ANYWHERE Detection Dashboard.mobile.phone

Detection Dashboard

Topics Discussed

In the **Detection** screen, the **Detection** score focuses on the incoming activity of Armor services. You can use these scores to determine if Armor is receiving the necessary data to perform useful security checks for your environment.

For **Armor Anywhere**, these services are:

- Malware Protection
- FIM
- IDS
- Filebeat (for Linux)
- Winlogbeat (for Windows)
- Vulnerability Scanning

Widgets and Graph

Widget	Description
Detection Score	This widget calculates a score based on: • Armor services that are collecting logs • Agents that are powered on **Score range** / **Health status** **10 - 8** — Good **7 - 4** — Fair **3 - 1** — Poor
Events Analyzed	An event is any log that passes an Armor agent. Malware Protection, File Integrity Monitoring, and Log and Event Management contain a subagent. This widget displays data from the previous month.
Services Reporting	This widget displays the percentage of agents that are receiving events. You can use this number to determine overall if your subagents are running properly.
Detection Score Trend	This graph displays the history of your detection scores.

Detection Events

The **Detection Events** table displays information for the past seven days. This table will update every day.

Column	Description
Date	This column displays the date that Armor received the log.
Total Events	This column displays the number of logs received for that day.

Category	This columnd display the type of log received from the **Total Events** column. This column lists the subagent for the collected logs.

Highest Risk Assets

The **Highest Risk Assets** table displays virtual machines that contain the installed Armor Anywhere agent that are considered highly vulnerable. This table is based on the findings of the weekly vulnerability scanning report.

Column	Description
Asset Name	The name of the virtual machine that contains the installed Armor Anywhere agent.
Status	This column displays if the virtual machine was successfully **Scanned** or if the virtual machine is **Offline**.
Critical	This column displays the number of vulnerabilities that contained a score of 10.
High	This column displays a vulnerability that scored between 7 to 10 on the CVSS.
Medium	This column displays a vulnerability that scored between 4 to 7 on the CVSS.
Low	This column displays a vulnerability that scored between 0 to 4 on the CVSS.
Info	This column displays activity information regarding corresponding plugins from a third-party vendor.

Top Vulnerabilities

The **Top Vulnerabilities** table displays the most critical vulnerabilities found in your environment. This table is based on the findings of the weekly vulnerability scanning report.

Column	Description
Vulnerability Name	This column displays the name of the vulnerability. ⚠ You can click the **Vulnerability Name** to learn more about the vulnerability. You will be taken to a description page where you can review a description of the vulnerability, including the solution.
Affected Assets	This column displays the virtual machines (host / asset) affected by the vulnerability. ⚠ If you are unfamiliar with the name of a virtual machine, you can use the **Virtual Machines** screen to search. 1. Copy the desired virtual machine name (host name or CoreInstance ID). 2. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**. 3. Click **Virtual Machines**. 4. In the search field, paste the virtual machine name (host name or CoreInstance ID), and then click the magnifying glass icon.
Date Discovered	This column displays the date the vulnerability was discovered. • This date will correspond with the date of the scan.
CVSS	This column displays the CVSS, a score attached to a vulnerability to determine the vulnerability's severity. • To learn more, please see the National Vulnerability Database website.

Severity	This column displays the severity of the vulnerability.
	
	There are four severity types, based on the vulnerability's CVSS:
	
	• Critical
	  • Critical vulnerabilities receive a score of 10.
	• High
	  • High vulnerabilities receive a score of 7-10.
	• Medium
	  • Medium vulnerabilities receive a score of 4-7.
	• Low
	  • Low vulnerabilities receive a score of 0-4.
	
	⚠ There is an additional severity type called **Info**. Although **Info** is listed as a severity type, in reality, **Info** simply displays activity information for corresponding plugins from third-party vendors.

Improve Your Detection Score

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Detection**.
2. Under the **Top Vulnerabilities** table, click a specific vulnerability type.
   - This action will take you the **Vulnerability Scanning** details screen where you can view a description of the vulnerability and the affected virtual machine.