Qualys Container Security

Release Notes

Version 1.26

June 26, 2023

What's New?

Container Security Sensor Updates

Upgrade your sensor to version 1.26 or later to benefit from the above-mentioned enhancements. Refer to the Container Security Sensor 1.26 Release Notes for the sensor updates.

API Changes

Refer to the Container Security API 1.26 Release Notes for the API changes in this release.

Issues Addressed

Qualys Container Security 1.26 brings you many more improvements and updates! Learn more

What's New?

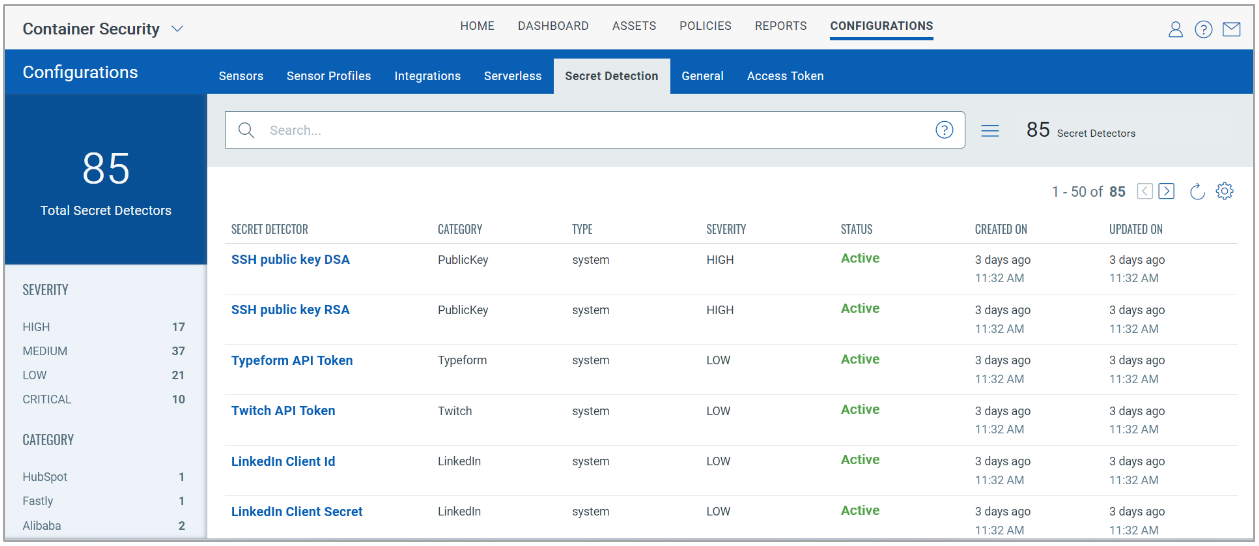
Detecting Container Secrets

Container secrets are digital credentials providing identity authentication and authorizing access to privileged accounts, applications, and services. They can include passwords, API keys, and other credentials that are needed for applications to function properly. If these secrets are not properly secured, they can be accessed by unauthorized users, leading to malicious attacks. Therefore, discovering secrets is one of the important aspects of container security that organizations must prioritize to protect their sensitive data, meet compliance requirements, and reduce the risk of security incidents.

Starting this release, Container Security can now detect secrets within container images.

In the **Configuration > Secret Detection** tab, you can see the secret detectors or the set of rules for identifying various types of secrets. Currently, only the default system-defined detectors are available.

Click **View Details** from the **Quick Actions** menu to view the details of a detector.
Note that it is currently not possible to create new detectors or modify existing ones.



85
Total Secret Detectors

SEVERITY	
HIGH	17
MEDIUM	37
LOW	21
CRITICAL	10

CATEGORY	
HubSpot	1
Fastly	1
Alibaba	2

SECRET DETECTOR	CATEGORY	TYPE	SEVERITY	STATUS	CREATED ON	UPDATED ON
SSH public key DSA	PublicKey	system	HIGH	Active	3 days ago 11:32 AM	3 days ago 11:32 AM
SSH public key RSA	PublicKey	system	HIGH	Active	3 days ago 11:32 AM	3 days ago 11:32 AM
Typeform API Token	Typeform	system	LOW	Active	3 days ago 11:32 AM	3 days ago 11:32 AM
Twitch API Token	Twitch	system	LOW	Active	3 days ago 11:32 AM	3 days ago 11:32 AM
LinkedIn Client Id	LinkedIn	system	LOW	Active	3 days ago 11:32 AM	3 days ago 11:32 AM
LinkedIn Client Secret	LinkedIn	system	LOW	Active	3 days ago 11:32 AM	3 days ago 11:32 AM

You can search for secret detectors using search tokens. For more information about available tokens, see Searching for Secret Detectors.

To view detected secrets for a particular image:

1. Navigate to the image details and select the **Secrets** section. This section displays the secrets identified for the image, categorized by the corresponding detectors. It also provides information such as associated files with their paths, severity levels, and more.

   You can search for secrets using search tokens. For more information about available tokens, see Online Help: Searching for Secrets.

2. To see the secret details, click the secrets count under the **Detected Secrets** column. A new dialog box displays the matching text and the start and end lines where the secret is located in the file. By referring to the indicated file and reviewing the mentioned lines,

you can verify the existence of the secret.

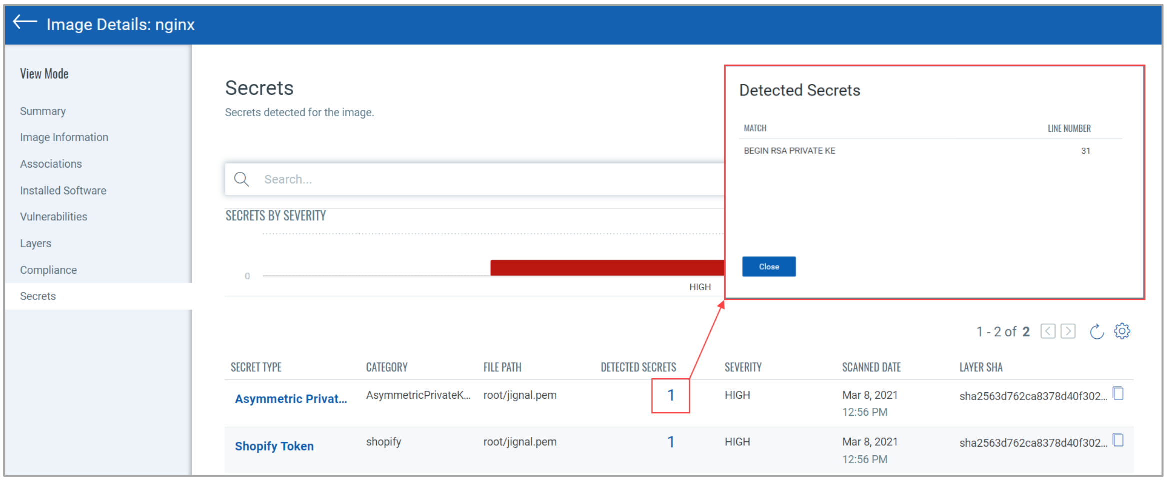


Image Details: nginx

Secrets

Secrets detected for the image.

Detected Secrets

MATCH	LINE NUMBER
BEGIN RSA PRIVATE KE	31

SECRET TYPE	CATEGORY	FILE PATH	DETECTED SECRETS	SEVERITY	SCANNED DATE	LAYER SHA
Asymmetric Privat...	AsymmetricPrivateK...	root/jignal.pem	1	HIGH	Mar 8, 2021 12:56 PM	sha2563d762ca8378d40f302...
Shopify Token	shopify	root/jignal.pem	1	HIGH	Mar 8, 2021 12:56 PM	sha2563d762ca8378d40f302...

Note: Secret detection is supported only on:

- **Sensors**: CICD and registry
- **OS**: Linux
- **Runtimes**: Docker, Containerd, and CRI-O

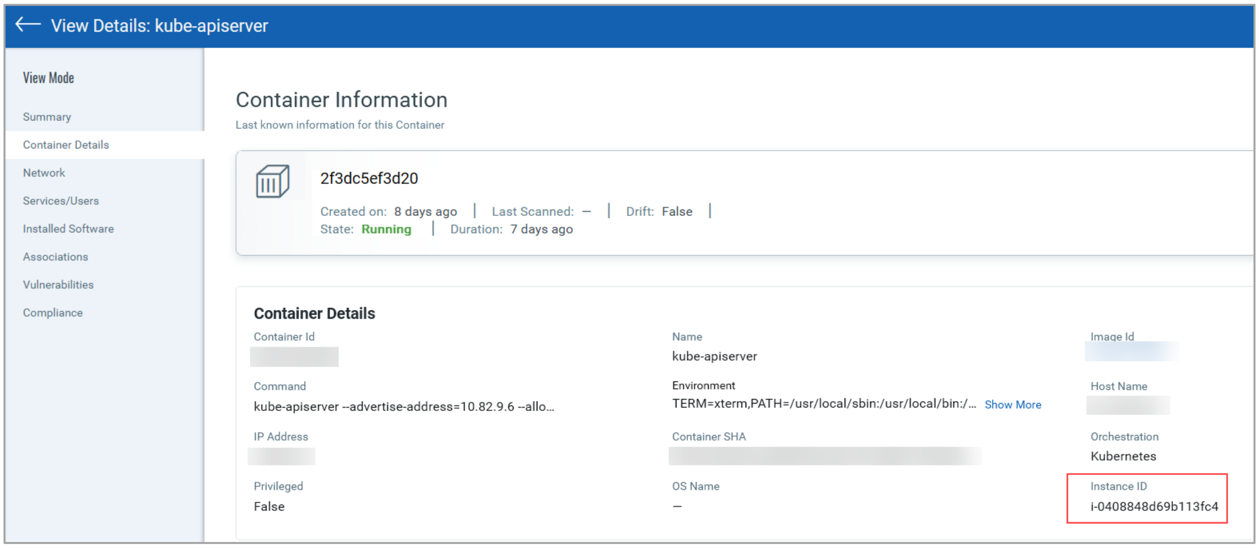
Secret detection involves scanning the filesystem. It does not detect secrets that are stored as environment variables or passed as arguments within the image. Therefore, the performance of secret detection depends on the number of files present in the image.

For more information, see Online Help: Detect Container Secrets.

Showing AWS EC2 Instance ID in Sensor and Container Details

As the IP address of a host is not always unique and may change, searching for assets on a specific host using the host's IP address may provide inaccurate results. Cloud providers add an instance ID to hosts to uniquely identify them within the cloud environment.

With this release, for the sensor hosted in the AWS EC2 environment, the AWS EC2 instance ID of the host is now displayed in the sensor details and the details of containers being scanned by the sensor.



Container Information

Last known information for this Container

2f3dc5ef3d20

Created on: 8 days ago | Last Scanned: – | Drift: False |
State: Running | Duration: 7 days ago

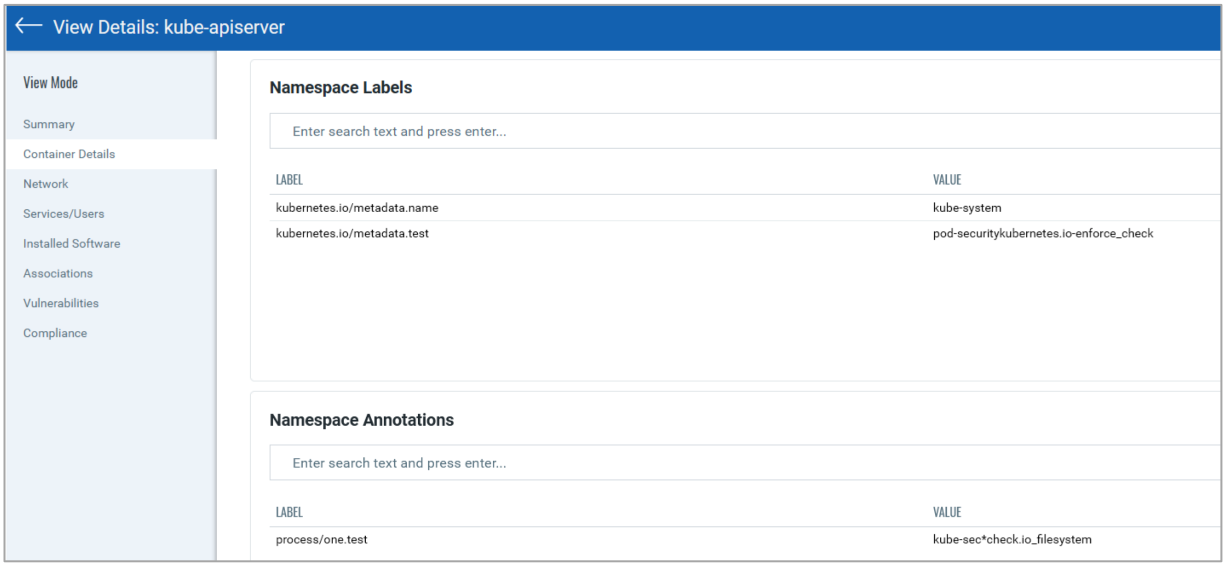
Container Details

Container Id [redacted]	Name kube-apiserver	Image Id [redacted]
Command kube-apiserver --advertise-address=10.82.9.6 --allo...	Environment TERM=xterm,PATH=/usr/local/sbin:/usr/local/bin:/...	Host Name [redacted]
IP Address [redacted]	Container SHA [redacted]	Orchestration Kubernetes
Privileged False	OS Name –	Instance ID i-0408848d69b113fc4

Capturing Namespace Labels and Annotations in Kubernetes Metadata

With this release, the sensor deployed on the Kubernetes cluster now captures the namespace labels and annotations assigned to containers. This provides you with more visibility into the virtual Kubernetes clusters.

You can view these labels and annotations as part of the container and sensor details.



Namespace Labels

LABEL	VALUE
kubernetes.io/metadata.name	kube-system
kubernetes.io/metadata.test	pod-securitykubernetes.io-enforce_check

Namespace Annotations

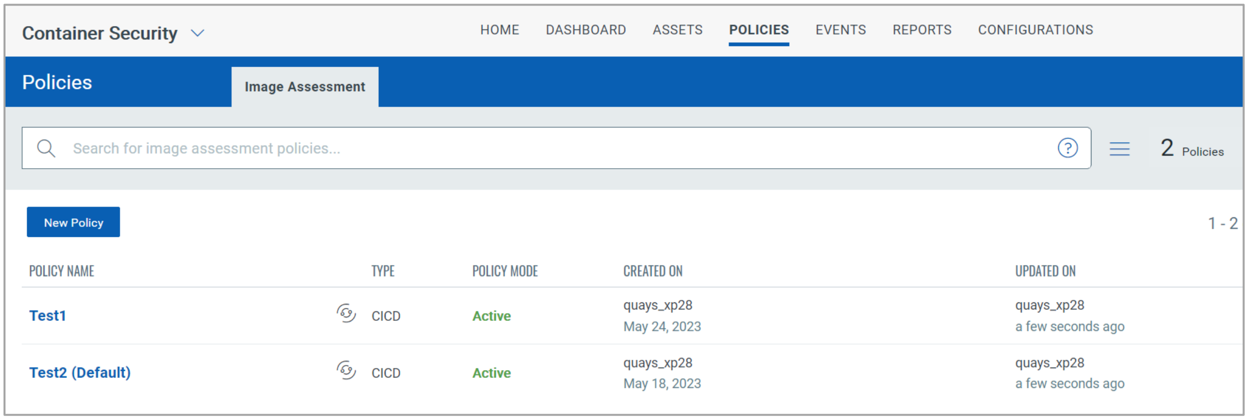
LABEL	VALUE
process/one.test	kube-sec*check.io_filesystem

Introducing Security Policies

With this release, Container Security introduces policies for managing configurations, vulnerability management, compliance, access, and auditing in containerized environments, thus automating the process of securing images and containers.

Policies provide a combination of rules that assess specific artifacts such as images, and containers, and provide actions associated with the rules.

In this release, you can create policies only for image assessment in the CICD environment. You can define rules and specify the actions to be taken if the rule is fulfilled, such as blocking CICD build or triggering alerts.



POLICY NAME	TYPE	POLICY MODE	CREATED ON	UPDATED ON
Test1	CICD	Active	quays_xp28 May 24, 2023	quays_xp28 a few seconds ago
Test2 (Default)	CICD	Active	quays_xp28 May 18, 2023	quays_xp28 a few seconds ago

Currently, only one image assessment rule is available, which lets you specify the action to be taken if the count of vulnerabilities of specific severity is exceeded.

Policies can be assigned or mapped to different events or utilities, CICD pipelines for example, using tags. Use the same tags while configuring your events or utilities. A policy that matches all the specified tags is evaluated during scanning. If the tags combination does not match, the default policy is applied. For a CICD pipeline, use the same tags as parameters when configuring the pipeline using the QScanner utility.

To search policies in the **Policies > Image Assessment** tab, you can use search tokens. For more information, see Online Help: Searching for Image Assessment Policies.

For more information, see Creating Security Policies.

Issues Addressed

The following issues have been fixed with this release:

- Users received an error when trying to create a sensor inactive window with end time as 11:59 PM. This issue is now fixed.
- Few users were unable to download a CSV report from the images and containers tabs. The issue now fixed.
- A typo has been fixed on the **Host > Asset Details** page.
- On rare occasions, when using the List Images API on two different days, the last scanned date for an image that had no vulnerabilities displayed an earlier date during the second occurrence. This situation rarely happens when there is a lag in the search or indexing service.