Tenable SecurityCenter Vulnerability Management Tool - UCI User Guide

- Overview
- How To Get Access
- Training Video
- Basic Usage
  - Accessing The Web Console
  - Viewing My Systems' Overall Status (Dashboards)
    - Switching Between Dashboards
    - Setting a Default Dashboard
    - Adding a New Dashboard
    - Managing & Deleting Dashboards
  - Viewing My Systems' Vulnerabilities
    - Navigate to Vulnerabilities from Dashboard Items
    - Vulnerability Analysis
      - Filtering Vulnerabilities
      - Creating Queries
  - Viewing My World Reachable Systems' Vulnerabilities (Loading a Pre-Defined Query)
  - Understanding My Systems' Vulnerabilities
    - Synopsis
    - Description
    - Solution
    - See Also
    - Discovery
    - Host Information
    - Risk Information
    - Exploit Information
    - Plugin Details
    - Vulnerability Information
    - Reference Information
  - Addressing Vulnerabilities
    - Verifying Remediation
    - Accepting Risk (Won't/Can't fix with no other measures in place to lower risk)
    - Recasting Risk (Won't/Can't fix but with other measures in place to lower risk)
  - Basic Reporting
  - Workflow Features
    - Setup Alerts
    - View Accept/Recast Risk Rules
  - Advanced Usage - TBD
    - Creating Custom Scans
    - TBD

Overview

Tenable SecurityCenter is an enterprise vulnerability management tool that UCI has purchased to expand our vulnerability management initiative campus-wide. SecurityCenter is being offered as a self-service tool that systems administrators, management and business owners can use to track the vulnerability status of their systems as well as track the mitigation progress.

How To Get Access
To request access please fill out this ServiceNow Request Form which will be submitted to the OIT Security Team for processing.

Please be sure to list any IP/Networks you or your group are responsible for so they can be added to the system for vulnerability scanning.

Training Video

UCI Tenable SecurityCenter Training Video

Basic Usage

Accessing The Web Console

**NOTE** This is a site that requires Duo Multi-Factor authentication to login into, if you do not have a DUO token please see Duo Security Multi-Factor Authentication - UCI User Guide for instructions on how to get one.

Once your access request has been completed by the OIT Security Team, you will be able to login to the system.

The web console can be accessed at https://securitycenter.oit.uci.edu.

If you have a Smartphone DUO token, to login just enter your UCInetID/password and a push will automatically be sent to your smartphone device to accept. If you have a hardware DUO token when entering your UCInetID password you will need to then put a ",," and your 6-digit token code from your hardware device. Ex: P@ssW0rd,957832

Viewing My Systems' Overall Status (Dashboards)

Once logged in, you will be automatically taken to the "Dashboard" screen. This screen is designed to give you an overall snapshot of your environment. There are many different default dashboards you can choose from if you want to get metrics on something in particular and you can also create a custom dashboard if you desire.

Switching Between Dashboards

If you have multiple dashboard's you would like to navigate in-between, in the upper right hand of your screen, right under your name choose the drop down button "Switch Dashboard" and choose the dashboard you would like to navigate to.

Setting a Default Dashboard

If you would like to change your default dashboard for when you login, navigate to the dashboard you desire, then click on the "Options" button and choose "Set as Default" from the drop down. The next time you login the dashboard you have marked as default should display.

Adding a New Dashboard

In SecurityCenter there are many default template dashboards you can choose from. To add a new dashboard to your dashboard list, navigate to the "Options" button on the dashboard screen. In the drop down select "Add a Dashboard". You will then be taken to a list of templates you can choose from to create a new dashboard. Once added the dashboard will show up in your "Switch Dashboard" or "Manage Dashboard's" lists.

Managing & Deleting Dashboards
If you would like to remove a dashboard from your "Switch Dashboard" list or delete a dashboard entirely you can navigate to the "Options" button on the dashboard screen. In the drop down select "Manage Dashboards". On the manage dashboard screen you can choose to unpin a dashboard so it no longer appears in your available list of dashboards to view. You can also edit, share and delete dashboards under this screen.

**Viewing My Systems' Vulnerabilities**

If you want to take a deeper look at the vulnerabilities within your system there are several different ways to navigate to that data as well as filter & sort it to meet your criteria.

**Navigate to Vulnerabilities from Dashboard Items**

If you wish to take a deeper look at a certain item on a dashboard you can do so by simply clicking on the "Browse Component Data" arrow in the upper right of the table in the dashboard. This will take you to the "Vulnerability Analysis" screen with filter's pre-selected as they display on the dashboard screen.

**Vulnerability Analysis**

To view all vulnerabilities without any pre-defined filters navigate to "Analysis" -> "Vulnerabilities" on the top menu bar in SecurityCenter. From this screen you can see all the vulnerabilities within your group and can choose from the drop down how you would like to sort the data, Ex. DNS Name Summary if you want to sort by host name or IP Summary if you want to sort by IP.

**Filtering Vulnerabilities**

From the vulnerability analysis screen you can narrow down the vulnerabilities that are displayed by filtering the data to fit your search criteria. To do this click on the "Double Blue Arrow" on the left hand of the screen and this will pop out the filter selection screen. From the pop out screen you can select filters and choose new filters to help narrow down your search criteria. You can also clear existing filters or load saved queries.

**Creating Queries**

Once you have used filter's to narrow down your search criteria you can save these settings into a query so that it can be used for future searches. From the screen that you have all the filters set on navigate to "Options" in the upper right hand corner and choose "Save Query" from the drop down menu. You will be prompted to enter a name for your query and once saved this query can be located in the menu bar from "Analysis" -> "Queries".

**Viewing My World Reachable Systems' Vulnerabilities (Loading a Pre-Defined Query)**

As part of an OIT Security Team initiative in late 2015 we are running weekly vulnerability scans of the campus systems that are open through our campus border firewall, meaning they are accessible from the world. Since these particular systems have high visibility they could potentially be at a higher risk for exploitation. As such we have made it easy for users of SecurityCenter to narrow down their vulnerability search criteria to just these systems in order to quickly address any vulnerabilities on these systems. This is a query that we have already created for you. To load this query simply navigate to the "Vulnerability Analysis" screen and expand out the "Filters" section. Choose "Load Query" from the bottom of the filter's and select "Systems Open at Campus Border (World Reachable)" from the list. This will display only the systems that belong to your group that are world reachable.

**Understanding My Systems' Vulnerabilities**
Once you have narrowed down your search criteria you can navigate into a particular vulnerability to find out more detailed information regarding what the vulnerability scan discovered. Within the vulnerability detailed screen you will see several sub-areas with more detailed information.

**Synopsis**
Gives a simplistic narrative of the vulnerability found.

**Description**
Gives a detailed breakdown of what this vulnerability entails.

**Solution**
If available, a recommended solution to mitigate the vulnerability will be provided.

**See Also**
Links to outside resources that have posted more detailed information regarding the vulnerability.

**Discovery**
Let's you know when this vulnerability was first discovered from our scanning as well as the last time it was seen via the scanning. (This comes in handy when you are doing re-occuring scanning on assets)

**Host Information**
Gives you both the IP Address and the DNS name of the host if it was able to resolve the information.

**Risk Information**
Details the score & risk classification this vulnerability received based on the Common Vulnerability Scoring Systems (CVSS). Based on the score received this will determine if the vulnerability is Critical, High, Medium or Low.

**Exploit Information**
Explains when a patch was published for this vulnerability and also details if an exploit is currently available for this vulnerability, if an exploit is available it will also detail what it can be exploited with ex. Malware

**Plugin Details**
This is an internal Tenable designation that will tell you the number assigned to this vulnerability within Tenable as well as when it was published to SecurityCenter and last updated.

**Vulnerability Information**
Gives details on when this vulnerability was first discovered and had information released about it.

**Reference Information**
Links to outside sources with more information regarding this specific vulnerability.
Addressing Vulnerabilities

Once you have analyzed the data provided from the vulnerability scan there are three main options for addressing the vulnerability.

Verifying Remediation

If you were able to remediate the vulnerability by applying the solution provided you can click on the "Launch Remediation Scan" button from the vulnerability detailed screen. This will auto-launch a screen to start a new scan testing for that particular vulnerability on that particular host. In this screen you can also choose to add other hosts to scan for this vulnerability as well. If the remediation scan comes up that the vulnerability is indeed resolved it will fall off your reports and be moved into any reports showing "mitigated hosts". To see the results of this scan you can navigate to "Scans" -> "Scan Results" and located the scan you just did for the vulnerability in the list.

Accepting Risk (Won't/Can't fix with no other measures in place to lower risk)

If you are unable to remediate a vulnerability and there are no other measures in place to lower the risk, you can choose to click the "Accept Risk" button from the vulnerability detailed screen. This will pop out a new screen where you can put in a comment regarding why you are accepting the risk. In this screen you can also set an expiration date for the accepted risk as well as input the targets/assets you want to accept the risk on. Once you accept this risk for a vulnerability on a system, the vulnerability will be hidden from reports and placed in a repository of accepted risks with the name of the user who submitted it. The vulnerability will stay hidden on reports either until it's deleted or hits the expiration date, at which time it will then re-appear on the reports during the next scan.

Accepted Risk Example: A vulnerability is found on a sever that is going to be decommissioned in 2 weeks, you may choose to accept this risk for the remaining two weeks rather than spend time addressing a vulnerability that will be resolved by decommissioning the server.

Recasting Risk (Won't/Can’t fix but with other measures in place to lower risk)

If you are unable to remediate a vulnerability but there are other measures in place to lower the risk, you can choose to click the "Recast Risk" button from the vulnerability detailed screen. This will pop out a new screen where you can change the vulnerability to a new severity level and add a comment regarding why you are changing the severity level. You can then choose to apply this to one or multiple hosts with that vulnerability. Once you recast this risk it will be re-classified on reports and placed in a repository of recast risks with the name of the user who submitted it.

Recast Risk Example: A high vulnerability is found on a system regarding FTP, however to get into that system you have to use VPN and multi-factor authentication and the system only allows users with appropriate access into the system. There are several layers of protection here that would make it very difficult to exploit. Therefore you might recast the risk from a "high" to a "medium".

Basic Reporting

Reporting can be used if you wish to send vulnerability snapshots to someone who is not using SecurityCenter dashboards. Reporting can be accessed by going to "Reporting" drop down from the main menu bar. Within the "Reports" area you can choose to add a new report from hundreds of templates, or you can choose to create a custom report. While creating the report you can also choose if you want to run the report on all the systems in your group or just a particular asset or host. Once the report is created it will show in a list under "Reports", you then have an option to "Run" the report, results from the report being run will be placed in "Reporting" -> "Report Results".
Workflow Features

The Workflow section contains options for alerting and ticketing. These functions allow the user to be notified of and properly handle vulnerabilities and events as they come in.

Setup Alerts

SecurityCenter can be configured to perform actions, such as email alerts, for select vulnerability or alert occurrences. To setup an alert navigate from the main menu bar to "Workflow" -> "Alerts". Here you can choose to "Add" a new alert and choose the criteria that you would like to be notified when its met and the action you would like to take place when it occurs.

Alert Example: When more than 10 vulnerabilities are discovered that have an exploit available email me.

View Accept/Recast Risk Rules

From the main menu bar under "Workflow" -> "Accepted Risks" or "Recast Risks" you can view the list of currently created rules or accepted or re-cast risks. This enables users to obtain information on what particular vulnerabilities or hosts have been declared accepted or re-cast as well as who created the rule and any comments that were put in regarding the rule.

Advanced Usage - TBD

Creating Custom Scans

TBD

30-321271885