

All Things Assets – Part 3

David Brothers

Kenna Security, Customer Success Engineer

06/26/2020



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 logo and menu items: Home, Dashboard, Explore, AppSec, VI, and Connectors. On the right of the navigation bar, there are notification and settings icons, and the text '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 several 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 note 'Keyboard shortcuts available' with a 'Take the tour' link.

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...

Asset Scoring

Asset Score =

(“High Water Mark” x Asset Priority) + [Optional Ext IP “bump”]

Notes:

- 0 - 1000
- 200pt bump for “External” IP Addresses
- Maximum of 1000

Score	Name	Scanner IDs	Service Ticket
100 / 100 CVSS 2: 6 CVSS 3: 9.1	CVE-2018-10933 A vulnerability was found in libssh's server-side state machine before versions 0.7.6 and 0.8.4. A malicious client could create channels without first performing authentication, resulting in unauthorized access.	197280	External ID: Status: +
100 / 100 CVSS 2: 7 CVSS 3: 7.8	CVE-2017-8291 Artifex Ghostscript through 2017-04-26 allows -dSAFER bypass and remote command execution via .rdsparams type confusion with a "OutputFile (%pipe%" substring in a crafted .eps document that is an input to the gs program, as exploited in the wild in April 2017.	196768	External ID: Status: +
96 / 100 CVSS 2: 5 CVSS 3: 7.5	CVE-2016-9079 A use-after-free vulnerability in SVG Animation has been discovered. An exploit built on this vulnerability has been discovered in the wild targeting Firefox and Tor Browser users on Windows. This vulnerability affects Firefox < 50.0.2, Firefox ESR < 45.5.1, and Thunderbird < 45.5.1.	196637	External ID: Status: +
86 / 100 CVSS 2: 9	CVE-2018-16509 An issue was discovered in Artifex Ghostscript before 9.24. Incorrect "restoration of privilege" checking during handling of /invalidaccess exceptions could be used by attackers able to supply crafted PostScript to execute code using the "pipe" instruction.	197255	External ID: Status: +



Asset Priority – Use Cases

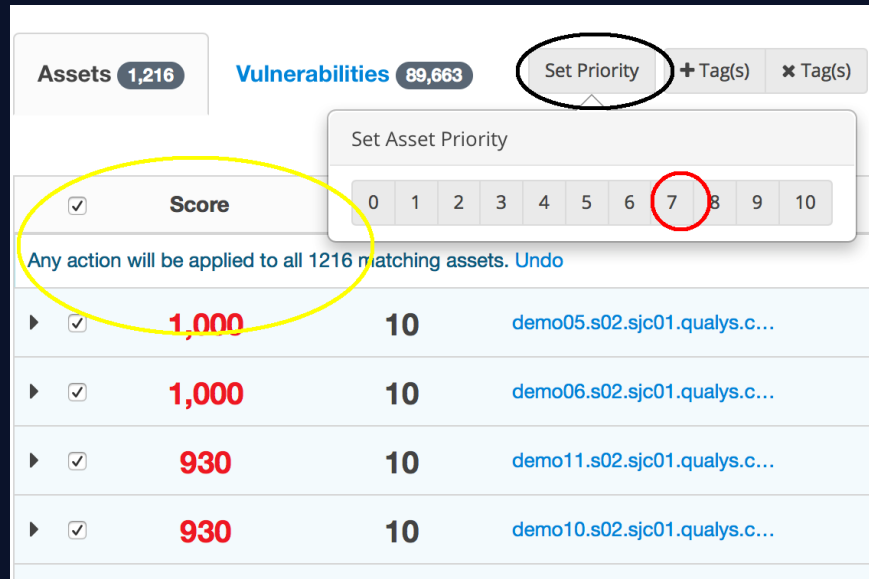
vuln	priority									
	10	9	8	7	6	5	4	3	2	1
100	1000	900	800	700	600	500	400	300	200	100
90	900	810	720	630	540	450	360	270	180	90
80	800	720	640	560	480	400	320	240	160	80
70	700	630	560	490	420	350	280	210	140	70
60	600	540	480	420	360	300	240	180	120	60
50	500	450	400	350	300	250	200	150	100	50
40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

- Used to incorporate risk appetite
- Don't hide Risk unintentionally
- Have a documented plan

Asset Priority – Setting Priority

Kenna UI:



The screenshot shows the Kenna UI interface. At the top, there are buttons for 'Assets 1,216', 'Vulnerabilities 89,663', 'Set Priority', '+ Tag(s)', and 'x Tag(s)'. The 'Set Priority' button is circled in black. Below it, a 'Set Asset Priority' dropdown menu is open, showing a range from 0 to 10, with the number 7 circled in red. The main table below has a 'Score' column circled in yellow. The table contains the following data:

Score	Priority	Asset ID
1,000	10	demo05.s02.sjc01.qualys.c...
1,000	10	demo06.s02.sjc01.qualys.c...
930	10	demo11.s02.sjc01.qualys.c...
930	10	demo10.s02.sjc01.qualys.c...

Can set priority:

- Kenna UI
- Kenna API

Kenna API:

<http://api.kennasecurity.com>

<https://apidocs.kennasecurity.com/reference>

Assets – Risks and Pitfalls

- **Don't Hide Data**
 - Define your Asset Prioritization Rules
- **Watch your Asset Counts**
 - Are you appropriately licensed?
 - Do you have active assets that don't have Vulns?
- **CMDB data enrichment**
 - Define data matching rules.
 - Use good sources (clean, consistent.)
 - Do authenticated scans when possible.
 - Determine the best “source of truth”.

Assets Section in Help Center

The screenshot displays the Kenna Security Help Center interface. At the top left is the Kenna Security logo, and at the top right are buttons for 'Submit a Request' and 'Sign in'. A search bar is centered below the header. The main content area is divided into three columns of article links, each with a section header and a 'SEE ALL' button.

Kenna BASICS
[Creating an Effective Change Management Strategy](#)
[New Navigation Bar](#)
[Kenna.VI \(Vulnerability Intel\)](#)
[Kenna and PCI Compliance](#)
[Kenna.AppSec](#)
[Kenna Home Page](#)
SEE ALL 14 ARTICLES

Security Tool/Vulnerability Scanner Connectors
[CrowdStrike Spotlight Connector](#)
[Getting data into Kenna without a connector](#)
[Setting up the Kenna Virtual Tunnel](#)
[Setting Up the Kenna Agent](#)
[Kenna Data Importer \(JSON Connector\)](#)
[Tenable IO / cloud.tenable.com](#)
SEE ALL 17 ARTICLES

Dashboard / Risk Meters
[Setting Up Your Risk-Based SLAs](#)
[Default Dashboard](#)
[Global and Shared Dashboards](#)
[General Guidelines when using vulnerability based Risk Meters](#)
[How can I create risk meters for infrastructure vs application remediation teams?](#)
[Dashboard Features](#)
SEE ALL 10 ARTICLES

Searching and Filtering
[Query Syntax Changes June 2020](#)
[Test Title](#)

Assets
[Asset Status - Kenna.VM](#)
[Asset Prioritization In Kenna](#)

Vulnerabilities
[Vulnerability Scoring in Kenna](#)
[Predicted Exploits](#)

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

Q & A



Thank you

David Brothers
Kenna Security, CSE

