How to Use Assets with Dashboards

SecurityCenter allows you to easily build customized dashboards using components that provide insight into the vulnerabilities and events occurring on your network. Each component type can visualize data in a unique way for instant analysis of important network anomalies. You can also drill down into the underlying data set for further evaluation of vulnerabilities and events.

Dashboards allow SecurityCenter users to organize and consolidate components in a single view. For example, instead of having 20 discrete components in a single dashboard collection, you can create multiple dashboards grouped by function, each with a subset of the components. Users can then easily switch between dashboards as needed to focus security analysis on different risk profiles or threats. For example, you can set up one dashboard to include five components related to active scanning, while a second dashboard would contain seven components related to passive monitoring.

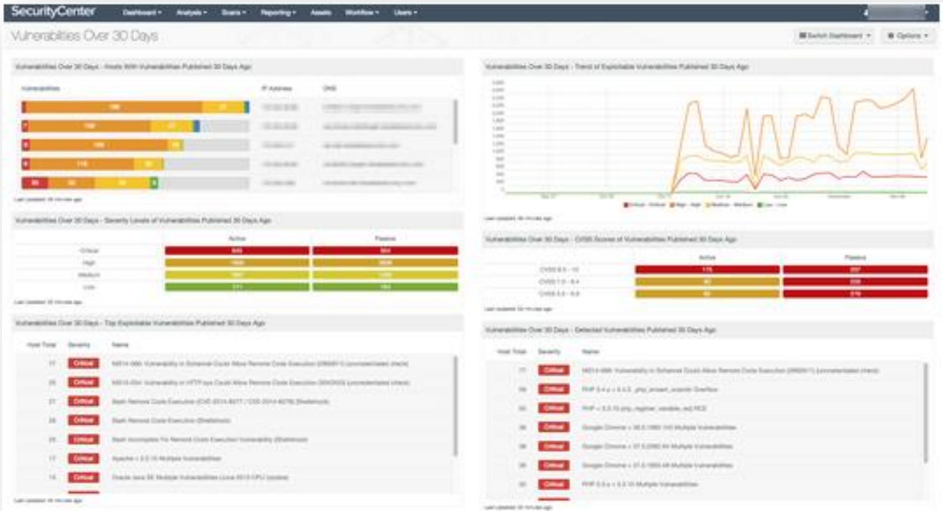
There are preconfigured dashboards and components available in the SecurityCenter Feed, a comprehensive collection of dashboards, reports, Assurance Report Cards (ARCs), and assets. When selecting a preconfigured dashboard, you may want to limit the focus of the dashboard to only the relevant network segments, systems, or repositories that you want to analyze.

In this guide, we'll cover how you can use **Assets** to provide the necessary focus. We'll use the **Vulnerabilities Over 30 Days** dashboard as an example of how to add assets and apply them to dashboards and components.

Note: this guide assumes that Assets are already available in SecurityCenter. For information on how to add Assets, see our "How to Add Assets to SecurityCenter" how-to guide.

Adding Dashboards and Components with Assets

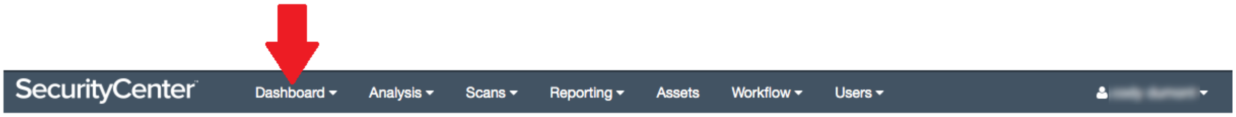
Applying assets to your dashboard or component allows you to view the exact set of information you need to make important security decisions. For this guide, we will show you how to add the **Vulnerabilities Over 30 Days** dashboard with a focus on the LAN 113 asset.



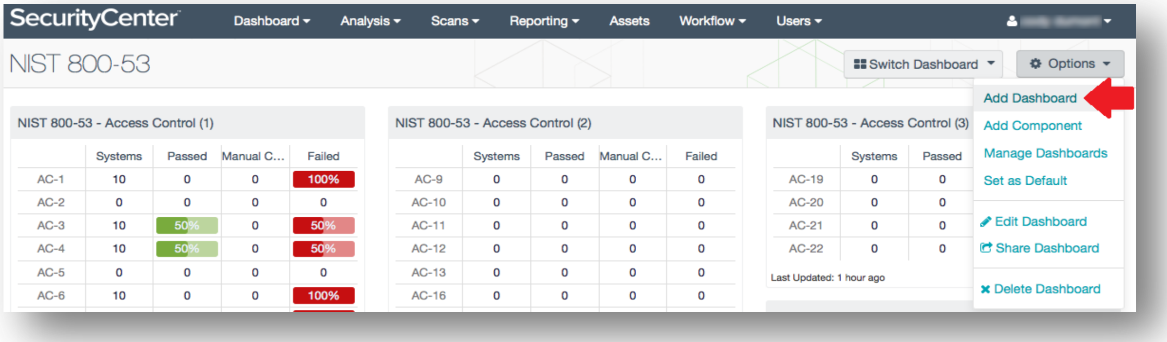
This dashboard will help you identify hosts with vulnerabilities published more than 30 days ago. Despite best intentions, all vulnerabilities are usually not patched organization-wide on a consistent basis. To keep analysts informed of potential risk, not only are vulnerabilities listed, but detailed information is provided about how to remediate issues using a risk-based approach. With the included components, analysts get quick visibility into those vulnerabilities that are exploitable, have a high CVSS rating, or affect a large number of hosts.

Adding and Modifying a Dashboard

To add a dashboard, click on **Dashboard** in the top menu in SecurityCenter.



Next, click on the **Options** drop-down in the upper right-hand corner and select **Add Dashboard**.



NIST 800-53

NIST 800-53 - Access Control (1)

	Systems	Passed	Manual C...	Failed
AC-1	10	0	0	100%
AC-2	0	0	0	0
AC-3	10	50%	0	50%
AC-4	10	50%	0	50%
AC-5	0	0	0	0
AC-6	10	0	0	100%

NIST 800-53 - Access Control (2)

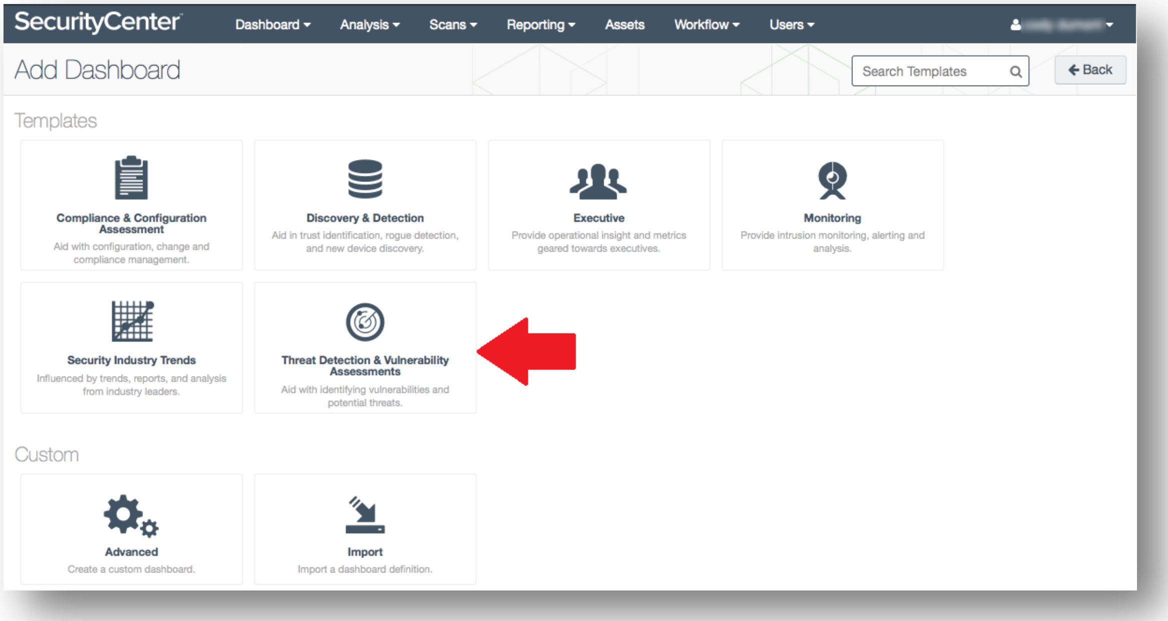
	Systems	Passed	Manual C...	Failed
AC-9	0	0	0	0
AC-10	0	0	0	0
AC-11	0	0	0	0
AC-12	0	0	0	0
AC-13	0	0	0	0
AC-16	0	0	0	0

NIST 800-53 - Access Control (3)

	Systems	Passed
AC-19	0	0
AC-20	0	0
AC-21	0	0
AC-22	0	0

Last Updated: 1 hour ago

When the Add Dashboard screen appears, click on **Threat Detection & Vulnerability Assessments**, since we are creating the **Vulnerabilities Over 30 Days** dashboard.



Add Dashboard

Templates

Compliance & Configuration Assessment
Aid with configuration, change and compliance management.

Discovery & Detection
Aid in trust identification, rogue detection, and new device discovery.

Executive
Provide operational insight and metrics geared towards executives.

Monitoring
Provide intrusion monitoring, alerting and analysis.

Security Industry Trends
Influenced by trends, reports, and analysis from industry leaders.

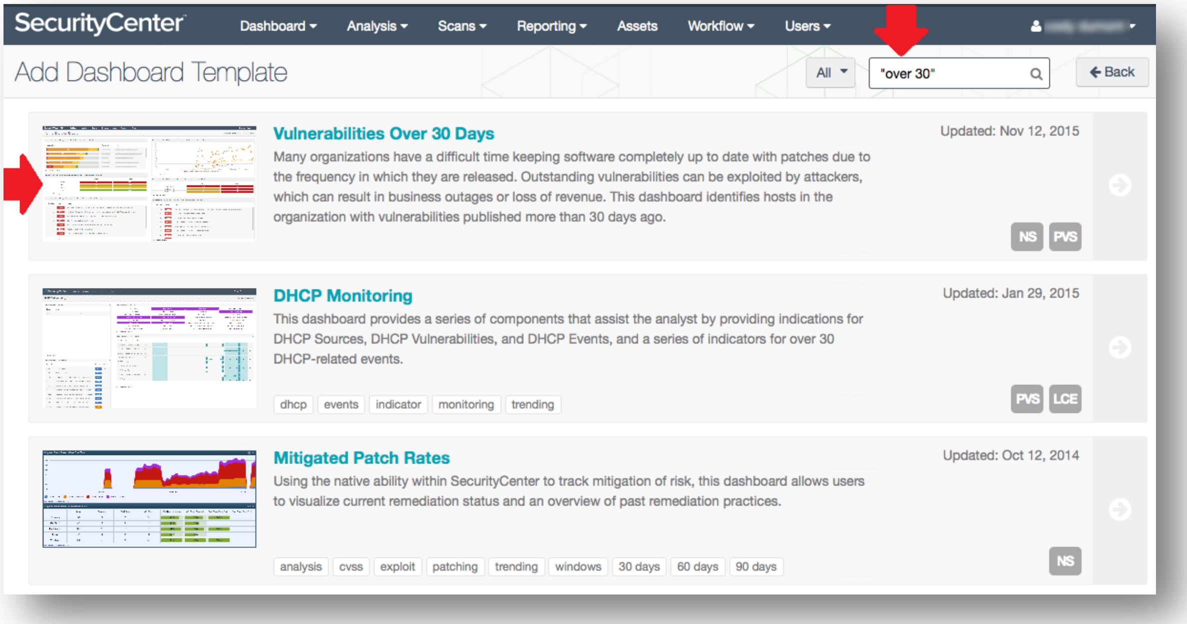
Threat Detection & Vulnerability Assessments
Aid with identifying vulnerabilities and potential threats.

Custom

Advanced
Create a custom dashboard.

Import
Import a dashboard definition.

You can narrow your options by entering “over 30” in the **Search** box at the top of the Add Dashboard Template screen.



Vulnerabilities Over 30 Days

Updated: Nov 12, 2015

Many organizations have a difficult time keeping software completely up to date with patches due to the frequency in which they are released. Outstanding vulnerabilities can be exploited by attackers, which can result in business outages or loss of revenue. This dashboard identifies hosts in the organization with vulnerabilities published more than 30 days ago.

NS PVS

DHCP Monitoring

Updated: Jan 29, 2015

This dashboard provides a series of components that assist the analyst by providing indications for DHCP Sources, DHCP Vulnerabilities, and DHCP Events, and a series of indicators for over 30 DHCP-related events.

dhcp events indicator monitoring trending

PVS LCE

Mitigated Patch Rates

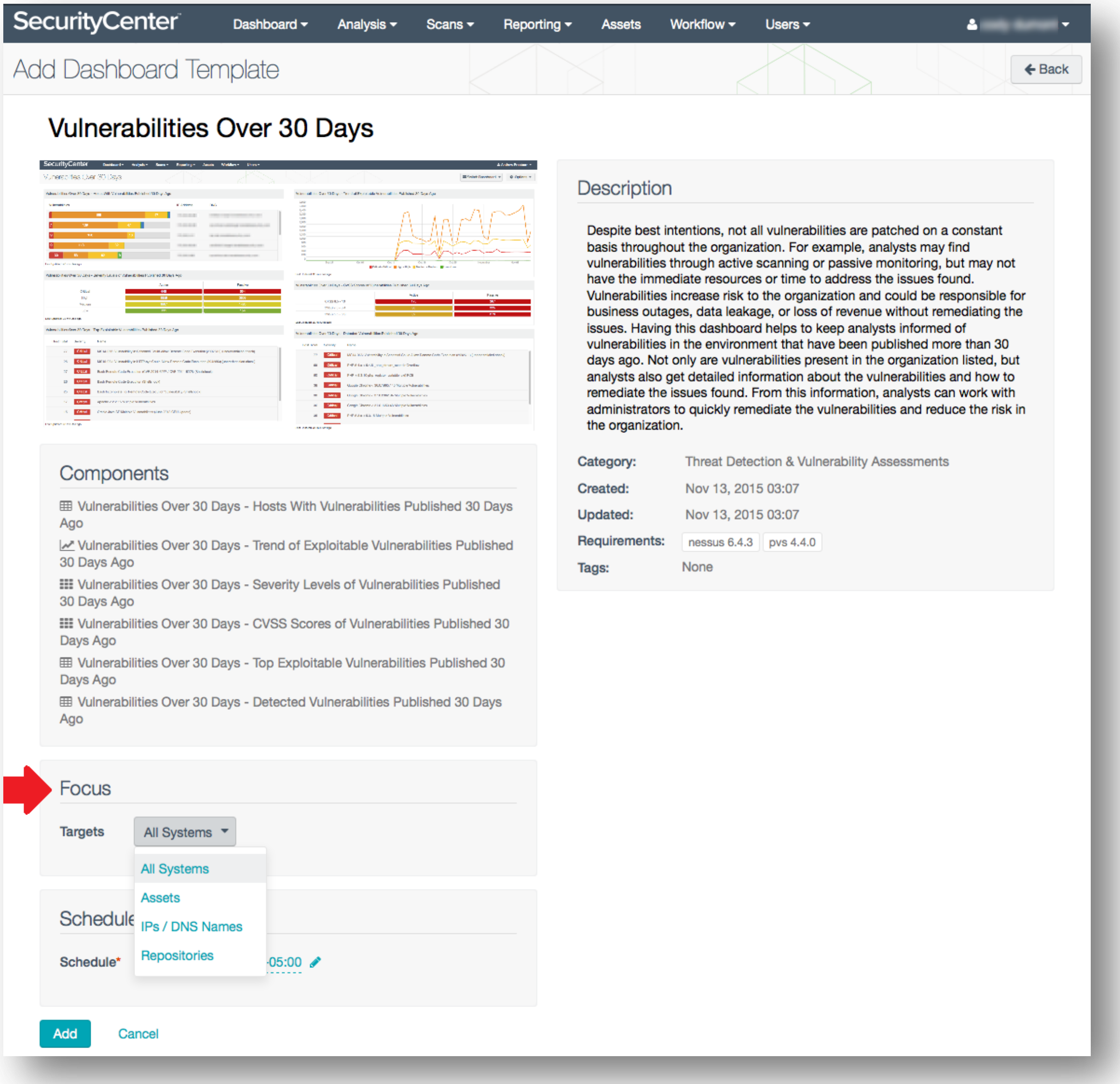
Updated: Oct 12, 2014

Using the native ability within SecurityCenter to track mitigation of risk, this dashboard allows users to visualize current remediation status and an overview of past remediation practices.

analysis cvss exploit patching trending windows 30 days 60 days 90 days

NS

From this list, select the dashboard template to add to SecurityCenter. The next screen will provide you with a detailed description on the collection and a list of all components. This screen is also where you apply your asset to focus the dashboard display on the specific data set you need to view. Under the Focus section, you can refine your view by Asset, IP address/DNS Name, or Repository in the **Target** drop-down menu. In our example, we will select **Assets**, as we want to focus on the LAN 113 asset.



Add Dashboard Template

Vulnerabilities Over 30 Days

Description

Despite best intentions, not all vulnerabilities are patched on a constant basis throughout the organization. For example, analysts may find vulnerabilities through active scanning or passive monitoring, but may not have the immediate resources or time to address the issues found. Vulnerabilities increase risk to the organization and could be responsible for business outages, data leakage, or loss of revenue without remediating the issues. Having this dashboard helps to keep analysts informed of vulnerabilities in the environment that have been published more than 30 days ago. Not only are vulnerabilities present in the organization listed, but analysts also get detailed information about the vulnerabilities and how to remediate the issues found. From this information, analysts can work with administrators to quickly remediate the vulnerabilities and reduce the risk in the organization.

Category: Threat Detection & Vulnerability Assessments
Created: Nov 13, 2015 03:07
Updated: Nov 13, 2015 03:07
Requirements: nessus 6.4.3 pvs 4.4.0
Tags: None

Components

- Vulnerabilities Over 30 Days - Hosts With Vulnerabilities Published 30 Days Ago
- Vulnerabilities Over 30 Days - Trend of Exploitable Vulnerabilities Published 30 Days Ago
- Vulnerabilities Over 30 Days - Severity Levels of Vulnerabilities Published 30 Days Ago
- Vulnerabilities Over 30 Days - CVSS Scores of Vulnerabilities Published 30 Days Ago
- Vulnerabilities Over 30 Days - Top Exploitable Vulnerabilities Published 30 Days Ago
- Vulnerabilities Over 30 Days - Detected Vulnerabilities Published 30 Days Ago

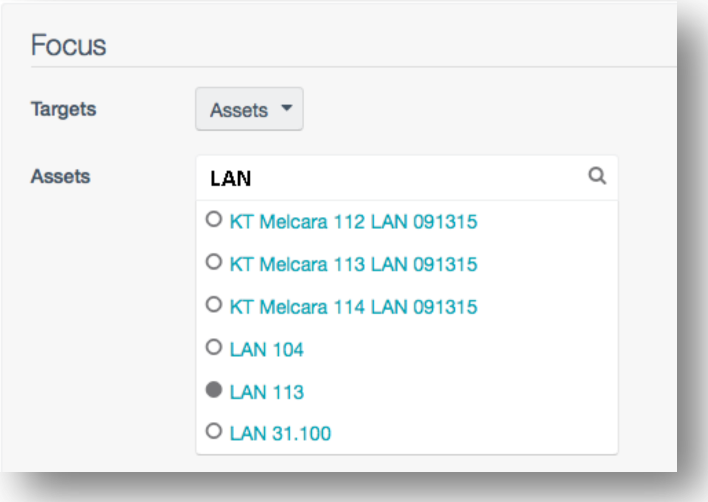
Focus

Targets: All Systems ▾

Schedule

Schedule* -05:00

Searching for “LAN” in the search field will allow you to easily find and select **LAN 113**.



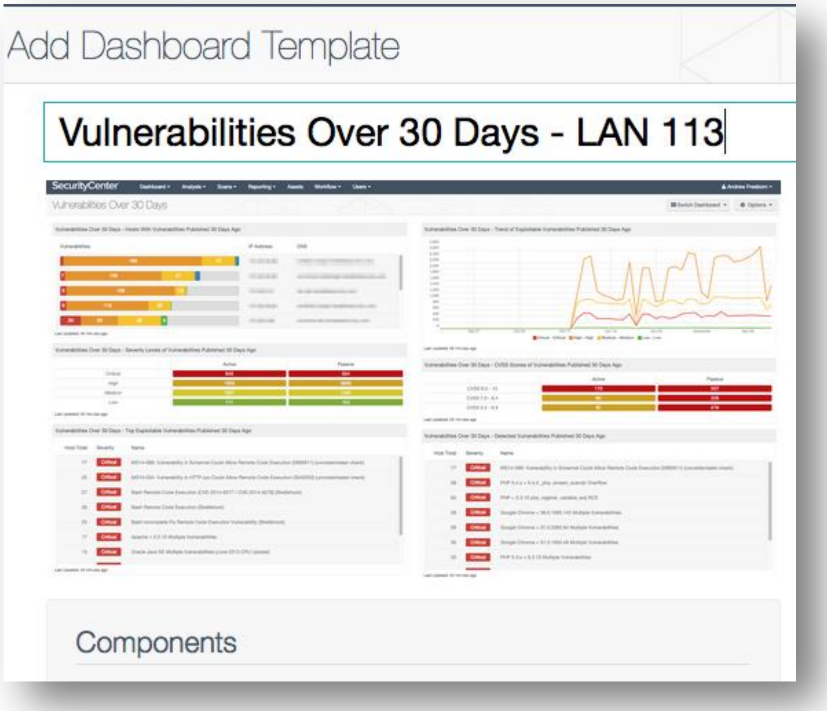
Focus

Targets: Assets

Assets: LAN

○ KT Melcara 112 LAN 091315
○ KT Melcara 113 LAN 091315
○ KT Melcara 114 LAN 091315
○ LAN 104
● LAN 113
○ LAN 31.100

You can click on and modify the dashboard title to keep track of which asset data is being presented in this dashboard.

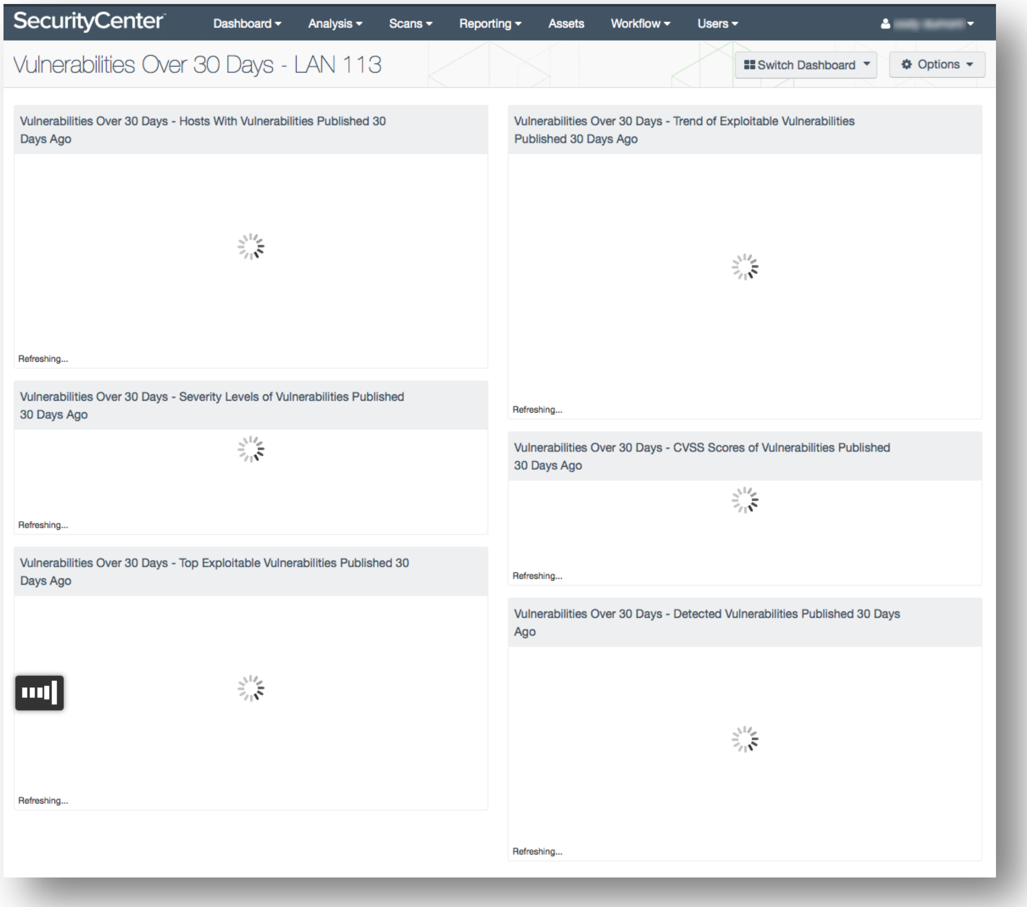


Add Dashboard Template

Vulnerabilities Over 30 Days - LAN 113

Components

Finally, hit **Add** at the bottom of the page to create your dashboard. Loading the dashboard may take a few minutes. You will see icons that show the data is loading.



Vulnerabilities Over 30 Days - LAN 113

Vulnerabilities Over 30 Days - Hosts With Vulnerabilities Published 30 Days Ago

Refreshing...

Vulnerabilities Over 30 Days - Trend of Exploitable Vulnerabilities Published 30 Days Ago

Refreshing...

Vulnerabilities Over 30 Days - Severity Levels of Vulnerabilities Published 30 Days Ago

Refreshing...

Vulnerabilities Over 30 Days - CVSS Scores of Vulnerabilities Published 30 Days Ago

Refreshing...

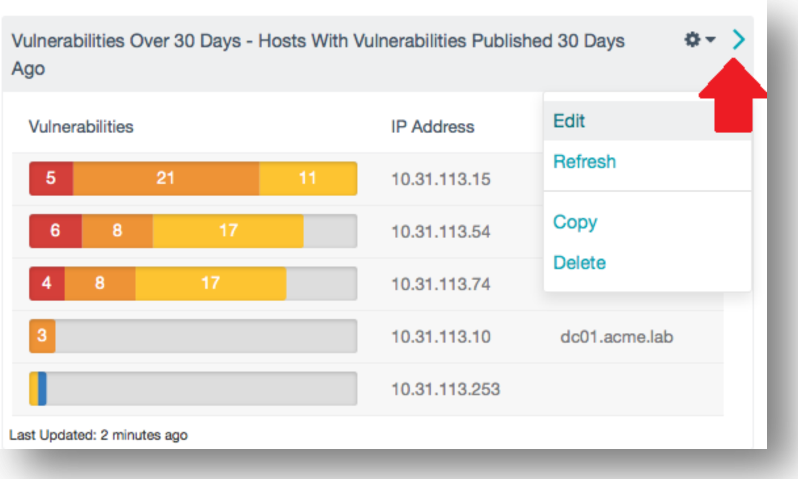
Vulnerabilities Over 30 Days - Top Exploitable Vulnerabilities Published 30 Days Ago

Refreshing...

Vulnerabilities Over 30 Days - Detected Vulnerabilities Published 30 Days Ago

Refreshing...

Once the data loads, you can drill down into that component by clicking on the arrow in the upper-right corner.

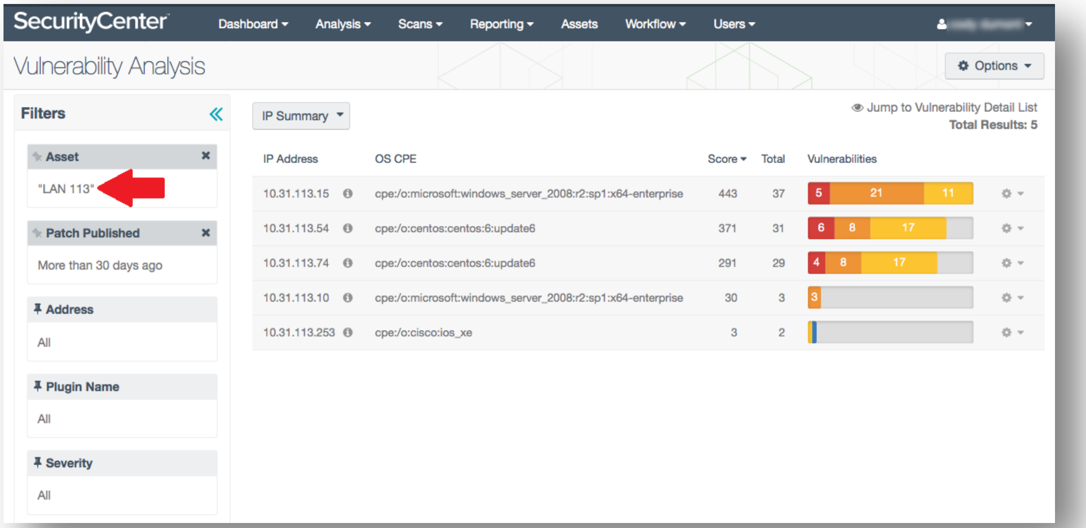


Vulnerabilities Over 30 Days - Hosts With Vulnerabilities Published 30 Days Ago

Vulnerabilities	IP Address	
5 21 11	10.31.113.15	
6 8 17	10.31.113.54	
4 8 17	10.31.113.74	
3	10.31.113.10	dc01.acme.lab
	10.31.113.253	

Last Updated: 2 minutes ago

Components displaying vulnerability data will bring the user to the Vulnerability Analysis screen for the associated asset and other applied filters. You can see that the asset is correctly applied in the upper left-hand corner.



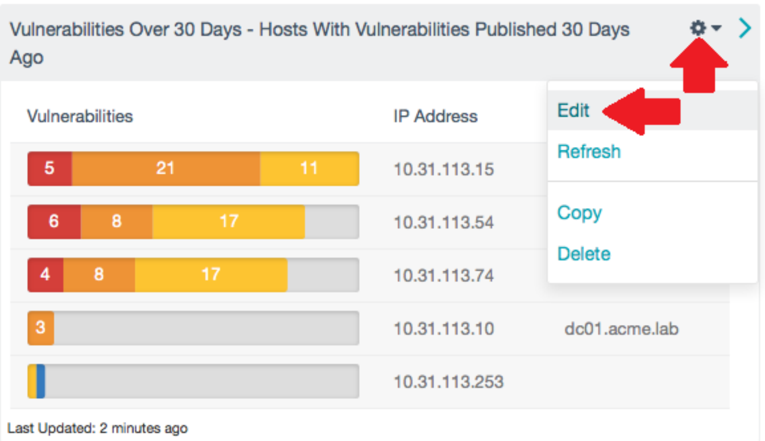
Total Results: 5

Filter	Value
Asset	"LAN 113"
Patch Published	More than 30 days ago
Address	All
Plugin Name	All
Severity	All

IP Address	OS CPE	Score	Total	Vulnerabilities
10.31.113.15	cpe:/o:microsoft:windows_server_2008:r2:sp1:x64-enterprise	443	37	5 21 11
10.31.113.54	cpe:/o:centos:centos:6:update6	371	31	6 8 17
10.31.113.74	cpe:/o:centos:centos:6:update6	291	29	4 8 17
10.31.113.10	cpe:/o:microsoft:windows_server_2008:r2:sp1:x64-enterprise	30	3	3
10.31.113.253	cpe:/o:cisco:ios_xe	3	2	

Editing Dashboard Components

Once your dashboard is created, you can edit the filters behind the components. Simply click on the gear icon in the upper right-hand corner of the component and select **Edit** from the drop-down menu.



Vulnerabilities Over 30 Days - Hosts With Vulnerabilities Published 30 Days Ago

Vulnerabilities	IP Address	
5 21 11	10.31.113.15	
6 8 17	10.31.113.54	
4 8 17	10.31.113.74	
3	10.31.113.10	dc01.acme.lab
	10.31.113.253	

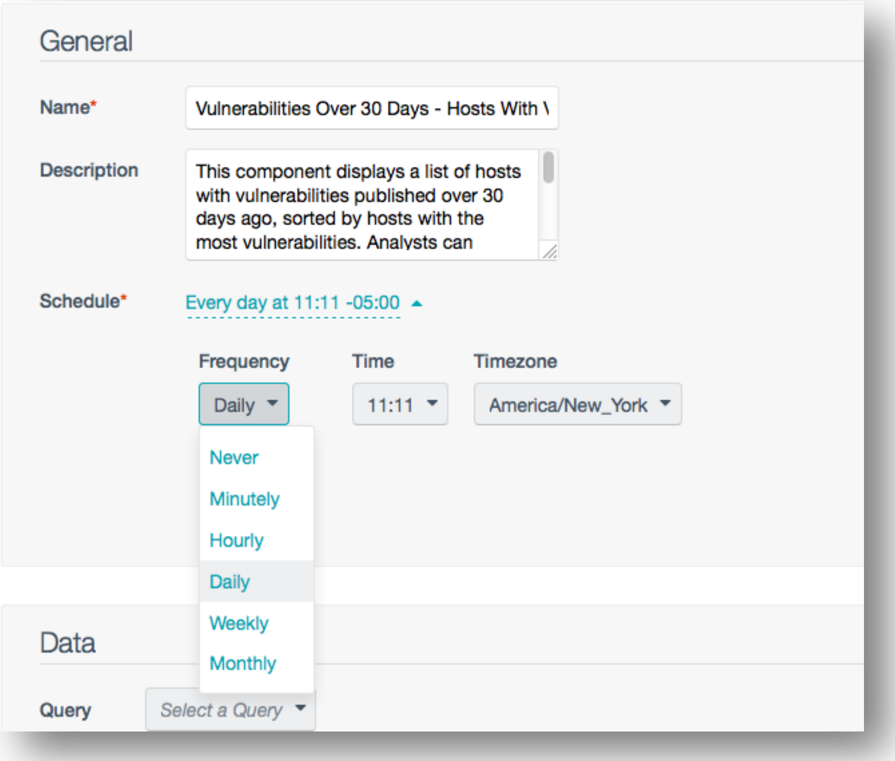
Last Updated: 2 minutes ago

There are six component types available in a dashboard: Table, Line Chart, Area Chart, Bar Chart, Pie Chart, and Matrix, and each has a unique set of options for how to view and filter data. We will briefly cover the main distinctions between component types below.

Table, Bar Chart, and Pie Chart Components

Table, Bar Chart, and Pie Chart all offer the same set of filter and view options. We'll use the Table Component for this example, but the functionality is the same for any of the three component types.

When you click on the gear icon of a Table Component, the Edit Table Component screen will appear. Under General, you can change the schedule of how often the query is run.



General

Name* Vulnerabilities Over 30 Days - Hosts With \

Description This component displays a list of hosts with vulnerabilities published over 30 days ago, sorted by hosts with the most vulnerabilities. Analysts can

Schedule* Every day at 11:11 -05:00

Frequency: Daily

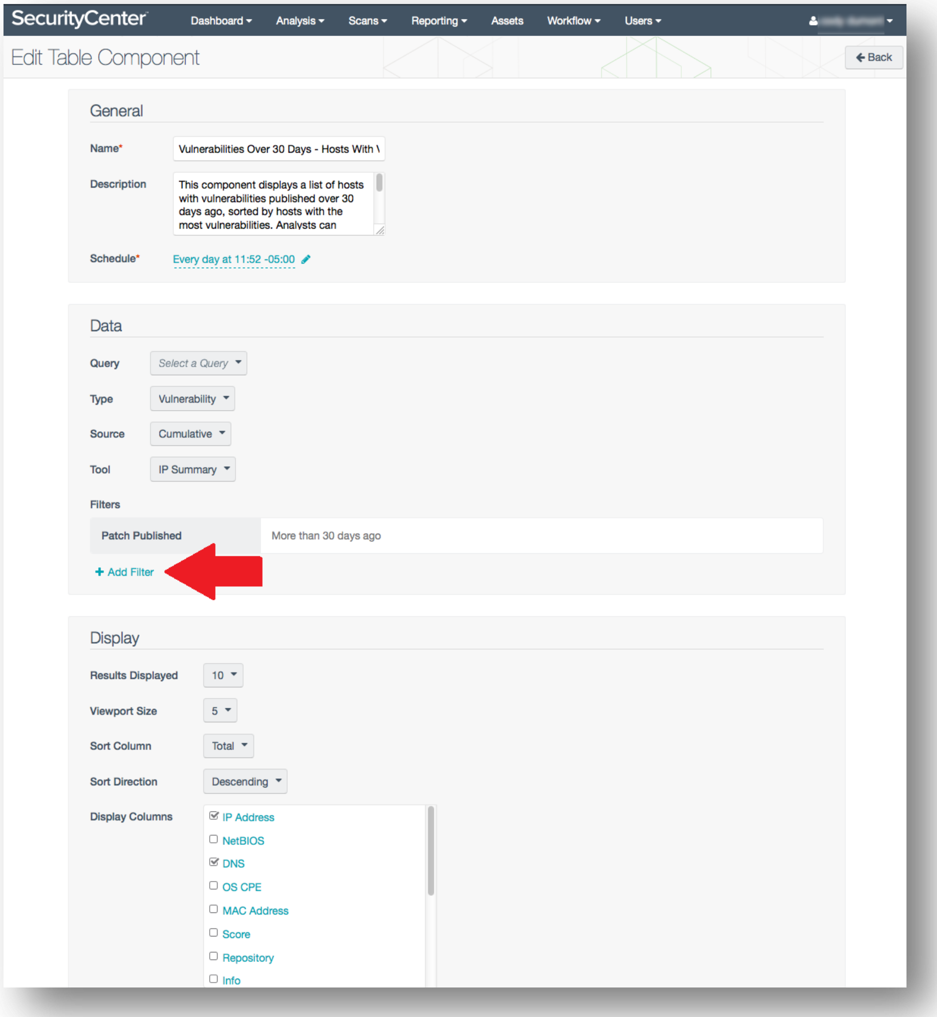
Time: 11:11

Timezone: America/New_York

Data

Query: Select a Query

In the Data section, you can insert additional filters to provide finer granularity. Simply click **Add Filter**.



Edit Table Component

General

Name*: Vulnerabilities Over 30 Days - Hosts With \

Description: This component displays a list of hosts with vulnerabilities published over 30 days ago, sorted by hosts with the most vulnerabilities. Analysts can

Schedule*: Every day at 11:52 -05:00

Data

Query: Select a Query

Type: Vulnerability

Source: Cumulative

Tool: IP Summary

Filters

Patch Published: More than 30 days ago

Display

Results Displayed: 10

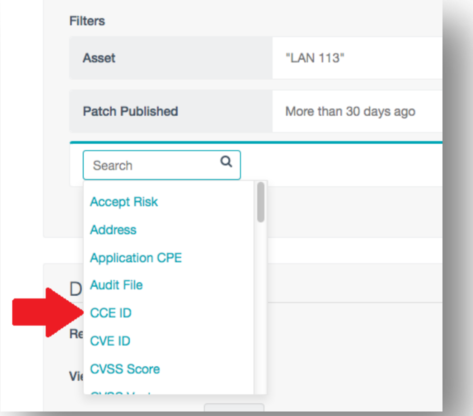
Viewport Size: 5

Sort Column: Total

Sort Direction: Descending

Display Columns:
- ☑ IP Address
- □ NetBIOS
- ☑ DNS
- □ OS CPE
- □ MAC Address
- □ Score
- □ Repository
- □ Info

The drop-down list provides you with a list of choices to further filter the data. You can, for example, select to filter by CCE IDs for a specific year.



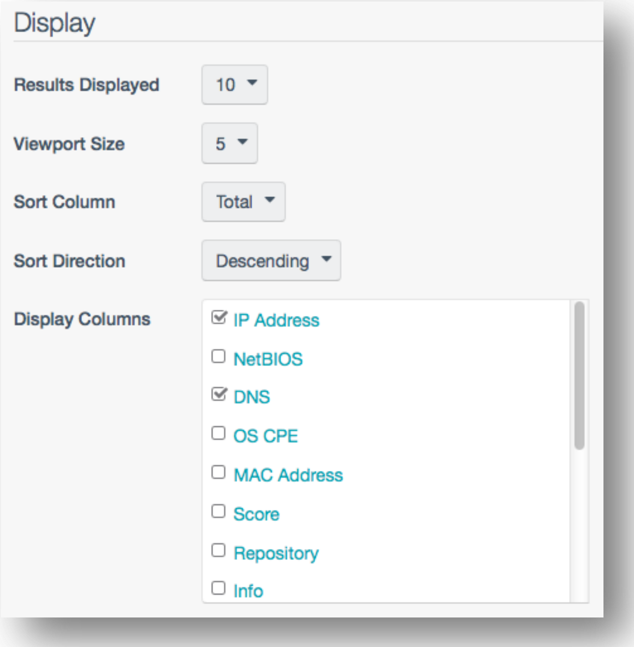
Filters

Asset	"LAN 113"
Patch Published	More than 30 days ago

Search

- Accept Risk
- Address
- Application CPE
- Audit File
- CCE ID
- CVE ID
- CVSS Score

You can also change display options, including which direction – ascending or descending – that data is sorted, as well as which columns show up. The Viewport size will determine how many results show up in the component window, ranging from 5 to 50.



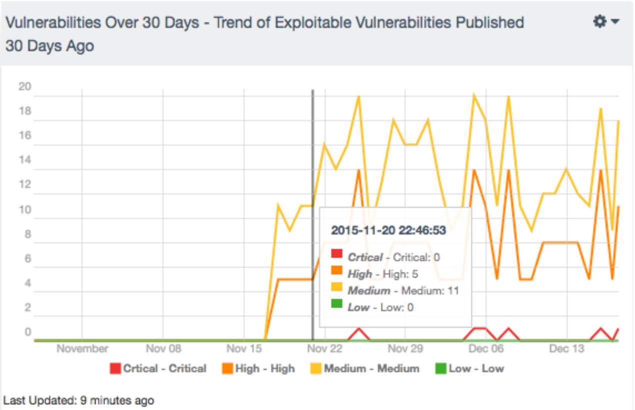
Display

Results Displayed	10
Viewport Size	5
Sort Column	Total
Sort Direction	Descending
Display Columns	☑ IP Address □ NetBIOS ☑ DNS □ OS CPE □ MAC Address □ Score □ Repository □ Info

Line Chart and Area Chart Components

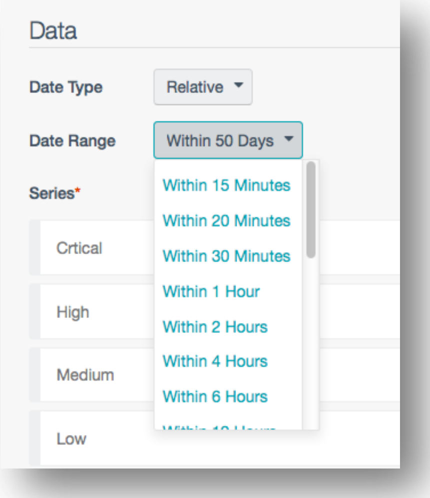
Line Chart and Area Chart offer the same data filtering and display options. The only difference is that the Area Chart will fill in the space between lines on the chart.

These charts are distinctive because you can select date range options and you have the ability to view roughly 40-50 total data points at one time. Mousing over the line will show you the data for each data point. This chart shows data for every 24 hours for a period of 50 days – so about one data point each day.



Vulnerabilities Over 30 Days - Trend of Exploitable Vulnerabilities Published 30 Days Ago

Last Updated: 9 minutes ago



Data

Date Type: Relative

Date Range: Within 50 Days

Series*

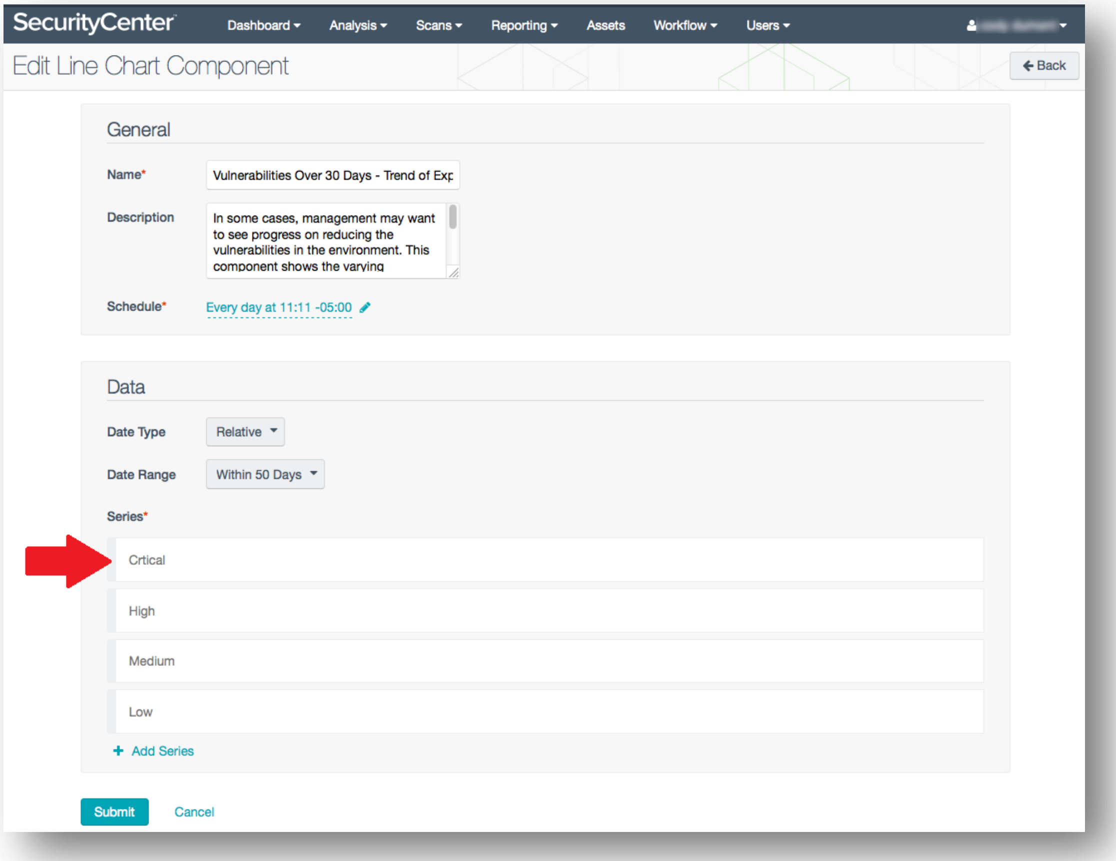
Crtical

High

Medium

Low

There are separate filters in the Data section that will allow you to edit Series Data.



Edit Line Chart Component

General

Name*: Vulnerabilities Over 30 Days - Trend of Exp

Description: In some cases, management may want to see progress on reducing the vulnerabilities in the environment. This component shows the varying

Schedule*: Every day at 11:11 -05:00

Data

Date Type: Relative

Date Range: Within 50 Days

Series*

Crtical

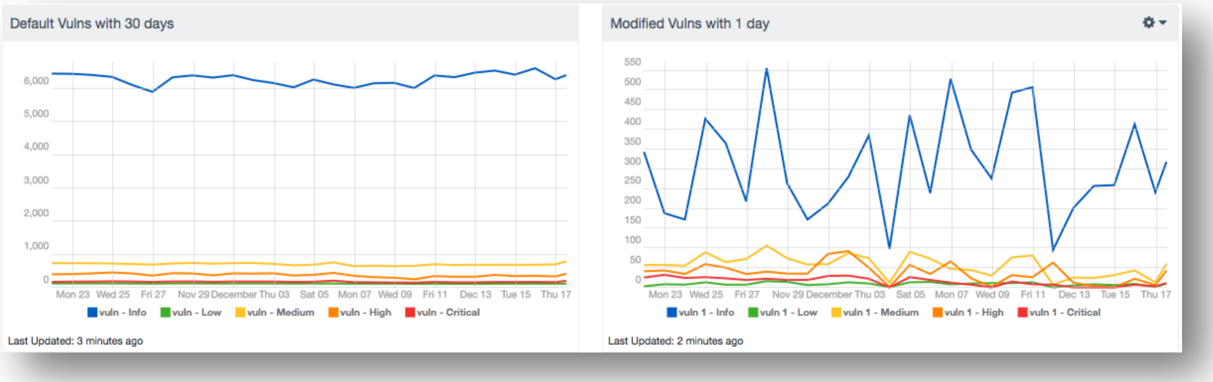
High

Medium

Low

Having a clear understanding of the default filter setting is important. Depending on how your data is defined, you may end up getting very flat lines on your chart – which doesn't prove very useful at-a-glance data for analysts.

In the example below, we are using a chart showing severity levels. The default setting for Vulnerability Last Observed and Vulnerability Discovered is 30. The default setting means that each data point is showing for 30 days from the point of discovery (see the example blue line on left below). With that setting, you will not really see much change over time. However, if you set the series to show you the change in vulnerabilities over one day (see the example blue line on right below), you will get a much clearer, more dynamic picture of the security risks and changes in your environment.



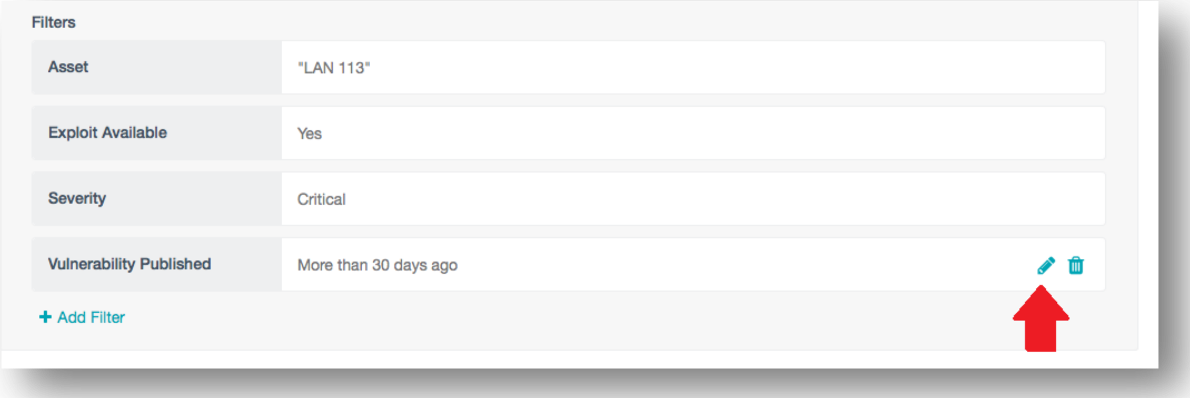
Default Vulns with 30 days

Last Updated: 3 minutes ago

Modified Vulns with 1 day

Last Updated: 2 minutes ago

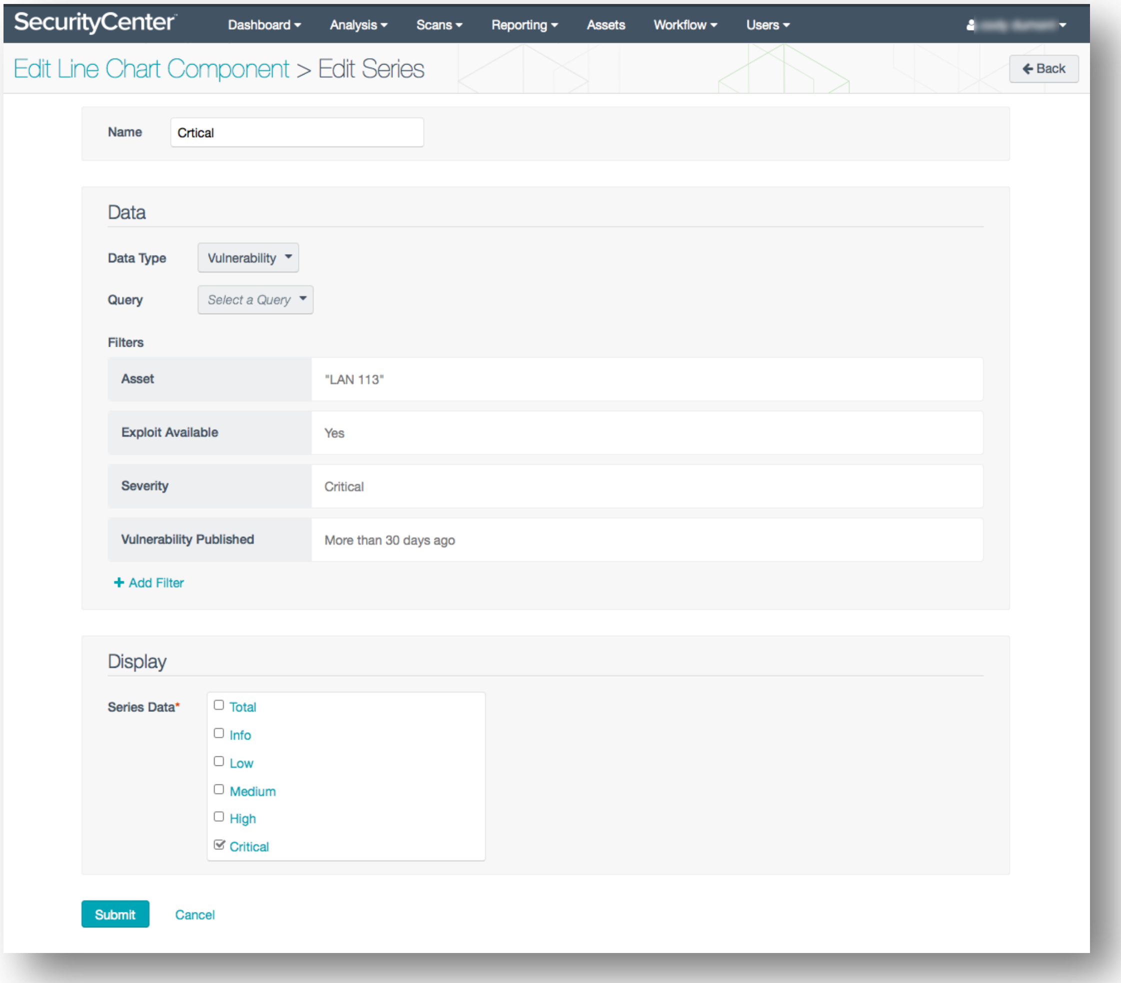
Editing Series Data is very straightforward. Just click on the pencil icon that appears when you mouse over the field you want to edit.



Filters

Asset	"LAN 113"
Exploit Available	Yes
Severity	Critical
Vulnerability Published	More than 30 days ago

When editing, you can change any of the fields to meet your requirements.



Edit Line Chart Component > Edit Series

Name: Crtical

Data

Data Type: Vulnerability ▾

Query: *Select a Query* ▾

Filters

Asset	"LAN 113"
Exploit Available	Yes
Severity	Critical
Vulnerability Published	More than 30 days ago

+ Add Filter

Display

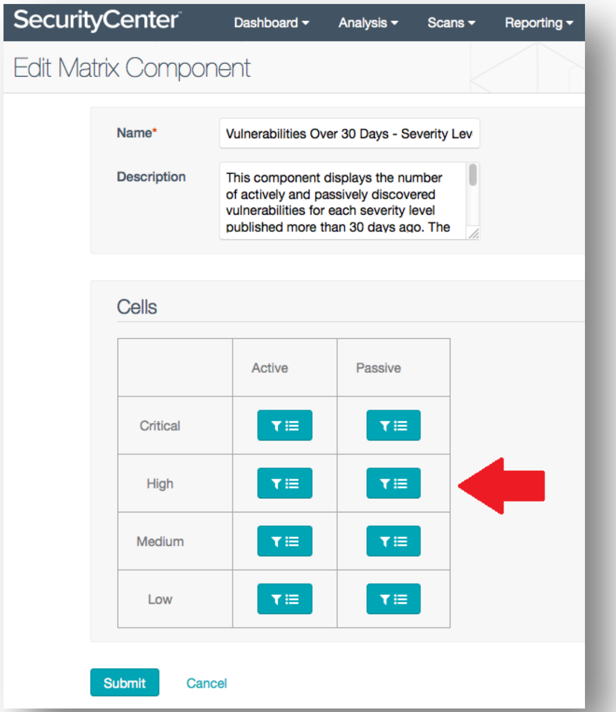
Series Data*

- ☐ Total
- ☐ Info
- ☐ Low
- ☐ Medium
- ☐ High
- ☑ Critical

Submit Cancel

Matrix Component

The final component type is the Matrix, which has unique data filtering and display options. To edit a Matrix component, click on the gear drop-down and select **Edit**, then select a cell to edit in the Edit Matrix Component screen.



Edit Matrix Component

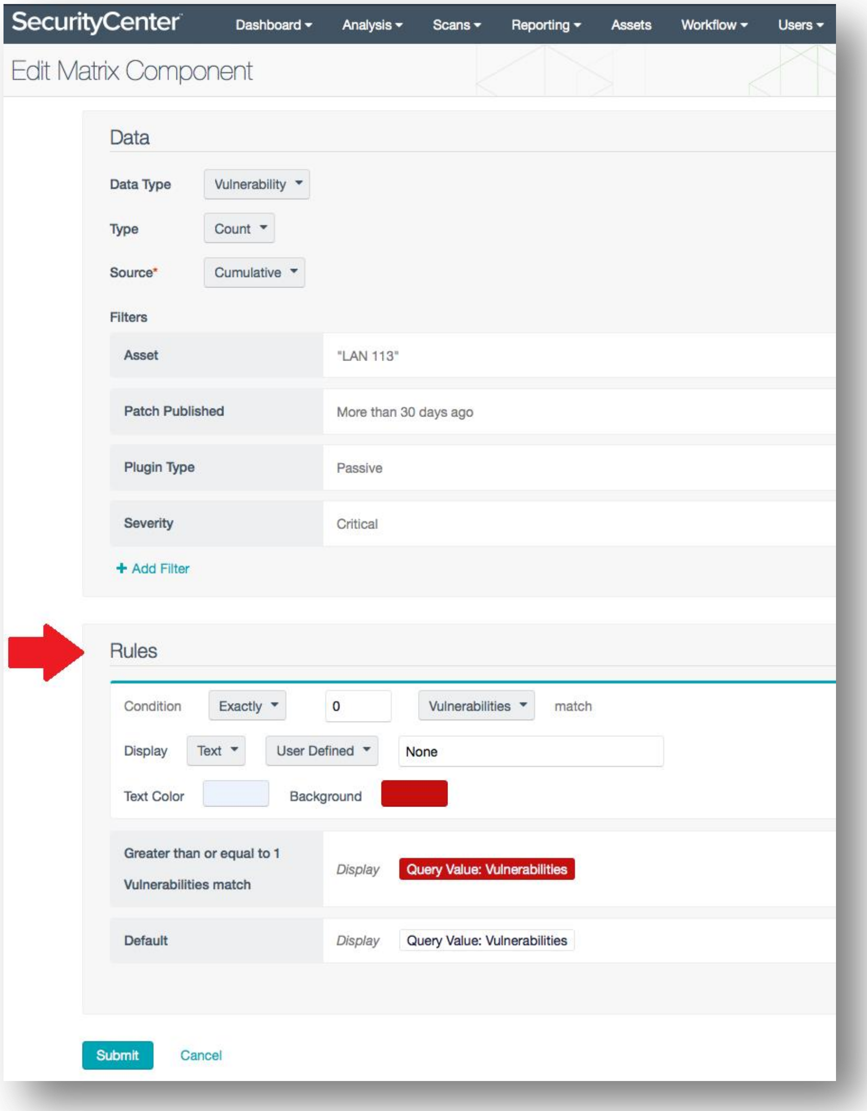
Name* Vulnerabilities Over 30 Days - Severity Lev

Description This component displays the number of actively and passively discovered vulnerabilities for each severity level published more than 30 days ago. The

Cells

	Active	Passive
Critical	▼≡	▼≡
High	▼≡	▼≡
Medium	▼≡	▼≡
Low	▼≡	▼≡

Matrix components allow you to create rules that can do anything from change colors, to print text, to create a ratio bar. The default setting for a matrix cell is to display the results of the query. For more information on creating Matrix components, please see the SecurityCenter User Guide.



Edit Matrix Component

Data

Data Type: Vulnerability

Type: Count

Source*: Cumulative

Filters

Asset	"LAN 113"
Patch Published	More than 30 days ago
Plugin Type	Passive
Severity	Critical

Rules

Condition: Exactly 0 Vulnerabilities match

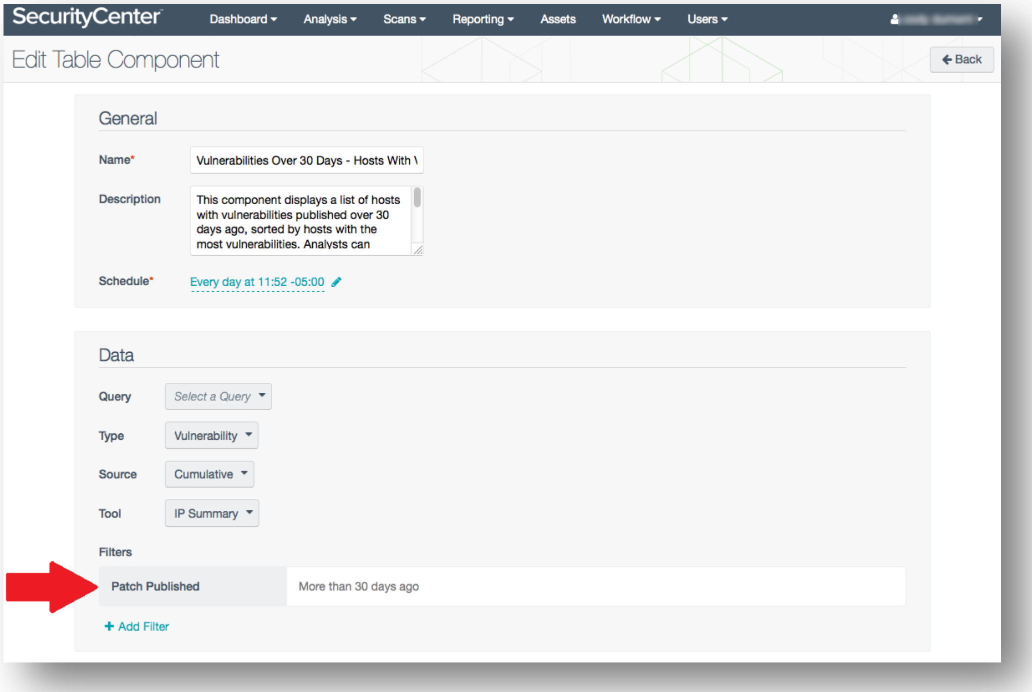
Display: Text User Defined None

Text Color: ⬜ Background: 🟥

Greater than or equal to 1 Vulnerabilities match	*Display* Query Value: Vulnerabilities
Default	*Display* Query Value: Vulnerabilities

Modifying Dashboards or Components without Assets

If a dashboard or component is created without any assets, you can always go in and add the assets at a later time. Below is an example of a Table Component that was created without any assets.



Edit Table Component

General

Name* Vulnerabilities Over 30 Days - Hosts With \

Description This component displays a list of hosts with vulnerabilities published over 30 days ago, sorted by hosts with the most vulnerabilities. Analysts can

Schedule* Every day at 11:52 -05:00

Data

Query Select a Query

Type Vulnerability

Source Cumulative

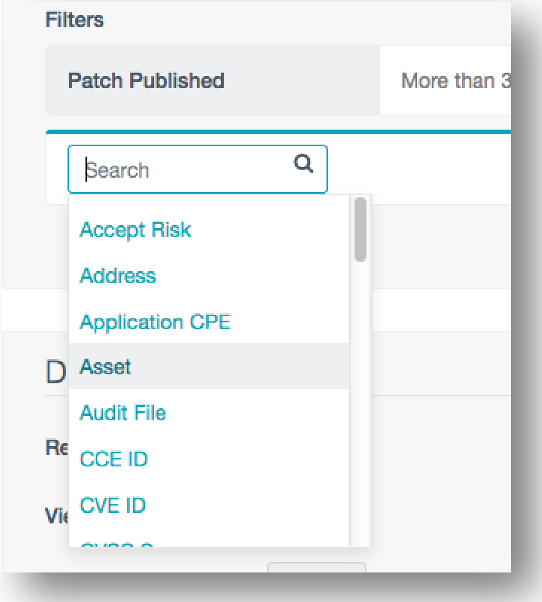
Tool IP Summary

Filters

Patch Published More than 30 days ago

+ Add Filter

To add an asset, you will simply click on **Add Filter** and select **Assets** from the drop-down list.

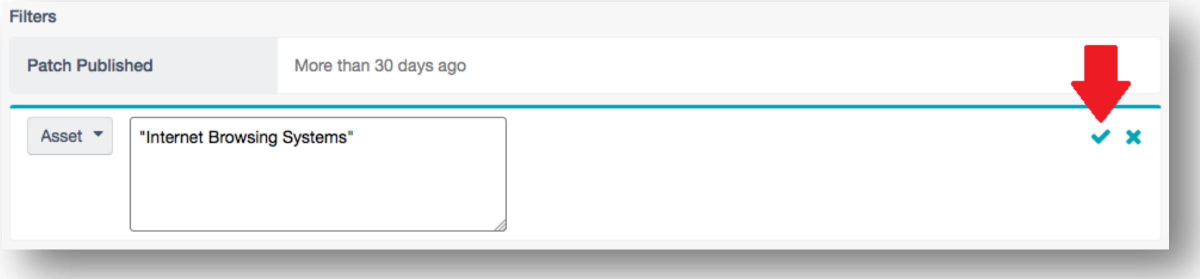


Filters

Patch Published More than 3

Search

Next, select the type of asset from the list. In this case, we selected **Internet Browsing Systems**. Click the checkmark to add the asset.

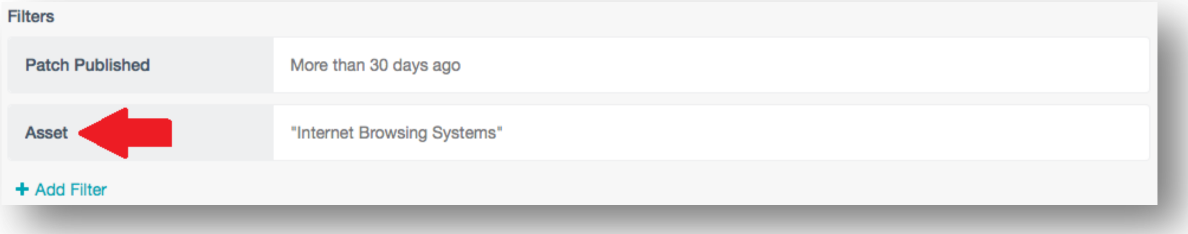


Filters

Patch Published: More than 30 days ago

Asset: "Internet Browsing Systems"

You will see that the asset (in this case a dynamic asset) is now added to the component.



Filters

Patch Published: More than 30 days ago

Asset: "Internet Browsing Systems"

For More Information

If you would like more information about adding and using assets, visit the SecurityCenter Discussion Forum and SecurityCenter Dashboard blog, or refer to your SecurityCenter User Guide.

About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.