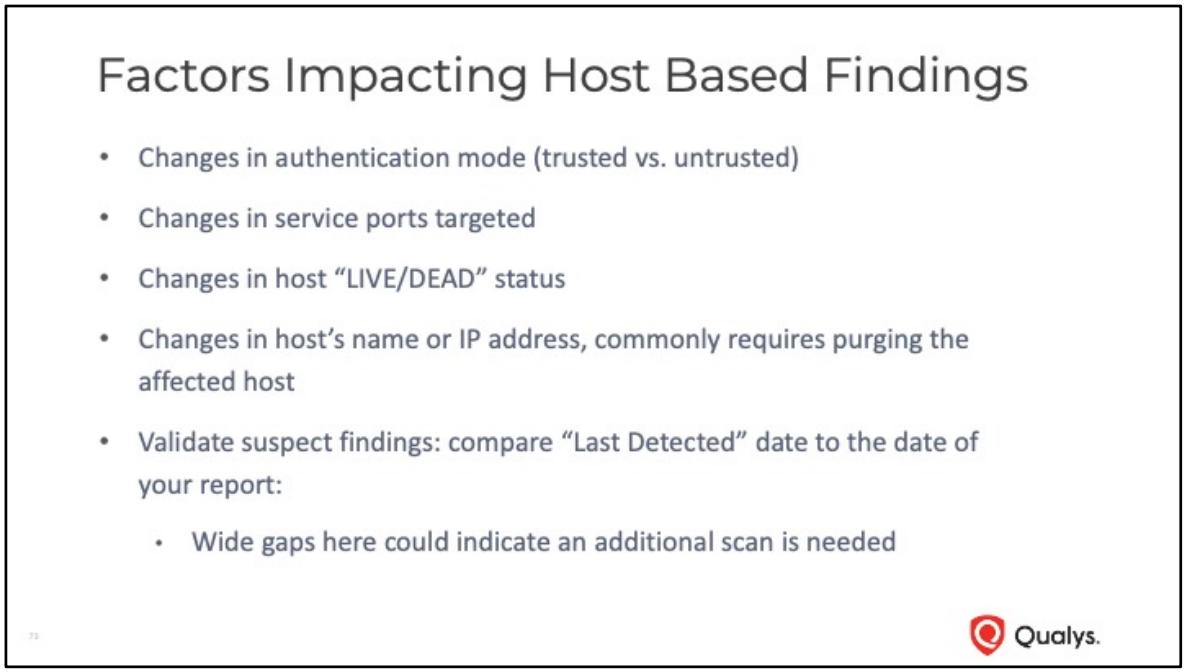
Scan Based findings are occasionally used to view a past-dated posture of the asset or for troubleshooting purposes – like how did it take to scan a host on a day, did authentication pass or fail, which authentication protocol was used, how many hops were detected, etc.



All Scan Based findings are poured into another bucket known as the Host Based findings.

The Host Based findings database collects data from completed scans and indexes each detected vulnerability according to the "tracking method" you have selected for each host asset.

Host Based findings will allow you to view the vulnerability history of any host asset, and unlike Scan Based findings; Host Based findings allow you to create vulnerability "trend" reports that track the status of any vulnerability (from new, to active, fixed, or reopened) on any host.



When working with Host Based findings, be aware of the impact made by: 1) Changes in authentication mode, 2) Changes in the targeted service ports, and 3) Changes in host "LIVE/DEAD" status

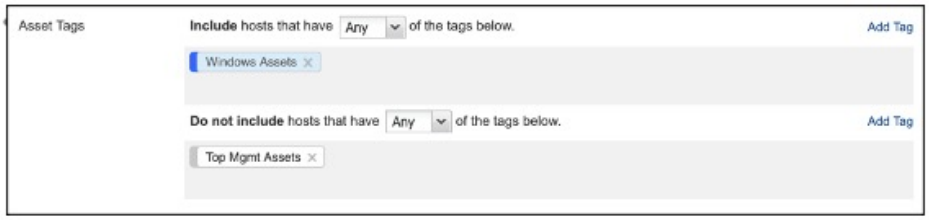
Another factor to consider when working with Host Based findings are changes in host name or IP address. If a host is configured to use its host name or IP address to track its detected vulnerabilities, any changes to the host name or IP address could potentially result in vulnerabilities being associated with the wrong host. Purging the host-based findings immediately following a host name change or IP address change, is a commonly used practice.

Keep in-mind that discrepancies in your vulnerability findings (perhaps a finding is displayed as ACTIVE, and you were expecting to see FIXED) can be resolved by performing an additional scan.

When analyzing such discrepancies, compare the "last detected" date of the suspect finding to the date of your report. Wide gaps between the last detected date and the report date could be an indicator that an additional scan is required.

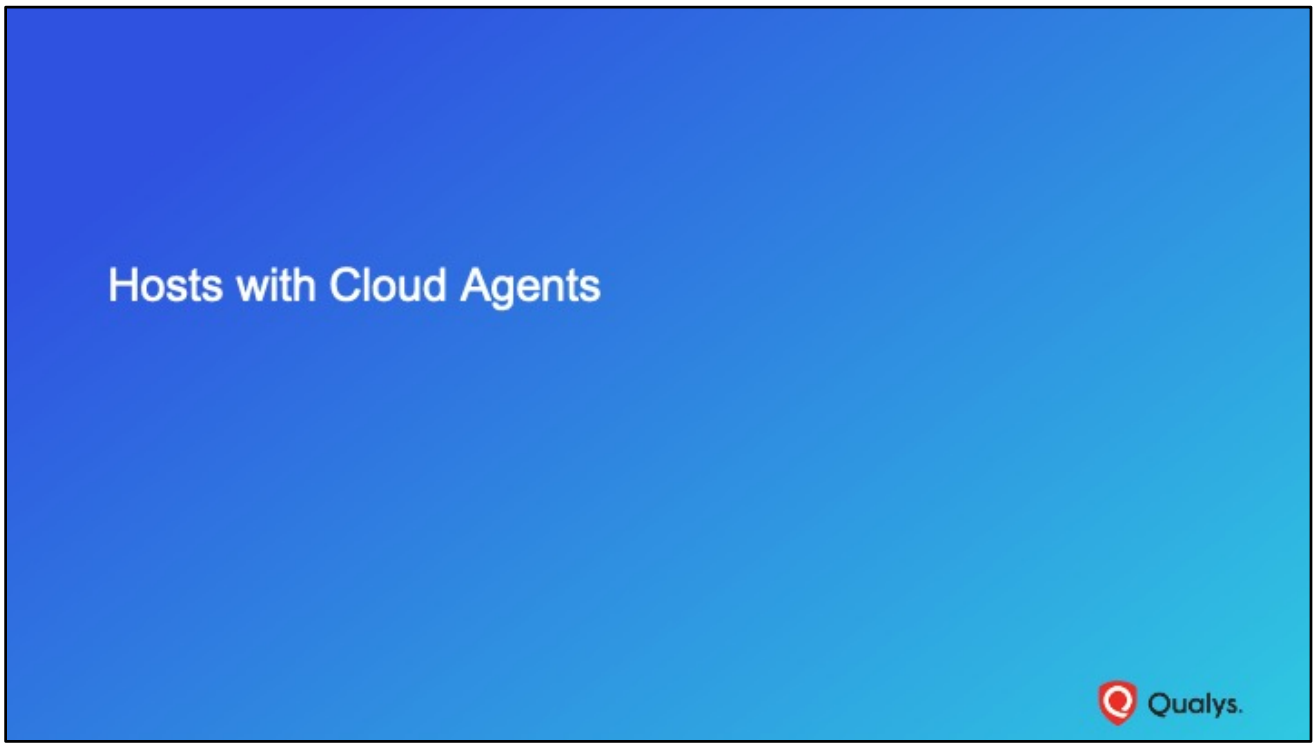
Report Source - Asset Tags

- Using Asset Tags allows you to include hosts that match certain criteria, even if your network is constantly changing as hosts are added and removed

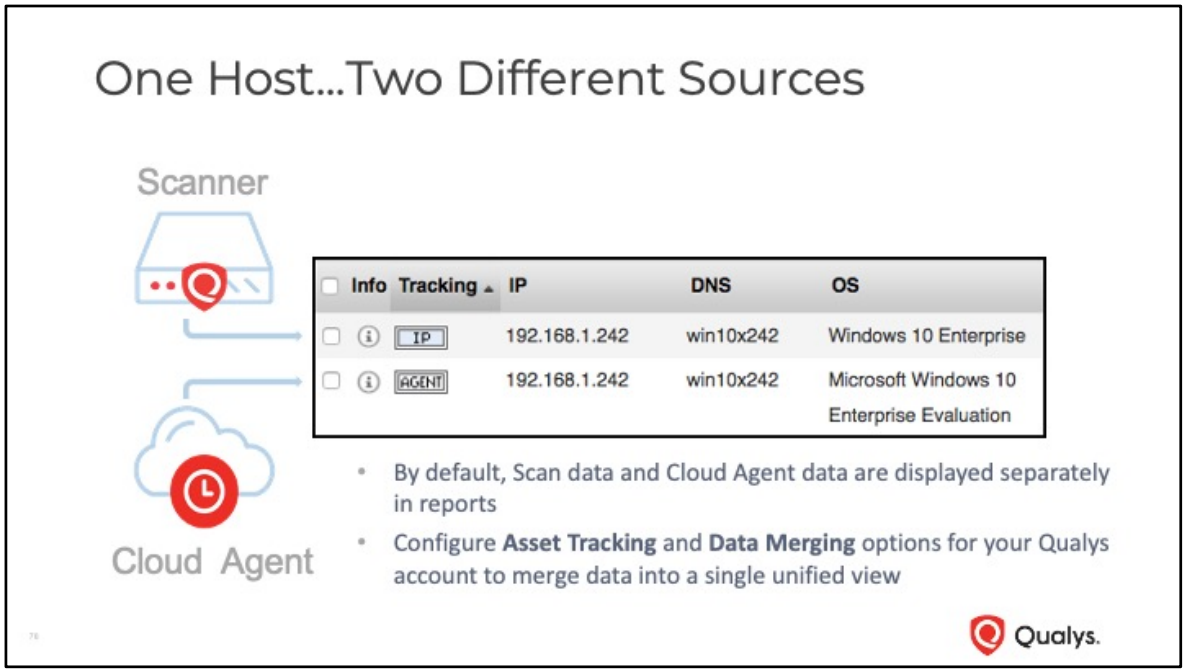


Qualys.

Asset Tags can be used as targets for your reports. Tags allow you to target hosts without worrying about hosts changing IP addresses. Asset Tags support include/exclude where asset groups and IP ranges do not, or not without extra effort.



In this section, we'll focus on report settings and options available for Cloud Agent hosts that are also scanned with a scanner appliance.



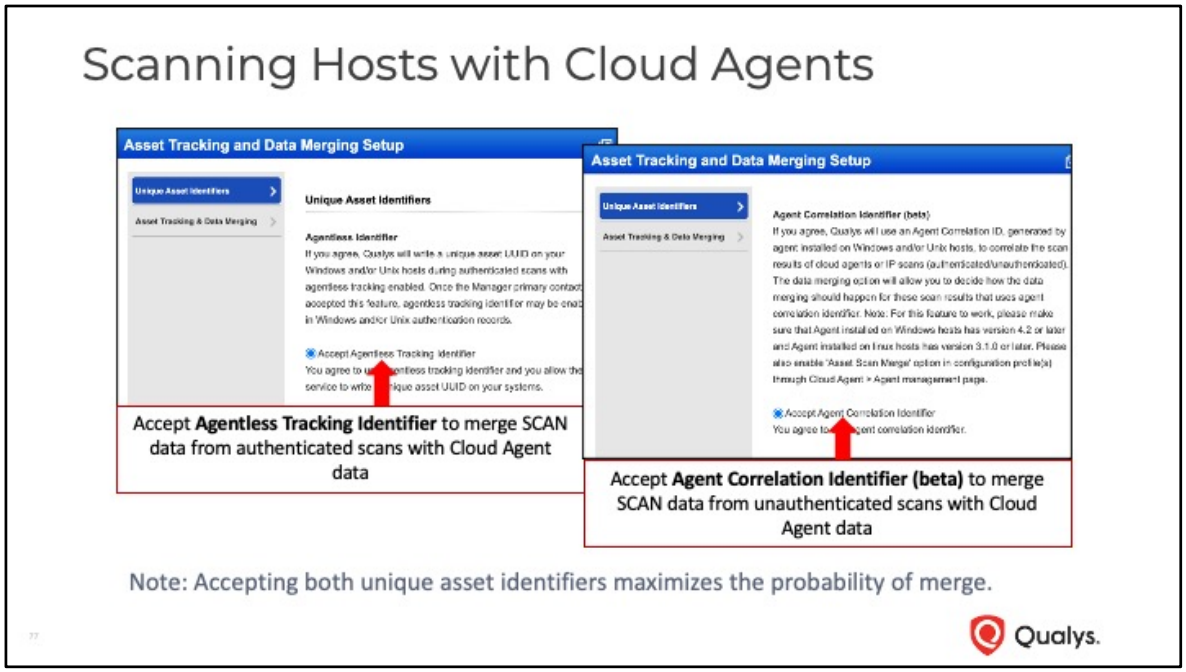
When you use a Qualys scanner appliance to scan a cloud agent host, the scan data in your account is kept separate from the agent data.

In this example a Windows host (IP address 192.168.1.242) is the source of both AGENT data as well as SCAN data.

By default, when you run a report on this host you will see two records for the same host. One record contains data collected by the scanner appliance, and another contains data collected by the Cloud Agent. This is true for both authenticated and unauthenticated scans.

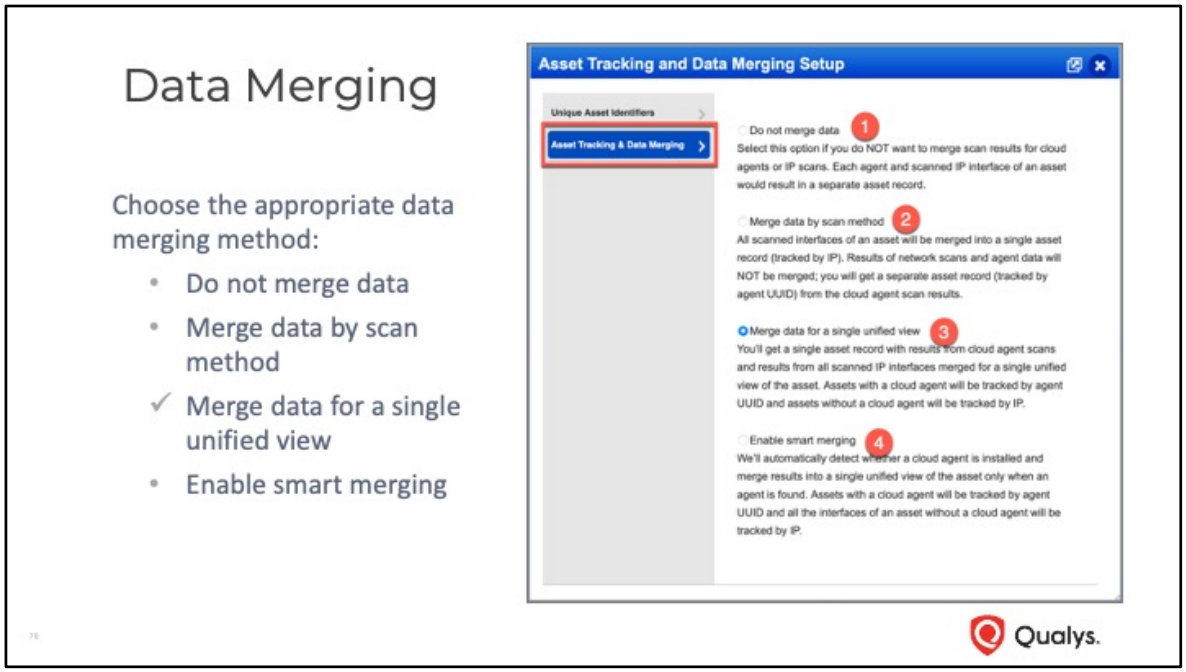
Unifying scan data and agent collections is key for asset management, metrics and understanding the overall risk for each asset.

To merge data from the scanner and the Cloud Agent into a single unified view, you must enable appropriate **Asset Tracking and Data Merging** options for your Qualys account. This is explained further in the subsequent slides.



- Use the **Agentless Tracking Identifier** feature to merge **authenticated** vulnerability scan results from scanned IP interfaces and agent VM scans for your Cloud Agent assets.
- Use the **Agent Correlation Identifier** to merge **unauthenticated** vulnerability scan results from scanned IP interfaces and agent VM scans for your Cloud Agent assets.
- Please consult the following link for more information on Agent Correlation Identifier and the Unauthenticated Scan Merge feature. https://success.qualys.com/discussions/s/article/000006550
- You can use one or both identifiers. Accepting both unique asset identifiers for your account will in fact maximize the probability of merge.

Note that once accepted, there are additional steps that must be completed before you can start scanning with Agentless Tracking Identifier or the Agent Correlation Identifier.

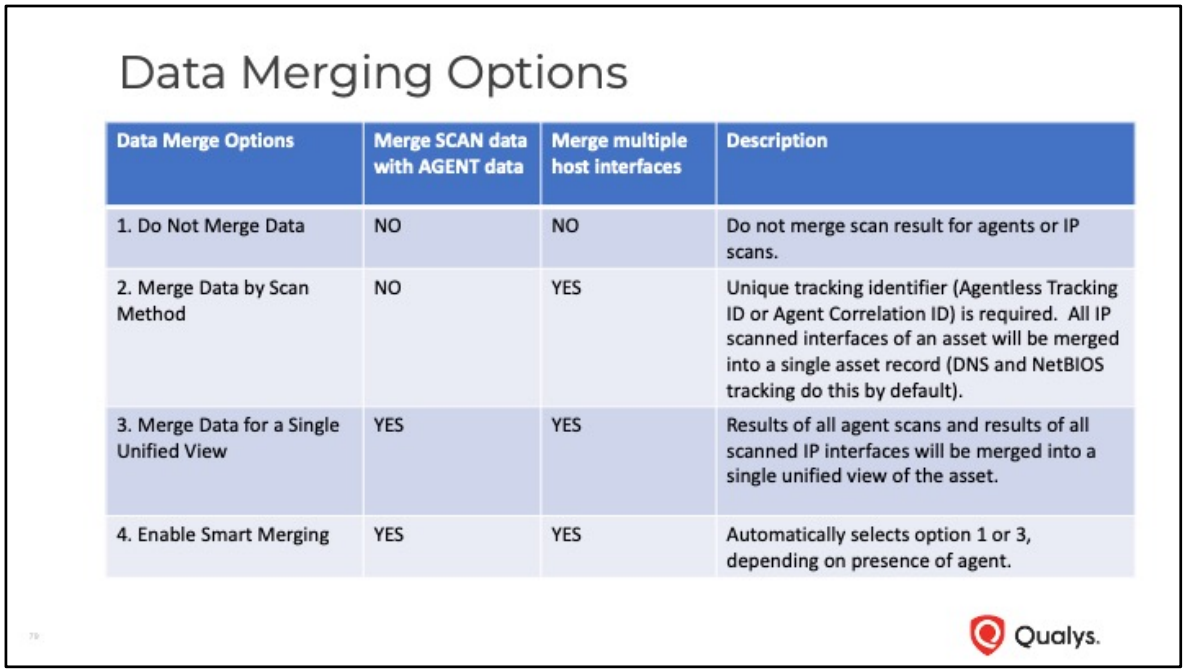


The next step is to configure the appropriate Data Merging option**.**

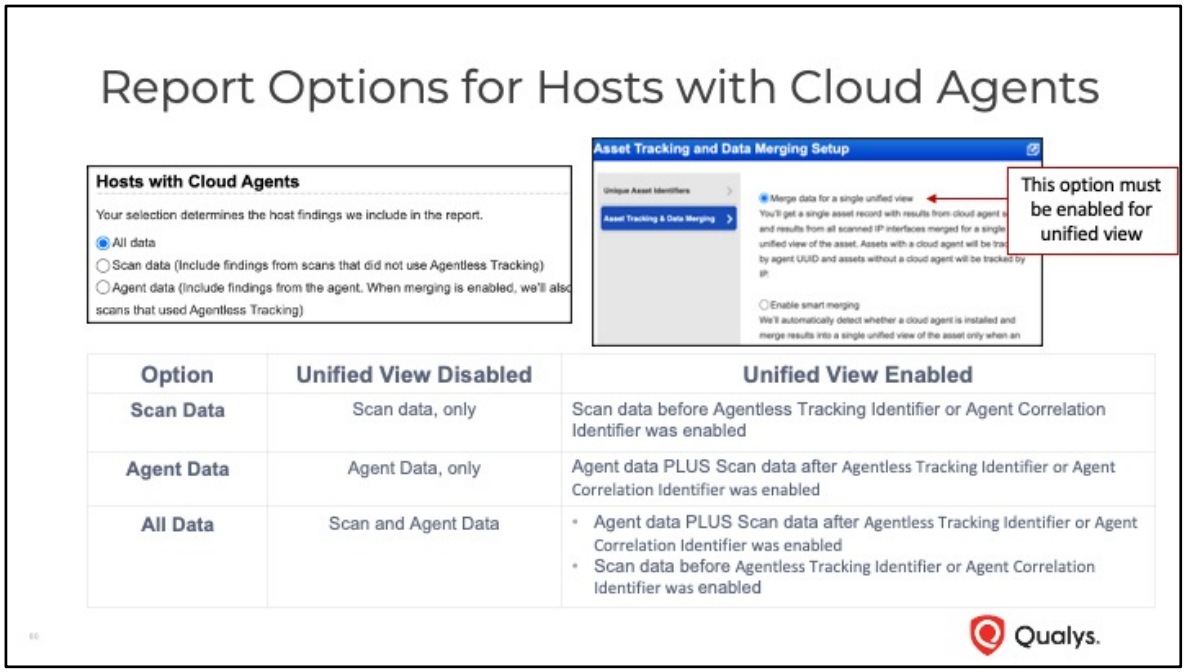
MERGE OPTIONS:

1. Do not merge data - Data collected from agents are displayed separate from data collected by scanner appliances. Hosts with IP tracking enabled will display separate asset records for all scanned interfaces.
2. Merge data by scan method - When combined with the Agentless Tracking Identifier, option two merges data collected from from all scanned interfaces (i.e., IP tracking enabled) into a single asset record.
3. Merge data for a single unified view - Data collected from agents are merged with data collected from scanner appliances into a single unified view.
4. Enable smart merging - Option three will be automatically selected for hosts with agents installed. Option one will be used for hosts without agents.

When option number three is selected, SCAN data and AGENT data are merged together into a single unified view.



The table in this slide indicates scenarios where Scan data from one or more IP interfaces is merged with Cloud Agent data depending the Data Merging options configured in the Qualys account.



When configuring the report template, under the Findings tab, we have a setting that applies to hosts with Cloud Agents. Here we can choose to display the scan data or data collected by the agent or both. When you make the selection here, the data shown in the report is dependent on whether Unified View is enabled for your subscription or not.

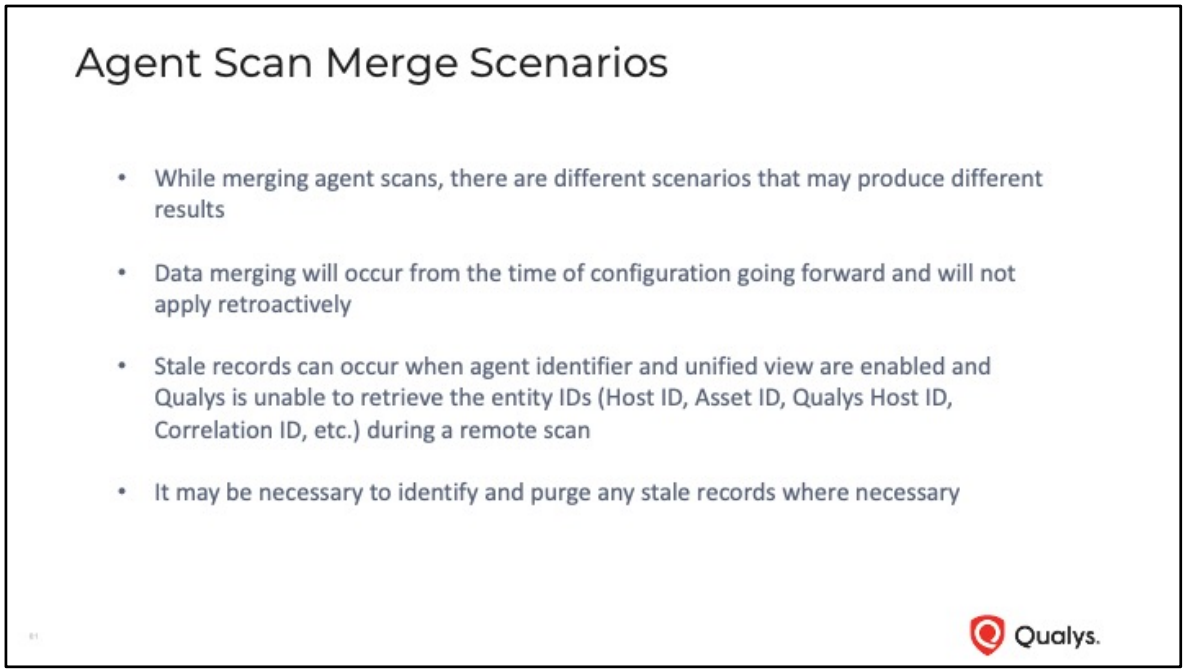
When you have Unified View disabled for your subscription, choosing scan data will only produce scan data, agent data will only produce agent data and all data will include both scan data and agent data displayed as 2 separate records.

When you have Unified View enabled for your subscription, and you select SCAN data, the report will only include scan data before any of the unique asset tracking identifiers were enabled for your subscription.

Choosing the Agent data option, will include AGENT data and any SCAN data that was generated after any of the unique asset tracking identifiers were enabled for the subscription.

And lastly, with All data selected, the report will include SCAN data from both before

and after any of the unique asset tracking identifiers were enabled. Plus you will also have agent data.



While merging Cloud Agent data with scan data, there are different scenarios depending on whether a scan (authenticated\unauthenticated) was run first or Cloud Agent data was collected before any scan. These scenarios may produce different results. Here are some of the scenarios to consider:

- Agent Collection followed by Unauthenticated scan
- Unauthenticated scan followed by Agent Collection
- Agent Collection followed by Authenticated scan
- Authenticated scan followed by Agent Collection
- EC2 hosts- Agent Collection followed by Internal EC2 scan
- EC2 hosts- Appliance Scan first (No IP tracked record and no agent tracked record)
- EC2 hosts- Agent Collection first (No IP tracked record and no agent tracked record)

What happens to my current duplicate records?
The merging will occur from the time of configuration going forward. Qualys will not retroactively clean up any IP-tracked assets generated due to previous configuration.

Also, stale records can occur when unique asset identifiers and unified view are

enabled but the scanner is unable to retrieve the Agentless Tracking Identifier (due to failed authentication*)* or the Agent Correlation ID (ports blocked, QID 48143 not included in scan, etc.).

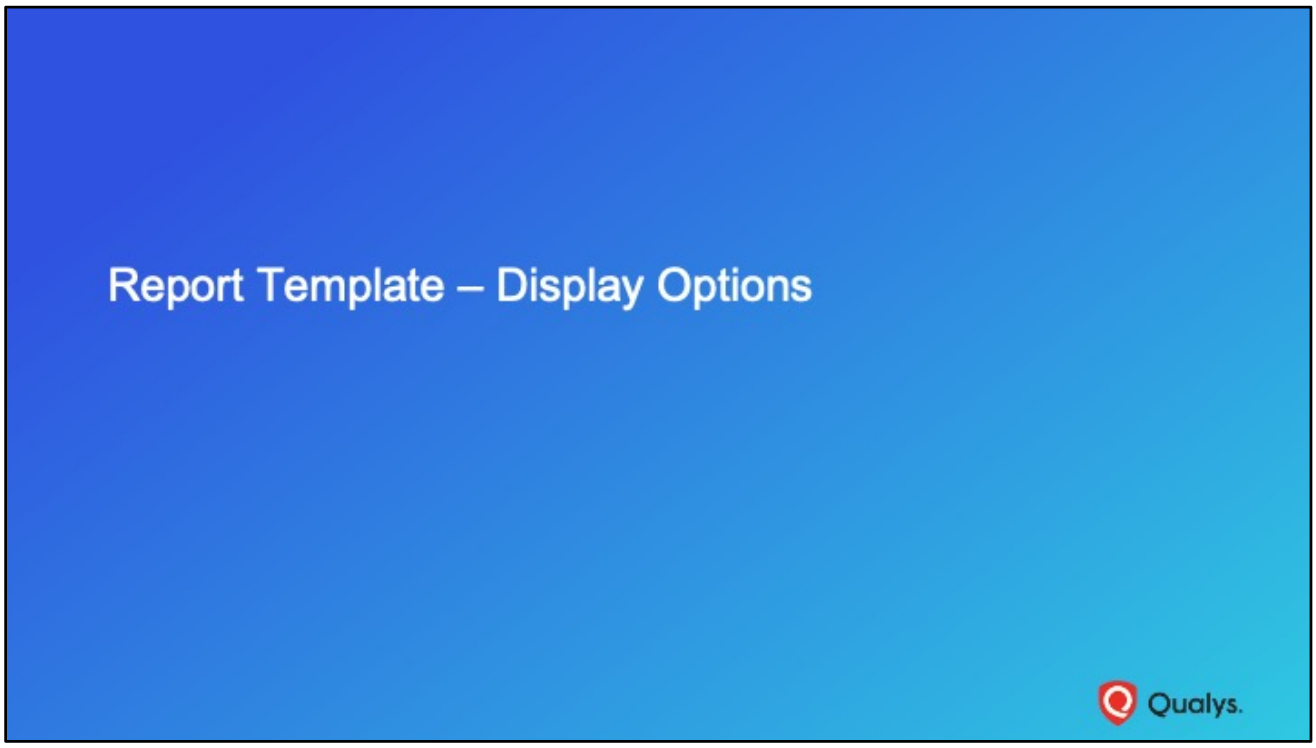
It's necessary to identify and purge any stale records when above conditions exist.

Please consult the following documents for more information:

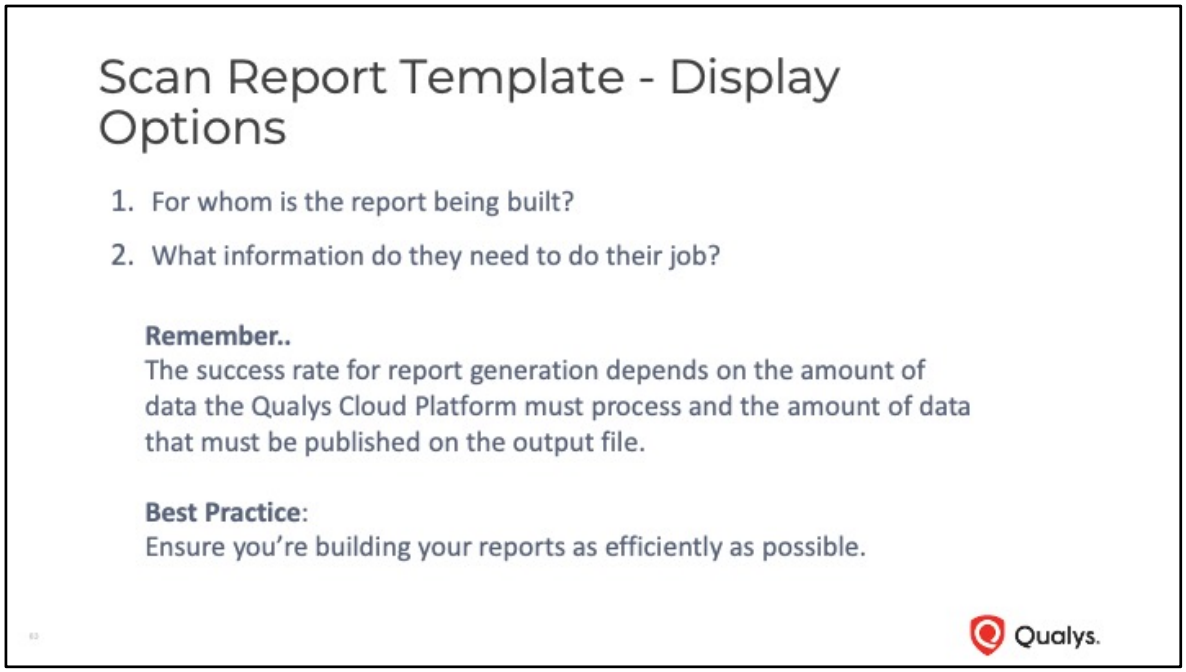
Agent Scan Merge Cases
https://success.qualys.com/support/s/article/000006543

Understanding Entity IDs in VM
https://success.qualys.com/support/s/article/000006216

Identification of Stale Records with Agentless Identifier and Unified View Enabled
https://success.qualys.com/support/s/article/000006149



In this section, we'll breakdown the various "Display" options in a Scan Report Template.

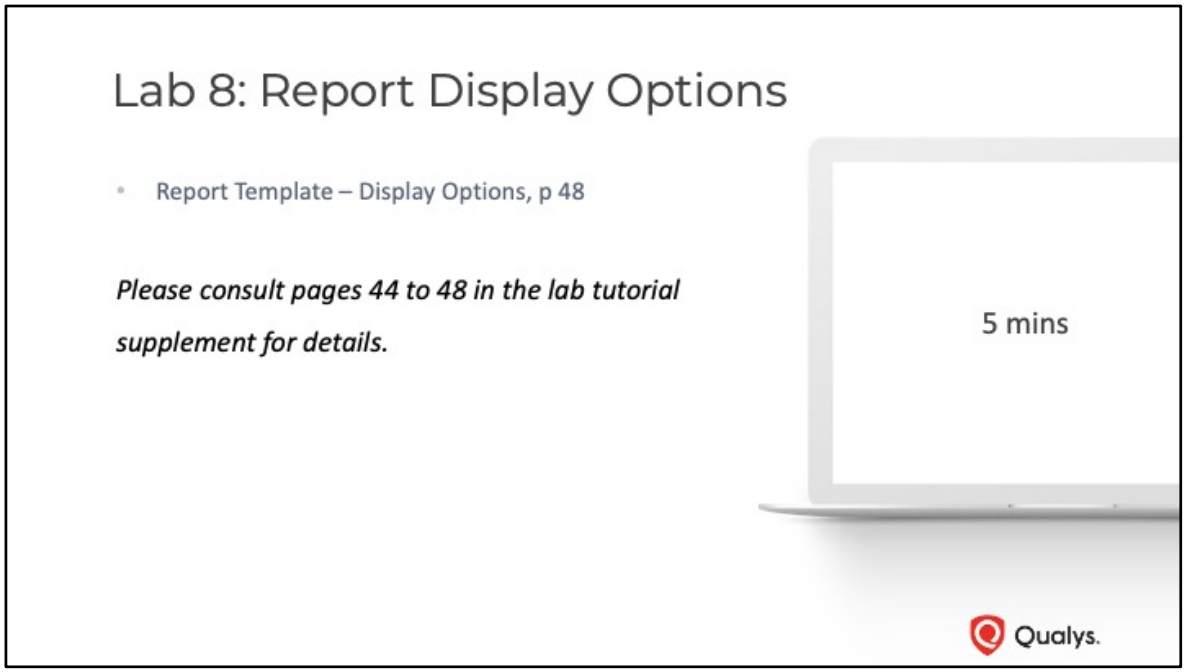


A common theme you'll find when building reports is considering the audience. Whenever building a report, ask the question, for whom am I building this report?

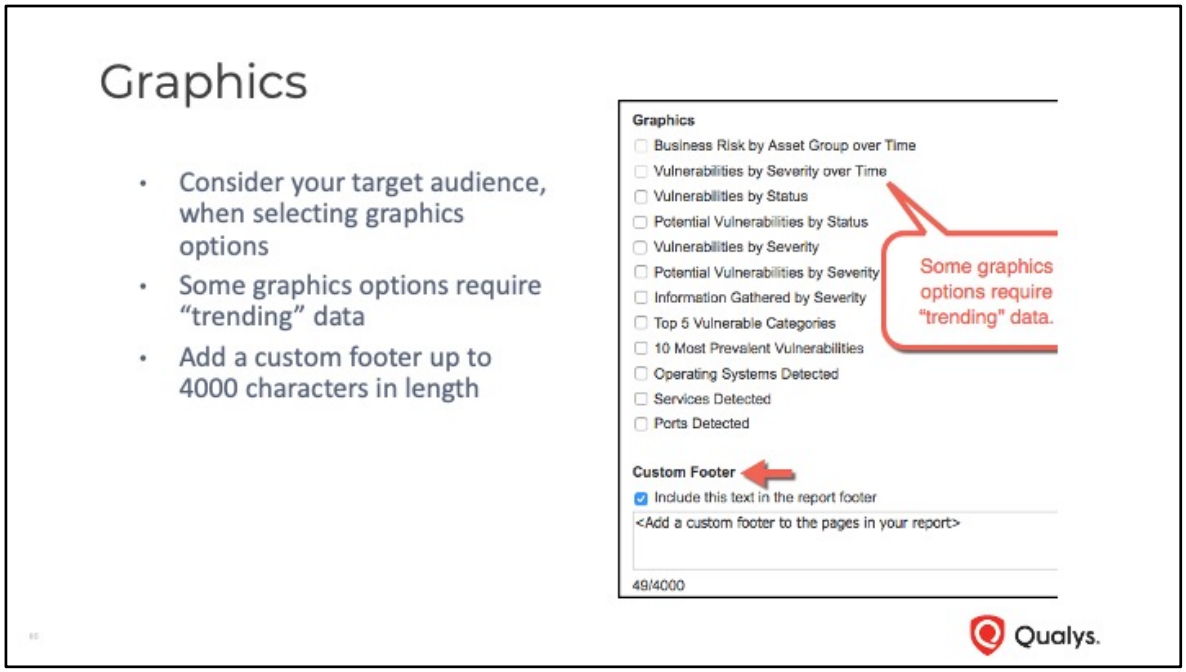
Are you sharing this report with a high-level executive, or are you sharing it with a sys admin who is going to be part of the patching program? Obviously, that will dictate what goes in your report.

The next question you should ask is, what do they need to see?

The point is to make your reports as succinct at possible. You can always add more information to your template if requested. Best practice is to ensure you're building your reports as efficiently as possible.



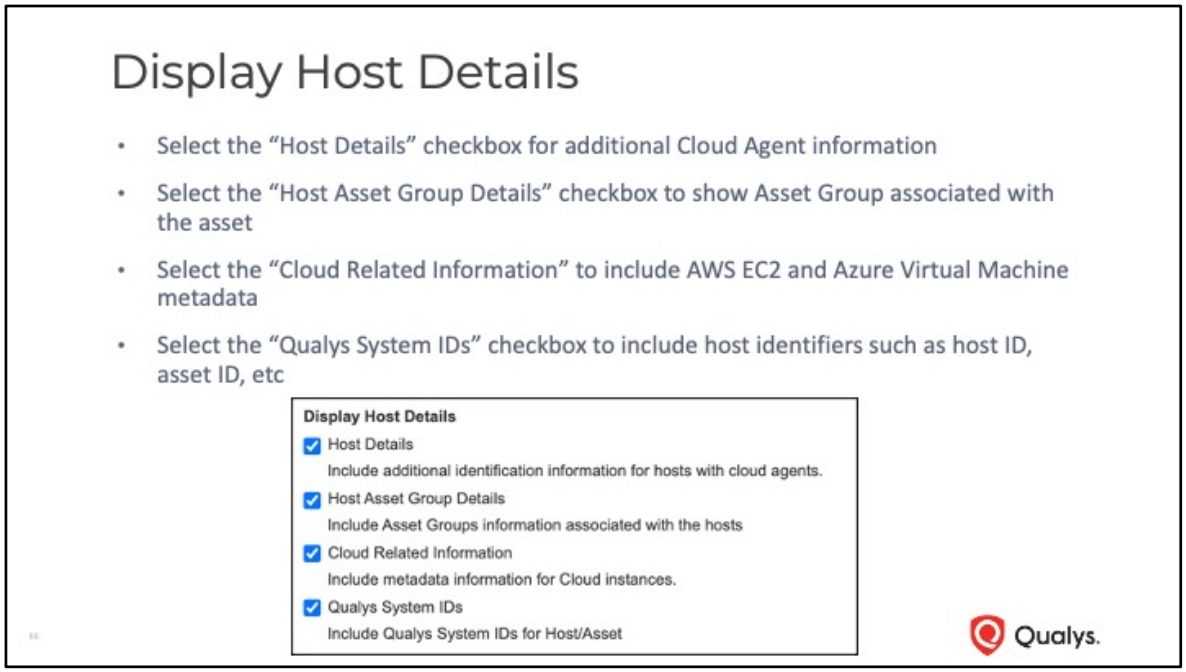
- Here you will edit a template and the activity will take you through the Display tab.
- At the end of the activity notice how the Display settings impacted the report Detailed Results.



The next item we come to in the display section is graphics. Does the person viewing the report care to see a graphic in the report that provides a breakdown what you've checked?

A quick note on a couple of these options. If using the top two graphic options, you have to be using trending host based findings over a period of time, otherwise these options will be greyed out.

The custom footer allows you to put information at the bottom of your report. Maybe you are distributing the report, and you want people know that it's confidential.

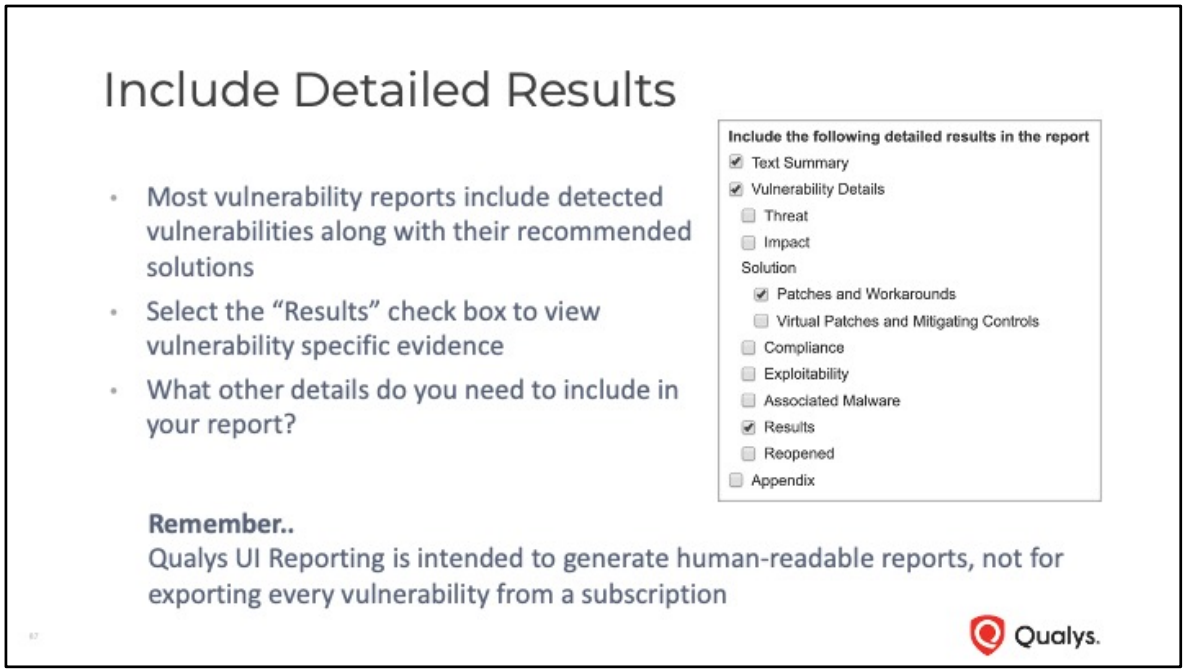


Select Host Details for information about Cloud Agent hosts.
Specifically, it will give us the Asset ID for the Agent host. This is the unique identifier associated with all Cloud Agent assets.

Select the “Host Asset Group Details” checkbox to show Asset Group associated with the asset.

For reports that target AWS EC2 and Azure Virtual Machine assets, select the “Cloud Related Information” check box.
Azure metadata information: public IP address, image offer, image version, subnet, VM state, private IP address, size, subscription ID, location, and resource group name
EC2 metadata information: public and private DNS name, image ID, VPC ID, instance state, instance type, account ID, region code and subnet ID.

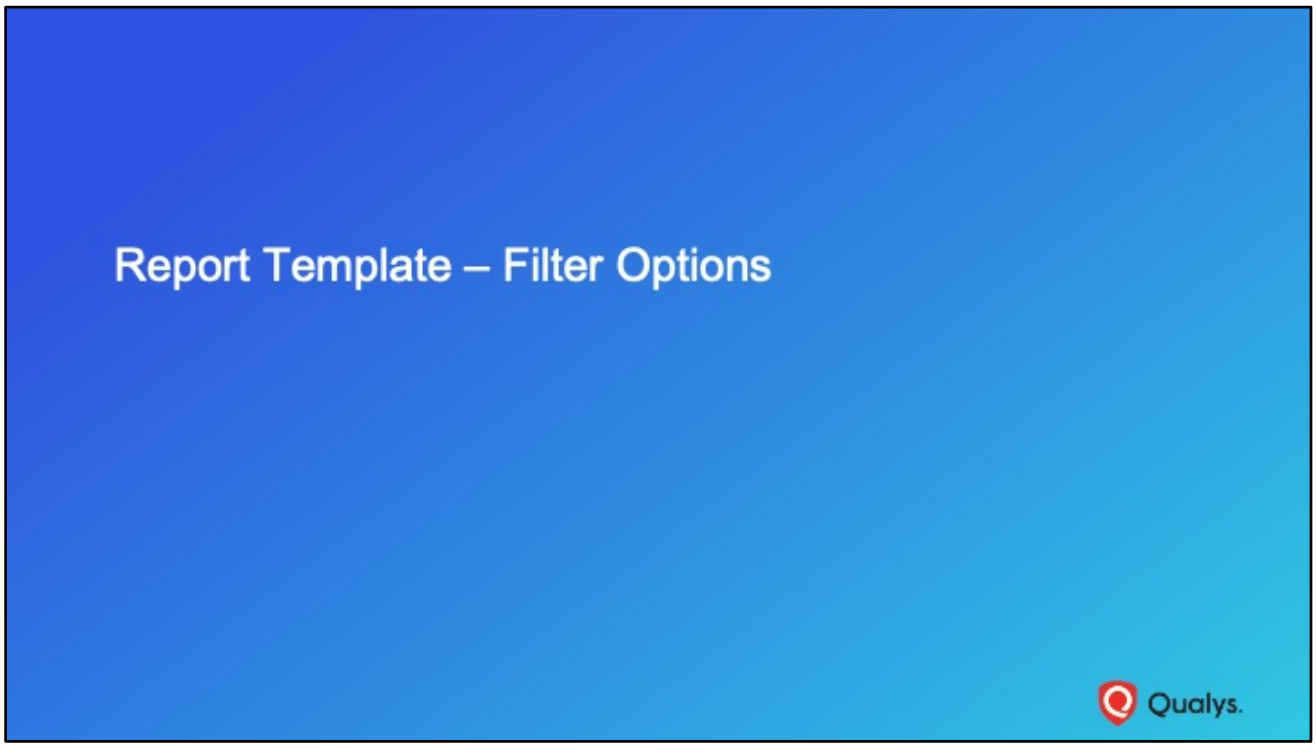
Select the "Qualys System IDs" check box to include host identifiers such as host ID, asset ID in the host-based scan report template.



If you've taken the Qualys vulnerability management course, you know that all vulnerabilities or QIDs include A LOT of information.

Checking all boxes will increase the amount of detail, as well as the report size and the amount of time required to generate the report.

When selecting included details ask: "What does the target audience need to see?" What information is required to meet the objective at hand?

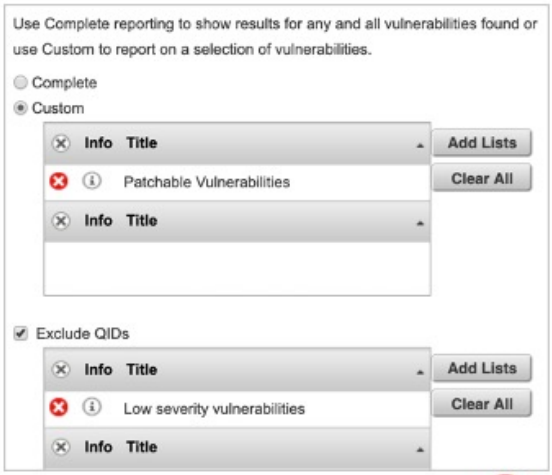


In this section we will breakdown the filter options within the Scan Report Template.

- You will attach a Search List to filter to only Microsoft vulnerabilities.

Filter Reports Using Search Lists

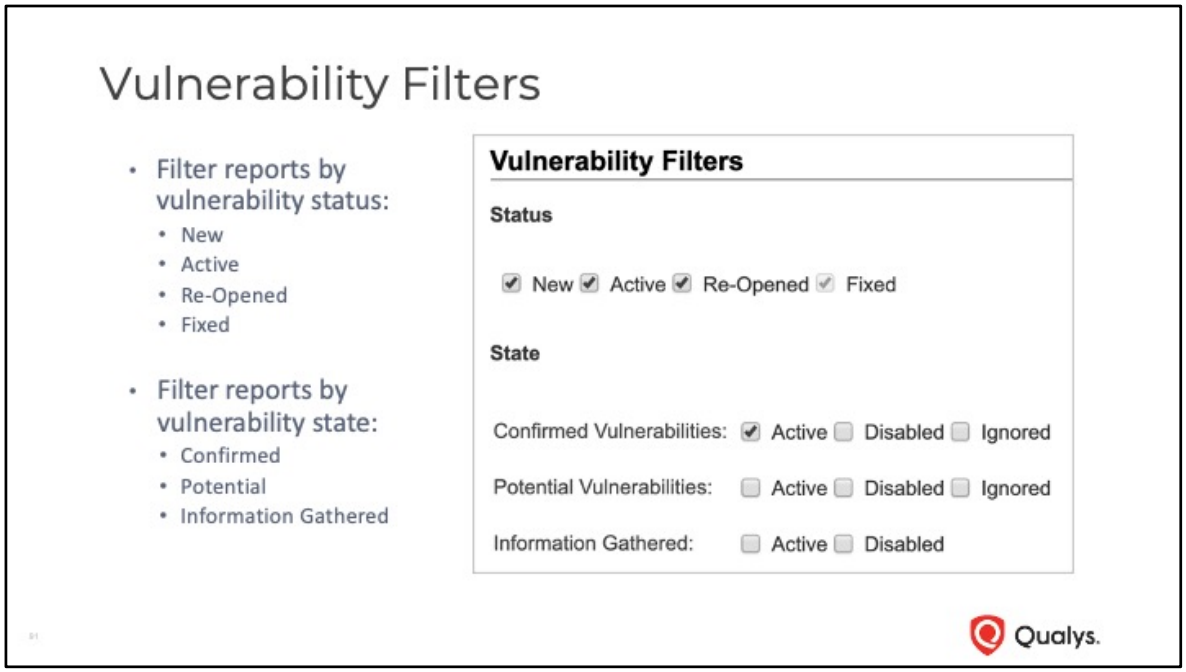
- Use search lists to filter the QID's included in the report
- Add one or more search lists
- Use search lists to also exclude QID's from the report



Qualys.

Search Lists can be used to focus on specific vulnerabilities like patchable vulnerabilities, high severity vulnerabilities, vulnerabilities with exploits etc. It can also be used to exclude specific vulns from the report. Combined with Asset Tags, it can be used to create very targeted reports.

Example: A Search List to include all patchable severity 3, 4 and 5 vulnerabilities or a Search List to exclude all Severity 1 and 2 type of vulnerabilities.



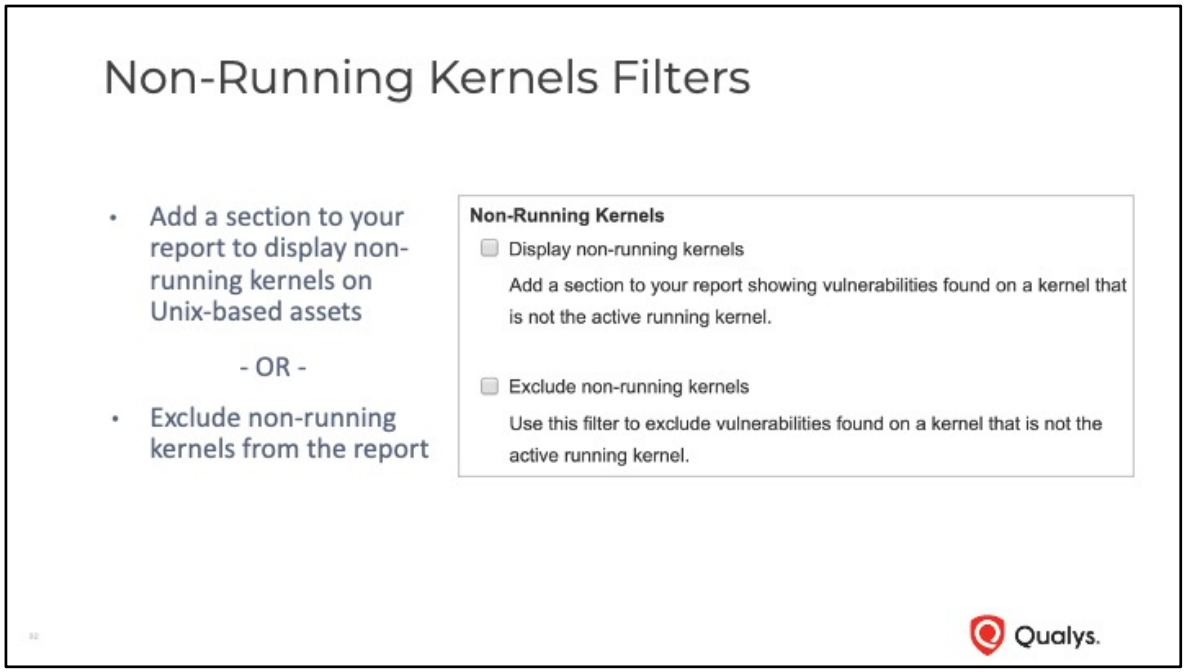
Vulnerability Filters allows you to define the status of the vulnerabilities you wish to see in the report. A vulnerability can one of four statuses:

The first time a vulnerability is detected on an asset it's status will be new. For any vulnerabilities that have been detected more than once it's status will be active. When a vulnerability is no longer detected then it's status will be fixed. For any vulnerabilities that have been fixed and are rediscovered then the status is re-opened. Please note that if you want to report on fixed vulnerabilities you need to have the trending option in the findings enabled.

Along with the its status a vulnerability also has a state, with the default state being active. Meaning that it actively scanned for and reported on. A vulnerability can also be disabled via the knowledge base. Meaning it is globally filtered out from all hosts in the scan report

For specific reasons sometimes, a vulnerability may be disabled or ignored for a period of time. If you wish to report on these then you will need to relevant state option.

An ignored vulnerability is a specific vulnerability that is ignored on a specific asset.



By default, we report all vulnerabilities on all Linux kernels (the running kernel and non-running kernels). Choose the display option to add a new section to your report listing vulnerabilities on non-running kernels or choose the exclude option to filter them out.

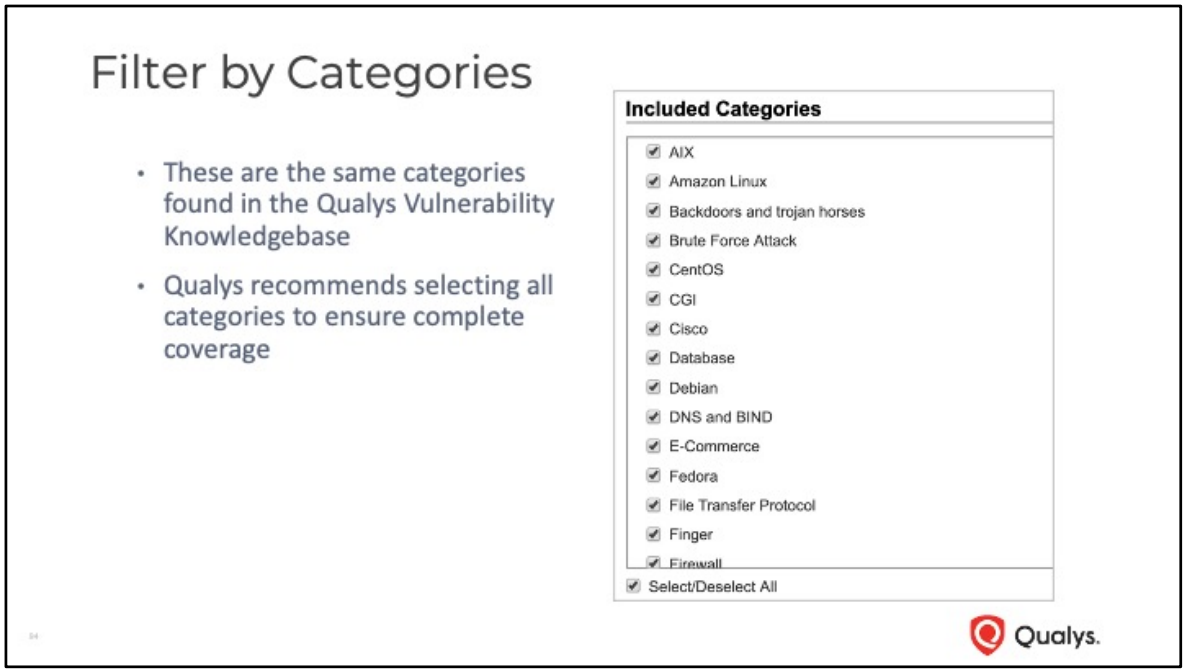
Please consult https://qualys-secure.force.com/discussions/s/article/000006209 for more information on using reporting by Running and Non-Running Kernels when using VM APIs for reporting.

Pre-defined QID Filters

- Pre-defined QID filters only apply to a specific list of vulnerabilities
- Click the "View QIDs" link to display the impacted vulnerabilities

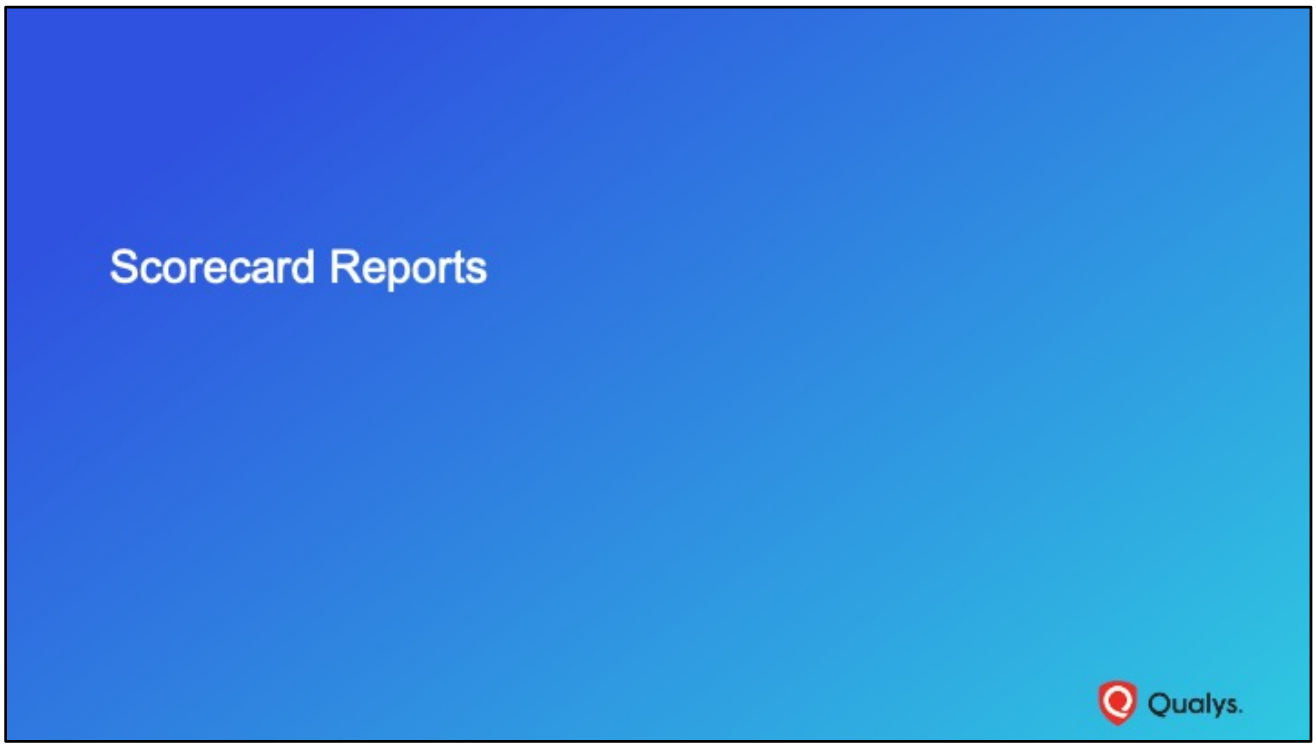
Qualys.

Select filters to exclude certain vulnerabilities from your reports like vulnerabilities found on non-running ports/services and vulnerabilities that can't be exploited because of a host configuration. These filters apply to certain QIDs only.

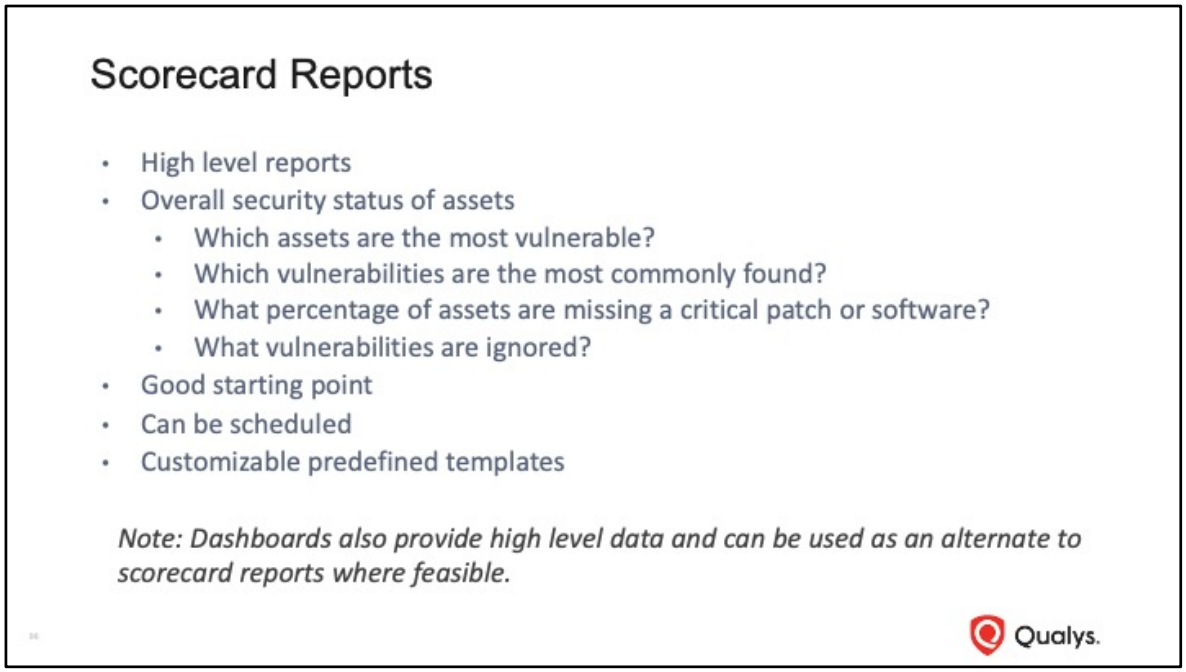


Each the QID's in the Knowledge base are assigned a category. If you wish can filter down the QID's listed in the reporting by their category. For example. If you just wanted to report on vulnerabilities in the TCP/IP category.

Qualys would normally recommend that you have all categories selected therefore reducing the chances of some vulnerabilities not appearing in the report. If you want to see a list of the vulnerabilities in a category this can be done using the search feature in the knowledge base.



In this section we'll explore the different types of Scorecard Reports.



The scorecard reports are designed to be high level reports. In that they do not contain any technical details on the vulnerabilities or patches. Instead, they are there to give you the overall security status of your assets.

This can help you get quick answers to questions like:
-Which are the most vulnerable assets
-Which are the most commonly found vulnerabilities
-How many assets are missing a critical patch or software
-Which vulnerabilities have been ignored

The scorecard report has a set of predefined templates that can be customized or used as is to run reports. These reports can also be scheduled to run automatically so stakeholders regularly get high-level reports that help them understand the overall security posture.

Please note that dashboards also provide high level data and can be considered instead of scorecard reports where applicable. However, be aware of the differences between these reporting tools. For instance, dashboards can only be accessed by a Qualys user whereas you can schedule and share your scorecard reports to non-

Qualys users too.

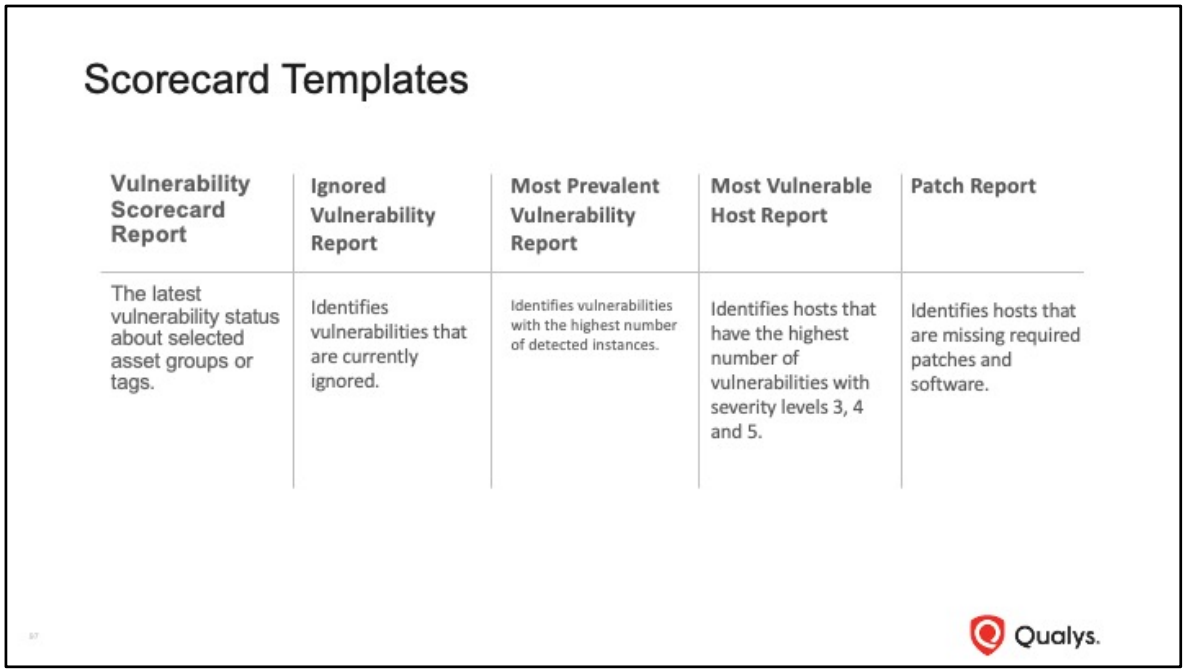
Some considerations...

•All dashboards are not created equal

•To process historical data properly, be sure to specify date/time in queries: lastVmScanDate, lastPcScanDate, lastCheckedIn, firstFound, lastFound.

•Comparing dashboarding and reporting data is not as cut and dry as you might think. In-depth understanding of your detection data, proper query formatting and proper template/search list selections is/are required.

Also, dashboard trend graphs are not meant to be an audit-ready method of tracking data over time. The data is too volatile for that, as it can easily be wiped with a widget change. It is designed to be a visual indicator that something changed, so a major change in the widget count can be noticed. It only provides context for the count, because without it, you only have a current-state number.



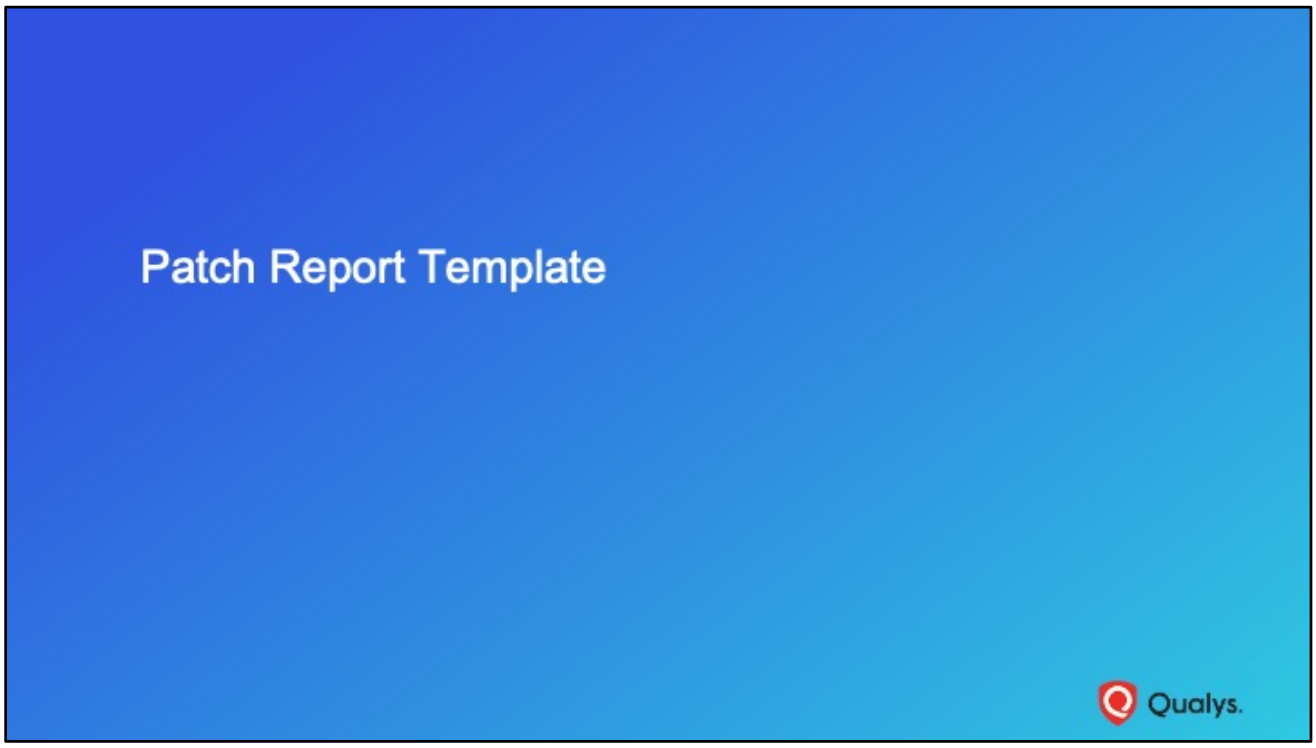
These templates are, the Vulnerability scorecard report which shows the latest vulnerability status of the selected assets.

The Ignored Vulnerability report, will list the ignored vulnerabilities on the selected assets.

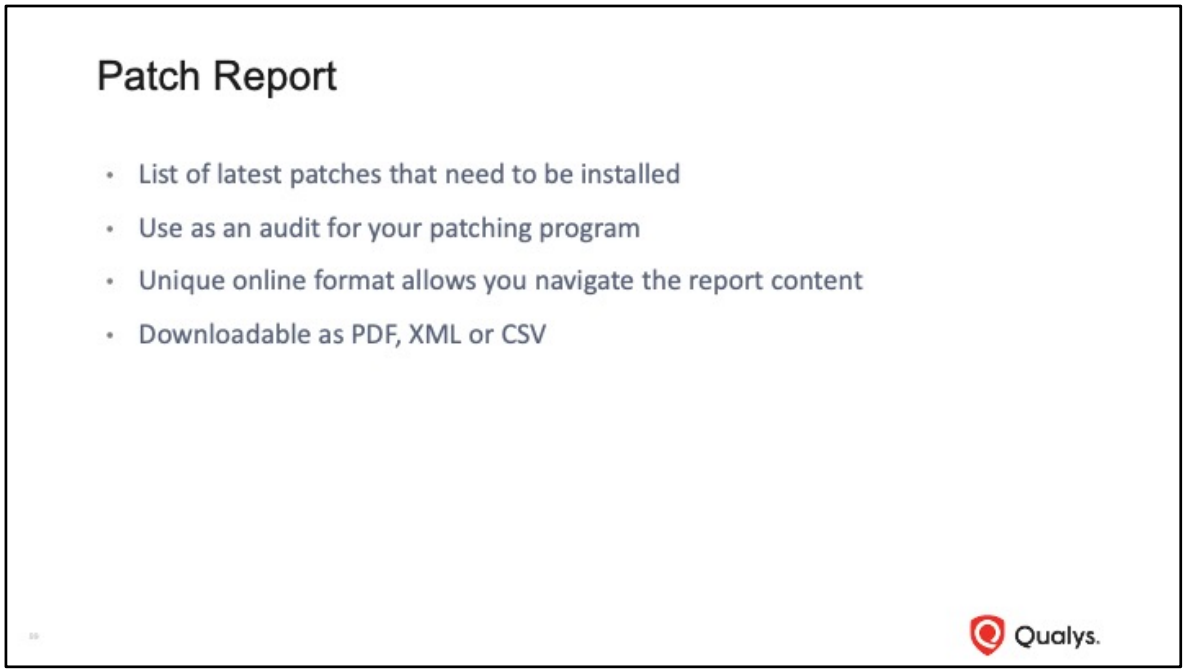
The most prevalent vulnerability report will list the top 10 most prevalent vulnerabilities and the affected assets.

Most vulnerable hosts, will list the top vulnerable hosts with the number of vulnerabilities at the defined severity.

The patch report will list assets that are missing specific patches and software.



This section explains the different options that can be configured in a Patch Report Template.



The patch report is designed to list patches that need to be installed to fix the current discovered vulnerabilities.

The patch report is most commonly used as online report which means that a person viewing the report can navigate through the report content.

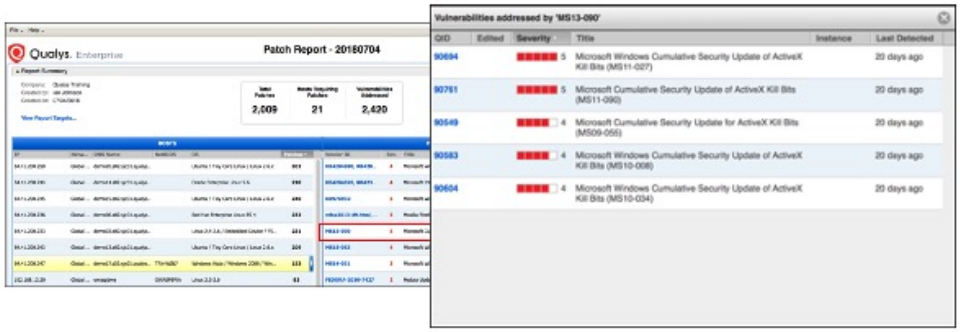
In this online format the report cannot be downloaded, but there are options to download the report content in a PDF, XML, or CSV format.

Anyone who wishes to view this repot in its online format must have an account in your subscription.

- In this activity you will generate a Patch Report and it will show you how to use the online format.
- The online format is designed to let you sort to determine which patches should be priority for your patch team.

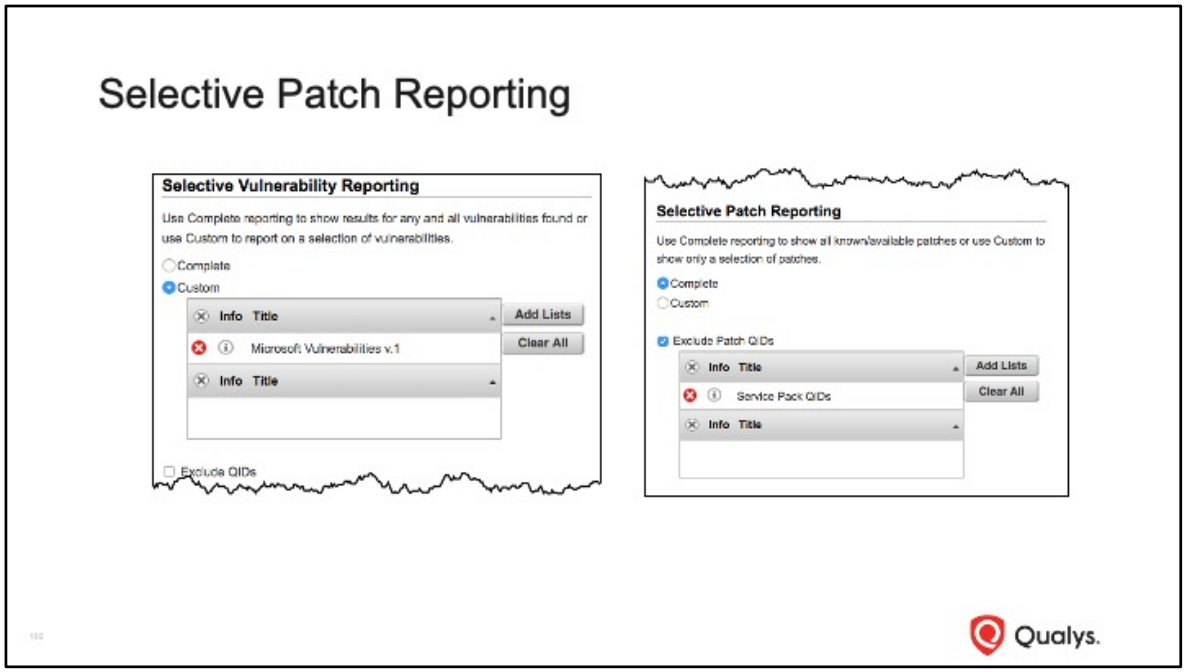
Patch Reports with Supersedence

- Patch report will always use display the latest patch
- The listed patch may be used to fix multiple QID's



Qualys.

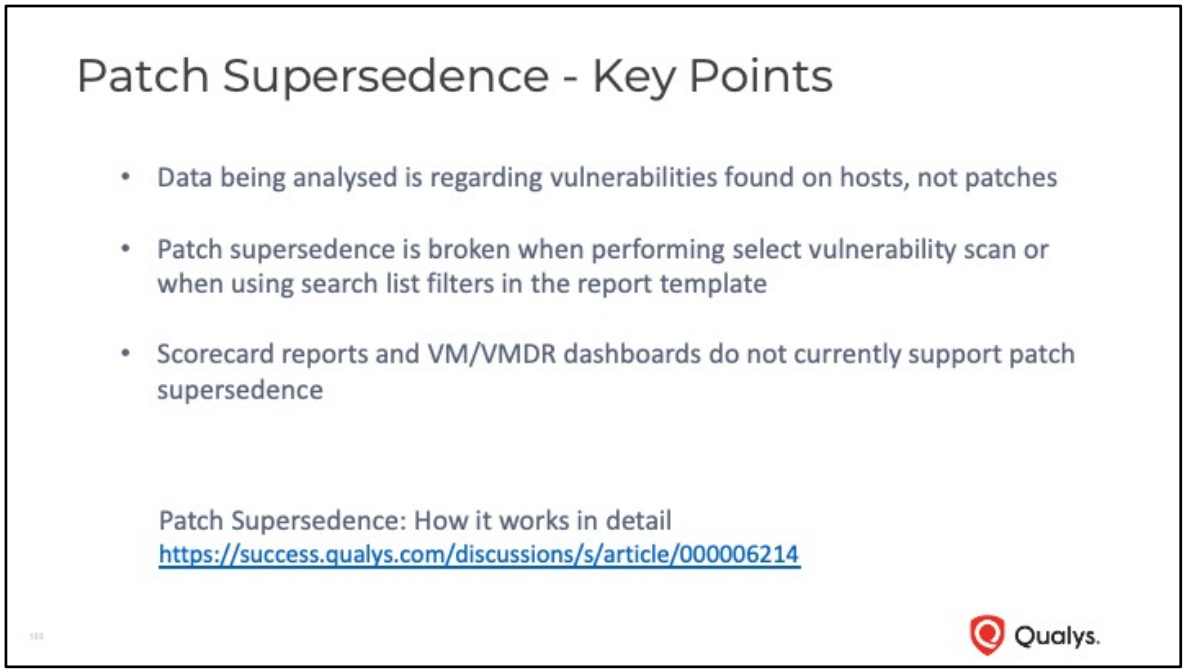
When you use the patch report, the Qualys platform will automatically use the patch supersedence. This means that any patches displayed in report will be latest patches required to fix the QID. That patch may also be used to fix other QID's and in that case all those QID's will be group together.



By default, all available patches are included in the report. The filter option “Selective Patch Reporting” allows you to identify patch QIDs to include or exclude from the report. select Complete to show all known patch QIDs, select Custom to show only specific patch QIDs, and select Exclude Patch QIDs to filter out certain patch QIDs from the report.

For example, if you want to generate a patch report of Microsoft vulnerabilities but you want to filter out service pack QIDs. In this case, you need 2 search lists. The first search list includes vulnerabilities associated with the vendor Microsoft. The second search list includes all vulnerabilities with “Service Pack” in the vulnerability title.

Use the “Selective Vulnerability Reporting” and select “Custom” and then add the Microsoft Vulnerabilities search list. Only vulnerabilities associated with the vendor Microsoft will be included in the report. Next use “Selective Patch Reporting” to identify the patch QIDs you want to filter out of the report. Select “Exclude Patch QIDs” and then add the Service Pack search list. Any QID associated with a Service Pack will be filtered out of the report. Patch reports generated with this template will include all Microsoft vulnerabilities that are not associated with service packs.



Remember using the 'Exclude Superseded Patches' feature is analyzing QIDs that are flagged on hosts, not whether or not patches are installed or missing on those hosts.

Patch supercedence should not be applied to generate report data meant to influence security, executive, auditor assessments and decision-making regarding risk (vulnerability) in their environment.
Suppression via QID supercedence is only applicable, and may offer some small potential value when risk (vulnerability) detection data is sourced to identify and produce a grocery list of patches for manual application for/by a technical remediation audience. So, consider using patch supersedence judiciously.

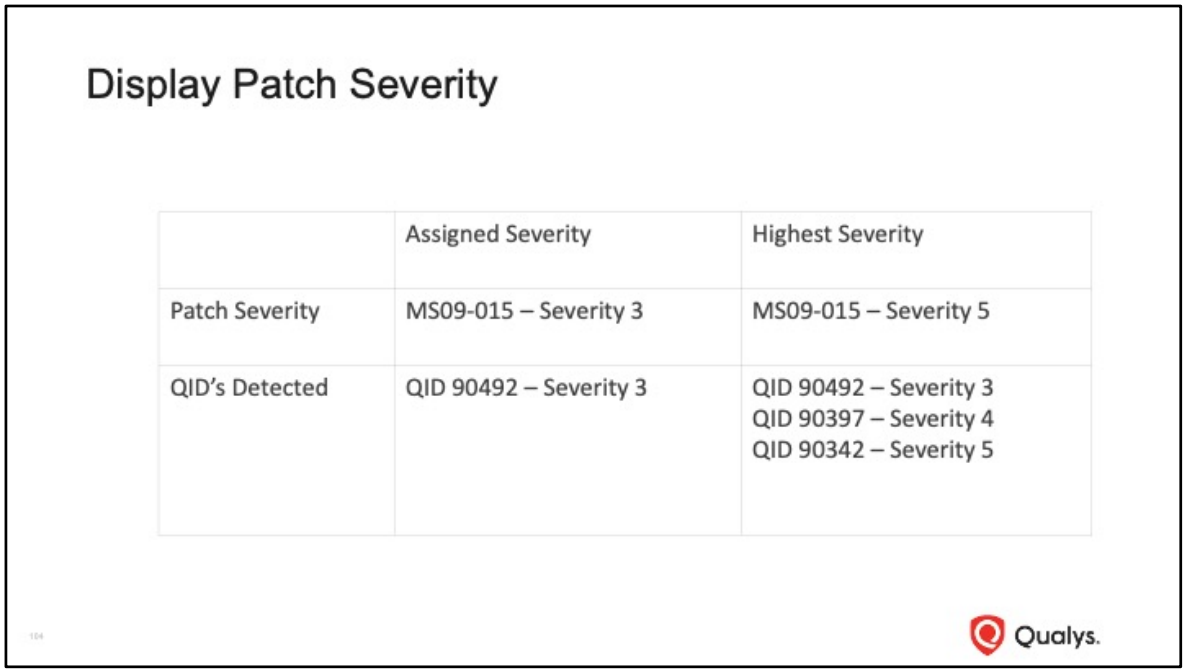
Patch supersedence logic is performed by traversing a tree of patches based on operating system and detected QIDs to find the highest lead node that satisfies the OS and other criteria. When QIDs are filtered out, either from vulnerability scanning (i.e. custom rather than complete vulnerability scanning) in the Option Profile, or by using Threat Protection RTIs or customer Search Lists to filter reporting, this can lead to gaps in the tree structure and break the supersedence logic. Please consult https://qualysguard.qg2.apps.qualys.com/qwebhelp/fo_portal/search_lists/search_lists_exclude_superseded_patches.htm to know more about report results when using

search lists and patch supersedence.

Note that Scorecards reports and VM/VMDR dashboards do not currently support patch supercedence.

Please consult the following links for more information on Patch Supersedence:
Patch Supersedence: How it works in detail
https://success.qualys.com/discussions/s/article/000006214

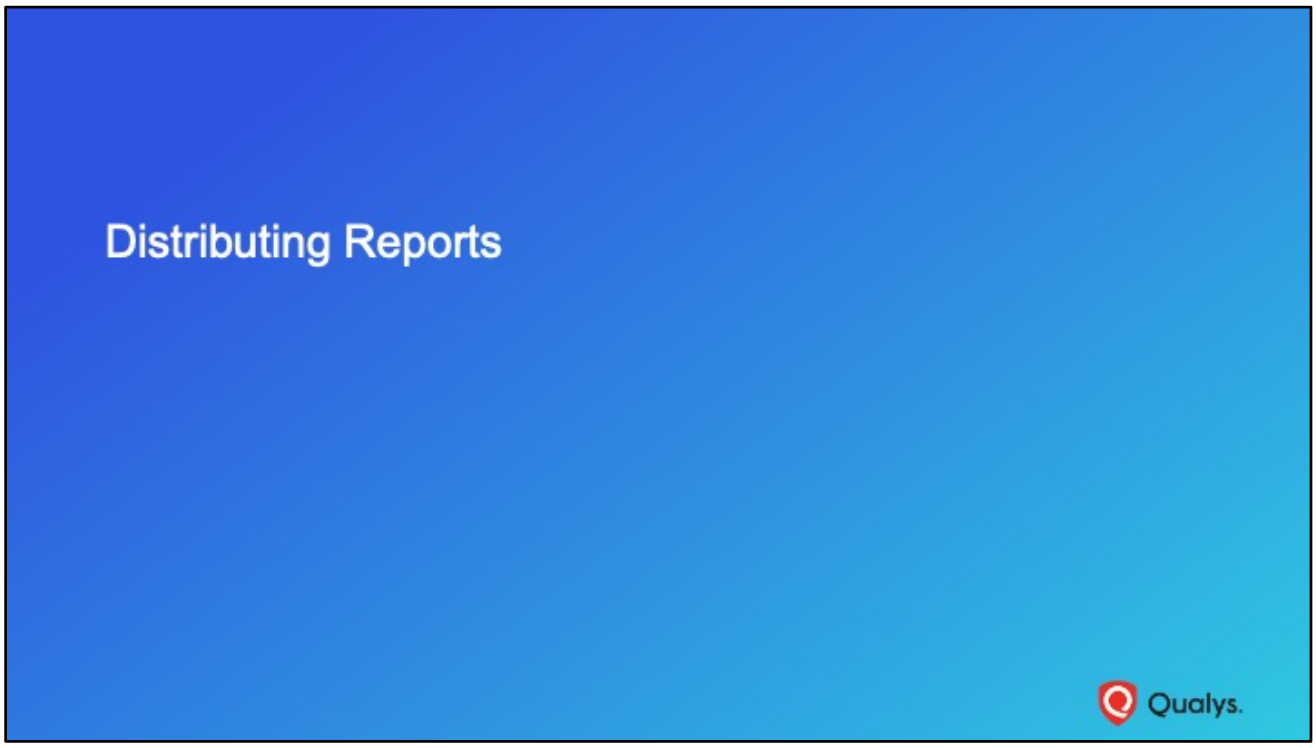
How does QualysGuard deals with superseded Microsoft patches?
https://success.qualys.com/discussions/s/article/000003506



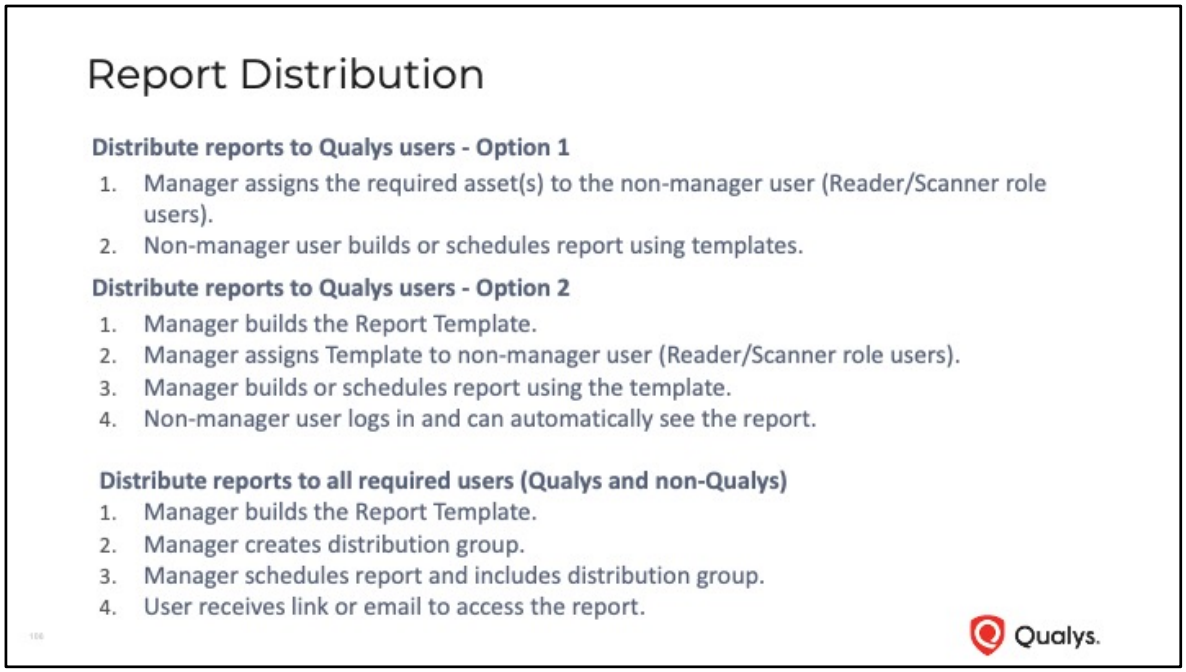
With the Display patch severity setting you can define how the severity level for each patch is displayed. The default of Assigned Severity means the patch severity in the report will match the severity assigned to the QID for the recommended patch. For example, if the KnowledgeBase has a QID for MS09-015 with severity 3, then the patch for MS09-015 is listed with severity 3, even if other vulnerabilities fixed by the patch have a higher severity.

If you wish to see the patch severity in the report to match the highest severity across all QIDs detected on the host that can be fixed by the patch, then select Highest Severity. For example, let's say patch MS09-015 fixes three QID's at severity levels 3, 4, and 5. If all three QIDs are detected on the host, then the patch severity is 5. If QID at severity 5 is not detected on the host but the other QIDs are, then the patch severity is 4.

QID 90492 (severity 3), QID 90397 (severity 4) and QID 90342 (severity 5). If all three QIDs are detected on the host, then the patch severity is 5. If QID 90342 is not detected on the host but the other QIDs are, then the patch severity is 4.



In this section, we will discuss configuring Qualys in a scalable way to distribute reports.



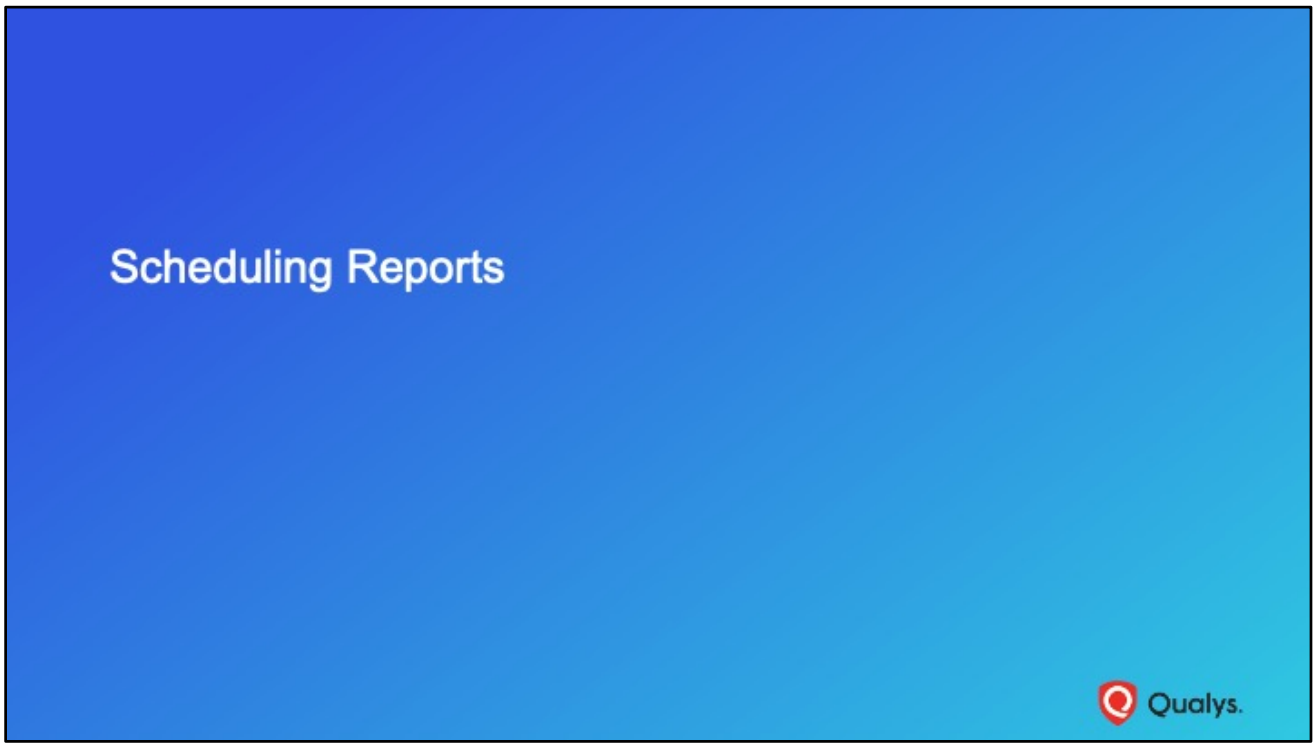
There are multiple ways to distribute reports:

1. Distributing reports to Qualys users- Option 1
- Manager assigns the required asset(s) to the user (Reader/Scanner role users).
- User builds or schedules report using the template.

2. Distributing reports to Qualys users- Option 2
- The Manager user builds a report template that will be used to generate the reports.
- The Manager user then assigns users to the Report Template.
- Now when this template is used to run a report, the users assigned to the Template will be able to view it even if they do not have access to the assets included in the template.

3. Distributing reports to all required users (Qualys and non-Qualys users)
- The Manager user builds a report template.
- The Manager user creates a Distribution group containing users with Qualys accounts and email addresses of people without accounts

- The Manager user schedules a report and includes the distribution group.
- When the report runs at the scheduled time, the users in the distribution group will receive an attachment or link (depending on the configuration) to access the report.

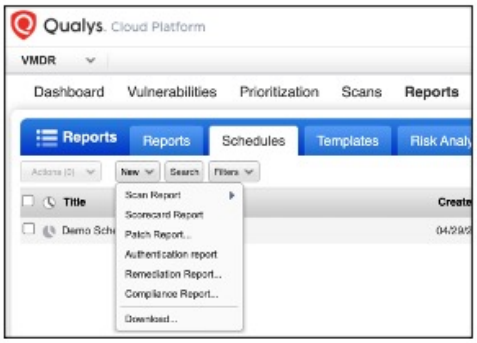


This section outlines the process of scheduling reports.

Scheduled Reporting

Several report types that can be scheduled:

- Template-based scan reports (using Host Based Findings)
- Scorecard reports
- Patch reports
- Authentication reports
- Remediation reports



Qualys.

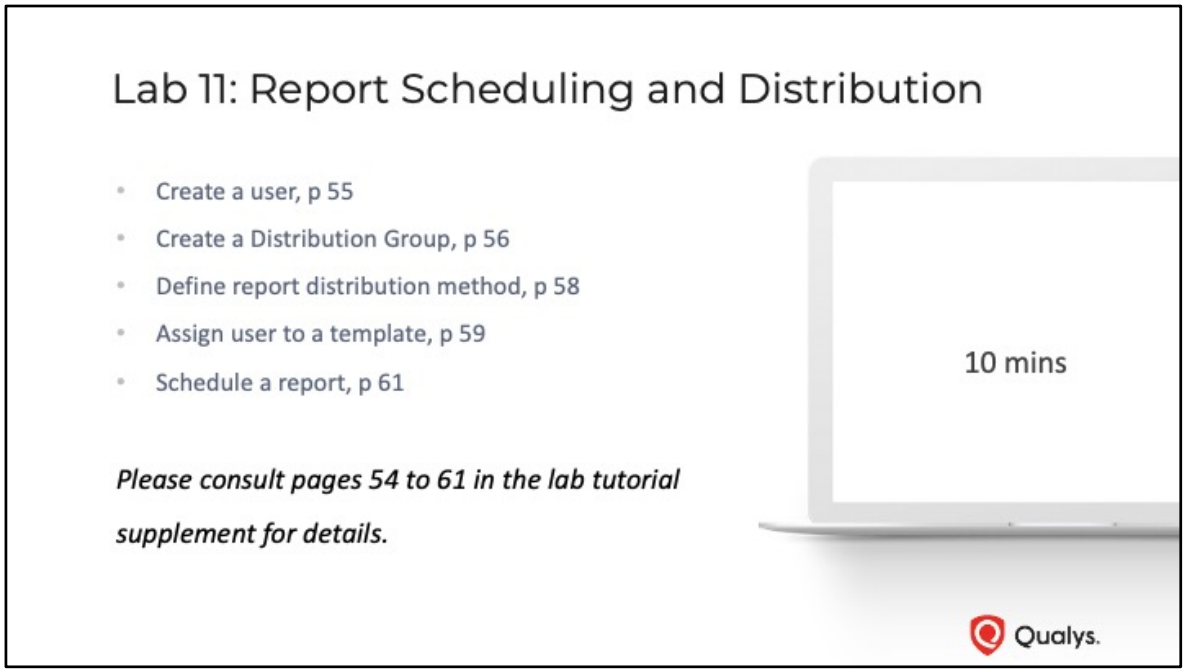
Scheduled Reporting

Like with mapping and scanning, users can schedule reports to run automatically at a scheduled time, on a recurring basis. Users can also set options to notify select distribution groups when a report is complete and ready for viewing.

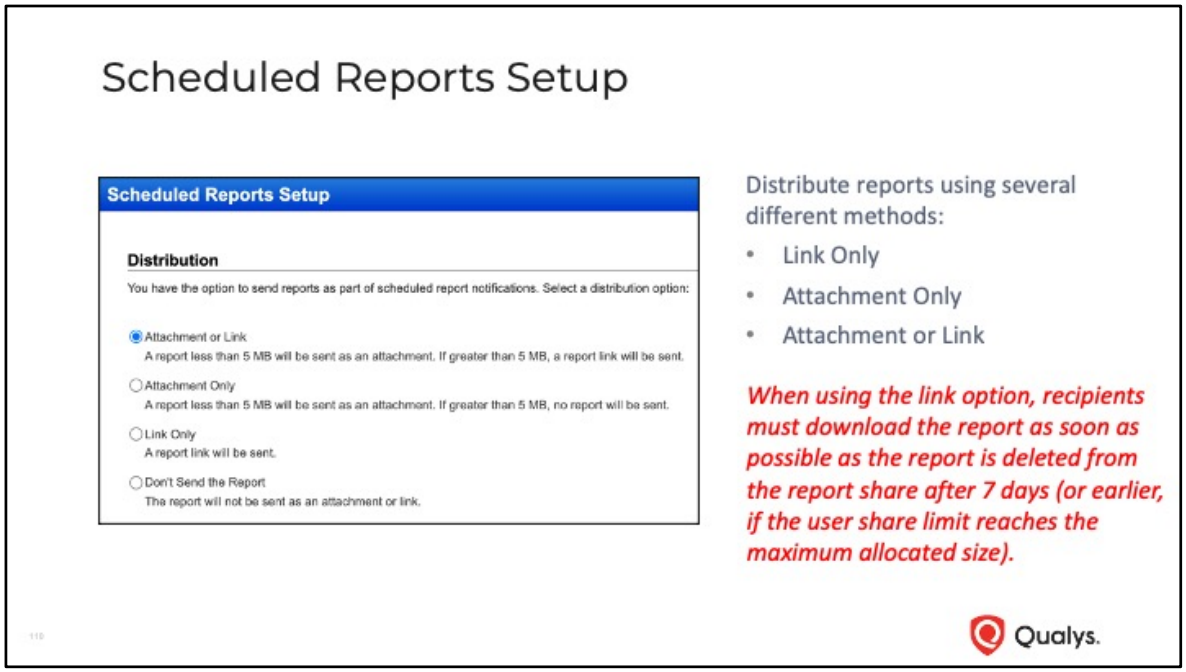
Schedule a Report

There are several report types that can be scheduled. You can schedule template-based scan reports (set to Auto source selection), scorecard reports, patch reports, template-based compliance reports and remediation reports.

To create a new report schedule, go to Reports > Schedules and select the type of report you're interested in from the New menu. In the example below, a new template-based scan report will be scheduled.

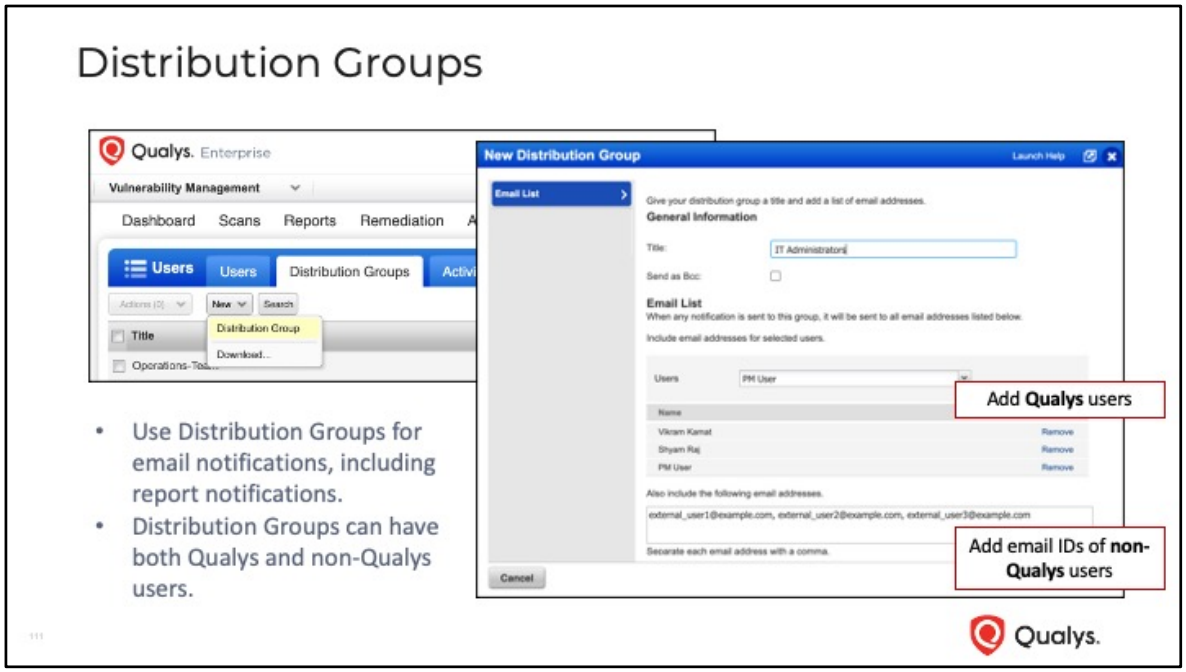


- Recommend reading along in the pdf for this one.
- Activity 1, you'll make a Reader user that has privileges for running reports.
- Activity 2, you'll make a distribution group which will include email addresses to distribute reports to.
- Activity 3, you can setup how your scheduled reports will be distributed (attachment or link).
- Activity 4, shows how to assign another Qualys user to a report template.
- Activity 5, shows how to schedule a daily report that gets sent to a distribution group.



When configuring scheduled reports, there are four options to distribute them:
Attachment or Link – with this option, the report is sent as an attachment if it's under 5MB in size, else a link is sent.
Attachment Only – with this option, the report is sent an an attachment if it's under 5MB in size, else no report is sent.
Link Only – with this option, a report link is always sent.
Don't Send the Report – with this option, the report is not sent as an attachment or link. The user will need to login to the Qualys console to view the report.

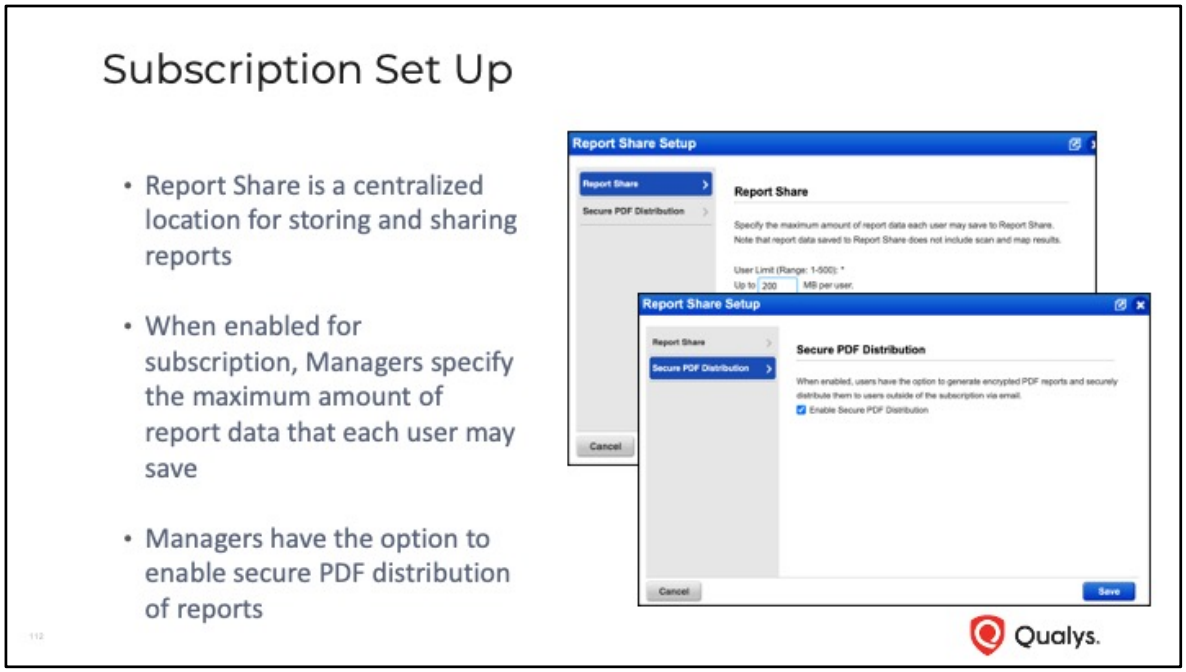
Note that when a report is sent as a link recipients must download the report from the link as soon as possible as the report is deleted from the report share after 7 days or earlier (if the user share limit reaches the maximum allocated size).



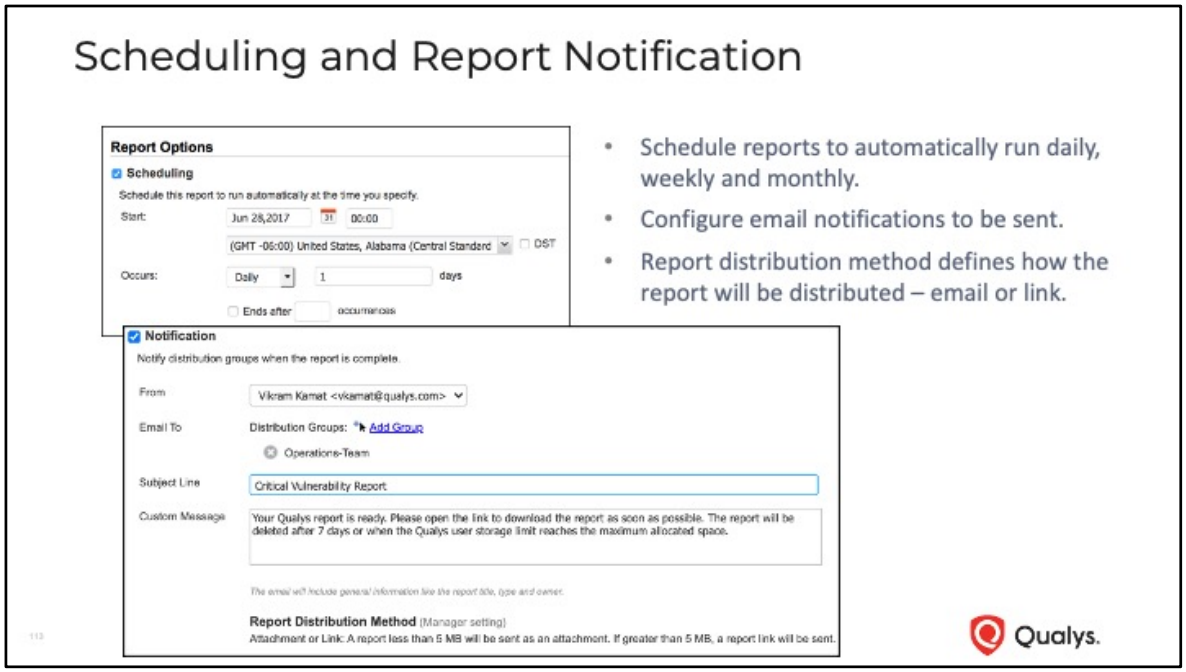
You can choose distribution groups for several email notifications, including scan notifications, report notifications and the vulnerability notification. For example, you can notify the group when a scan or report is finished.

You can create Distribution Groups from under the User-> Distribution Groups tab in the VM application.

You can include email addresses for users in the subscription (simply select users from the list) and include email addresses for users outside of the subscription by typing them into the field provided.



By default, every Qualys user has 200 MB for report storage. A Manager user can increase this to up to 500 MB per user.
Secure PDF distribution can be enabled to encrypt the PDF reports.
These settings can be found under Reports > Setup > Report Share.



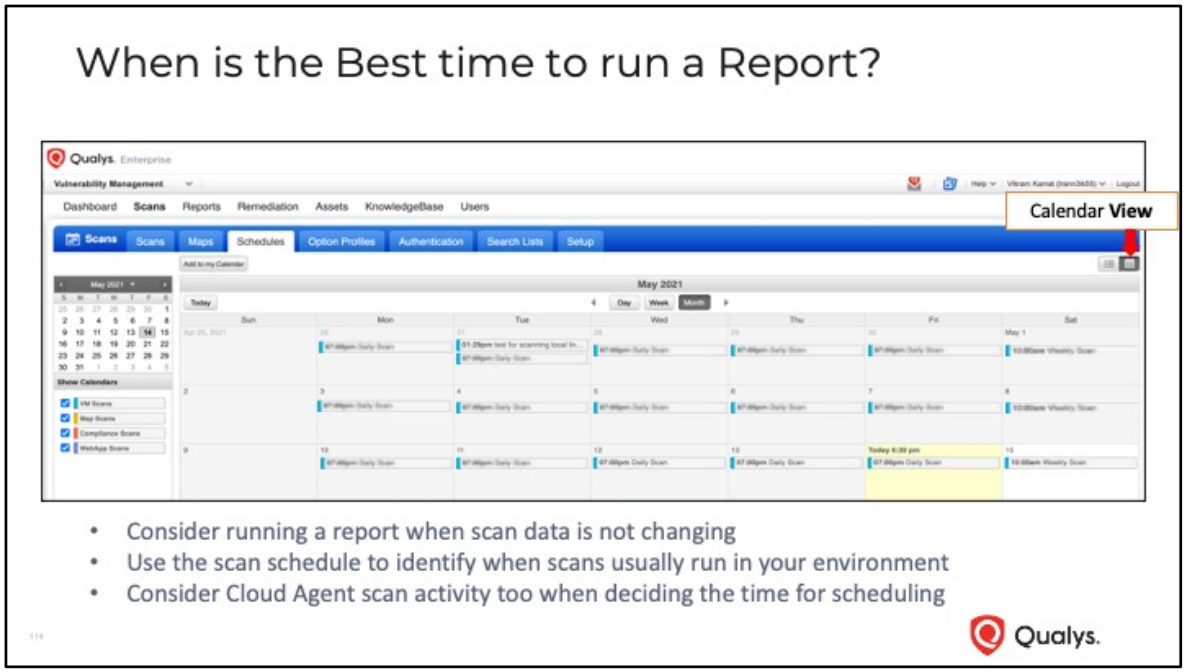
To create a new report schedule, go to Reports > Schedules and select the type of report you're interested in from the New menu. The New Scan Report page appears.

SCHEDULING
Define a start date and time for your scheduled report, and how often you'd like the report to run. You can schedule the report to run daily, weekly or monthly on the days that you specify.

REPORT NOTIFICATION
Define who should be notified when the report is complete and ready for viewing. The report notification will be sent to all email addresses listed in the selected distribution groups, including users with Qualys accounts and those who do not have accounts. You may customize these attributes of the email: the sender (you or Qualys Support), the subject line, and the body of the email. If the generated report is less than 5MB it will be sent as an attachment to the email in the format in which it was generated. If greater than 5MB a link will be provided in the email instead of the attachment.

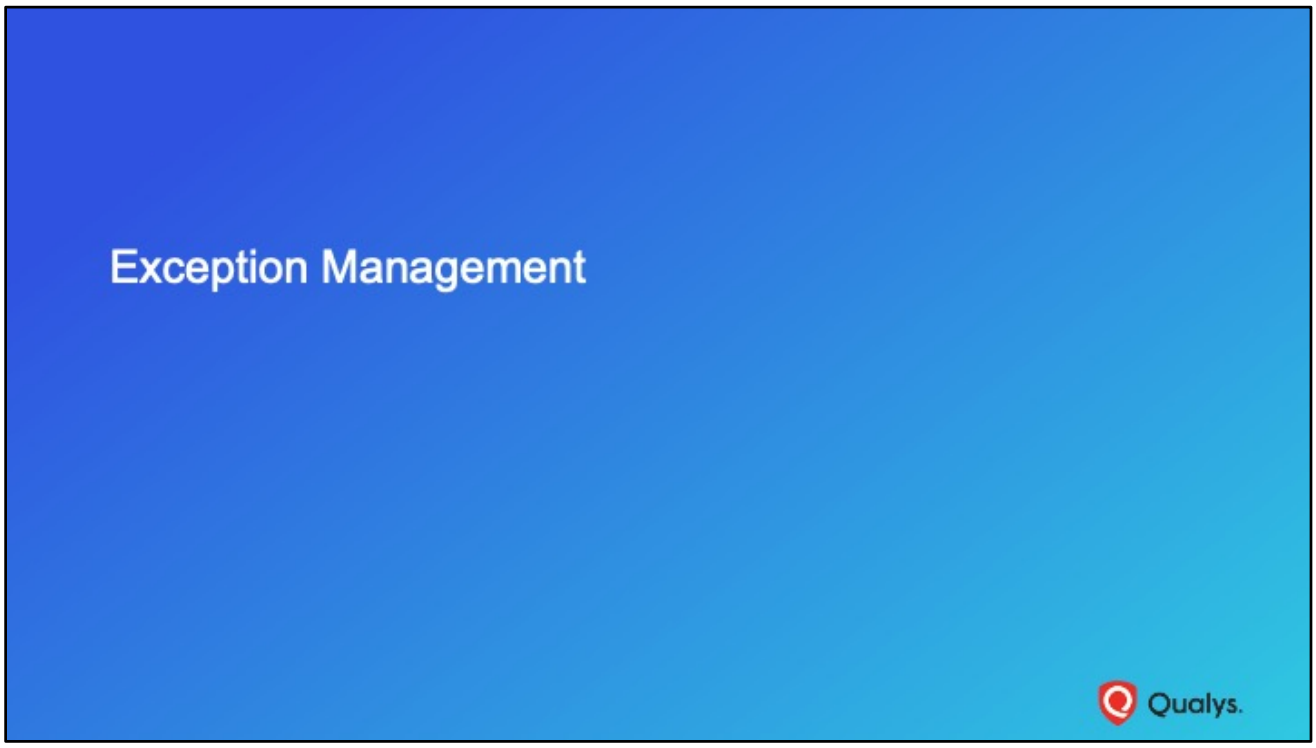
Note that when a report is sent as a link recipients must download the report from the link as soon as possible as the report is deleted from the report share after 7 days or earlier (if the user share limit reaches the maximum allocated size). A good practice is to add such information to the Custom Message area so that report recipients are aware.

Scheduled reports will appear on the Schedules list and your report will run at its scheduled time.

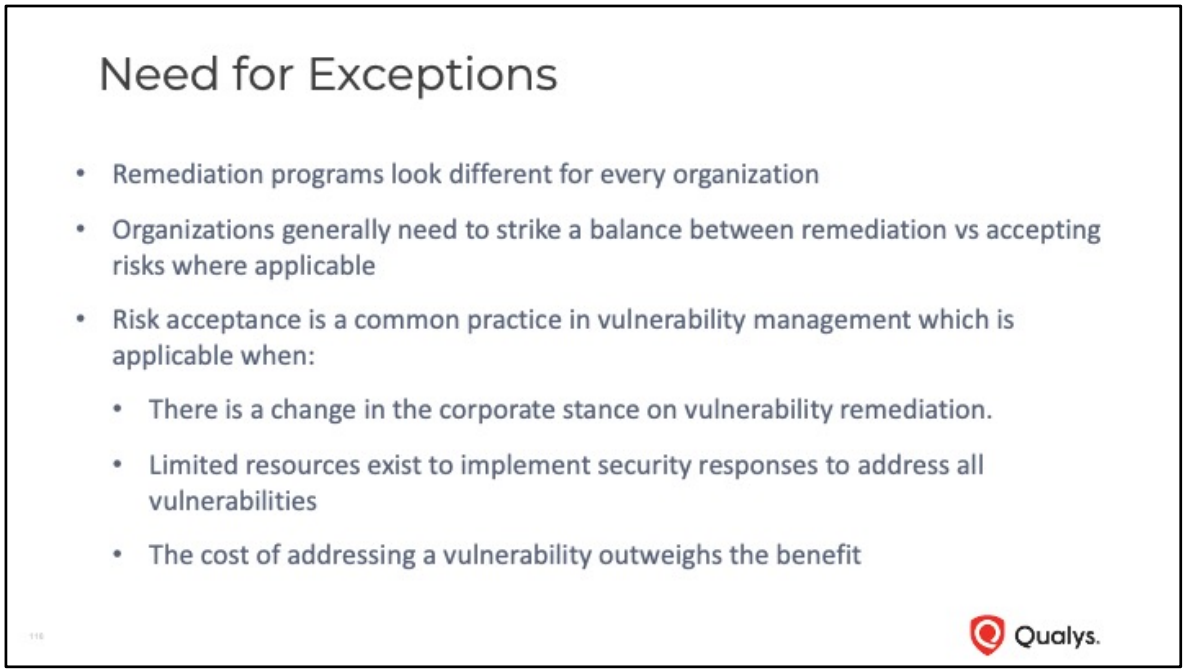


Reporting is meant to provide a comprehensive, focused view of a technical infrastructure's risk landscape based upon the data already available in a subscription thus empowering teams to transform detection data acuity into actionable data-driven decisions. Running a report when scan data is changing in your account can result in inconsistent reports. So, consider running\scheduling reports when no scans are running in your environment. You can view the scan schedule under Scans-> Schedules tab in the VM application to identify when scans usually run in your environment.

You should also consider Cloud Agent scan activity when reporting on agent hosts. This part is a little trickier as not all cloud agents may upload scan data to the Qualys cloud platform at the same time. Using queries (lastFullScan) or dashboards to track Cloud Agent activity to determine the best time to run reports on agent hosts in your environment.



This section outlines the process of managing vulnerability exceptions.



Remediation programs look different for every organization depending on the available resources and specific risks your organization faces. While both identifying and evaluating possible threats are important steps, the most time-consuming step is actually treating the vulnerability. Here's where vulnerability remediation vs ignoring a vulnerability (exception management) by accepting the corresponding risk come into play. Both are different approaches to dealing with a vulnerability, and each has its own merits depending on the specific vulnerability you are dealing with.

Accepting the risk posed by a vulnerability is not really a mitigation strategy because accepting a risk does not *reduce* its effect. However, risk acceptance is a legitimate option in vulnerability management.

In situations where the cost outweighs the benefit of addressing a vulnerability or limited resources exist to implement security responses, most organizations choose to accept a risk rather than spend time or resources mitigating it.

In the context of reporting, exceptions are used to suppress (hide) information from vulnerability counts. While our vulnerability flag is Closed/Ignored, it is important to note that the detection information is still in the subscription database.

Here are some scenarios where vulnerability remediation or mitigation may not be possible or practical.

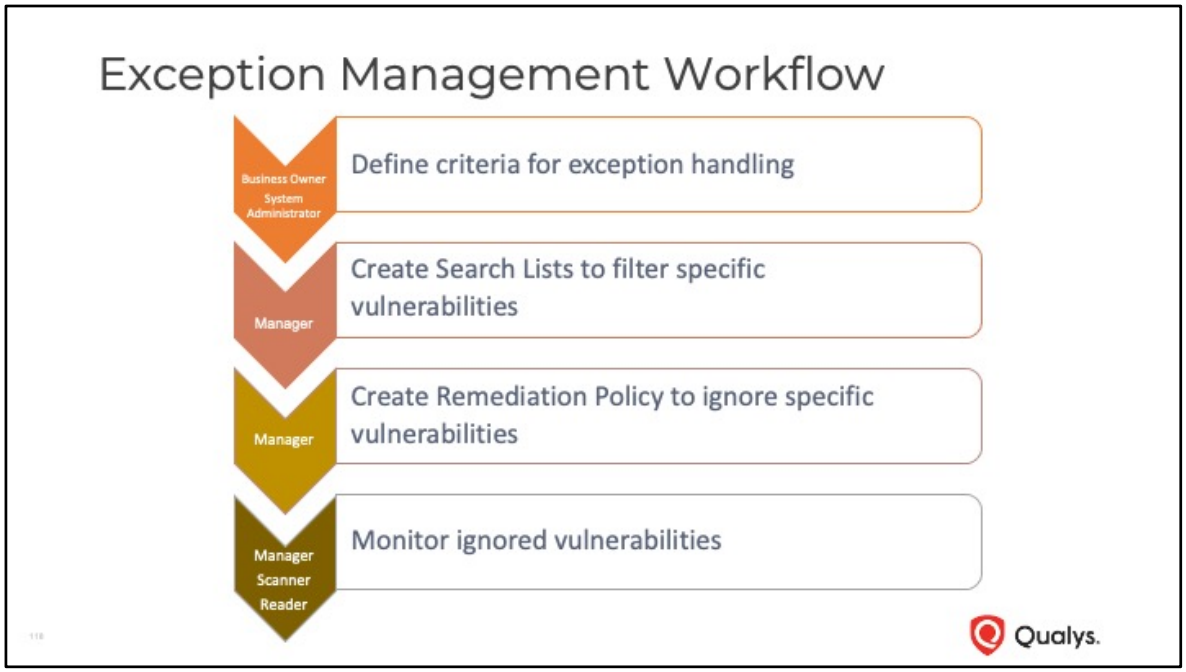
Firstly, not all vulnerabilities need to be fixed. For example, if the vulnerability is identified in Adobe Flash Player but the use of Flash Player is already disabled in all web browsers and applications company-wide, there is no need for action.

Sometimes you might be prevented from taking remediation action by a technology challenge, where a patch isn't yet available for the vulnerability in question.

Other times, you may experience pushback from your own organization. This often happens when a vulnerability is on some type of customer-facing system and your company wants to avoid the downtime required to
patch a vulnerability.

Lastly, you may need to temporarily close a vulnerability due to various reasons. For instance, you may have to an ongoing investigation for a false positive case where in the vulnerability does not exist but is falsely identified as being present and you may want to temporarily close such vulnerabilities until you have conclusive data. Another

instance could be that your patching team needs time to test patches in a test or UAT environment before deploying in production and you want to temporarily close such vulnerabilities that will be patched later. Or it could be a scenario where your organization may have imposed a change freeze and you may need to temporarily close specific vulnerabilities and defer remediation activities to a later date.



This slide outlines the steps to setup exception handling using remediation policies in Vulnerability Management.

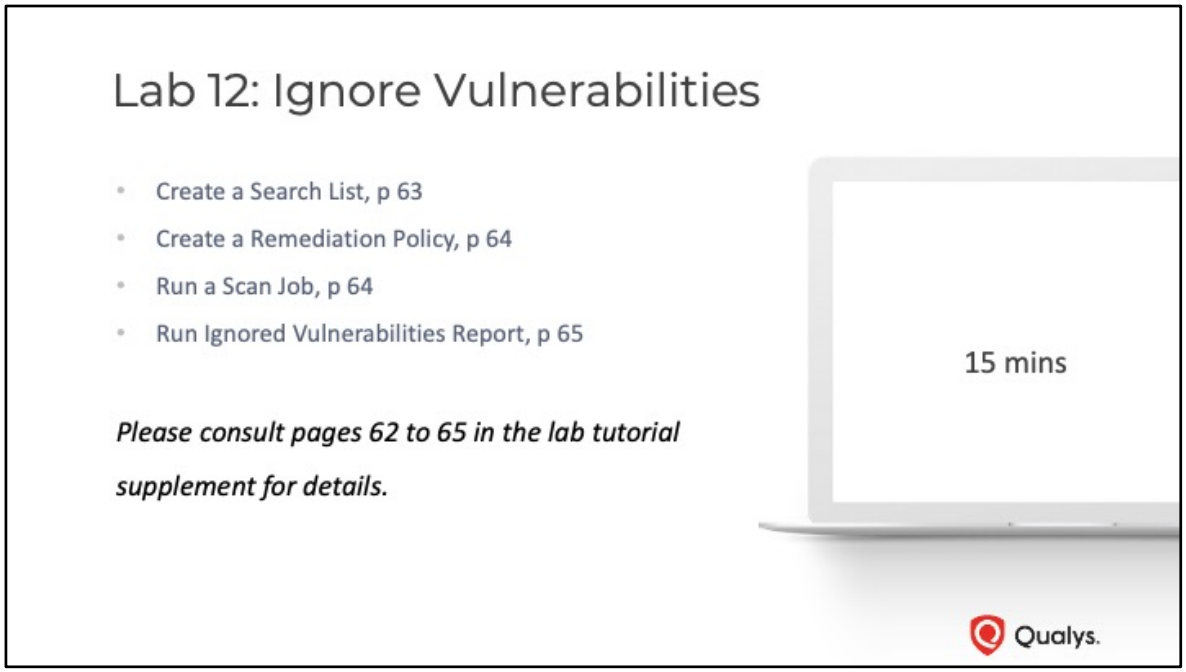
When creating and approving exceptions, it's important to understand that they address sensitive business issues. When an exception is approved, it also means that you're accepting a risk because you're acknowledging and agreeing to the consequences of not remediating the vulnerability. So how these exceptions will be evaluated and how they will be granted is important. Hence, it's recommended to have a clear and well-defined process for managing exceptions.

Business or asset owners and system administrators should be a part of setting the criteria for raising and approving exceptions. And any deviations from established processes should go through proper approval and change management process.

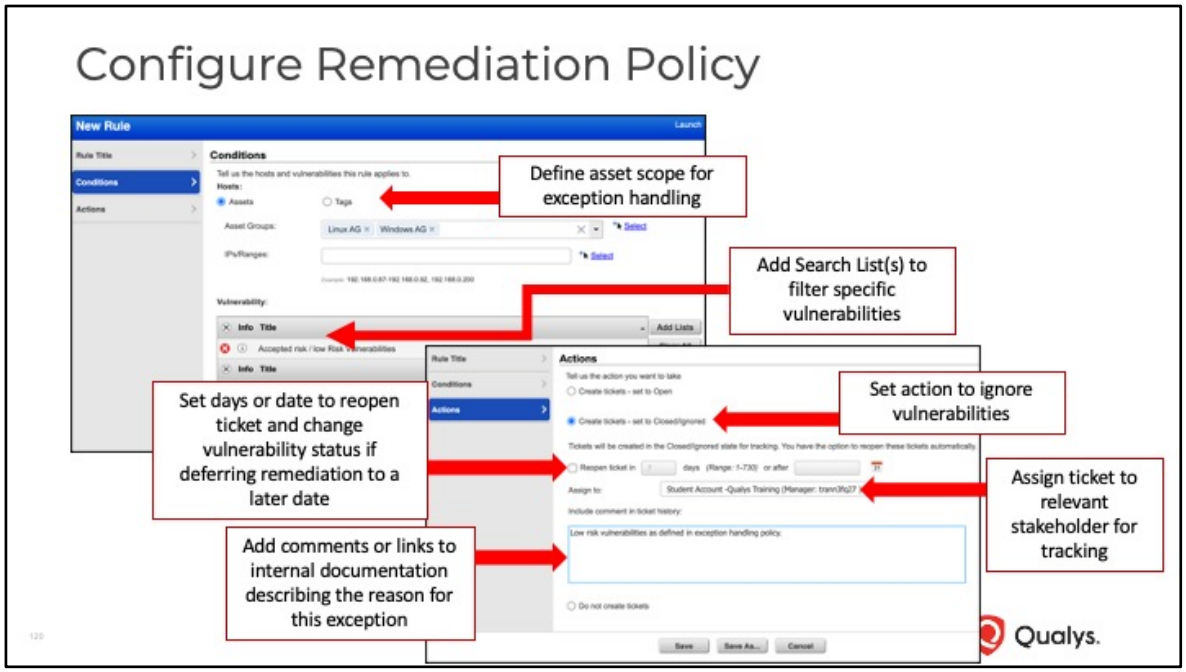
The next step is to apply the criteria to identify vulnerabilities that qualify for exception handling. You can use Search Lists (static and dynamic) to filter specific vulnerabilities matching your exception handling criteria. The Qualys Manager user account has permissions to setup search lists.

Remediation policies are commonly used to assign detected vulnerabilities to remediation owners for mitigation. However, these policies can also be used to automatically ignore vulnerabilities and hence accept risk for vulnerabilities you do not plan to address as per your exception handling criteria. You can also ignore vulnerabilities manually using scan reports (HTML format) based on host-based findings and from host information
available through asset search results.

Lastly, you need to track, and monitor ignored vulnerabilities to ensure that the exception handling process is functioning as desired. You can use filters in your scan report template to report on all ignored vulnerabilities in your account.



- Activity 1, you will make a Search List that targets the Adobe flash player.
- Activity 2, you will make a Remediation Policy to use the Search List to ignore flash player vulnerabilities.
- Activity 3, you run a scan and confirm the vulnerabilities are ignored.
- Activity 4, you run a Scorecard Report on the ignored vulnerabilities.



Remediation Policy (Exception rules) Overview

A policy includes a set of rules that tell us when to create tickets, who to assign them to, and how quickly they should be resolved. You can have one global policy for the subscription and one policy for each business unit. Remediation policy rules enable you to automate the process for ignoring (and hence accepting risk) for select vulnerabilities. Automation minimizes the risk of missing service level agreements and makes it easier
to manage multiple items, because you are eliminating manual intervention.

You can set up a rule for vulnerabilities that can't be remediated or the ones that need to be deferred for a specific period, by identifying the impacted vulnerabilities through a search list (static or dynamic). This way you can automate the process to ignore select vulnerabilities.

Remediation policies contain two basic components:
1.Conditions (that identify the asset and vulnerability scope of the policy) and
2.Actions (that identify the task to be performed, if the target conditions are met).

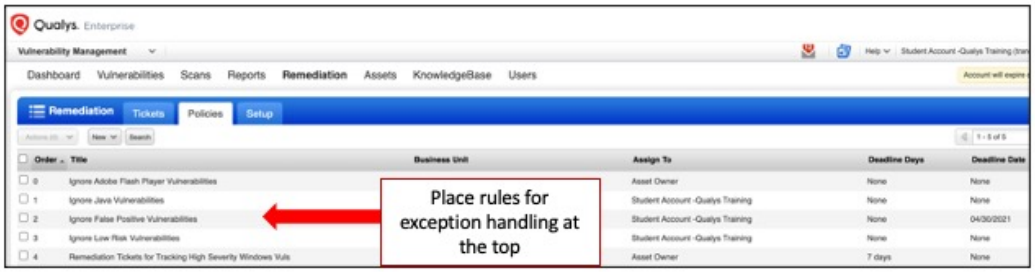
Create tickets - set to Closed/Ignored

Tickets will be created in Closed/Ignored state and assigned to a user.

Expiry of an exception request

When you ignore a vulnerability, you can defer the remediation of a vulnerability for a specified period. For example, as a remediation owner, you can ignore a vulnerability if a patch is currently not available for a host or
if the patching activity is scheduled to run at a later date to allow time for testing and deployment. After the the vulnerability is ignored, its status changes to **Fixed** and the corresponding ticket changes to **Closed** state. When an exception request for a particular vulnerability expires (applicable if option to Reopen ticket is set in the rule), the impacted vulnerability reverts to its **New** or **Active** state and the corresponding ticket is set to **Open** state. If an ignored vulnerability is no longer present in the next scan, the vulnerability status changes to **Fixed** and the corresponding ticket changes to **Closed** state.

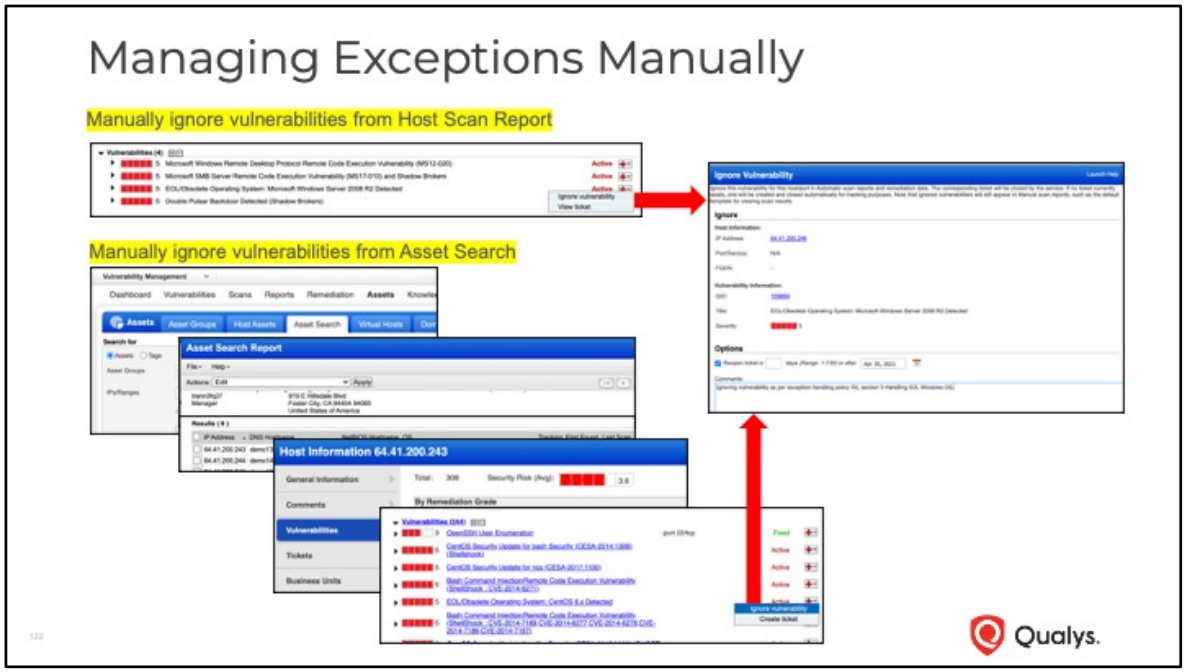
Prioritize Rules to Ignore Vulnerabilities



- Remediation policy rules are applied to scan results in the order in which they are listed
- When a rule is applied on a vulnerability, no subsequent rules are applied on it again even if the condition matches the vulnerability
- Recommended to place rule(s) meant for exception handling at the top

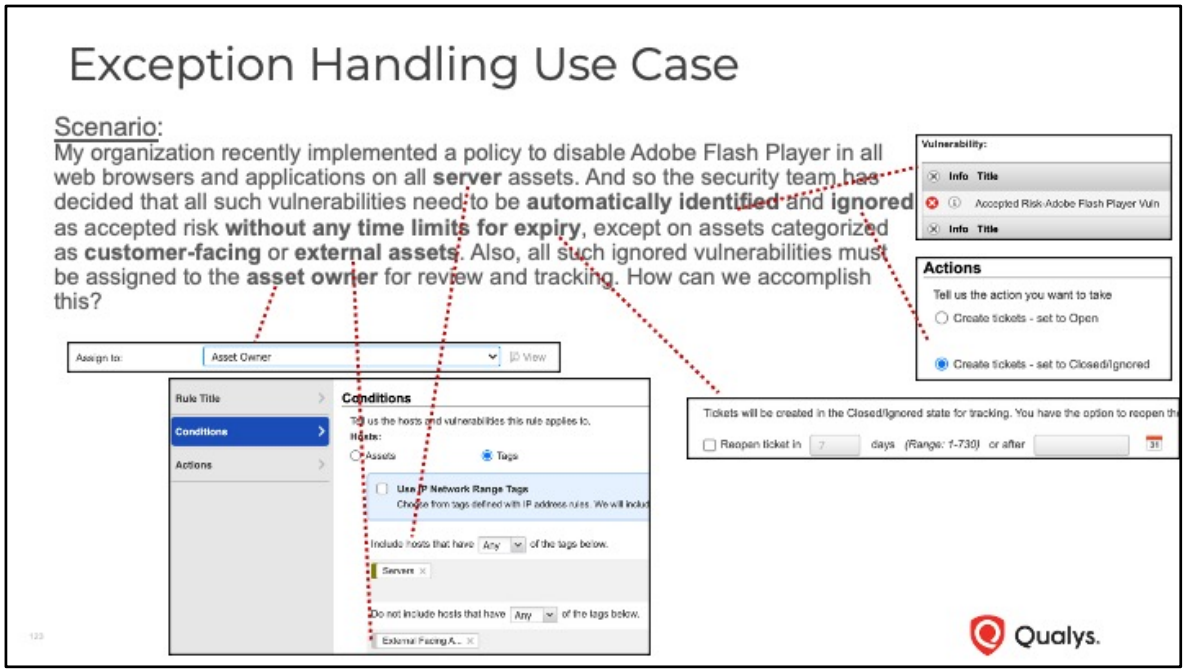
Qualys.

Remediation rules support ordering, that is, the rule with the highest priority is run first. When a rule is applied on a vulnerability, no subsequent rules are applied on it again even if the condition matches the vulnerability.
So, it's important that you place the rule(s) to ignore vulnerabilities at the top of the rule list so that they are applied first.



You can manually ignore any vulnerability instance directly from within a vulnerability report (HTML format) or ignore a vulnerability from host information.

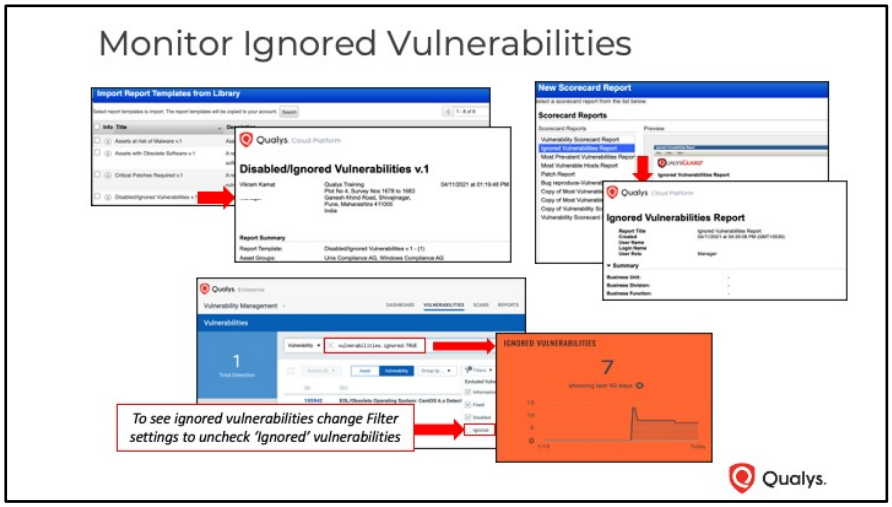
To ignore a vulnerability from host information, go to VM/VMDR > Assets > Host Assets or Assets > Asset Search, find a vulnerable host and then open the Host Information page for that host. Select Vulnerabilities on the left side and view the list of vulnerabilities (or potential vulnerabilities). Click + next to the vulnerability instance you want to ignore and then choose Ignore Vulnerability from the menu that appears.



Let's consider the following scenario where you are required to create a remediation policy to ignore specific vulnerabilities automatically as per the criteria set up by your security team:
"My organization recently implemented a policy to disable Adobe Flash Player in all web browsers and applications company-wide. And so the security team has decided that all Adobe Flash Player vulnerabilities need to be ignored as accepted risk without any time limits for expiry, except on assets categorized as customer-facing or external assets. Also, all such ignored vulnerabilities must be assigned to the Qualys Manager user for review and tracking. How can we accomplish this?"

The slide illustrates a remediation policy rule in the Vulnerability Management application to fulfill this requirement.

Note that policy rules are applied to scan results in the order in which they are listed. If a detected vulnerability matches more than one rule, the action specified for the first rule it matches takes precedence. So, it's important that you place the rule(s) to ignore vulnerabilities at the top of the rule list so that they are applied first.



You can track ignored vulnerabilities using various report options.

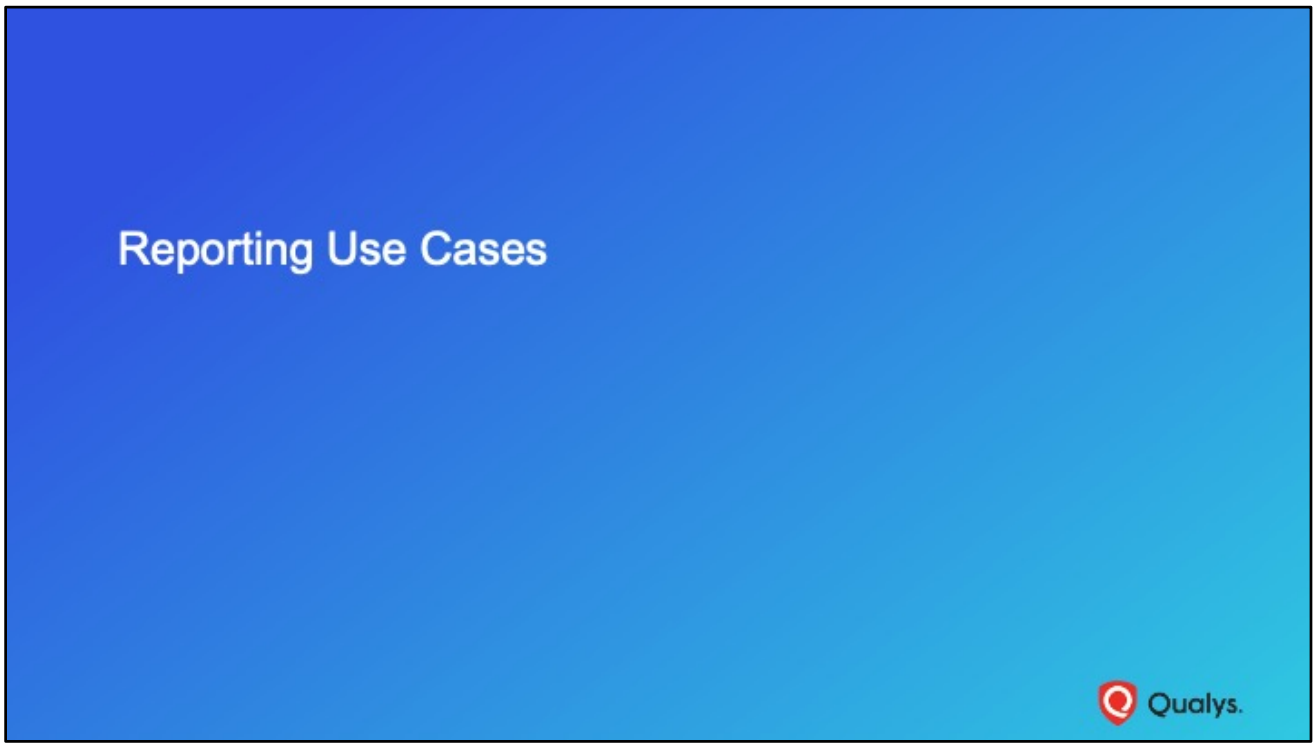
You can use the **Disabled/Ignored Vulnerabilities v.1** template from the template library which is configured to display both disabled and ignored vulnerabilities in your environment.

The **Ignored Vulnerabilities Report** which is available as a part of the **Scorecard** report can also be used to generate this report. The report identifies vulnerabilities that are currently ignored. Each targeted asset group is listed with vulnerabilities that are ignored on hosts in the group. The report provides host details, vulnerability details, and remediation ticket details.

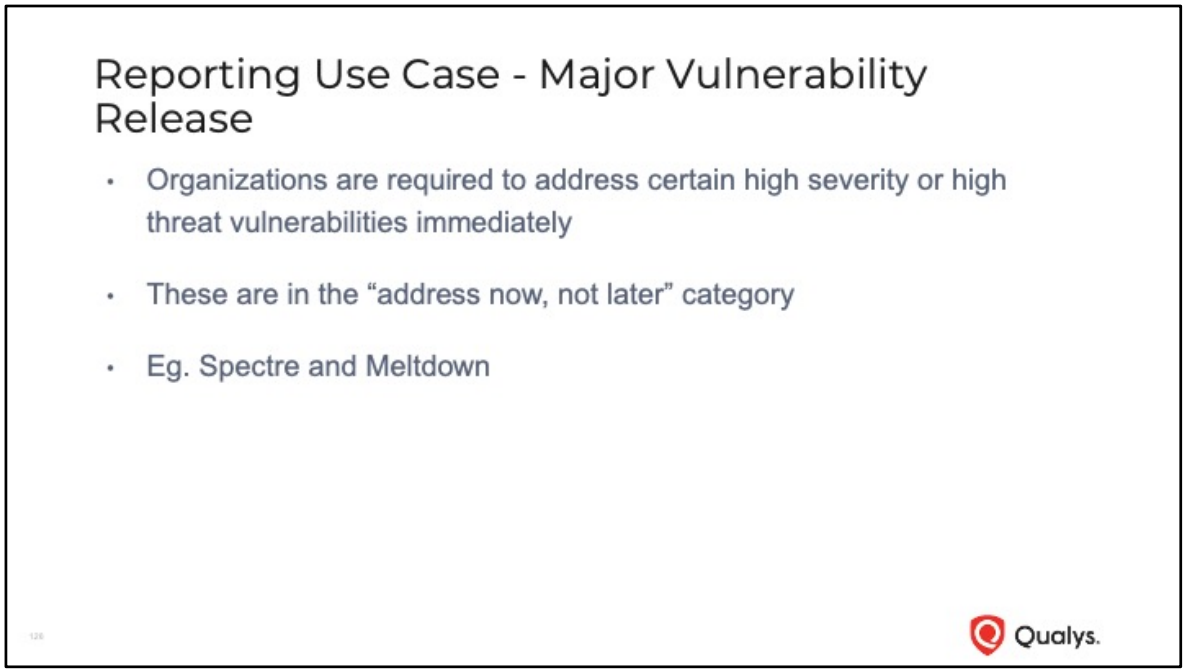
Lastly, you can use a search query to list ignored vulnerabilities. The query **Vulnerabilities.ignored: TRUE** will display ignored vulnerabilities in the search results. *However please note that Ignored vulnerabilities are not listed in the search query results by default. To see these vulnerabilities, change Filter settings and uncheck 'Ignored' vulnerabilities.*

You can use the same search query and the corresponding filter setting to create a

dashboard widget to track ignored vulnerabilities. We recommend enabling trend data collection in the widget to track ignored vulnerabilities over time.

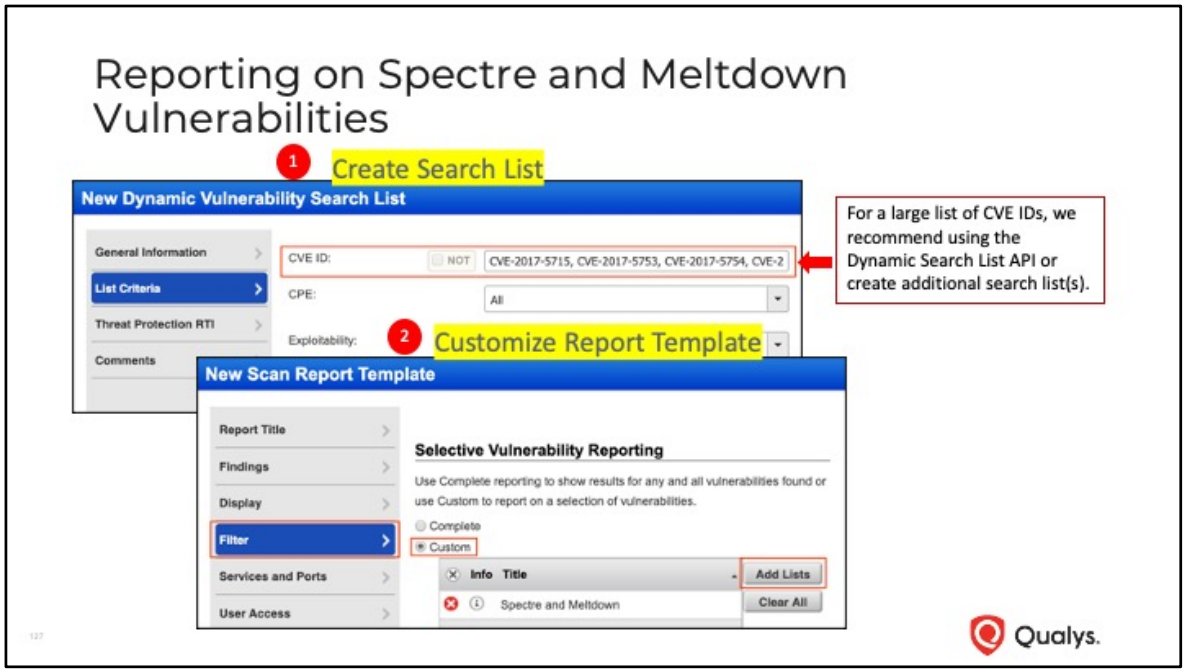


In this section, we'll discuss how to address vulnerability reporting for a couple of practical use cases including the lifecycle of identifying the QID's associated with a major vulnerability, building the required search lists and managing Patch Tuesday release updates using search queries and dashboard widgets.



In some cases, organizations are required to address certain high severity or high-threat vulnerabilities immediately. These types of vulnerabilities are in the “address now, not later” category.

Example: Spectre and Meltdown, vulnerabilities published as a part of the Patch Tuesday release, etc.



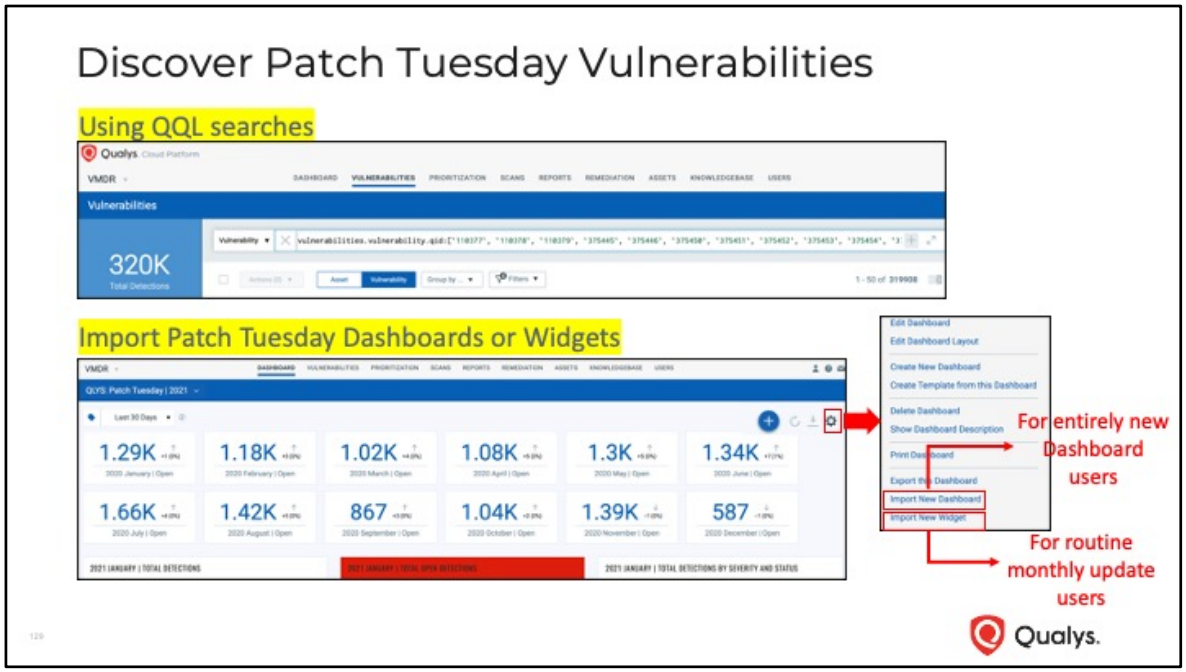
The first step is to detect the vulnerability. A normal VM scan will target all QID's (default setting in Option Profile).

You can create a Search List that only includes the required QID's for reporting. Eg. Spectre and Meltdown vulnerabilities. Once a Search List has been created, it can be used as a vulnerability filter within a report template– this will result in the report only including QIDs matching the Search List configuration.

Note that the UI is limited in the number of characters you can enter. If you are building a Search List which has a very large list CVE IDs, we recommend using the Dynamic Search List API. Refer to the VM API user guide for more information. Alternately, you can create additional search list(s). You can include more than one search list in the report template for reporting.

Patch Tuesday (also known as **Update Tuesday)** is an unofficial term used to refer to when Microsoft, Adobe, Oracle and others regularly release software patches for their software products. It is widely referred to in this way by
the industry. Microsoft formalised Patch Tuesday in October 2003. Patch Tuesday occurs on the second, and sometimes fourth, Tuesday of each month in North America. Minor updates are also released outside Patch Tuesday.
Please consult the following WIKI article to know more about Patch Tuesday
https://en.wikipedia.org/wiki/Patch_Tuesday

Qualys Advisory overview
Qualys Vulnerability R&D Lab releases new vulnerability checks in the Qualys Cloud Platform to protect organizations against vulnerabilities that are fixed in the security bulletins announced by Microsoft as a part of the Patch
Tuesday release each month. Details of these vulnerabilities are published regularly as a part of the **Qualys Security Alerts** and can be viewed here:
https://www.qualys.com/research/security-alerts/.
Customers can immediately audit their networks for these and other new vulnerabilities by accessing their Qualys subscription.



Qualys VM/VMDR automatically detects new Patch Tuesday vulnerabilities using continuous updates to its Knowledge Base (KB). Following a new scan, you can see the hosts impacted by these vulnerabilities using QQL queries.

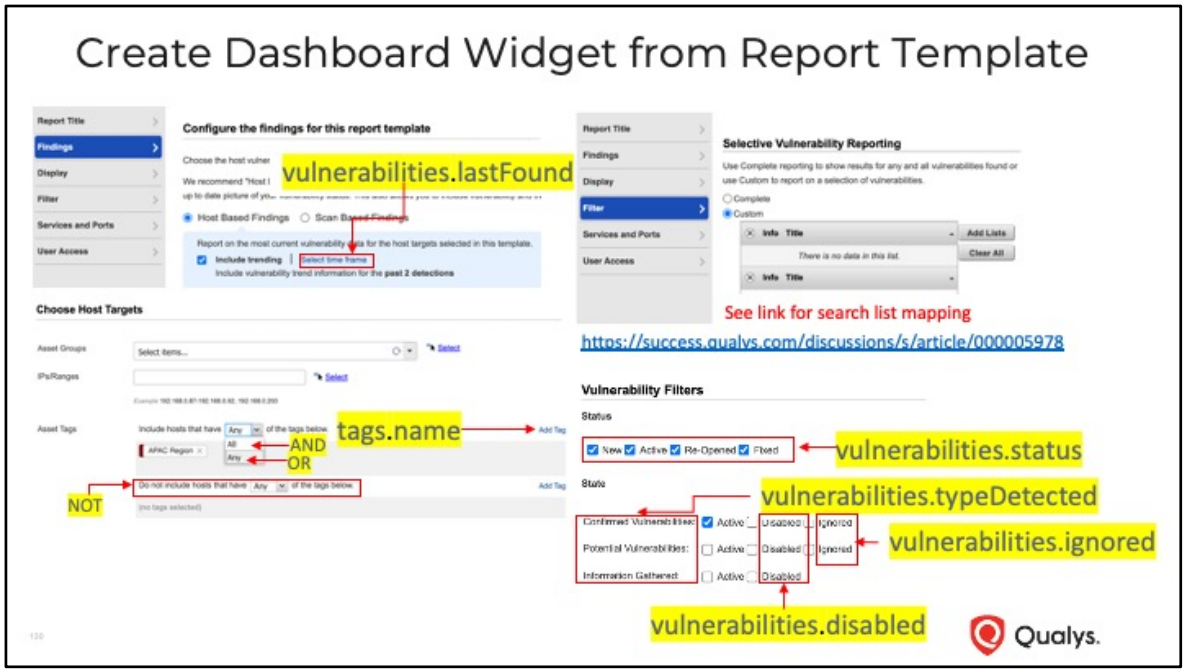
Qualys also provides dashboards and widgets for each Patch Tuesday release. The query strings used in this dashboard are created leveraging the monthly Qualys Security Alerts posts that include the QIDs released for Microsoft and Adobe for the indicated monthly Patch Tuesday cycle. Bookmarking Qualys Security Alerts for future reference is highly recommended.

Latest Patch Tuesday dashboards and widgets are available for download on this link: https://success.qualys.com/discussions/s/article/000006505.

For entirely new Dashboard users, please download and import (contains a single json) from the file named: QLYS_Patch_Tuesday_2021-xx-Month_Vmdashboard.
For routine monthly update users, please download and import (contains multiple widget json files) from the file named: 2021-xx-Month_UDWidget_JSON.

You need to enable "**Enable historical data collection**" following your JSON import(s).

Please consult https://success.qualys.com/discussions/s/article/000006156 for information on enabling historical data collection for your dashboard widgets.



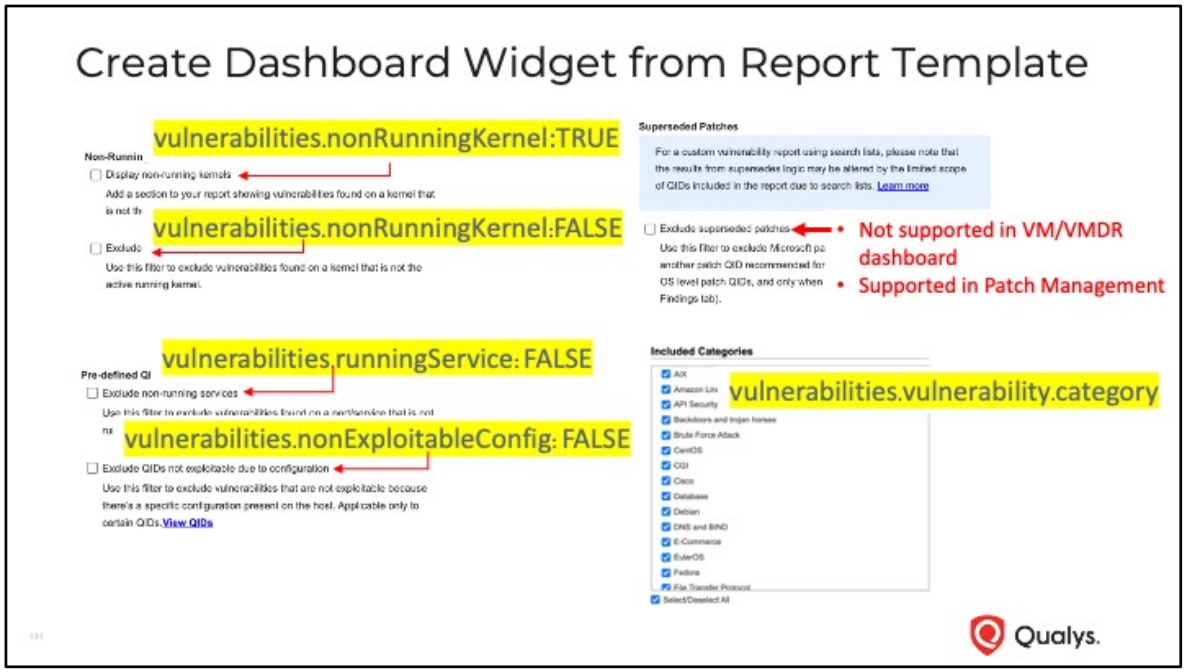
You may want to create dashboard widgets mapped to a report template for better data visualization. Its important to understand how your report template settings\fields map to the VM query tokens as otherwise your batch report counts will not match your dashboard counts. The slide illustrates images that map VM query tokens to Scan Report Template Findings/Detection Date, Asset Selection Fields and vulnerability filter settings.

Please consult the following documents for more information:
Dashboard Toolbox - VM DASHBOARD: Mapping of Scan Report Template/Findings/Detection Date and Asset Selection Fields to VM Dashboard Tokens
https://success.qualys.com/discussions/s/article/000005934

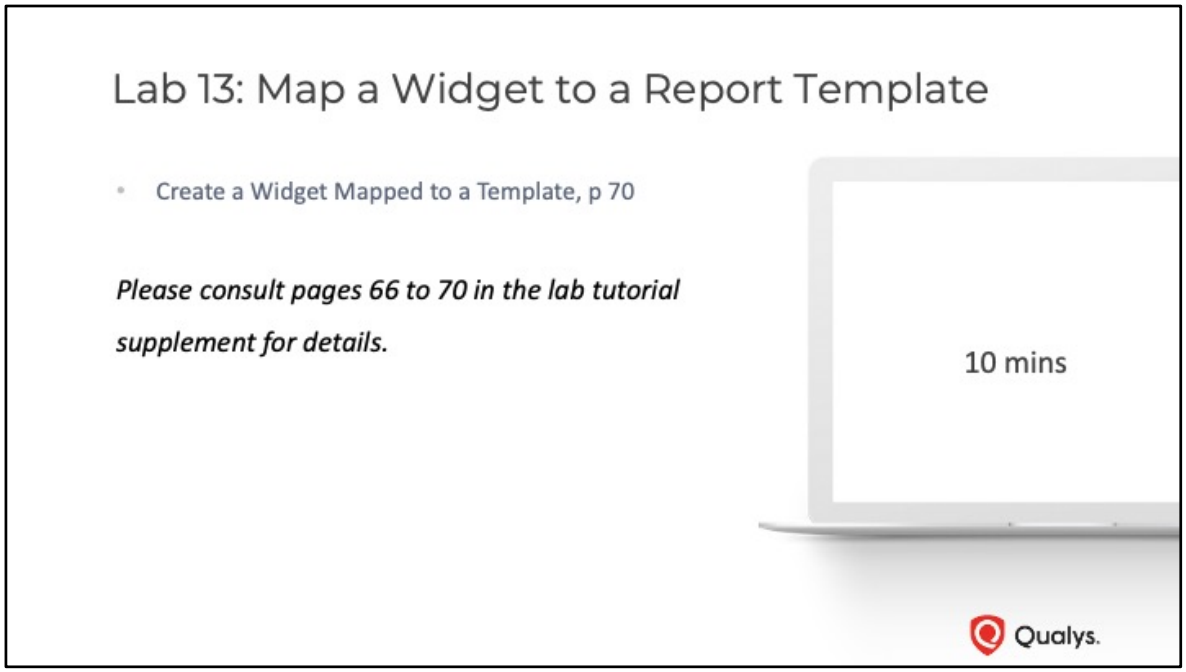
Dashboard Toolbox - VM DASHBOARD: Mapping of VM Search List Criteria to VM Dashboard Tokens v2
https://success.qualys.com/discussions/s/article/000005978

Dashboard Toolbox - VM DASHBOARD: Mapping of Scan Report Template/Filters to VM Dashboard Tokens

https://success.qualys.com/discussions/s/article/000005938

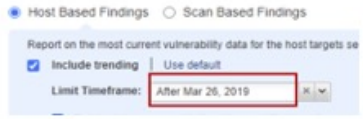


Please note that patch supersedence is currently not supported in VM/VMDR dashboard. It is supported in the Patch Management application.



- In this lab you will create a dashboard-widget based on settings of a custom report template.
- It steps through the whole process from Search List to Report Template to widget.

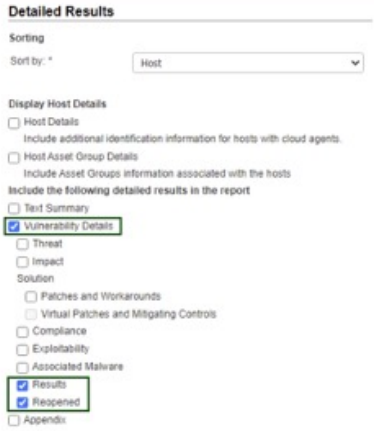
Report takes too long to generate and/or errors out

Template Section	Comments	Recommendations & Resources
	Last detected date or the Last fixed date of the vulnerability must occur during the specified timeframe. Excessive timeframes may lead to timeouts or errors during report generation.	• Any detection with a last detected or last fixed date outside of the last 90-days offers little value. • Running a 90-day host-based trend report at the end of every routine scanning cycle is recommended.
	If a single person is the intended recipient of the report, All may be appropriate, but this is not common. Excessive Asset scopes may lead to timeouts or errors during report generation.	• Reporting Toolbox: Reporting Best Practices FAQ • Refocus Asset Scope in reports to match the recipients.

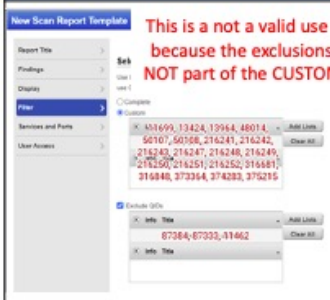
Qualys.

You may come across a situation where the report takes too long to generate and\or sometimes errors out. These conditions usually occur due to selection of excessive timeframes, or a very large asset scope or other settings, which when used in conjunction with excessive detection timeframes and large asset scope may lead to long time for report data processing and errors. This use case analyzes some of the areas in the VM report template which can be fine tuned to execute your reports efficiently, effectively and successfully.

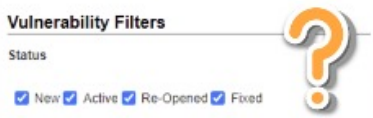
Report takes too long to generate and/or errors out

Template Section	Comments	Recommendations & Resources
	Only include what is needed. Fine tune data selections to create a template that will execute efficiently, effectively, and successfully. The choices in this section are on point and align with the above statement.	Check in with your report recipients to make sure having the report sorted by host works for them.  **Food for Thought** • Often Windows Admins prefer sort by OS • Database teams often prefer sort by Vulnerability • Network teams tend to like Asset Groups sorts, especially if your asset groups are IP ranges

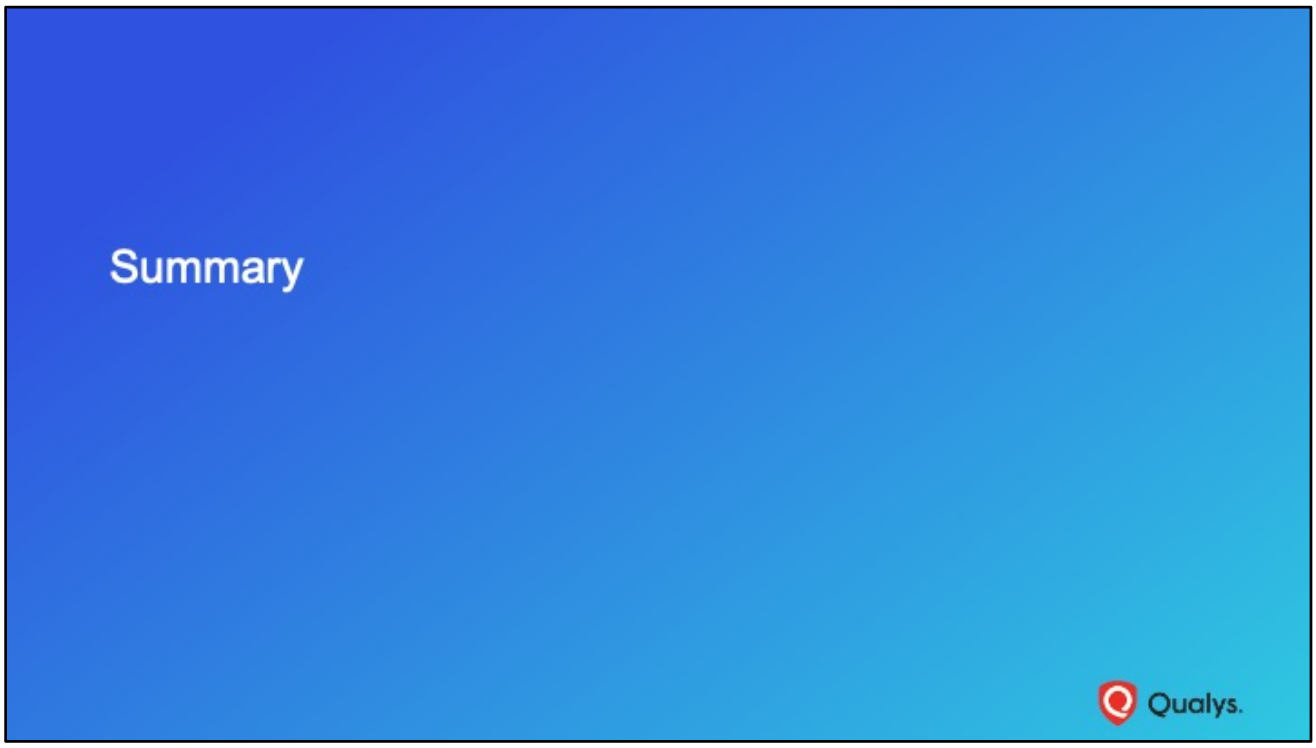
Report takes too long to generate and/or errors out

Template Section	Comments	Recommendations & Resources
 This is a not a valid use case because the exclusions are NOT part of the CUSTOM list	The custom include QID search list doesn't include the QIDs in the Exclude QIDs list.	 This is a valid use case because the exclusions are part of the CUSTOM list  This is a valid use case because the exclusions are part of the CUSTOM list

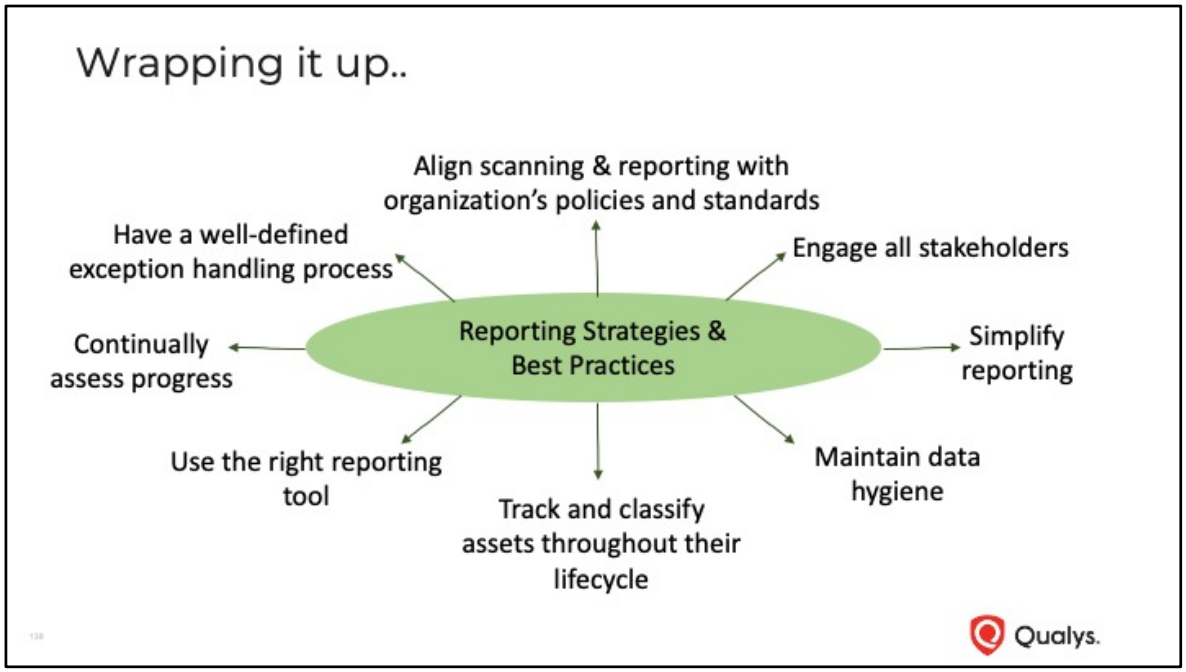
Report takes too long to generate and/or errors out

Template Section	Comments	Recommendations & Resources
	Only include what is needed. Fine tune the data selections to create a template that will execute efficiently, effectively, and successfully.	• Make sure the selections in this section align to the scope of the report. If your policy is "We remediate Confirmed, Severity 3, 4 & 5", then there are too many boxes checked. • In trend reports, it is rare to see information gathered data included in the report data selection criteria. • Consider running a set of reports for all OPEN items (e.g. New, Active and Reopened); and a separate report for Closed items (e.g. Fixed). • Breaking reports into Open and Closed makes for smaller, more digestible reports for recipients, and reduces the chances of error conditions.

Qualys.



This section summarizes the key points covered in this course to drive an effective reporting strategy.



Reporting is a critical aspect of a vulnerability management program. By taking reporting best practices into consideration and taking your core goals into consideration throughout, you'll create reports that gets real results.

Here's a summary of the key points covered in this course:

Align reports with your organization's security standards, policies and guidelines
Start by defining what you want to achieve, why you need to write that report, and who you are writing it for. This will give you a clear idea about your deliverables.

Coordinate and collaborate with all stakeholders
Develop your reports collaboratively. Different stakeholders have different needs – keep in mind who will read your report so as to know what you need to focus on. When improving and enhancing your reports and dashboards, you should work as a tight-knit team, taking everyone's ideas and perspective on board. This will give you a clear idea about the target audience of your deliverables.

Track and classify assets throughout their lifecycle by regular assessment of your IT infrastructure. This way you can identify inactive, decommissioned and repurposed

assets proactively and take steps to purge stale data from your Qualys account.

Maintain data hygiene
Put a plan in place for identifying and purging decommissioned assets to remove stale vulnerability data. Automate stale data removal where possible using appppropriate asset housekeeping options in Qualys.

Use the right reporting tool
If you're looking for an answer to a quick question, use a Query. If you'd like to visually represent a query, use a Widget. Dashboards are made up of multiple widgets. Widgets having a common theme are placed in a single dashboard. Use report templates if you are looking for detailed vulnerability information or if you want to audit your patch management program and so on. Remember Qualys UI Reporting is not intended to export every vulnerability from a subscription or for large scale data exports. Consider using Qualys APIs for large data exports.

Simplify report data
Reports should make it easy for end users to get the information they need to do a better job-whether it's monitoring remediation SLAs, running ad hoc analysis to investigate problems, or analyzing new vulnerability trends and so on. Use common metrics that everyone who will read the report can understand and has experience with using.

Have a clear and well-defined process for managing exceptions
When creating and approving exceptions, it's important to understand that they address sensitive business issues. When an exception is approved, it also means that you're accepting a risk because you're acknowledging and agreeing to the consequences of not remediating the vulnerability. So how these exceptions will be evaluated and how they will be granted is important. Hence, it's recommended to have a clear and well-defined process for managing exceptions.

Use reports to assess progress of your vulnerability management program
Remember the primary goal of vulnerability reporting is to assess impact of vulnerabilities and to devise effective mitigation strategies. Use reports to measure security risks, remediation SLAs and other key metrics that define the success of your vulnerability management program.

Qualys.

Continuous Security

Thank You

training@qualys.com