

CISCO
SECURE

All About Assets

April 25, 2023



The bridge to possible



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

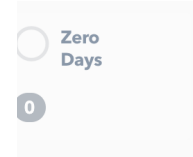
Assets in your environment:

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

The screenshot displays a security dashboard with a navigation bar at the top containing 'VM', 'AppSec', 'VI', and 'Connectors'. The main content area is titled 'All Groups-' and features several summary cards: 'Top Priority' (57,282), 'Active Net Breaches' (10,251), 'Easily Exploitable' (44,072), 'Predicted Exploitable' (1,546), 'Malware Exploitable' (9,300), 'Popular Targets' (41,525), and 'Zero Days' (0). Below these cards is a table with columns for 'Assets' (40,341), 'Vulnerabilities' (400,428), and 'Fixes' (7,689). The table lists assets with columns for Status, Score, Locator, OS, Type, and Tags. The first row shows an asset with a score of 1,000, locator 'kemast-aws-win19-1', OS 'MSServer2019Datacenter - Version 1809 (OS Build 17763.1192)', and tag 'csw'. A right sidebar contains a large circular gauge showing '590', a 'CUSTOM QUERY STRING' input field with the example 'e.g. tag:"Region - US1" AND os:"Windows"', and an 'ASSET FILTERS' section with checkboxes for 'Active/Inactive' and various tags like 'securityscorecard', 'pii', 'bitsight', and 'bitsight_cat_low'.

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*



Display ▾



CUSTOM QUERY STRING ?

e.g. tag:"Region - US1" AND os:"Windows"



ASSET FILTERS ▾

Active/Inactive ▾

all

active

inactive

40,341

58

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

Settings » Asset Settings

[+ Update Settings](#)

Setting Name	Value	Description
Asset Inactivity Limit	Not Set	If an asset is not seen by a scanner for this number of days it will automatically be marked as inactive.
Asset Purge Period	100000 Days	After an asset flips to inactive it will be deleted from the Kenna Security platform after this number of days if not returned to active.

Settings » [Asset Settings](#) » Edit

- Asset Inactivity Limit**
- 30 Days
 - 90 Days
 - 180 Days
 - Custom Days

We recommend a value between 30 and 180 for Asset Inactivity Limit.

- Asset Purge Period**
- 30 Days
 - 90 Days
 - 180 Days
 - Custom Days
-

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

<input type="checkbox"/>	Status	Score	Priority	Locator	OS
▶ <input type="checkbox"/>		800	8	[REDACTED]	AXIS - Linux - Linux - 2.6)

<input type="checkbox"/>	<input type="checkbox"/>	Score	Name
<input type="checkbox"/>	<input type="checkbox"/>	100 / 100	CVE-2011-3192 The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.
<input type="checkbox"/>	<input type="checkbox"/>	CVSS 2: 7.8	
<input type="checkbox"/>	<input type="checkbox"/>	0 / 100	Weak Cryptographic Key
<input type="checkbox"/>	<input type="checkbox"/>	0 / 100	Unencrypted Telnet Service Available

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.

Assets	Vulnerabilities	Fixes	Status	Score	Priority	Locator	Tags	Owner	Created	Last Seen
4,507	331,428	7,646	<input type="checkbox"/>							
			<input type="checkbox"/>	1,000	10	/install.php	CsServer JavaScript JavaScript_Low_Visibility JavaScript_Medium_Threat TEST12345 app_portfolio log test1234		3 years ago	3 years ago
			<input type="checkbox"/>	1,000	10	/index.php	CsServer JavaScript JavaScript_Low_Visibility JavaScript_Medium_Threat PHP_PHP_High_Risk Php_Low_Visibility app_portfolio test1234		3 years ago	3 years ago

Tag	Count
<input type="checkbox"/> securityscorecard	30,631
<input type="checkbox"/> pii	4,514
<input type="checkbox"/> bitsight	3,159
<input type="checkbox"/> bitsight_cat_low	3,018
<input type="checkbox"/> bitsight name: saperix, inc.	1,751
<input type="checkbox"/> expanse	981
<input type="checkbox"/> riskiq	745
<input type="checkbox"/> armis_site:000 - corporate	597
<input type="checkbox"/> hostconn	521
<input type="checkbox"/> armis_tags:guest	376
<input type="checkbox"/> contact	328
<input type="checkbox"/> asn	292
<input type="checkbox"/> businessunit:vandelay import-export	131
<input type="checkbox"/> vandelay import-export	99
<input type="checkbox"/> armis_tags:guest, corporate	66
<input type="checkbox"/> businessunit:acme latex supply	62
<input type="checkbox"/> cloudplatform:aws	61
<input type="checkbox"/> amex provided	60
<input type="checkbox"/> armis_tags:corporate, guest	54
<input type="checkbox"/> businessunit:vandelay industries	53
<input type="checkbox"/> acme latex supply	48
<input type="checkbox"/> bitsight_cat_critical	47
<input type="checkbox"/> riq_reviewed	47
<input type="checkbox"/> category9	46
<input type="checkbox"/> category2	45
<input type="checkbox"/> riq_rev_host_ip	45

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”).

It's a  Match!

CISCO
SECURE

Demo Time!

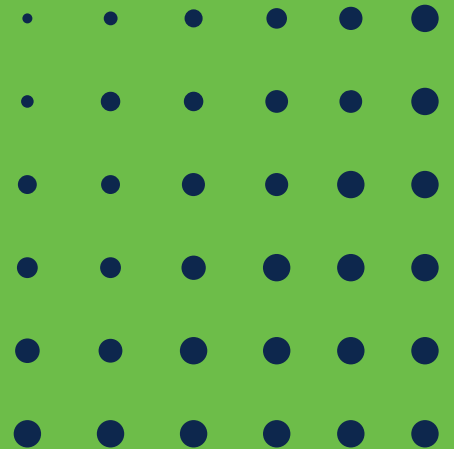


The bridge to possible



	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!

