CISCO
SECURE

All About Assets

April 25, 2023

Presenters:

Tony Mills

Technical Account Manager

Stephanie Deirmentzoglou

Customer Success Manager

Jamey McGrath

Customer Success Operations Specialist

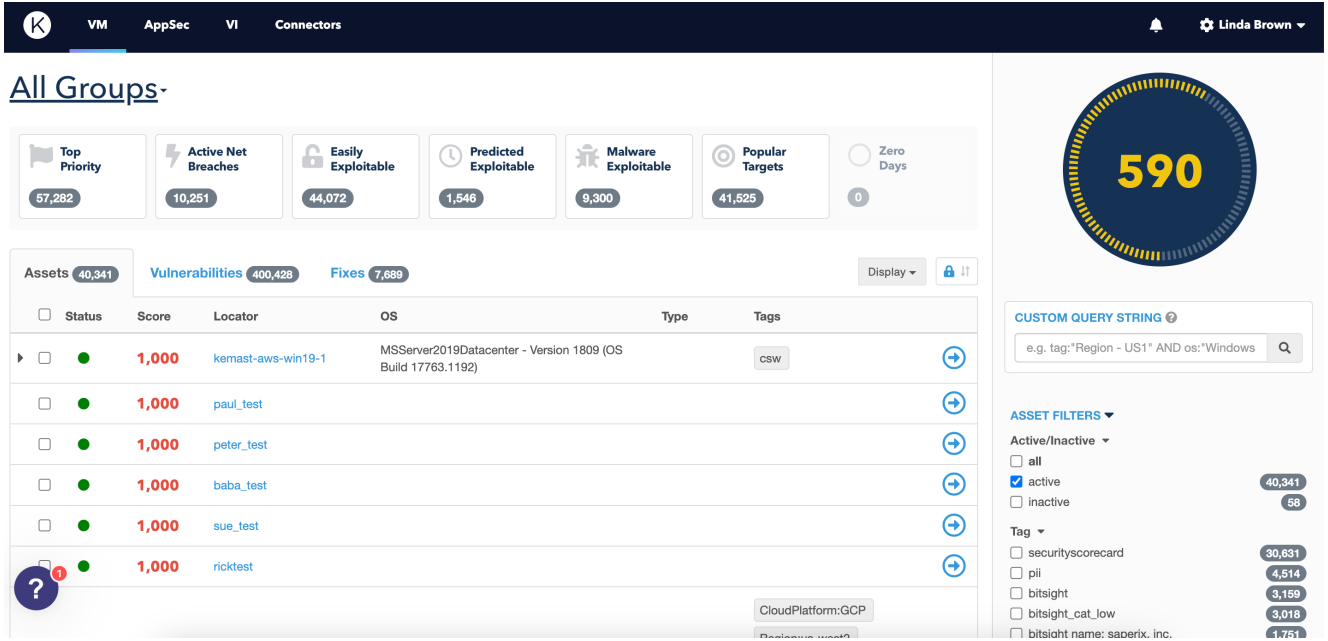
Agenda

- Active and Inactive Assets
- Asset Scoring and Prioritization
- Asset Tags
- Locator Order/Deduplication
- Demo
- Q&A

Assets are where the vulnerabilities are

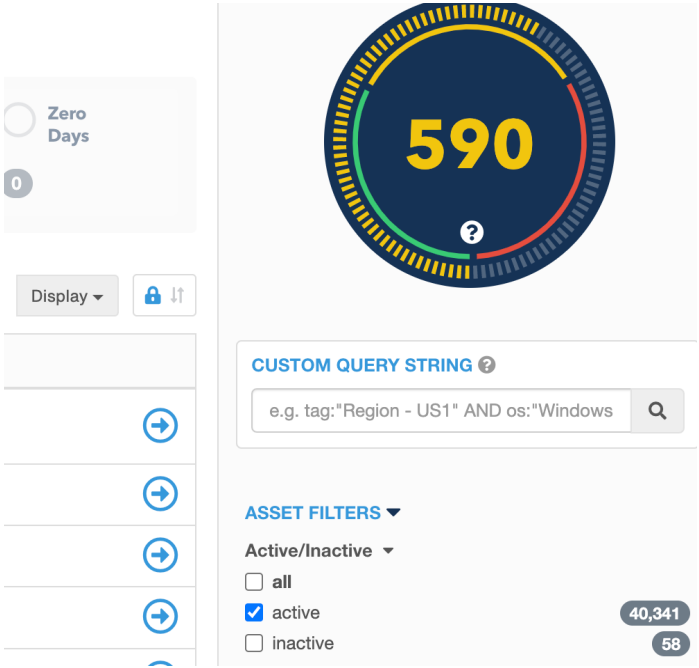
Assets in your environment:

- Traditional: Part of your infrastructure
- Non-traditional:
  -Source code file
  -Webpage
  -Docker container



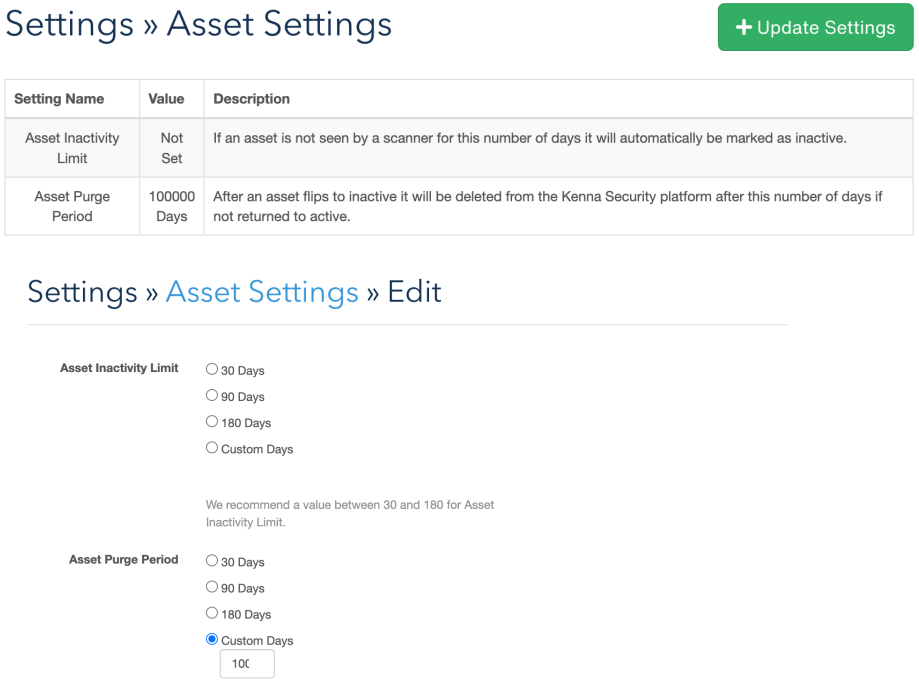
Active and Inactive Assets

- 2 main asset statuses in the UI
- By default, Kenna will only display Active assets these are assets that have at least one open risk associated vulnerability
- Asset status can be changed by adjusting the Asset Inactivity limit or Manually*



Asset Settings- Your Limits

- Flips an asset to inactive state if it has not been seen in the time period configured in the 'Asset Inactivity Limit' setting.
- The asset will automatically flip back to 'Active' if subsequently seen by the scanner and ingested.
- Inactive assets will remain in Kenna until the end of the Asset Purge Period

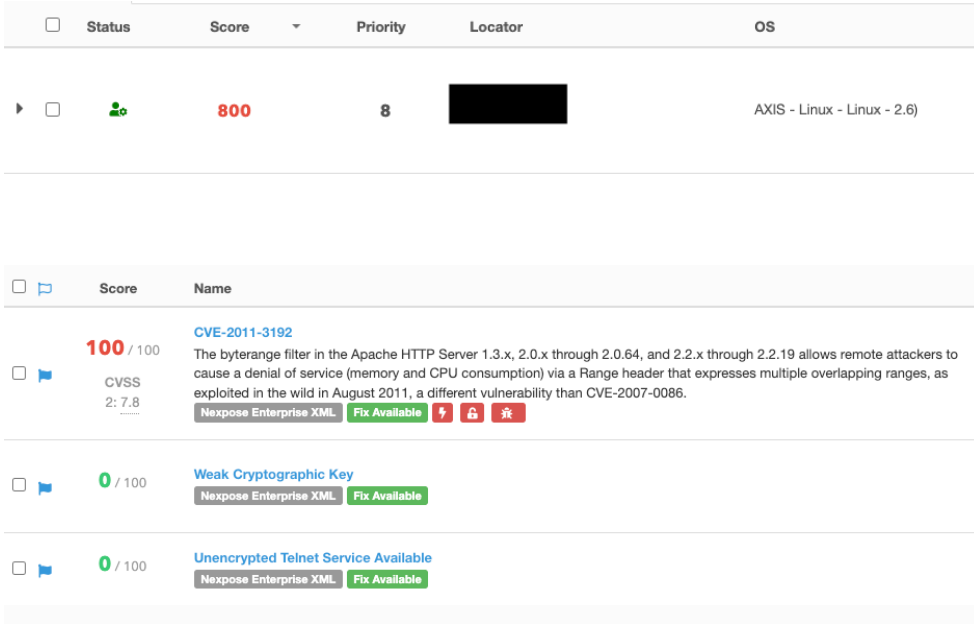


Inactive / Purge – What is the difference?

- In Kenna.VM, active assets count towards your purchased license amount, including assets that have no vulnerabilities. Inactive assets do not count toward your purchased license amount.
- Risk Meters and dashboard visualizations which include inactive assets may change when assets are purged.
- Purging assets is permanent and will also purge all vulnerabilities associated with the assets.
- Connector runs will not import assets which fall outside of the Asset Purge Period.

Kenna Asset Score

- Kenna applies a score to assets
- The score ranges from 0 – 1000
- The asset score is calculated by the highest level vulnerability multiplied by the asset priority
- Kenna will apply a 200-point bump to an asset score if we think its external
- An IP other than 10.*, 172.16.0.0 – 172.31.255.255 and 192.168.* to be external



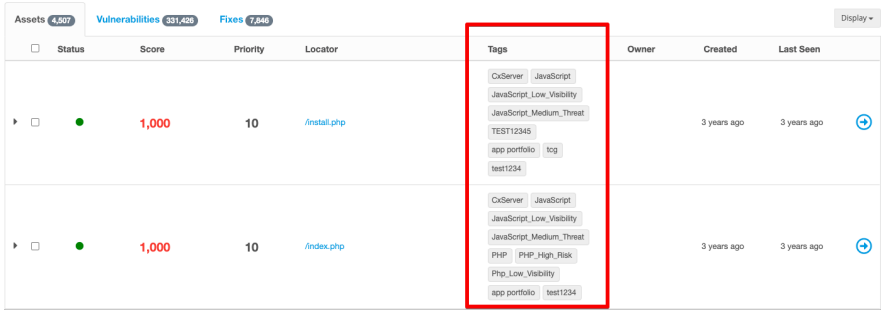
Asset Priority

- Kenna allows customers to prioritize assets within the platform
- Asset prioritization allows customers to identify and manage assets that are critical to the organization
- The asset priority range is 0 – 10
- We do not advise customers to set prioritization below a 7

vuln	priority									
	10	9	8	7	6	5	4	3	2	1
100	1000	900	800	700	600	500	400	300	200	100
90	900	810	720	630	540	450	360	270	180	90
80	800	720	640	560	480	400	320	240	160	80
70	700	630	560	490	420	350	280	210	140	70
60	600	540	480	420	360	300	240	180	120	60
50	500	450	400	350	300	250	200	150	100	50
40	400	360	320	280	240	200	160	120	80	40
30	300	270	240	210	180	150	120	90	60	30
20	200	180	160	140	120	100	80	60	40	20
10	100	90	80	70	60	50	40	30	20	10

Asset Tags

- What is an asset tag - Metadata about assets are called Tags in Kenna.
- Kenna ingests asset tags from the data source. Tags may also be added via the UI or API.
- Searchable and filterable within the platform. Can create risk meters based on Asset Tags.
- Tags added from connector runs cannot be removed from the UI. These tags must be maintained at the source, whether that is a scanner or the KDI.



Asset Locators & De-duplication

- In a customer environment where multiple sources of vulnerability data are ingested and where those may include the same asset, Kenna makes every attempt not to create duplicate assets.
- To achieve this, Kenna uses a process called "locator ordering" (aka asset matching) which is a step system based upon matching conditions of 'true', false' or nil'.
- Each connector* is set to a default locator order for the step system to match to, in sequential order.
- The locator order can be modified to allow a particular asset value to take priority.

- * There are a couple of unique exceptions where this does not apply

Default locator order per connector is as follows:

1. Container identifier
2. Image identifier
3. EC2 identifier
4. MAC address
5. NetBIOS
6. external IP address
7. hostname
8. URL
9. file name
10. fully qualified domain name (FQDN)
11. internal IP address (RFC 1918)
12. scanner-specific asset ID (eg Qualys host ID, Nexpose device-id)
13. database
14. application

Deduplication process

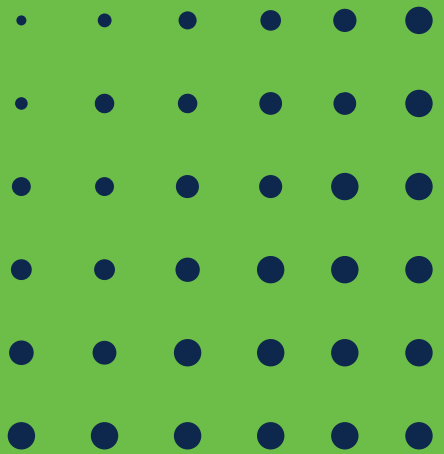
- **TRUE:** Using the default locator ordering on the previous page, the first thing Kenna will do is check the Container identifier field on the incoming asset to see if it matches a Container identifier that you already have in Kenna (“true”). If the incoming asset matches an asset that is already in Kenna, Kenna will update any of the other locator fields that have new, non-nil values since the last connector run so that your data is current.
- **FALSE:** If there is a Container identifier field on the incoming asset and it does not match an asset already in Kenna (“false”), it will create a new asset.
- **NIL:** If there is no Container identifier on the incoming asset (“nil”), Kenna will move to the next locator in the priority list and continue down the list until Kenna finds an incoming locator that has data on which to match (“true”) or not match (“false”).

CISCO
SECURE

Demo Time!

	Qualys (incoming asset)	Kenna (existing asset)
MAC	xyz	xyz
NetBIOS	cba	abc
Hostname	abc.local	abc.local
IP	1.2.3.5	1.2.3.4
Scanner ID	4321	4321
Outcome	**Skips Container, Image, and EC2 identifiers since there are none; matches on MAC address (“true”); updates NetBIOS to “cba” and IP to “1.2.3.5” for the asset in Kenna because the scanner is bringing in updated information**	

Ensuring Your Success



Appreciate your time and patience!

Thank You!