

All Things Assets – Part 2

David Brothers

Kenna Security, Customer Success Engineer

5/29/2020



All Things Assets – 3 Part Series (Review)

Part 1 – Asset Status (April)

- Introduction to Assets
- Active and Inactive Assets – What does that really mean?
- Why letting Kenna control the asset status makes sense.
- Exceptions to the rule – When making manual decisions make sense.
- What is the “*by human flag*” and how to remove it?
- Creating a risk meter to show inactive assets that have been seen within the asset inactivity window.
- Creating a risk meter to show active assets that fall outside the asset inactivity window

Part 2 – Asset Management (May)

Part 3 – Asset Priority Best Practices (June)

All Things Assets – 3 Part Series (Today)

Part 1 – Asset Status (April)

Part 2 – Asset Management (May)

- Deduplication - Locators
- Tagging Strategy - Bringing in tags
- Asset Ownership – Keeping it up to date
- Discovery & Data Enrichment – Using CMDB data

Part 3 – Asset Priority Best Practices
(June)

All Things Assets – 3 Part Series

Part 1 – Asset Status (April)

Part 2 – Asset Management (May)

Part 3 – Asset Priority Best Practices (June)

- Asset Scoring
- Asset Priority – Use Cases
- Risks and Pitfalls

Introduction to Assets

The screenshot displays the KENNA Security dashboard. At the top, there is a navigation bar with the KENNA Security logo and menu items: Home, Dashboard, Explore, AppSec, VI, and Connectors. On the right side of the navigation bar, there are notification and settings icons, and a user profile labeled 'Demo Inc'. Below the navigation bar, there are seven summary cards for different categories: Top Priority (2,349), Active Net Breaches (410), Easily Exploitable (1,976), Predicted Exploitable (73), Malware Exploitable (600), Popular Targets (5,614), and Zero-Day Vulns (0). A large circular gauge on the right shows a count of 510. Below these cards, there are tabs for Assets (33), Vulnerabilities (15,173), and Fixes (909). A table lists assets with columns for Score, Locator, OS, and Tags. The table contains six rows of asset data. On the right side of the dashboard, there is a search bar, a 'Reset Filters' button, a 'Save Group' button, and sections for 'GROUPS', 'ASSET FILTERS', and 'VULNERABILITY FILTERS'. At the bottom right, there are buttons for 'Export this view' and 'Link to this view', and a footer with 'Keyboard shortcuts available' and 'Take the tour'.

Score	Locator	OS	Tags
1,000	dendesktop	Windows 10 Pro 64 bit Edition Version 1903	Cloud Agent
1,000	jwilliams-virtual-machine	Ubuntu Linux 14.04.5	Zeroth-Ubuntu
1,000	z2016-01.zeroth.local	Windows Server 2016 Standard 64 bit Edition Version 1607	Operating Systems Windows Windows Server Zeroth
1,000	z7-01.zeroth.local	Windows 7 Ultimate 64 bit Edition Service Pack 1	Operating Systems Windows Workstation Zeroth
860	z7-03.zeroth.local	Windows 7	Operating Systems Windows Workstation Zeroth
860	dc-01.zeroth.local	Windows Server 2016 Standard 64 bit Edition AD Version 1607	Operating Systems Windows Windows Server

Where the Vulns Live...

Deduplication - Locators

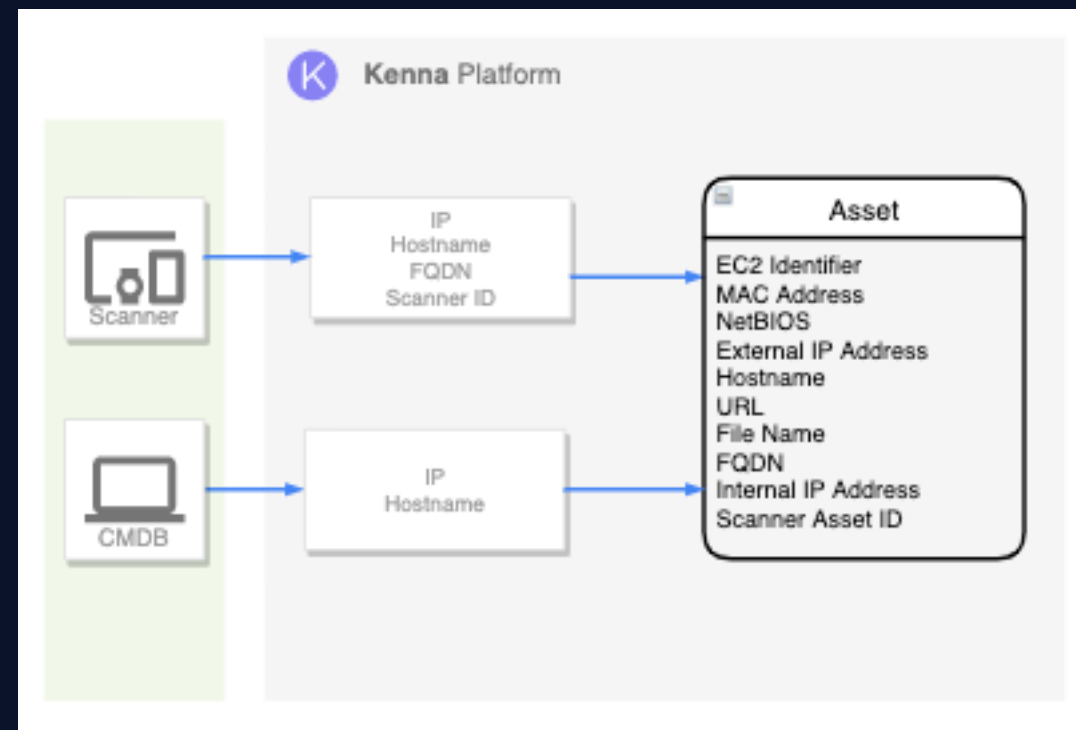


1. EC2 identifier
2. MAC address
3. NetBIOS
4. External IP address
5. Hostname
6. URL
7. File Name
8. FQDN
9. Internal IP Address (RFC1918)
10. Scanner-Specific Asset ID (Qualys, Nexpose)

Notes:

- Not all sources provide the same locators
- Only one spot per locator type
- Can be defined at the System level OR the connector level.

Deduplication - Locators



Tags



Intro to tags:

- What are Tags?
- Clear strategy helps.

Tags



Sources

- **Scanner** – Qualys, Nexpose, Tenable, etc.
- **CMDB** - ServiceNow CMDB
- **API** – apidocs.kennasecurity.com
- **Kenna Data Importer (KDI)**
- **Kenna User Interface (UI)**

Tags



Things to consider:

- **A Tag is a Tag is a Tag**
- **Prefixes are COOL**
- **Text Search is COOL**

Tags



DEMO

- **Where Tags appear**
- **Filters**
- **Text Search**

Ownership



Ownership

- Asset Ownership is very important
- More complicated than you may think
 - Multiple owners
 - No clear owners
- Need Evergreen process



Ownership



Owners within Kenna:

- Where to see Owners
 - Owner column
 - Tags
- How to manage/set
 - UI
 - CMDB connectors
 - Kenna Data Importer (KDI)
 - API/Scripts

DEMO

Discovery



Discovery



Asset Discovery Data in Kenna:

- NMAP
- ServiceNow CMDB
- Custom
 - API/Script
 - KDI

CMDB



Discovery



servicenow
CMDB

Steps for CMDB success with Kenna:

- **What?**
 - Identify the desired data from your CMDB
 - Two Types of data to consider
 - Matching Data
 - Enrichment Data
- **Where?** (cmdb_ci is the default)
 - Where is this data currently located?
 - One table or is a view needed to consolidate
- **How?**

CMDB – How?



1. Contact your ServiceNow Admin
2. Review data and decide on a Table or a View
3. Determine permissions needed for service account. (read-only)
4. Data Verification
 1. Locators
 2. Tag data
5. Locator Setup
 1. Locator mapping
 2. Locator order
6. Filtering?
7. Tag Prefixes?

CMDB – How?



1. Contact your ServiceNow Admin
2. Review data and decide on a Table or a View
3. Determine permissions needed for service account. (read-only)
4. Data Verification
 1. Locators
 2. Tag data
5. Locator Setup
 1. Locator mapping
 2. Locator order
6. Filtering?
7. Tag Prefixes?

CMDB – How?



1. Contact your ServiceNow Admin
2. Review data and decide on a Table or a View
3. Determine permissions needed for service account. (read-only)
4. Data Verification
 1. Locators
 2. Tag data
5. Locator Setup
 1. Locator mapping
 2. Locator order
6. Filtering?
7. Tag Prefixes?

CMDB – How?



1. Contact your ServiceNow Admin
2. Review data and decide on a Table or a View
3. Determine permissions needed for service account. (read-only)
4. **Data Verification**
 1. Locators
 2. Tag data
5. Locator Setup
 1. Locator mapping
 2. Locator order
6. Filtering?
7. Tag Prefixes?

CMDB – How?



1. Contact your ServiceNow Admin
2. Review data and decide on a Table or a View
3. Determine permissions needed for service account. (read-only)
4. Data Verification
 1. Locators
 2. Tag data
5. Locator Setup
 1. Locator mapping
 2. Locator order
6. Filtering?
7. Tag Prefixes?

CMDB – How?



1. Contact your ServiceNow Admin
2. Review data and decide on a Table or a View
3. Determine permissions needed for service account. (read-only)
4. Data Verification
 1. Locators
 2. Tag data
5. Locator Setup
 1. Locator mapping
 2. Locator order
6. Filtering?
7. Tag Prefixes?

CMDB – How?



1. Contact your ServiceNow Admin
2. Review data and decide on a Table or a View
3. Determine permissions needed for service account. (read-only)
4. Data Verification
 1. Locators
 2. Tag data
5. Locator Setup
 1. Locator mapping
 2. Locator order
6. Filtering?
7. Tag Prefixes?

All Things Assets – 3 Part Series

Part 1 – Asset Status (April)

Part 2 – Asset Management (May)

- Deduplication - Locators
- Tagging Strategy - Bringing in tags
- Asset Ownership – Keeping it up to date
- Discovery
- Data Enrichment – Using CMDB data

Part 3 – Asset Priority Best Practices (June)

Q & A



Thank you

David Brothers
Kenna Security, CSE

