GCP CLOUD WORKLOAD PROTECTION

Agent-less discovery for no-scan always on detection powered by ThreatWorx

1

CONFIGURING OS INVENTORY MANAGEMENT

Follow the instructions provided here to enable cloud inventory collection for compute instances and enable guest attributes,

OS Inventory Management

Enable Guest Attributes

2

INSTALL GOOGLE CLOUD SDK

Follow the instructions outlined here to install the Google Cloud SDK. The SDK should be installed on the same host that has twigs installed.

SDK Install

3

RUN TWIGS

Open a terminal and ensure twigs is installed.
twigs gcp -h
(You will need to get a TWIGS API key from ThreatWorx I3 console)

Sign-in to your GCP instance on the box where twigs is installed, using gCloud CLI as described here,

gCloud Sign-In Instructions

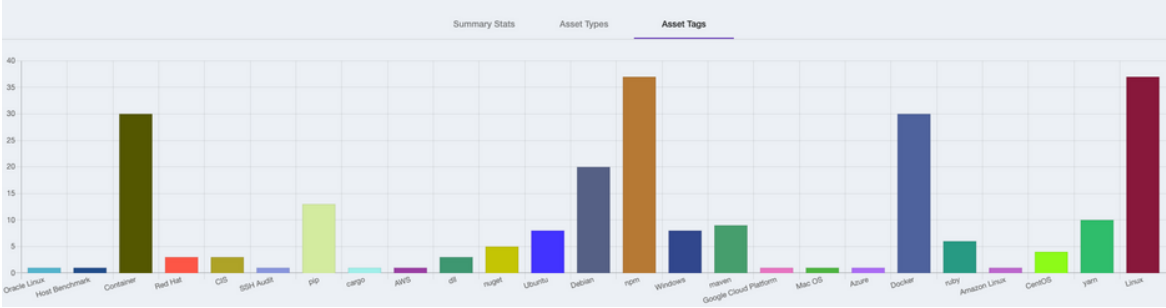
Finally run the following command to discover and report all meta data related to compute instances into ThreatWorx and run vulnerability and configuration checks.

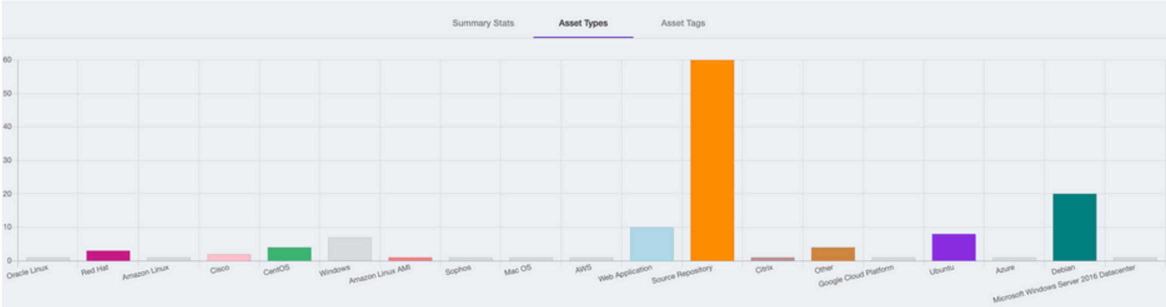
```
twigs gcp [--enable_tracking_tags]
twigs gcp_cis --assetid [ASSET_ID]
```

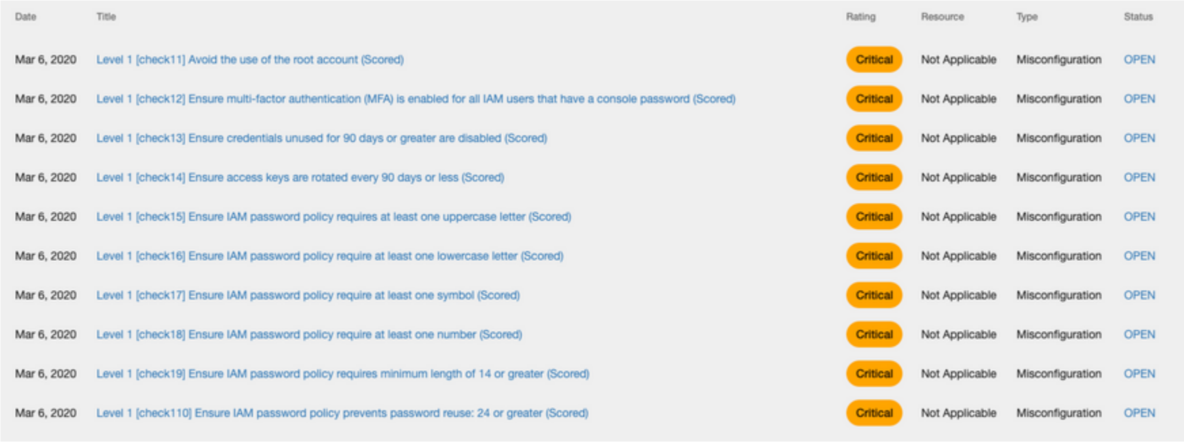
Addition help can be found,
https://twigs.threatworx.io/guide

4 THREATWORX CONSOLE

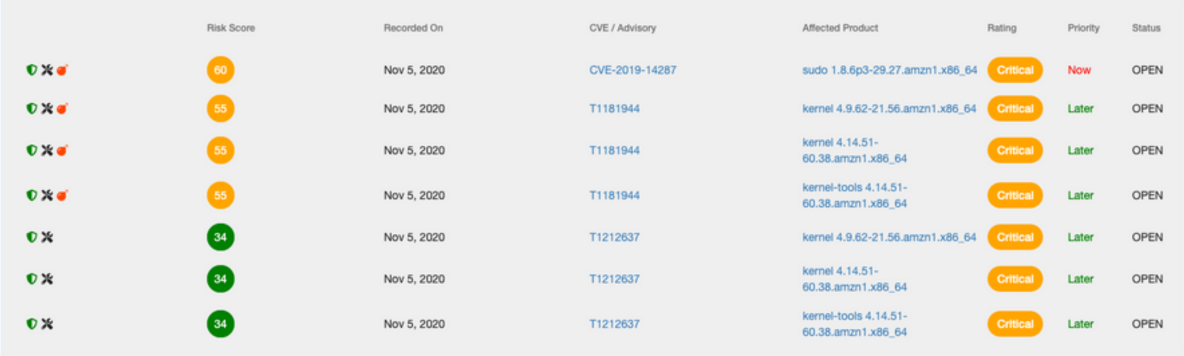
Analytics, security vulnerabilities, mis-configurations, static and dynamic analysis for base images, running apps and containers can now be managed from the I3 console.







Date	Title	Rating	Resource	Type	Status
Mar 6, 2020	Level 1 [check11] Avoid the use of the root account (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check12] Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check13] Ensure credentials unused for 90 days or greater are disabled (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check14] Ensure access keys are rotated every 90 days or less (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check15] Ensure IAM password policy requires at least one uppercase letter (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check16] Ensure IAM password policy require at least one lowercase letter (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check17] Ensure IAM password policy require at least one symbol (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check18] Ensure IAM password policy require at least one number (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check19] Ensure IAM password policy requires minimum length of 14 or greater (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check110] Ensure IAM password policy prevents password reuse: 24 or greater (Scored)	Critical	Not Applicable	Misconfiguration	OPEN



	Risk Score	Recorded On	CVE / Advisory	Affected Product	Rating	Priority	Status
🛡 🛠 💣	60	Nov 5, 2020	CVE-2019-14287	sudo 1.8.6p3-29.27.amzn1.x86_64	Critical	Now	OPEN
🛡 🛠 💣	55	Nov 5, 2020	T1181944	kernel 4.9.62-21.56.amzn1.x86_64	Critical	Later	OPEN
🛡 🛠 💣	55	Nov 5, 2020	T1181944	kernel 4.14.51-60.38.amzn1.x86_64	Critical	Later	OPEN
🛡 🛠 💣	55	Nov 5, 2020	T1181944	kernel-tools 4.14.51-60.38.amzn1.x86_64	Critical	Later	OPEN
🛡 🛠	34	Nov 5, 2020	T1212637	kernel 4.9.62-21.56.amzn1.x86_64	Critical	Later	OPEN
🛡 🛠	34	Nov 5, 2020	T1212637	kernel 4.14.51-60.38.amzn1.x86_64	Critical	Later	OPEN
🛡 🛠	34	Nov 5, 2020	T1212637	kernel-tools 4.14.51-60.38.amzn1.x86_64	Critical	Later	OPEN