Tenable.io Evaluation Workflow

Last Revised: March 05, 2020
# Table of Contents

**Welcome** ................................................................................................................................. 4

**Part One** .................................................................................................................................. 6

Create Users, Groups, and Access Groups .................................................................................... 7
(Optional) Create Networks ............................................................................................................ 9
Link a Scanner and Begin Scanning ................................................................................................. 10
Link and Configure Nessus Scanners .............................................................................................. 11
Create Centralized Credentials ...................................................................................................... 12
Create an Internal Scan .................................................................................................................... 13
Create an External Scan ................................................................................................................... 14
(Optional) Create Exclusion Lists ................................................................................................... 15
(Optional) Use Agents .................................................................................................................... 16
  Link and Configure Agents ............................................................................................................ 17
  Create the Agent Scan .................................................................................................................. 19
  Configure Cloud Connectors ......................................................................................................... 20

**Part Two** .................................................................................................................................. 21
Create and Organize Tags ................................................................................................................ 22
Create and Customize Dashboards ................................................................................................... 24
Create and Customize Widgets ......................................................................................................... 26
Create and Customize Saved Searches ............................................................................................. 27
Advanced Search Examples - Vulnerabilities Dashboard ................................................................. 28
Advanced Search Examples - Assets Dashboard ............................................................................... 30
(Optional) Create Recast & Accept Risk Rules ............................................................................... 32

Copyright © 2020 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Lumin, Assure, and the Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
(Optional) Create Scanner Groups (Scan Distribution) .............................................................. 33

Part Three .................................................................................................................................. 34

Understand and Utilize Vulnerability Priority Rating (VPR) ...................................................... 35

Visualize VPR in Tenable.io ........................................................................................................ 36

Create a Saved Search for VPR .................................................................................................... 38

Create a Custom VPR Widget ........................................................................................................ 39

Utilize Tenable.io VM Solutions .................................................................................................. 40
Welcome

Use this document to evaluate Tenable.io for your organization. For more comprehensive feature and configuration information, see the Tenable.io User Guide.

Before you begin:

- Sign up for a Tenable.io evaluation.

To get started in your evaluation period with Tenable.io:

Part 1

1. Create Users, Groups, and Access Groups
2. (Optional) Create Networks
3. Link a Scanner and Begin Scanning
4. Link and Configure Nessus Scanners
5. Create Centralized Credentials
6. Create an Internal Scan
7. Create an External Scan
8. (Optional) Create Exclusion Lists
9. (Optional) Use Agents

Part 2

10. Create and Organize Tags
11. Create and Customize Dashboards
12. Create and Customize Widgets
13. Create and Customize Saved Searches
14. (Optional) Create Recast & Accept Risk Rules
15. (Optional) Create Scanner Groups (Scan Distribution)

Part 3
16. **Understand and Utilize Vulnerability Priority Rating (VPR)**

17. **Visualize VPR in Tenable.io**

18. **Create a Saved Search for VPR**

19. **Create a Custom VPR Widget**

20. **Utilize Tenable.io VM Solutions**
Part One

**Note:** Tenable.io is currently going through a UX design change. Upon initial login, you access the Classic Interface. As all new features and updates take place only in the New Interface, please select the **New Interface** button at the top of the page to begin configuring Tenable.io. For more information, see [Transition to the New Interface](#).

1. **Create Users, Groups, and Access Groups**
2. **Create Target Group(s)**
3. **(Optional) Create Exclusion Lists**
4. **Create an External Scan**
5. **Link a Scanner and Begin Scanning**
6. **(Optional) Use Agents**
Create Users, Groups, and Access Groups

1. Log in to Tenable.io.

2. In the upper-left corner, click the button. The left navigation plane appears.

3. Click Settings.

4. Click the Users widget.

5. Create your first user and select the applicable permissions.

   **Best Practice:** Most users require the Standard role. The two additional user roles, Scan Manager and Scan Operator, are specific to scan management use cases.

6. Create your first group:
   a. In the upper-left corner, click the button. The left navigation plane appears.
   b. Click Settings.
   c. Click the Groups widget.
   d. Next to User Groups, click the button. The Create User Group plane appears.
   e. Select the group members to add to the group.
   f. Click Create.

7. Create your first access group:

   **Tip:** As the initial user, in order to start scanning, you must create an Access Group with the Scan Target permission to scan all subnets within scope. This is due to the fact that there are no assets to "manage" during initial configuration.

   **Best Practice:** The most secure practice is to disable this setting for the System All Assets Access Group. Then, create other access groups with unique network ranges to implement least privilege access control. For more information, see Access Groups.
a. In the upper-left corner, click the button. The left navigation plane appears.

b. Click Settings.

c. Click the Access Groups widget.

d. In the top right corner of the page, click Create Access Group.

e. In the Name box, type a name for the access group.

   **Note:** The name must be unique within your organization.

f. Based on the identifiers for the targets you want to scan, click the appropriate access group type.

   If you create an access group of one type, then change the type during configuration, Tenable.io prompts you to confirm the action. If you confirm, Tenable.io clears any previously added rule filters.

g. Assign Asset Rules(s) for specific criteria (e.g., IP address, AWS Account ID, and FQDN).

   **Tip:** When configuring an Access Group, you have two permission options: **Manage Assets** and **Scan Targets**. **Manage Assets** restricts a User/Group to only being able to scan existing assets (assets that have been tagged). The **Scan Target** permission supersedes the **Manage Assets** permission to also include the ability to scan IPs/FQDNs and IP ranges. The **Manage Asset** permission is designed for system admins to run remediation scans only on their existing and previously identified targets.

h. In the Users & Groups section, add appropriate User/Group access.

i. If you do not want to grant access to all users and groups, click Add Users and Groups. Then, search for and assign access to the appropriate user or group.

   **Example Scenario:** I'm creating a "New York" Access Group representing my New York Data-center. However, I don’t want to give the same permission set to a variety of different groups. As such, I can grant System Admins **Can Scan** permission while also allowing Senior Management **Can View** permissions without needing to create 2 separate Access Groups.

j. Click Save.
(Optional) Create Networks

Networks provide the ability to account for overlapping IP space. For example, your New York subnet of 192.168.1.1/24 is identical to a new merger/acquisition network. Tenable.io creates a unique identifier within the network in order to segment these overlapping networks.

1. In the upper-left corner, click the menu button.

   The left navigation plane appears.
2. Click Settings.
3. Click the Sensors widget.
4. Click Nessus.
5. Click the Networks tab.
6. In the upper-right corner, click Add Network.

   The Settings page appears.
7. Type a name for the network.
8. Click Create.
9. Associate the segmented network scanners to the appropriate network that you created.
Link a Scanner and Begin Scanning

1. Link and Configure Nessus Scanners
2. Create Centralized Credentials
3. Create an Internal Scan
4. Create an External Scan
Link and Configure Nessus Scanners

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. Click **Settings**.

3. Click the **Sensors** widget.

4. In the left navigation menu, click **Nessus**.

5. In the upper-right corner of the page, click **Add Nessus**.

6. In the **Linking Key** section, click **Copy**.

7. [Download Nessus](#).

8. Run the Nessus installer on your local/internal system and create a local Nessus user.

9. Select **Managed by Tenable.io** and copy / paste the Linking key copied from your Tenable.io instance. For more information, see [Link a Sensor](#).

   As soon as the scanner is linked, it appears as an available scanner within Tenable.io. Allow approximately 15-20 minutes for plugins to sync.

   **Tip:** Plugins continue to sync to the scanner(s) every 24 hours after initial linkage.

10. Once the scanner is ready to be used, configure the appropriate User/Group permissions for the scanner.

---

Copyright © 2020 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Lumin, Assure, and the Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
Create Centralized Credentials

1. In the upper-left corner, click the button.
   
The left navigation plane appears.
2. Click **Settings**.
3. Click the **Credentials** widget.
4. Click the **+** button next to the **Credentials** title.
   
The credential form plane appears.
5. Select the type of Credentials you want to create (Window, SSH, etc.).
6. Type your credentials and then select the appropriate permissions for the group/user that you want to allow access to use.
   
   **Tip:** This is typically done with *Can Edit* permissions.
7. Click **Save**.
Create an Internal Scan

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. In the left navigation plane, in the Tools section, click Scans.

3. In the upper-right corner of the page, click the Create a Scan button.
   The Select a Scan Template page appears.

4. Click Basic Network Scan.

5. Type a name for the scan.

6. Select an internally linked scanner, and not a Cloud Scanner.

7. In the Targets section, type the appropriate scan range (IP, Range, CIDR, FQDN).

   **Note:** Target Groups are being phased out in favor of Access Groups, but scanning by Access Group has not been implemented in the new Scan Configuration of Tenable.io, which requires manual input of your targets or the creation of Target Groups specific to the subnets you are scanning.

8. At the bottom of the page, add User/Group permissions as appropriate.

9. Leave Default group permission set to no access.

10. Click the Credentials tab.

11. Click Add.

12. From the Managed Credentials drop-down, select the appropriate credentials created in the previous section.

13. Click Save & Launch.
Create an External Scan

1. In the upper-left corner, click the  button.
   The left navigation plane appears.
2. In the left navigation plane, in the Tools section, click Scans.
3. In the upper-right corner of the page, click the +Create a Scan button.
   The Select a Scan Template page appears.
4. Click Basic Network Scan.
5. Type a name for the scan.
6. Select the US Cloud Scanner option.
7. In the Targets section, type the external scan range (IP, Range, CIDR, FQDN).
   Tip: This is typically done with Can Control permissions.
8. At the bottom of the page, add User/Group permissions as appropriate.
9. Leave Default group permission set to no access.
10. Click Save & Launch.
(Optional) Create Exclusion Lists

You can use exclusions to restrict the scanning of specific hosts based on a selected schedule.

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Tools** section, click **Exclusions**.

3. Create Exclusions as applicable.

   **Tip:** Exclusions without a schedule are set to *Always On.*
(Optional) Use Agents

1. Link and Configure Agents
2. Create the Agent Scan
Link and Configure Agents

1. In the upper-left corner, click the button. The left navigation plane appears.
2. Click **Settings**.
3. Click the **Sensors** widget.
4. Click **Agents**.
5. Similar to linking a scanner, download the OS-appropriate Nessus Agent package from the [Tenable Downloads](https://www.tenable.com/downloads) site.
6. Run the Nessus Agent installer and follow the [Link an Agent](https://www.tenable.io) steps in the Tenable.io user guide.
7. As soon as the Nessus Agents are linked, it shows up as an available agent within Tenable.io.
   - **Tip:** Plugins continue to sync to the Agent(s) every 24 hours after initial linkage.
   - **Best Practice:** When configuring agents, be sure to assign the Agent to an Agent Group.
   - **Tip:** You are required to scan via an Agent Group.
8. Create an Agent group.
9. Type a name for the agent group.
10. Click **Add Users and Groups**.
11. Select the individual agents you want to be part of this group.
   - **Best Practice:** Categorize Nessus Agents into Regional or OS-specific groups (or both).
12. Click **Save**.
13. In the upper-left corner, click the button. The left navigation plane appears.
14. Click **Settings**.
15. Click the **Sensors** widget.
16. Click **Linked Agents**.

17. Select the individual Agents you want to include in a group.

18. Click the folder option at the bottom right of screen to add Agent members to the group of choice.
Create the Agent Scan

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the Tools section, click Scans.

3. In the upper-right corner of the page, click the Create a Scan button.
   
   The Select a Scan Template page appears.

4. Click the Agent tab.

5. Click Basic Agent Scan.

6. Type a name for the scan.

7. Apply the appropriate Agent Group.

8. Choose an Agent Scan Window.

   **Best Practice:** Set the Scan Window to 12 hours or more. This will ensure that the agent(s) have enough time to check into Tenable.io, receive the scan job, run the scan job, and report back the results.

9. At the bottom of the page, add User/Group permissions as appropriate.

10. Leave Default group permission set to no access.

11. Click Save & Launch.
Configure Cloud Connectors

Please be sure to follow the Cloud Connector Config doc to ensure that your cloud environment is set up appropriately for the Connectors in Tenable.io - Docs can be found here

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. Click Settings.

3. Click the Connectors widget.

4. In the upper-left corner of the page near the Connectors label, click the button.
   
   The Select a Connector pane appears.

5. Select your cloud connector: AWS, Azure, or GCP.

6. Populate the parameters, as described in Create an AWS Connector, Create a GCP Connector, or Create a Microsoft Azure Connector in the Tenable.io Vulnerability Management User Guide.

7. (Optional) Configure schedule import for recurring synchronization.

8. Click Save & Import.
Part Two

1. Create and Organize Tags
2. Create and Customize Dashboards
3. Create and Customize Widgets
4. Create and Customize Saved Searches
5. (Optional) Create Recast & Accept Risk Rules
6. (Optional) Create Scanner Groups (Scan Distribution)
Create and Organize Tags

Best Practice: Tags are organized via Category:Value pairs. Tagging strategy depends on the assets within your environment(s). A list of targets, such as IP addresses, ranges, subnets, DNS names, can be used to create Tenable.io Tags. Example tagging categories include:

- Operating Systems (Windows, Linux, macOS)
- Application (DB, vCenter, etc.)
- Installed Software (Adobe, Java, Chrome, etc.)
- Geographical Region
- New York Data Centers, Remote workforce, etc.
- Business or Organizational Units
- Finance, IT, Prod/Dev, Cloud, etc.
- Network Devices (switch, router, firewall, etc)
- Credentialed scans are typically the fastest and will provide the most thorough vulnerability scan results.
- Publicly/Externally Facing
- Owner

For more information, see the Tagging Video Tutorial.

1. In the upper-left corner, click the button. The left navigation plane appears.
2. Click Settings.
3. Click the Tagging widget.
4. In the upper-right corner of the page, click the Create Tag button. The Create Tag page appears.
5. Click the Category drop-down box.
6. In the Add New Category box, type one of the categories mentioned above.
7. In the Value box, type a tag value.
8. Do one of the following:

**Tip:** There are two tag value types: **Static** and **Dynamic**. Static types can be used for IP and CIDR Ranges and are not contingent upon any Asset Rule Sets. Dynamic types are based upon Asset Rule Sets and are automatically applied to any Asset that meets the Asset Rule criteria moving forward.

- If you want to create a Static Tag type, click **Save**.
- If you want to create a Dynamic Tag type, enable the **Rules** section and select appropriate **Asset Rule** parameters. Click on the “Calculate Affected Assets” button to preview the list of Assets that would be associated with this dynamic tag for verification.
  
  a. Click **Save**.
Create and Customize Dashboards

Tip: Review the Dashboard templates and determine which specific templates are best for your use case. You can then delete any unnecessary widgets which will move the template dashboard to the “My Dashboard” section. From there, you can continue to remove any widget(s) that aren’t applicable. The Pre-Configured Dashboard templates are available in Standard or Detailed PDF exports. A Standard export is simply comprised of a PDF rendering of the dashboard while a Detailed export contains a detailed remediation breakdown of dashboard contents.

1. Click the ➕Dashboards button.

   The **Dashboards** plane appears with a list of configured dashboards.

2. In the **Dashboards** plane header, click the ➕ button.

3. Click **Template**.

   The **Add a Dashboard** plane appears.

4. In the list of templates, locate the template you want to use.

5. Click the ➕ button next to that template.

   **Tip:** To preview the dashboard, click the Dashboard Name rather than the ➕ button to view more details before adding the Dashboard.

   The new dashboard replaces the previously displayed dashboard. The new dashboard also appears with the name "*Copy of selected dashboard*" in the list of dashboards in the dashboards plane.

6. Rename the dashboard.

7. Edit each individual Widget in the dashboard in order to duplicate, configure, or delete that Widget.

8. Click a templated Widget to filter by All Assets (default), Target Group, or a Custom IP/CIDR range.

   **Note:** Currently, Access Groups and Tags are not available to be sorted on while using Widget/Dashboard templates. However, you can create custom Widgets in order to include these filter types.

9. Repeat steps 1-8 to add dashboards to your workflow.

   **Tip:** Alternatively, you can narrow a dashboard to one specific widget and title it accordingly. For example, you can title a widget “Top Ports per Regions”, and then duplicate that individual widget.
multiple times. Then, you can apply a unique target group to each widget, which gives you the ability to see one topic over multiple regions in one view.

10. Save your edits to the dashboard.

11. On the top right corner of the page, click More.

12. Click \(\rightarrow\)Exports.

   The Exports plane appears.

13. In the Actions section, click the button.

   An options menu appears.

14. Select PDF - Standard or PDF - Detailed.

   A confirmation message appears, informing you that the export is in progress.

   The export request and status appears in the exports table on the Exports plane.

**Best Practice:** There are two main ways of exporting data out of the Tenable.io platform. Exports via Dashboards are for the Executive/Management summary use cases. For more remediation specific workflows and detailed views, use the Export functionality on the Vulnerabilities Grid after configuring filters and/or Saved Searches.
Create and Customize Widgets

1. Click the "Dashboards" button.

   The Dashboards plane appears with a list of configured dashboards.

2. Click the dashboard that you want to edit.

3. Click the "Widgets" button.

   The Widgets plane appears.

4. Do one of the following:
   - Select a widget template from the list of widgets.

     **Note:** Choosing a widget template only gives you the option to add the widget to your existing Dashboard. From here, filter or edit the widget template as described in Create and Customize Dashboards.

   - Create a custom widget.

     **Note:** Creating a custom widget redirects you into the Create Widget page where you can customize vulnerability data and asset scope.

     a. Click Update. Tenable.io provides a preview of the filtered widget.

     **Note:** The order of the columns within the widget is dictated by the order in which you select the Data Preference fields during widget configuration. For more information, see Create a Custom Widget.
Create and Customize Saved Searches

1. Navigate to the **Vulnerabilities** dashboard.
2. In the **Filter** section, configure the query parameters for the search.
3. In the upper-right table header, click the icon.
   
   A text box appears.
4. Type a unique name for the search.
5. Click the button to save the search.

   The text box closes. The newly-saved search appears in the saved search drop-down box.

**Best Practice:** Click on the menu icon to the right of the saved search drop-down box and **Share** those searches to another User or Group.
Tip: If any of your filters include informational results, then you must use the filter ‘severity=info’ in order to see those results. Info severity plugins do not automatically show in the search.

Tip: Don’t forget the importance of the time period setting for each of these searches.

Authentication Failures

Critical and Exploitable

Newsworthy and Exploitable

Recast and Accept Risk Rules
### Advanced Search Examples - Assets Dashboard

#### Agent Assets

<table>
<thead>
<tr>
<th>Filters</th>
<th>Search</th>
<th>22 Assets</th>
<th>Clear Filters</th>
<th>Agents</th>
<th><strong>Apply</strong></th>
<th><strong>Add</strong></th>
<th><strong>Reset Filters</strong></th>
<th><strong>Cancel</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Match All</td>
<td></td>
<td></td>
<td></td>
<td>Agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>contains</td>
<td></td>
<td></td>
<td>Agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Understanding what is Licensed

<table>
<thead>
<tr>
<th>Filters</th>
<th>Search</th>
<th>437 Assets</th>
<th>Clear Filters</th>
<th>Licensed Assets 90 days</th>
<th><strong>Apply</strong></th>
<th><strong>Add</strong></th>
<th><strong>Reset Filters</strong></th>
<th><strong>Cancel</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Match All</td>
<td></td>
<td></td>
<td></td>
<td>Licensed Assets 90 days</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>is Licensed (VM)</td>
<td>is equal to</td>
<td>true</td>
<td></td>
<td>Licensed Assets 90 days</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Tip:** Make sure you change the time meter to Last 90 Days or another time period.

#### AWS Connector Discovered Assets

<table>
<thead>
<tr>
<th>Filters</th>
<th>Search</th>
<th>437 Assets</th>
<th>Clear Filters</th>
<th>AWS Assets</th>
<th><strong>Apply</strong></th>
<th><strong>Add</strong></th>
<th><strong>Reset Filters</strong></th>
<th><strong>Cancel</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Match All</td>
<td></td>
<td></td>
<td></td>
<td>AWS Assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>contains</td>
<td></td>
<td></td>
<td>AWS Connector</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Windows Operating systems

<table>
<thead>
<tr>
<th>Filters</th>
<th>Search</th>
<th>82 Assets</th>
<th>Clear Filters</th>
<th>Windows Systems</th>
<th><strong>Apply</strong></th>
<th><strong>Add</strong></th>
<th><strong>Reset Filters</strong></th>
<th><strong>Cancel</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Match All</td>
<td></td>
<td></td>
<td></td>
<td>Windows Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td>contains</td>
<td></td>
<td></td>
<td>Windows Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Installed Software
### Specific Tags

<table>
<thead>
<tr>
<th>Filters</th>
<th>Search</th>
<th>241 Assets</th>
<th>Clear All Filters</th>
<th>Match All</th>
<th>User Responsibility</th>
<th>contains</th>
<th>cancel</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
(Optional) Create Recast & Accept Risk Rules

After going through the vulnerability results and beginning to disseminate your workflows you will start to have certain vulnerabilities arise that cannot be patched or that can be adjusted in severity based on existing compensating controls. To take advantage of our Risk Rules engine, assemble a list of plugins that fit this criteria and follow the steps below.

1. In the upper-left corner, click the button.
   The left navigation plane appears.
2. Click Settings.
3. In the Rules section, click Recast.
   The Recast/Accept Rules page appears.
4. In the upper-right corner, click Add Rule.
   The Rule plane appears.
5. In the Action section, select whether you want to create a Recast or Accept rule.
6. Configure the Plugin ID, Scope, and other optional settings.
7. Click Save.

Tip: Be sure to allow a few minutes for the newly created rule to go through the vulnerability database and apply itself accordingly. The rule does not immediately take effect.
(Optional) Create Scanner Groups (Scan Distribution)

For a comprehensive overview into how scan distribution functions, refer to the Scan Distribution topic in the Tenable.io user guide.

1. In the upper-left corner, click the button.
   The left navigation plane appears.
2. Click Settings.
3. Click the Sensors widget.
4. In the left navigation menu, click Nessus.
5. Click Scanner Groups.
6. Click Add Scanner Group.
7. Type a name for the scanner group.
8. Select the appropriate permissions for the Users/Groups in the scanner group.
9. Save the scanner group.
10. In the upper-left corner, click the button.
    The left navigation plane appears.
11. Click the Sensors widget.
12. In the left navigation menu, click Nessus.
13. Select the appropriate scanner from the Available Scanners list.
14. Click Add Selected to Groups.

**Best Practice:** Taking advantage of scan distribution via scanner groups allows a significant drop in scan completion time by distributing scan jobs/tasks across multiple available scanners.

**Tip:** It’s important to apply scanners to a group that co-exists in the same geographical region to avoid scanning a target location with a scanner that can’t reach said targets.

15. When creating/editing scans, select the Scanner Group to distribute the scans across the group.
Part Three

1. Understand and Utilize Vulnerability Priority Rating (VPR)
2. Visualize VPR in Tenable.io
3. Create a Saved Search for VPR
4. Create a Custom VPR Widget
Understand and Utilize Vulnerability Priority Rating (VPR)

Predictive Prioritization is the process of reprioritizing vulnerabilities based on the probability that they will be leveraged in an attack and the output of that process is the VPR score.

What is the business value? VPR rates vulnerabilities based on the probability that it will be leveraged in an attack... it’s forward looking, most threat and vulnerability scoring mechanisms available today are backward looking (i.e. Is it easily exploitable?) and generally don’t change dynamically with the threat landscape.

- The VPR score combines over 170 distinct features (data sources/attributes), including Tenable Data Science Research, Tenable vulnerability data, and third-party vulnerability and threat data.
- It leverages a proprietary machine learning algorithms to identify the vulnerabilities with the highest likelihood of being exploited in the near future. As more and more data is fed into the model, it dynamically recalculates the priority of vulnerabilities on a daily basis to provide the most accurate rating possible.
- It remains true to the CVSS Framework (used as a foundation), but enhances it by replacing the CVSS exploitability and exploit code maturity with a threat score produced by machine learning.
- It can drastically change an organization’s remediation and patching processes for the better. Approximately 60% of all CVEs are rated High or Critical by CVSS, this percentage drops to just 3% when looking at it from a VPR perspective. Focusing on that 3% first maximizes the reduction of Cyber Risk with the same remediation effort.

For more information about Predictive Prioritization, see the [technical whitepaper](#).
Visualize VPR in Tenable.io

There are three main areas of reference for VPR in the new UI of Tenable.io.

First, in the **Vulnerability Management Overview** dashboard, you can see the **Vulnerability Priority Rating (VPR)** widget specific to the number of vulnerabilities in each severity level of VPR.

You can click one of the VPR category tiles to drill into your vulnerability data on the **Vulnerabilities** page. The next area of VPR focus is the last column. This column will highlight the current VPR score associated with a given vulnerability.

You can click one of the vulnerability rows to drill into the most detailed explanation of VPR in the **Vulnerability Details** page. This view provides the VPR Key Drivers and context indicating why a vulnerability has been assigned its current rating. This provides the analyst with some quick data points and evidence to reference when assigning remediation responsibilities to users.
CentOS 5 / 6 / 7: bash (CESA-2014:1293) (Shellshock)

1 VULNERABILITIES  9.6 VULNERABILITY PRIORITY RATING (VPR)

Vulnerability Information

VULN PUBLISHED: None
PATCH PUBLISHED: 09/23/14 at 8:00 PM
EXPLOITABILITY: ⚠️ ⚠️ ⚠️ ⚠️

Solution
Update the affected bash packages.

VPR Key Drivers

THREAT RECENTY: 0 to 7 days
EXPLOIT CODE MATURITY: High
AGE OF VULN: 731 days
PRODUCT COVERAGE: Low
CVSSv3 IMPACT SCORE: 5.0
THREAT SOURCES: Others; Mainstream Media; Code Repo and Paste Bins

1 Aged > 90 days

Filters
Search

supermicro.lab.tenablesec.
Create a Saved Search for VPR

Use the following examples to create two VPR-related saved searches.

Prioritized VPR

This saved query lets you quickly understand the vulnerabilities in your environment that need to be reprioritized based on your remediation SLAs that are typically mapped to the CVSS framework. That is, CVSS has rated these vulnerabilities in the medium and low categories while VPR has appropriately adjusted the scores to critical. This highlights the value of Tenable’s dynamic VPR rating that is constantly taking in daily threat information from the wild vs. the more static nature of the CVSS scoring system.

Deprioritized VPR

This saved query lets you quickly understand the vulnerabilities in your environment that need to be deprioritized based on your remediation SLAs that are typically mapped to the CVSS framework. That is, CVSS has rated the vulnerabilities in the high and critical categories (likely at the early point the CVSS score was first assigned) while VPR has appropriately adjusted the scores to medium and low given current understanding of the threat.
# Create a Custom VPR Widget

Tenable.io also comes with the capability to create your own custom widgets in the new UI. An example custom dashboard focusing on highest VPR scored vulnerabilities affecting high value assets can be seen below.

<table>
<thead>
<tr>
<th>VPR</th>
<th>High Value Assets (VPR &gt; 9.0)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Greatest Risk (VPR)</strong></td>
<td><strong>High Value Assets (VPR &gt; 9.0)</strong></td>
</tr>
<tr>
<td>PLUGIN ID</td>
<td>NAME</td>
</tr>
<tr>
<td>94202</td>
<td>CentOS 6: kernel...</td>
</tr>
<tr>
<td>79125</td>
<td>MS14-064:Vulner...</td>
</tr>
<tr>
<td>100760</td>
<td>KB4022715: Wind...</td>
</tr>
<tr>
<td>119463</td>
<td>KB4071331: Secur...</td>
</tr>
<tr>
<td>77823</td>
<td>Bash Remote Cod...</td>
</tr>
<tr>
<td>77913</td>
<td>Solaris 10 (sparc)...</td>
</tr>
</tbody>
</table>

| **Greatest Risk-New York (VPR)** | **Riskiest Cloud Assets (VPR > 9.0)** |
| **Greatest Risk-New York (VPR)** | **Riskiest Cloud Assets (VPR > 9.0)** |
| PLUGIN ID | NAME | VULN TOTAL | SEVERITY | VPR | IP ADDRESS | DNS NAME | OS | VULN TOTAL | VULNERABILITIES |
| 79125 | MS14-064:Vulner... | 1 | High | 9.8 | 16.20.1.4 | rsnuvy1deyrujarm... | Windows | 2 |
| 97833 | MS17-010:Secur... | 5 | Critical | 9.4 | 16.20.1.5 | rsnuvy1deyrujarm... | Windows | 2 |
| 100428 | CentOS 6 / 7: sam... | 9 | Critical | 9.2 | 16.20.1.9 | Microsoft Windows... | Windows | 2 |
| 80523 | CentOS 5 / 6 / 7: flap... | 3 | Critical | 9.2 | 16.10.1.126 | os-2-19-332-145-48... | Linux Kernel 3.16... | 1 |
| 100400 | RHEL 6 / 7: samb... | 2 | Critical | 9.2 | 16.20.1.7 | rsnuvy1deyrujarm... | Windows | 1 |

Copyright © 2020 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc., Tenable.sc, Lumin, Assure, and the Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
Utilize Tenable.io VM Solutions

The Tenable.io VM Solutions view helps you easily prioritize and direct your remediations. For more information, see Solutions in the Tenable.io user guide.

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. In the left navigation plane, in the Vulnerability Management section, click Solutions.
   The Solutions page appears.

   1. Do one of the following:
      - Click on a solution and investigate Solution Details.
      - Export a solution.
      - Export all solutions.

   **Tip:** When you export a solution, you have two export options:
   - **Solutions:** A list of the Solutions by Name presented in the UI (always enabled)
   - **Details:** A list of Assets to which the Solution(s) apply