KENNA Security

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)

KENNA Security

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)

KENNA Security

All Things Assets – 3 Part Series

Part 1 – Asset Status (April)

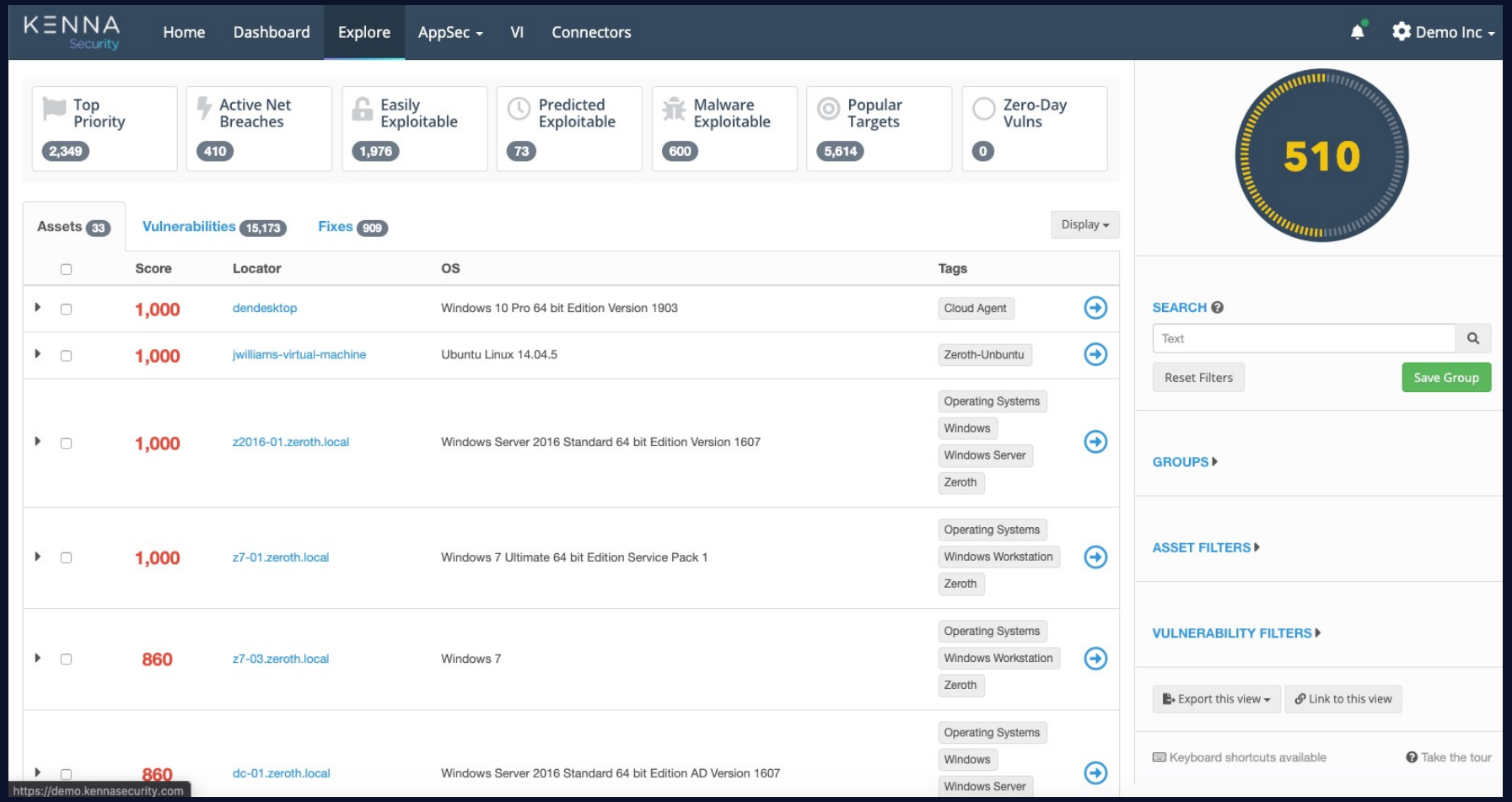
Part 2 – Asset Management (May)

Part 3 – Asset Priority Best Practices (June)

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

KENNA Security

Introduction to Assets



Where the Vulns Live…

KENNA Security

Deduplication - Locators

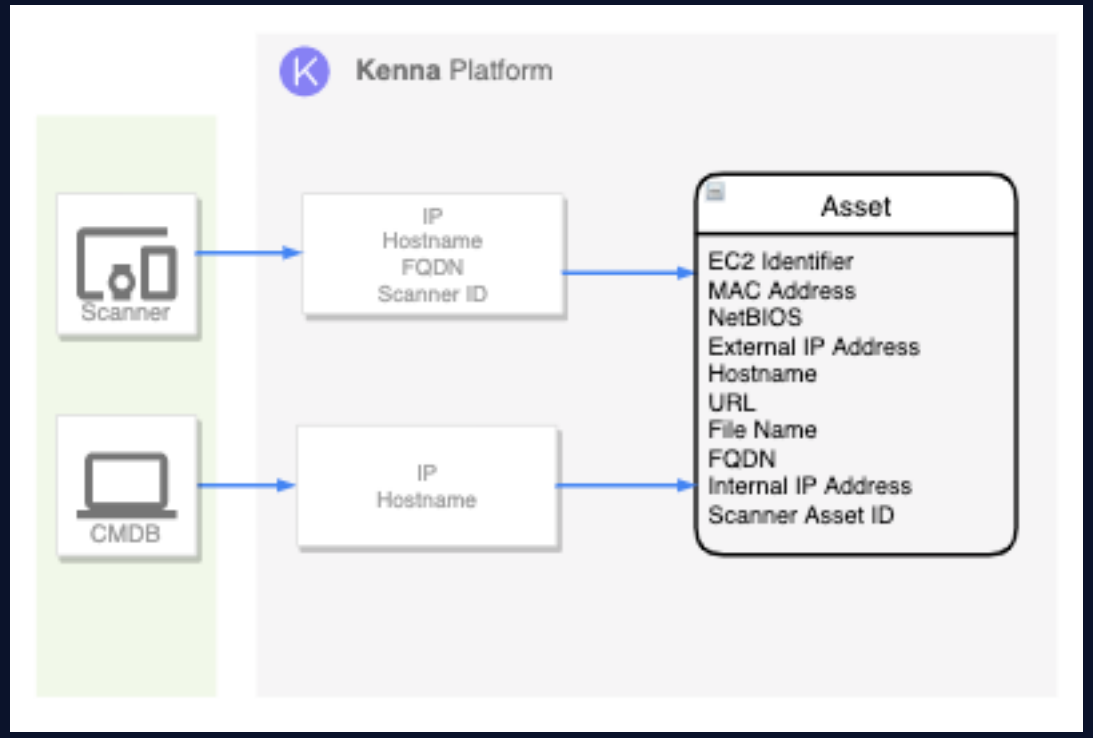
1. EC2 identifier
2. MAC address
3. NetBIOS
4. External IP address
5. Hostname
6. URL
7. File Name
8. FQDN
9. Internal IP Address (RFC1918)
10. Scanner-Specific Asset ID (Qualys, Nexpose)

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.

KENNA Security

Deduplication - Locators



KENNA
Security

Tags

Intro to tags:

- **What are Tags?**
- **Clear strategy helps.**

KENNA Security

Tags

Sources

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

KENNA Security

Tags

Things to consider:

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

KENNA Security

Tags

DEMO

- Where Tags appear
- Filters
- Text Search

KENNA Security

Ownership

Ownership

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

KENNA Security

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

KENNA Security

Discovery

Discovery

NMAP

servicenow CMDB

Asset Discovery Data in Kenna:

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

KENNA Security

CMDB

Discovery

NMAP

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?**

KENNA Security

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?

KENNA Security

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?

KENNA Security

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?

KENNA Security

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?

KENNA Security

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?

KENNA Security

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?

KENNA Security

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?

KENNA Security

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)

KENNA Security

Q & A

KENNA
Security

Thank you

David Brothers

Kenna Security, CSE