

Kenna Security Implementation Success Guide

Get up & running in under an hour

Table of Contents

3 - 10

Success Guide

Overview of the platform

11 - 38

Test Plan

What you need to do

39 - 40

Success Checklist

What you should measure

Success Guide

Welcome to Kenna!

A Risk & Vulnerability Intelligence platform used by leading organizations to automate and enhance their vulnerability management efforts. The primary benefits of Kenna are to:

Automate the tedious process of prioritization vulnerabilities and putting hours back in your team's day—ensuring that they are identifying critical vulns with real-time context, rather than static CVSS scores or other methods



fe83ebb8354ba...1c23f126a3b8
7f0d632b0926a...dc33dc7d8fbe
251c98e6cd1c2...3280adc33dc7c

This document is intended to help you embark on the implementation process, giving you valuable insights into how to use Kenna as well as creating a checklist for you to assess your efforts and the success of the platform.

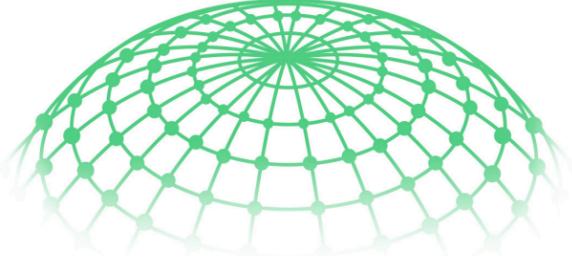
Gain a way to report on risk that's easy yet clearly communicable to the entire team—from security professionals to IT ops all the way to the executive suite



But remember—you always have access to us in-person. Contact the Sales Engineer assigned to your account, or email support@kennasecurity at any time.

We look forward to helping make you successful!

To enhance the efficacy of the entire security team by ensuring that they place their efforts on managing and reducing risk



Plan your Approach

Define Your Risk

How does your organization measure risk? With Kenna, you are able to create logical groups of assets and vulnerabilities on those assets. Each asset has a risk rating from 0 - 1000 based on the contextual threat data Kenna is constantly refreshing from many different threat sources. For each group you create, a Risk Meter becomes a way to understand and measure the risk posed to your networks based on the identified vulnerabilities, and how those vulnerabilities compare to current attacks, ease of exploit, and even potential zero days.

Risk Meter as a Foundation

Risk Meters provide the basis for measuring risk within the Kenna Platform. When planning for implementation, you should consider how you would group your assets to get the most benefit in the test environment.

How does your company work through the Vulnerability Management Lifecycle today? Are the teams who remediate all of your vulnerabilities divided up by business unit? By geography? By application stack? By technology?

When you initially create Risk Meters, it is helpful to consider how you communicate remediation information throughout your company and who consumes and takes action on that data.

Communicating Remediation

Once your groups are created you'll be sending prioritized fixes to your teams. For the scope of the implementation, do you have a test team ready to accept and use that list of prioritized patches? What does your current patch cycle look like? Would you be able to work through a cycle in 15 days? 30 days? Where would you like to improve?

Reporting

During implementation, you'll have the ability to review trending reports. The reports can both work to drive remediation, and to outline progress to management. In order to best take advantage of reporting, you should consider a few factors. First, especially if you are using file based connectors, you should plan to upload data at least twice, if not weekly. Second, if you are planning a management level presentation, the Risk Meters and trend reporting are key methods of communicating progress. Your Account Executive and Sales Engineer are also happy to assist with that presentation, just let them know.

Sync Your Data

Connectors

Kenna supports over 20 different vulnerability scanners today. You can sync both network and application scan data using our API based and File based connectors. Select **Connectors**, and then **+ Add Connector** to begin. Specific information for each connector is available in the application, and here is a brief description of each different category of connector:



View our Full List of Connectors here:
www.kennasecurity.com/connectors

API Connectors

An API connector can be scheduled to facilitate data sync within Kenna. Key considerations in scheduling the API sync are how often you scan, and which asset groups or IP ranges would be a good test environment. Scheduling of the Kenna API can then follow each scan, to pull back the results for analysis in the Kenna platform.

File Based Connectors

File based connectors are created/named; then manually run. For each supported file type, the overall process is similar. While specific detail about each file type is available in the application, key considerations with a file based connector would be having that file output synced at least twice during the implementation process. Then, the Kenna trend reports would be able to track changes over time and produce meaningful sample reports.

ServiceNow Connector

If your company is using ServiceNow as part of the remediation process, or you would like to test that functionality with Kenna, you will also configure a ServiceNow Connector on the Connectors page. You can choose to use the Kenna default ticket layout, or use one of your own incident templates. Your Sales Engineer can assist in this configuration - the ServiceNow connector requires the ITIL role.

Kenna's REST API

You may also be able to sync meaningful data to the platform using the Kenna REST API. While this can be a part of implementation, more often data from other systems like a CMDB system or GRC application is uploaded directly into the platform. Please work with your Sales team directly if you have data that you would like to sync during the process.

The Virtual Tunnel

To allow API connections to internal (non-routable) systems, Kenna has a solution which creates a VPN tunnel to facilitate the connection. You may work with your SE to utilize this option if needed.

Build Risk Meters

After your vulnerability and asset data is synced into the platform, you begin the process of organizing that data into meaningful groups to measure risk in your organization. While there are multiple ways to group your data, only you know the most meaningful groups to create. Here are a few methods typically used to create those Risk Meter groups.

Tags

On the **Home** page, you may use existing tags to group assets - and you can search or filter for those tags using the area on the right side of the home page. Today Kenna will auto-tag assets imported from Qualys, Nexpose, Veracode, WhiteHat and HP Foritfy.



SEARCH ?

Text Search:

os: "Windows Server*" ✕

GROUPS ▾

ASSET FILTERS ▾

Active/Inactive ▾

- All
- Active 2,004

Tag ▾

- Not Win 859
- Servers DMZ 674
- Kc2k3 534
- RDP 484
- Web Ports Open 458
- Open Ports Web 378

Build Risk Meters

Searches

On the **Home** page, you may use existing tags to group assets, and you can search or filter for those tags using the sidebar on the right side of the Home page. Today Kenna will auto-tag assets imported from Qualys, Nexpose, Veracode, WhiteHat and HP Foritfy.

Once the group is defined by search results, tags, or filters, select Save Group and give it a name. You have just created a Risk Meter.

Syntax Examples

Kenna offers many powerful ways to search your assets and vulnerabilities. Here are a few examples you might find useful. You can learn more about searching and other power tips by visiting: <https://help.kennasecurity.com>

Syntax	Meaning
<code>os: "Windows Server"</code>	Search Windows assets
<code>tag: "Chicago*"</code>	Search asset tags using wildcard
<code>ip:192.168.36.12</code>	Search assets by IP address range
<code>ip:[192.168.36.0 TO 192.168.36.255]</code>	Search assets by IP address range Search
<code>hostname:"internal.foo.com"</code>	Search assets by hostname
Other ways to search assets include: url , mac_address , netbios , fqdn , and file	
<code>asset_score:>=700</code> (0-1000 scale)	Search by asset risk scores of 700 or higher
<code>vulnerability_score:<50</code> (0-100 scale)	Search vulnerabilities with risk scores below 50
<code>cve:2014-0160</code>	Search vulnerabilities using the Heartbleed CVE
<code>cve_description:"shellshock"</code>	Search by vulnerability description, useful for returning vulnerabilities by specific technology (eg "adobe" or "java") or by management-friendly name (eg "ShellShock")
<code>wasc:WASC-13</code>	Search vulnerabilities by WASC ID

Remediate with Top Fixes

Once you have created Risk Meter groups, it's time to get that fix information into the right hands. We've collected the best individual fixes and grouped them to make your remediation workflow easier. Use Top Fix Groups to maximize impact with the least amount of effort.

Top Fix groups are available for any of the Risk Meter groups you have created - choose "View Reports" from the dashboard for any risk meter, and select Top Fixes from the top of the reporting view.

To send the remediation information to the right team, you can either send via email or download as a CSV. (If you have a ServiceNow connector configured, that is also an option for you to open tickets directly) Another approach would be to set up each system admin or business unit manager within Kenna and let them drive the remediation directly from the platform.

ACCA

[View Report](#)

[Explore](#)



Top Fix Groups ?



Group 1: Risk Score Reduction of 35, 1 Fix

[ServiceNow incident](#)

[Send via email](#)

[Send via CSV ▾](#)

Microsoft SMB Remote Code Execution Vulnerability (MS09-001) [↗](#)

1011 Vulns Affected Across All Data

Diagnosis

Consequence

Solution

CVEs Addressed **3**

Assets Affected **223**

Workaround:

TCP ports 139 and 445 should be blocked at the firewall to protect systems behind the firewall from attempts to exploit this vulnerability.

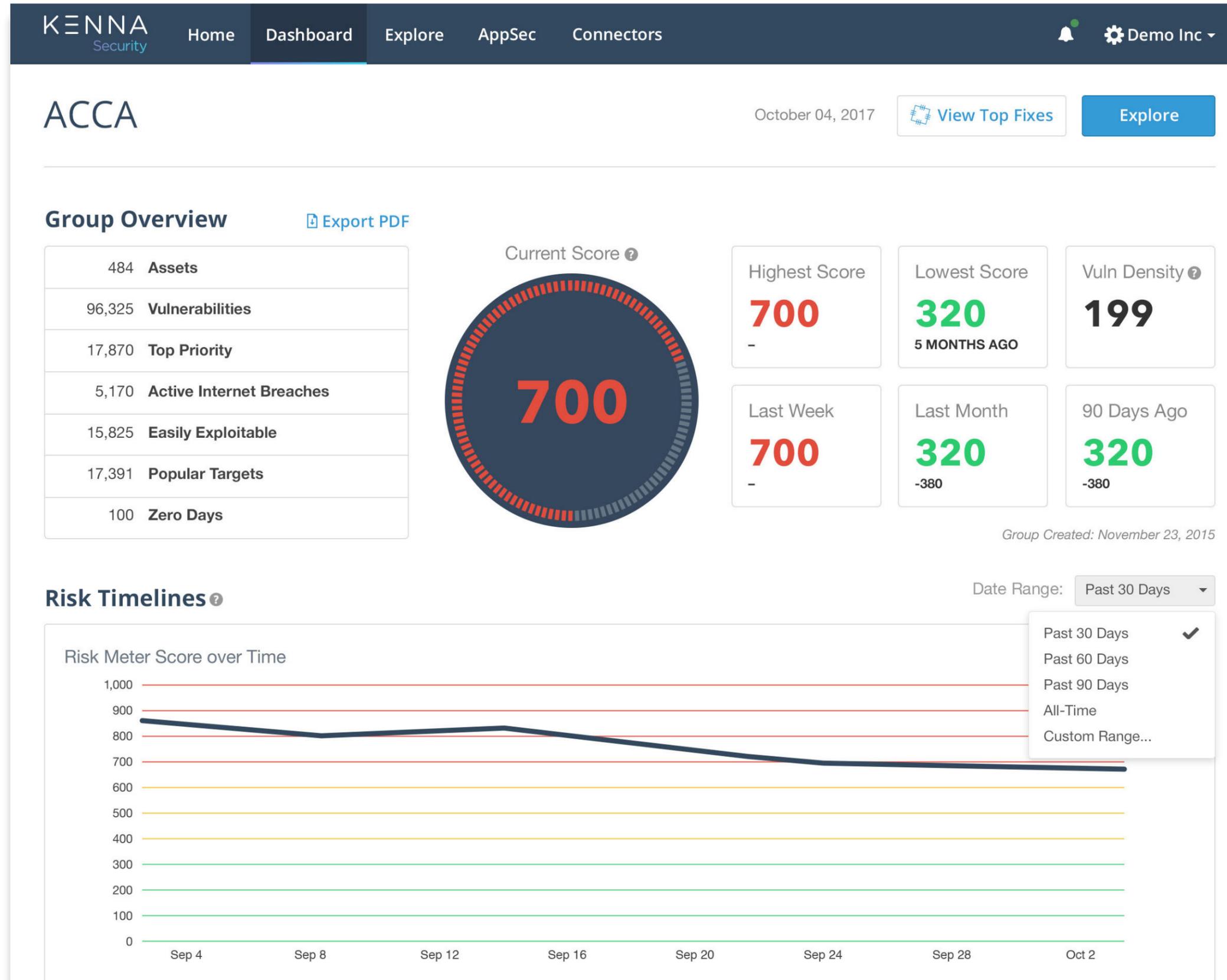
Impact of workaround: Blocking the ports can cause several windows services or applications using those ports to stop functioning.

Patch:

Report Trends

Finally, show management your great work.

Once you've synced, prioritized, patched, and synced again, you are ready to report on the progress. Choose "View Report" from the Dashboard for any Risk Meter - you'll see a collection of trending reports and KPIs specific to that group of assets.



Test Plan

Asset Management

Prioritize assets based on environmental factors (asset criticality, mitigating / compensating controls)

Asset priority values are used in calculating overall asset risk scores (highest vulnerability risk * asset priority = asset risk score)

KENNA Security Home Dashboard **Explore** AppSec Connectors Demo Inc

1

Top Priority: 37,662 | Active Breaches: 8,573 | Easy Exploits: 34,573 | Predicted Exploits: 33 | Malware Exploits: 39,943 | Popular Targets: 62,398 | Zero-Day Vulns: 204

Assets: 2,004 | Vulnerabilities: 224,626 | Fixes: 4,348

2 Select Assets

3 Set Priority

Score	Locator	OS	Created
1,000	bug-50125b	Windows 2000 Service Pack 3-4	11 months ago
1,000	bug-50125b	Windows 2000 Service Pack 3-4	11 months ago
1,000	10.10.25.123	Linux 2.3-2.6 / Embedded Device / F5 Networks Big-IP	11 months ago
1,000	10.10.26.140	Ubuntu Linux 7.04	11 months ago
1,000	2ksp4-25-175	Windows 2000 Service Pack 3-4	11 months ago

HUD: 600

SEARCH: Text

GROUPS

ASSET FILTERS: Active/Inactive (All, Active)

2,004

Tags

Organize assets by adding contextual tags (i.e. Asset Owner, Application, IT support organization)

Asset tags from vulnerability scanners will persist in Kenna. (i.e. Qualys Assets groups and tags, Nexpose Site Names and tags, etc). Asset tags are searchable with elastic search and may be leveraged to create Kenna Risk Meter groups.

TEST: Tags to be added for testing: (unit), P1 vs P2, BISO, ITRL, region, IT support org, asset owner, platform technology

Tags

Tags are displayed in the asset view and in the navigation side bar on the right:

Assets	Vulnerabilities	Fixes	Display	
2,004	224,626	4,348	▼	
Score	Locator	OS	Tags	Created
1,000	bug-50125b	Windows 2000 Service Pack 3-4	RDP, SLP Servers, Web ports open, kc2k3, open ports web, servers DMZ	11 months ago
1,000	bug-50125b	Windows 2000 Service Pack 3-4	RDP, SLP Servers, Web ports open	11 months ago
1,000	10.10.25.123	Linux 2.3-2.6 / Embedded Device / F5 Networks Big-IP	SLP Servers, Servers DMZ	11 months ago
1,000	10.10.26.140	Ubuntu Linux 7.04	RDP, SLP Servers, Web ports open	11 months ago
1,000	2ksp4-25-175	Windows 2000 Service Pack 3-4	RDP, SLP Servers, Web ports open, kc2k3, open ports web, servers DMZ	11 months ago
1,000	30-178	Windows 2000 Service Pack 3-4	RDP, SLP Servers, Web ports open, kc2k3, open ports web, servers DMZ	11 months ago
1,000	2k3sp2-26-239	Windows 2000 R2 Service Pack 2	RDP, SLP Servers	11 months ago
1,000	2k3sp2-26-230.patch.ad.vu...	Windows 2000 R2 Service Pack 2	RDP, SLP Servers	11 months ago
1,000	2k3sp2-26-244.patch.ad.vu...	Windows 2000 R2 Service Pack 2	RDP, SLP Servers	11 months ago
1,000	2k3sp2-26-256.patch.ad.vu...	Windows 2000 R2 Service Pack 2	RDP, SLP Servers	11 months ago



SEARCH ?

GROUPS

ASSET FILTERS

- Active/Inactive
 - All
 - Active 2,004
- Tag
 - Not Win 859
 - Servers DMZ 674
 - Kc2k3 534
 - RDP 484
 - Web Ports Open 458
 - Open Ports Web 378
 - Juniper 254
 - All Compliance Hosts 183
 - All Assets 175
 - All Compliance Assets 175

Risk Meter Creation

Organize, track, prioritize and report assets and vulnerabilities by business context

Risk meters may be grouped based on P1 vs P2 application, BISO, ITRL, device location (network segment), platform technology, etc

TEST: Create Risk Meter group based on Platform Operating System: Windows Servers:
1) Enter the following query in the search dialog box: **os:"Windows Server"**

The screenshot shows the KENNA Security dashboard with the 'Explore' tab selected. A red circle with the number '1' highlights the 'Explore' tab. Below the navigation bar, there are several summary cards for various security metrics: Top Priority (37,662), Active Breaches (8,573), Easy Exploits (34,573), Predicted Exploits (33), Malware Exploits (39,943), Popular Targets (62,398), and Zero-Day Vulns (204). Below these cards, there are tabs for Assets (2,004), Vulnerabilities (224,626), and Fixes (4,348). A table displays a list of vulnerabilities with columns for Score, Locator, OS, Tags, and Created. The table shows five entries, all with a score of 1,000. To the right of the table, there is a 'HUD' section with a large circular gauge showing the number '600'. Below the HUD, there is a search section with a red circle and the number '2' highlighting the search input field. The search input contains the query 'os: "Windows Server*"'. Below the search input, there are buttons for 'Reset Filters' and 'Save Group'. At the bottom of the search section, there is a 'GROUPS' section with a 'Group Name' input field and a 'Save' button.

1

KENNA Security

Home Dashboard **Explore** AppSec Connectors

HUD

Top Priority 37,662

Active Breaches 8,573

Easy Exploits 34,573

Predicted Exploits 33

Malware Exploits 39,943

Popular Targets 62,398

Zero-Day Vulns 204

Assets 2,004 Vulnerabilities 224,626 Fixes 4,348 Display

Score	Locator	OS	Tags	Created
1,000	bug-50125b	Windows 2000 Service Pack 3-4	RDP, SLP Servers, Web ports open, kc2k3, open ports web, servers DMZ	11 months ago
1,000	bug-50125b	Windows 2000 Service Pack 3-4	RDP, SLP Servers, Web ports open	11 months ago
1,000	10.10.25.123	Linux 2.3-2.6 / Embedded Device / F5 Networks Big-IP	SLP Servers, Servers DMZ	11 months ago
1,000	10.10.26.140	Ubuntu Linux 7.04	RDP, SLP Servers, Web ports open	11 months ago
1,000	2ksp4-25-175	Windows 2000 Service Pack 3-4	RDP, SLP Servers, Web ports open, kc2k3, open ports web, servers DMZ	11 months ago

2 Enter Search Query

SEARCH ?

os: "Windows Server*" 🔍

Text Search:
os: "Windows Server*" ✖

Reset Filters Save Group

GROUPS ▾

Group Name Save

Risk Meter Creation

2) Save the Group and provide a name: **Windows Servers**

600

SEARCH ?

os: "Windows Server*"

Text Search:
os: "Windows Server*" ✕

Reset Filters Save Group 1

GROUPS ▾

Group Name Save 2

ASSET FILTERS ▾

Active/Inactive ▾

- All
- Active 2,004

Tag ▾

- Not Win 859
- Servers DMZ 674
- Kc2k3 534
- RDP 484
- Web Ports Open 458
- Open Ports Web 378
- Juniper 254

Risk Meter Creation

TEST: Create Risk Meter group based on P1 Applications:

1) Enter the following query in the search dialog box: **tag:"P1"**

The screenshot shows the KENNA Security dashboard. The 'Explore' tab is active, indicated by a red circle with the number '1'. The dashboard features a navigation bar with 'Home', 'Dashboard', 'Explore', 'AppSec', and 'Connectors'. On the right, there are notification and user profile icons for 'Demo Inc'. Below the navigation bar, there are seven summary cards: 'Top Priority' (37,662), 'Active Breaches' (8,573), 'Easy Exploits' (34,573), 'Predicted Exploits' (33), 'Malware Exploits' (39,943), 'Popular Targets' (62,398), and 'Zero-Day Vulns' (204). Below these cards, there are tabs for 'Assets' (2,004), 'Vulnerabilities' (224,626), and 'Fixes' (4,348). A table displays a list of vulnerabilities with columns for 'Score', 'Locator', 'OS', 'Tags', and 'Created'. The table shows five entries, all with a score of 1,000. The first entry has a locator 'bug-50125b' and OS 'Windows 2000 Service Pack 3-4'. The second entry has a locator 'bug-50125b' and OS 'Windows 2000 Service Pack 3-4'. The third entry has a locator '10.10.25.123' and OS 'Linux 2.3-2.6 / Embedded Device / F5 Networks Big-IP'. The fourth entry has a locator '10.10.26.140' and OS 'Ubuntu Linux 7.04'. The fifth entry has a locator '2ksp4-25-175' and OS 'Windows 2000 Service Pack 3-4'. On the right side of the dashboard, there is a 'HUD' (Heads-Up Display) showing a large circular gauge with the number '600' in the center. Below the HUD, there is a search section with a red circle and the number '2' around the text 'Enter Search Query'. The search section includes a 'SEARCH' button, a search input field containing 'tag:"P1"', a 'Text Search:' section with 'tag:"P1"' and a close button, a 'Reset Filters' button, and a green 'Save Group' button. At the bottom right, there is a 'GROUPS' section with a 'Group Name' input field and a 'Save' button.

Top Priority

37,662

Active Breaches

8,573

Easy Exploits

34,573

Predicted Exploits

33

Malware Exploits

39,943

Popular Targets

62,398

Zero-Day Vulns

204

Assets 2,004

Vulnerabilities 224,626

Fixes 4,348

Display

Score	Locator	OS	Tags	Created
1,000	bug-50125b	Windows 2000 Service Pack 3-4	RDP, SLP Servers, Web ports open, kc2k3, open ports web, servers DMZ	11 months ago
1,000	bug-50125b	Windows 2000 Service Pack 3-4	RDP, SLP Servers, Web ports open	11 months ago
1,000	10.10.25.123	Linux 2.3-2.6 / Embedded Device / F5 Networks Big-IP	SLP Servers, Servers DMZ	11 months ago
1,000	10.10.26.140	Ubuntu Linux 7.04	RDP, SLP Servers, Web ports open	11 months ago
1,000	2ksp4-25-175	Windows 2000 Service Pack 3-4	RDP, SLP Servers, Web ports open, kc2k3, open ports web, servers DMZ	11 months ago

HUD



2 Enter Search Query

SEARCH

tag:"P1"

Text Search:

tag:"P1"

Reset Filters

Save Group

GROUPS

Group Name Save

Risk Meter Creation

2) Save the Group and provide a name: **P1 Application**

600

SEARCH ?

tag:"P1" 🔍

Text Search:
tag:"P1" ✕

Reset Filters Save Group 1

GROUPS ▾

Group Name Save 2

ASSET FILTERS ▾

Active/Inactive ▾

All

Active 2,004

Tag ▾

Not Win 859

Servers DMZ 674

Kc2k3 534

RDP 484

Web Ports Open 458

Open Ports Web 378

Juniper 254

Vulnerability Management

Calculate vulnerability risk using integrated threat / exploit context

Vulnerability risk scores are calculated using data feeds from the NIST NVD, scanning vendor KBs, Dell CTU, AlientVault OTX, Metasploit, ExploitDB, Shodan, Exodus Security and many others. Please see the following link for a comprehensive list: www.kennasecurity.com/partners

1

- Top Priority: 37,662
- Active Breaches: 8,573
- Easy Exploits: 34,573
- Predicted Exploits: 33
- Malware Exploits: 39,943
- Popular Targets: 62,398
- Zero-Day Vulns: 204

Assets 2,004 | Vulnerabilities 224,626 | Fixes 4,348

Edit ▾ | Display ▾

Score	Name	Asset	Created
100 / 100 CVSS: 9	CVE-2012-0013 Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka "Assembly Execution Vulnerability."	vinay-24-64.testing.compliance.vuln.qa.qualys.com SLP servers servers DMZ	11 months ago
100 / 100 CVSS: 9	CVE-2012-1823 sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of	vinay-24-64.testing.compliance.vuln.qa.qualys.com SLP servers servers DMZ	11 months ago

↑
Vulnerability Risk Score

← Integrated Threat / Exploit Data



SEARCH ?

GROUPS ▾

ASSET FILTERS ▾

- Active/Inactive ▾
- All
 - Active

Vulnerability Management

Threat / Exploit filters may be used to prioritize high risk vulnerabilities:

- Top Priority: 37,662
- Active Breaches: 8,573
- Easy Exploits: 34,573 ³
- Predicted Exploits: 33
- Malware Exploits: 39,943
- Popular Targets: 62,398
- Zero-Day Vulns: 204

Assets: 2,004 ² Vulnerabilities: 224,626 Fixes: 4,348

Edit ▾ Display ▾

Score	Name	Asset	Created
<input type="checkbox"/> 100 / 100 CVSS: 9	CVE-2012-0013 Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka "Assembly Execution Vulnerability."	vinay-24-64.testing.compliance.vuln.qa.qualys.com SLP servers servers DMZ	11 months ago
<input type="checkbox"/> 100 / 100 CVSS: 9	CVE-2012-1823 sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of	vinay-24-64.testing.compliance.vuln.qa.qualys.com SLP servers servers DMZ	11 months ago



SEARCH ?

GROUPS ▾

ASSET FILTERS ▾

- Active/Inactive ▾
- All
 - Active

Manage & Track Vulnerability SLA Due Dates

Vulnerability due dates may be set automatically or manually defined in the UI.

TEST: Automate SLA due dates based on group and vulnerability severity. Configure a new due date rule

The screenshot shows the user interface of Kenna Security. At the top right, there is a user profile dropdown menu with a gear icon and the text "Demo Inc" next to it, which is circled in red with the number "1". The dropdown menu is open, showing options: Profile, Users, User Roles, Custom Fields, Two-Factor Authentication, API Keys, Asset Settings, SLA Settings (circled in red with the number "2"), Upload a CSV, Alerts, Report Subscriptions, Release Notes, Contact Support, Help Center, and Log Out. Below the menu, there is a search bar with the text "os: 'Windows Se" and a "Text Search:" section with the text "os: 'Windows Server". At the bottom, there is a "GROUPS" section with a "Group Name" input field and a "Save" button.

The screenshot shows the "Settings » SLA Policies » New" configuration page. The page has a dark blue header with the Kenna Security logo and navigation links: Home, Dashboard, Explore, AppSec, and Connectors. The main content area is white and contains the following fields:

- Name:** A text input field containing "Critical SLA Policy".
- Apply To:** Radio buttons for "All vulnerabilities" and "Only vulnerabilities belonging to the following groups:". The second option is selected. Below it is a tag input field containing "Servers" and a red arrow pointing to the text "Select Applicable Asset Groups".
- Score Range:** Radio buttons for "All", "Medium or High (33-100)", "High (66-100)" (selected), and "Custom Range". Below it is the text "Only assign due dates on vulnerabilities within a specific score range".
- SLA Days:** A text input field containing "7" and a red arrow pointing to the text "Select SLA Days". Below it is the text "Vulnerability due date will be automatically set to this many days from when the vulnerability was found. If a vulnerability is covered by more than one SLA policy, it will be assigned the strictest (shortest) policy defined."

At the bottom of the page, there are two buttons: a green "Save" button and a blue "Cancel" button.

Manage & Track Vulnerability SLA Due Dates

TEST: Manually set a SLA due date for a vulnerability

KENNA Security Home Dashboard **Explore** AppSec Connectors Demo Inc

Top Priority: 37,662 | Active Breaches: 8,573 | Easy Exploits: 34,573 | Predicted Exploits: 33 | Malware Exploits: 39,943 | Popular Targets: 62,398 | Zero-Day Vulns: 204

Assets: 2,004 | **Vulnerabilities: 224,626** | Fixes: 4,348

Score	Name	Asset
100 / 100 CVSS: 9	CVE-2012-0013 Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka "Assembly Execution Vulnerability."	vinay-24-64.testing.compliance SLP servers servers DM
100 / 100 CVSS: 9	CVE-2012-1823 sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of	vinay-24-64.testing.compliance SLP servers servers DM

HUD
600

SEARCH ?
Text

GROUPS

ASSET FILTERS
Active/Inactive
 All
 Active

2,004 22

Manage & Track Vulnerability SLA Due Dates

TEST: Select the due date

The screenshot displays the KENNA Security dashboard. The top navigation bar includes 'Home', 'Dashboard', 'Explore', 'AppSec', and 'Connectors'. The main dashboard area features several metrics cards: 'Top Priority' (37,662), 'Active Breaches' (8,573), 'Easy Exploits' (34,573), 'Predicted Exploits' (33), 'Malware Exploits' (39,943), 'Popular Targets' (62,398), and 'Zero-Day Vulns' (204). A large circular gauge on the right shows a value of 600. The 'Vulnerabilities' section is active, showing a list of vulnerabilities. Two vulnerabilities are selected, and an 'Edit Custom Field Values' modal is open. The modal contains a text input field for 'Due Date' (circled with a red '1') and a 'Save Changes' button (circled with a red '2'). A calendar widget is open over the input field, showing the month of October 2016. The calendar grid is as follows:

October 2016						
Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

The background shows a list of vulnerabilities with columns for 'Score' and 'Name'. Two vulnerabilities are visible: CVE-2012-0013 and CVE-2012-1823, both with a score of 100/100 and CVSS: 9. The CVE-2012-0013 entry includes tags for 'QualysGuard', 'Fix Available', and 'Active Internet'. The CVE-2012-1823 entry includes tags for 'SLP servers' and 'servers D'.

Track Risk Acceptance & Exceptions

Vulnerabilities may be marked as "Risk Accepted" and custom fields (text, date, number) may be used to capture exception details.

TEST: Mark vulnerabilities as Risk Accepted

KENNA Security Home Dashboard **Explore** AppSec Connectors Demo Inc

Top Priority: 37,662 | Active Breaches: 8,573 | Easy Exploits: 34,573 | Predicted Exploits: 33 | Malware Exploits: 39,943 | Popular Targets: 62,398 | Zero-Day Vulns: 204

Assets: 2,004 | **Vulnerabilities: 224,626** | Fixes: 4,348

Set Status | Edit | ServiceNow incident | Display

Score	Name	Created
100 / 100 CVSS: 9	CVE-2012-0013 Incomplete blacklist vulnerability in the Windows Package configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka "Assembly Execution Vulnerability."	11 months ago
100 / 100 CVSS: 9	CVE-2012-1823 sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of	11 months ago

Set Vulnerability Status: Open, Closed, **Risk Accepted**, False Positive

SEARCH ?
Text

GROUPS

ASSET FILTERS
Active/Inactive
 All
 Active

2,004 24

Track Risk Acceptance & Exceptions

TEST: Create a custom field to capture Risk Acceptance justification

The screenshot shows the user interface of KENNA Security. At the top right, there is a user profile dropdown menu labeled 'Demo Inc' with a gear icon, circled with a pink '1'. The dropdown menu is open, showing options: Profile, Users, User Roles, Custom Fields (circled with a pink '2'), Two-Factor Authentication, API Keys, Asset Settings, SLA Settings, Upload a CSV, Alerts, Report Subscriptions, Release Notes, Contact Support, Help Center, and Log Out. Below the menu, there is a search bar with the text 'os: "Windows S...' and a 'Text Search:' section with the text 'os: "Windows Server...'. At the bottom, there is a 'GROUPS' section with a 'Group Name' input field and a 'Save' button.

The screenshot shows the 'Settings » Custom Field Definitions » New' page in KENNA Security. The page has a dark blue header with the KENNA Security logo and navigation links: Home, Dashboard, Explore, AppSec, and Connectors. The main content area is white and contains the following fields and options:

- Name:** A text input field containing 'Risk Acceptance Justification'.
- Description:** A text area containing 'Please provide a detailed description for the exception.' This field is circled with a pink arrow pointing to the text 'Custom Field Description'.
- Data Type:** A section with three radio button options:
 - String: up to 2000 characters of text (circled with a pink arrow pointing to the text 'Select Data Type')
 - Numeric: a number, with or without decimals
 - Date: a calendar date
- Faceted Search:** A section with one checked checkbox: Generate filter options for vulnerability search.

At the bottom of the form, there are two buttons: a green 'Save' button and a blue 'Cancel' button.

Track Risk Acceptance & Exceptions

TEST: Add Risk Acceptance justification details to vulnerability



Assets 2,004 **Vulnerabilities** 224,626 **Fixes** 4,348

Set Status Edit ▾ ServiceNow incident Display ▾

Score ▾	Name	Asset
<input checked="" type="checkbox"/> 100 / 100 CVSS: <u>9</u>	CVE-2012-0013 Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka "Assembly Execution Vulnerability."	vinay-24-64.testing.compliance SLP servers servers DM
<input checked="" type="checkbox"/> 100 / 100 CVSS: <u>9</u>	CVE-2012-1823 sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.	vinay-24-64.testing.compliance SLP servers servers DM

3
Select Vulnerabilities

- Internal Risk Rating
- Notification Date
- Notes
- Remediation Notes
- Development Team
- Project
- Person
- Priority
- Due Date
- 4** Risk Acceptance Justification
- Business Impact
- Reevaluation Date
- Risk Acc Criteria
- My SLA
- Owner



SEARCH ?

Text 🔍

GROUPS ▾

ASSET FILTERS ▾

Active/Inactive ▾

- All
- Active

2,004

Tag ▾

Track Risk Acceptance & Exceptions

TEST: Add justification details

The screenshot shows the KENNA Security dashboard with a modal window titled "Edit Custom Field Values". The modal contains a text input field for "Risk Acceptance Justification" and a "Save Changes" button. The background dashboard displays various security metrics and a list of vulnerabilities.

KENNA Security Home Dashboard Explore AppSec Connectors Demo Inc

Top Priority: 37,662 | Active Breaches: 8,573 | Easy Exploits: 34,573 | Predicted Exploits: 33 | Malware Exploits: 39,943 | Popular Targets: 62,398 | Zero-Day Vulns: 204

Assets: 2,004 | Vulnerabilities: 224,626

Edit Custom Field Values

Set Risk Acceptance Justification for 2 selected vulnerabilities.

Risk Acceptance Justification

1 Technical limitation, unsupported java library.

2 Save Changes

HUD

600

SEARCH ?

Text

GROUPS

ASSET FILTERS

Active/Inactive

All

Active

Tag

2,004

CVSS: 9

CVSS: 9

QualysGuard Fix Available Active Int

Business Impact

Reevaluation Date

Risk Acc Criteria

My SLA

Owner

vinay-24-64.testing.compliance

SLP servers servers D

Automatically prioritize vulnerabilities & recommend fixes based on risk

Access the latest information around available patches and receive contextualized remediation for your asset groups (as well as overall assets). These suggestions can be prioritized and sorted to display key remediation insights such as the highest risk reduction, patches containing the most CVEs and the most assets affected. Fixes also responds to any filtering that happens on the dashboard, so you can filter based on remediations for vulnerabilities containing active internet breaches, or those that are easily exploitable.

You can also preview how much your risk score will be adjusted by applying the patch before actually deploying. This ensures that you are fixing the most critical vulnerabilities first.

TEST: Review patch / fix recommendations for a Risk Meter group

The screenshot shows the KENNA Security Dashboard interface. At the top, there is a navigation bar with the KENNA Security logo and menu items: Home, Dashboard (highlighted with a pink circle '1'), Explore, AppSec, and Connectors. On the right of the navigation bar, there are notification and settings icons, and the text 'Demo Inc' with a dropdown arrow.

The main content area is titled 'Dashboard' and includes a search bar, a dropdown menu for 'Name (A - Z)', a 'Score' filter with three colored dots (green, yellow, red), a 'Size' filter with three colored squares (blue, grey, white), and a green '+ Add Risk Meter' button.

The 'My Risk Meters' section displays six risk meter cards in a grid. The first card, 'All Assets', shows a score of 600 and is highlighted with a pink circle '2'. Below the score are 'Reporting' and 'Top Fixes' buttons. The second card, 'Windows Servers', shows a score of 700 with similar buttons. The third card is a dashed placeholder. The bottom row contains three more cards: 'Application' (score 700), 'Active ServiceNow Tickets' (score 600), and 'Compliance' (score 620).

On the right side, the 'DASHBOARD VIEWS' sidebar lists several views: 'My Risk Meters', 'Chicago Data Center', 'Windows Machines' (which includes a sub-view for 'ACCA' with a score of 620 and a green checkmark), and 'South Region Offices'. At the bottom of this sidebar is a green dashed box with '+ Add Dashboard View' and a keyboard icon with the text 'Keyboard shortcuts available'.

Automatically prioritize vulnerabilities & recommend fixes based on risk

ACCA

October 04, 2017

3 View Top Fixes

Explore

Group Overview

Export PDF

484	Assets
96,325	Vulnerabilities
17,870	Top Priority
5,170	Active Internet Breaches
15,825	Easily Exploitable
17,391	Popular Targets
100	Zero Days

Current Score ?



Highest Score
700
-

Lowest Score
320
5 MONTHS AGO

Vuln Density ?
199

Last Week
700
-

Last Month
320
-380

90 Days Ago
320
-380

Group Created: November 23, 2015

Risk Timelines ?

Date Range: Past 30 Days



Automatically prioritize vulnerabilities & recommend fixes based on risk

ACCA

[View Report](#)

[Explore](#)



Top Fix Groups ?

Risk Reduction Scores



Group 1: Risk Score Reduction of 35, 1 Fix

[ServiceNow incident](#)

[Send via email](#)

[Send via CSV](#)

Microsoft SMB Remote Code Execution Vulnerability (MS09-001) [↗](#)

1011 Vulns Affected Across All Data

[Vulnerability Rollup](#)

[Diagnosis](#)

[Consequence](#)

[Solution](#)

[CVEs Addressed](#) 3

[Assets Affected](#) 223

[Assets Requiring Patch/Fix](#)

[Vendor Security Advisory](#)

Workaround:

TCP ports 139 and 445 should be blocked at the firewall to protect systems behind the firewall from attempts to exploit this vulnerability.
Impact of workaround: Blocking the ports can cause several windows services or applications using those ports to stop functioning.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[MS09-001: Microsoft Windows 2000 Service Pack 4](#)

[MS09-001: Windows XP Service Pack 2 and Windows XP Service Pack 3](#)

[MS09-001: Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2](#)

[MS09-001: Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2](#)

Reporting

Track / report vulnerability and asset risk scores over time

Detailed security metric and historical trending reports are available for each Risk Meter on the **Dashboard** page.

Dashboard

Search... 🔍 Name (A - Z) ▾ Score ●●● Size ■■■ [+ Add Risk Meter](#)

My Risk Meters

All Assets



600

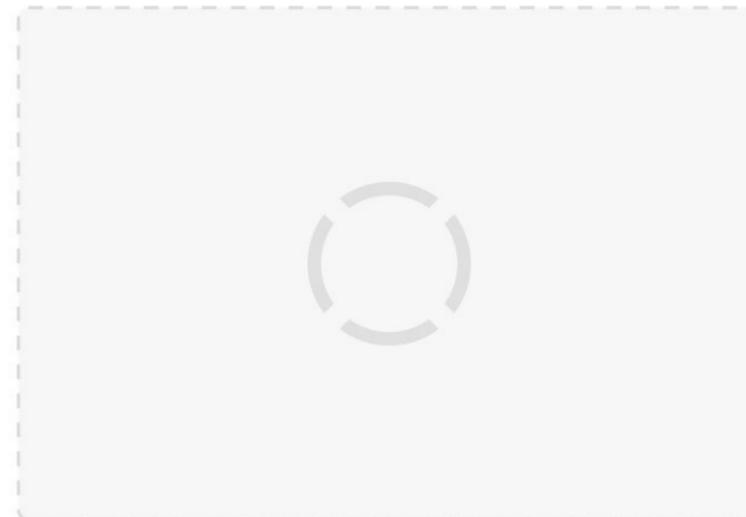
Reporting | Top Fixes

Windows Servers



700

2 Reporting | Top Fixes



Application



700

Reporting | Top Fixes

Active ServiceNow Tickets



600

Reporting | Top Fixes

Compliance



620

Reporting | Top Fixes

DASHBOARD VIEWS

My Risk Meters

Chicago Data Center

Windows Machines

ACCA ✓



620

South Region Offices

[+ Add Dashboard View](#)

🗂️ Keyboard shortcuts available

Reporting

Risk Meter group summary and score over time are tracked with historical trend.

Group Overview

[Export PDF](#)

484	Assets
96,325	Vulnerabilities
17,870	Top Priority
5,170	Active Internet Breaches
15,825	Easily Exploitable
17,391	Popular Targets
100	Zero Days

Current Score ?



Highest Score

700

-

Lowest Score

320

5 MONTHS AGO

Vuln Density ?

199

Last Week

700

-

Last Month

320

-380

90 Days Ago

320

-380

Group Created: November 23, 2015

Risk Timelines ?

Select Desired Date Range

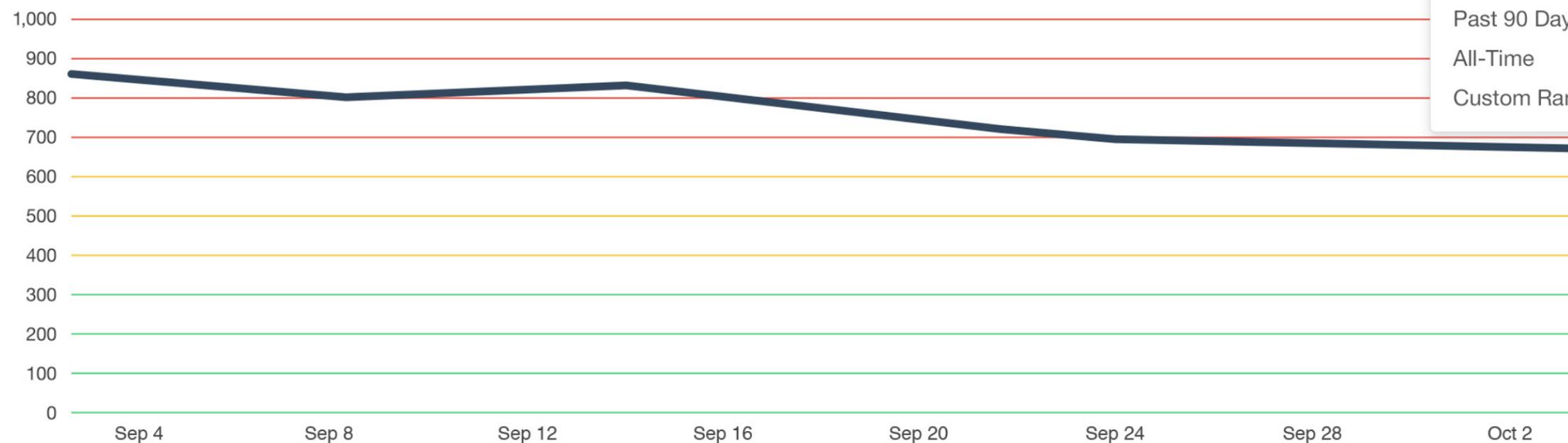
2

Date Range:

Past 30 Days

1

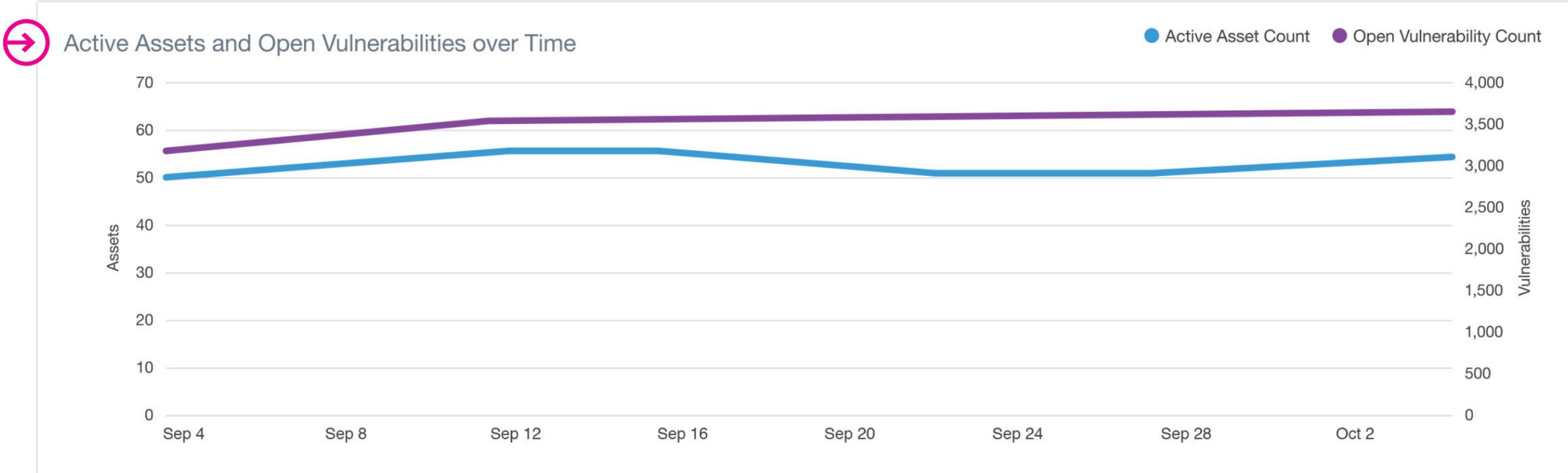
Risk Meter Score over Time



- Past 30 Days ✓
- Past 60 Days
- Past 90 Days
- All-Time
- Custom Range...

Reporting

Asset and Vulnerability Counts are also tracked over time.



Track / report SLA, vulnerability age, over due

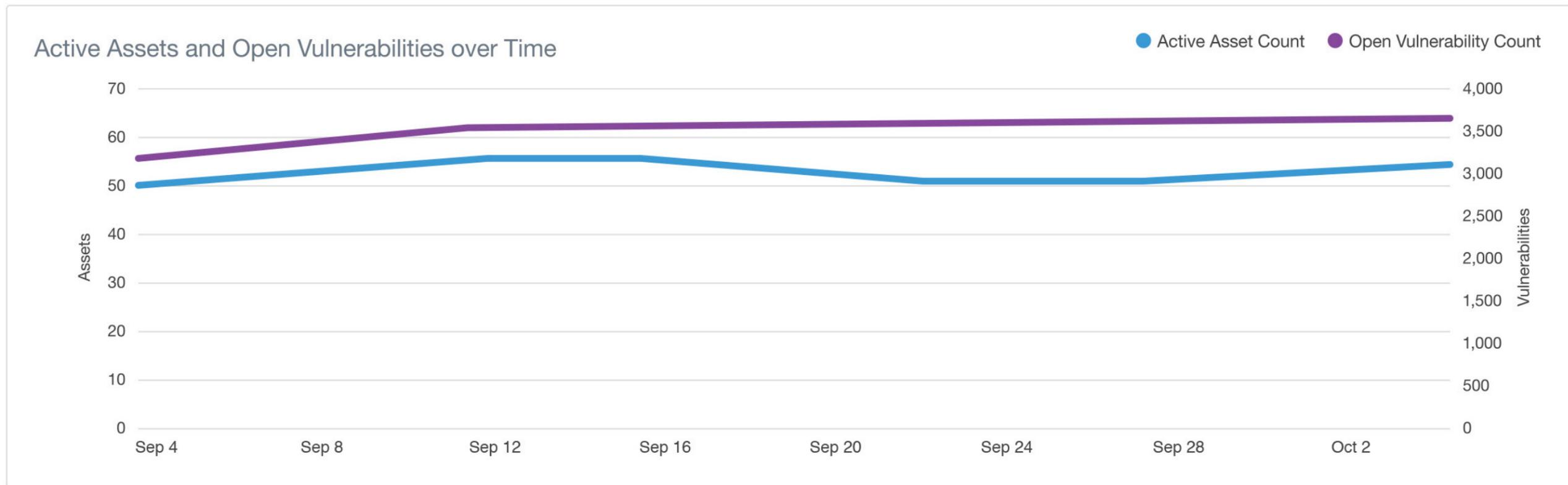
Vulnerability Reports may be based on SLA dates or vulnerability age and tracked over time. The sample report below shows all overdue vulnerabilities based on the following query: **due_date:<now**

Past Due

October 04, 2017

View Top Fixes

Explore



Track / report remediation effectiveness:
new vulnerabilities detected, closed
vulnerabilities, mean time to remediate:

Kenna will track when vulnerabilities are first detected in the environment and when vulnerabilities are closed. These dates are used to track mean time to remediate.

Past Due

October 04, 2017

[View Top Fixes](#)

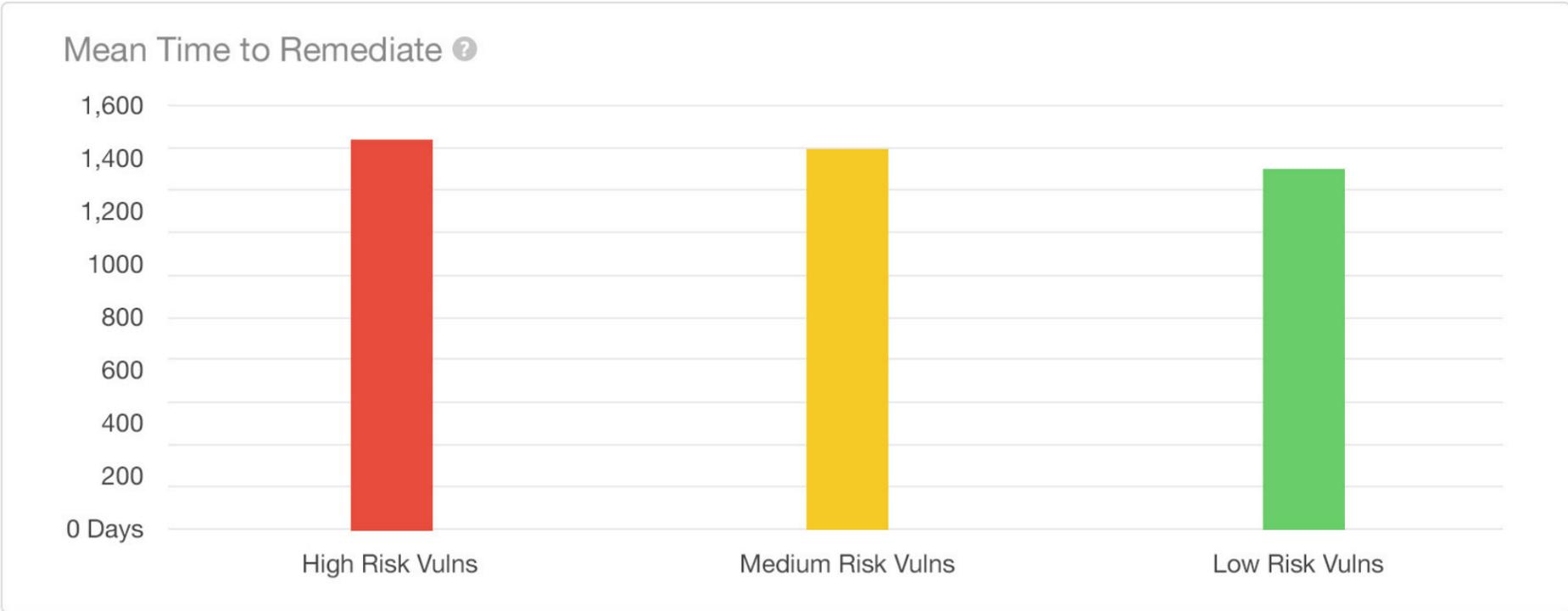
[Explore](#)

Historical Risk Information

Date Range: Jan 1, 2016 - Jan 1, 2017

New Vulnerabilities Found
12,552
120 ASSETS AFFECTED

Total Closed Vulnerabilities
8,680
227 ASSETS AFFECTED



Export reports to PDF

Group Overview

[Export PDF](#) 

484	Assets
96,325	Vulnerabilities
17,870	Top Priority
5,170	Active Internet Breaches
15,825	Easily Exploitable
17,391	Popular Targets
100	Zero Days

Current Score 



Highest Score

700

-

Lowest Score

320

5 MONTHS AGO

Vuln Density 

199

Last Week

700

-

Last Month

320

-380

90 Days Ago

320

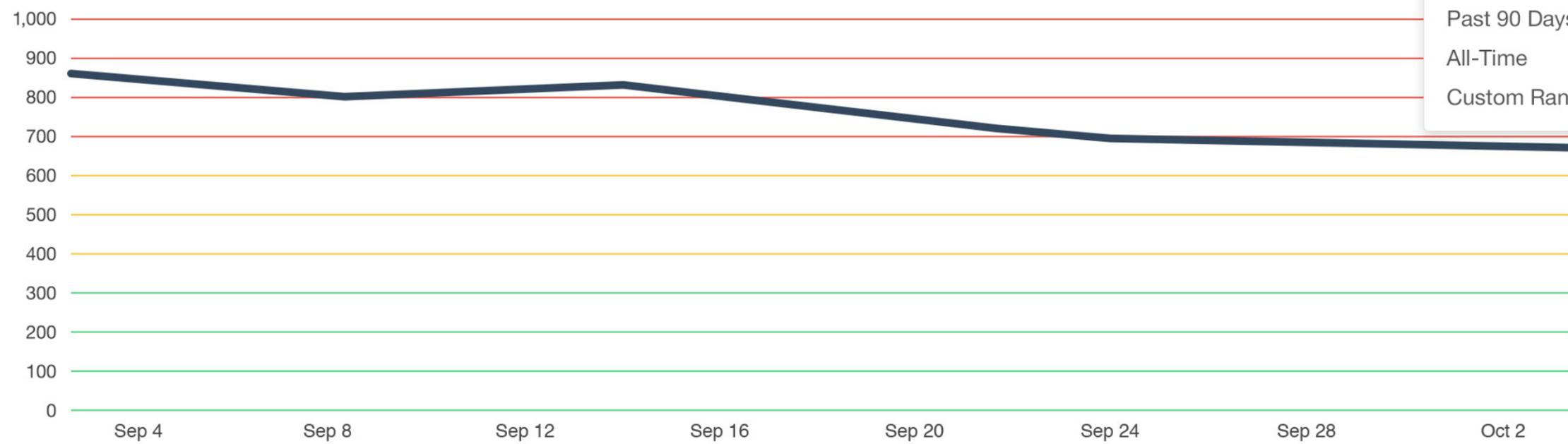
-380

Group Created: November 23, 2015

Risk Timelines

Date Range: Past 30 Days 

Risk Meter Score over Time



- Past 30 Days
- Past 60 Days
- Past 90 Days
- All-Time
- Custom Range...

Access Control

Create / manage user access to Kenna platform:

Additional users may be added to the platform using the settings console.

1

2

Profile

Users

User Roles

Custom Fields

Two-Factor Authentication

API Keys

Asset Settings

SLA Settings

Upload a CSV

Alerts

Report Subscriptions

Release Notes

Contact Support

Help Center

Log Out

SEARCH ?

os: "Windows Se

Text Search:

os: "Windows Server

Reset Filters

Save Group

GROUPS

Group Name

Save

KENNA Security

Home Dashboard Explore AppSec Connectors

New User

First Name

Last Name

Email

Phone

Default notification level

Emergency

Role

Administrator

Register Cancel

New Users Receive a Registration Email

Assigned Role determines permission rights

Role Based Access Control

Access to Risk Meter groups, assets, and vulnerability data may be granted / restricted based on user role:

TEST: Create a new user role

The screenshot shows the user interface of KENNA Security. At the top right, there is a user profile icon labeled 'Demo Inc' with a red circle '1' next to it. A dropdown menu is open, showing various settings options. The 'User Roles' option is highlighted with a red circle '2'. Below the menu, there is a search bar with the text 'os: "Windows S...' and a 'Text Search:' section with the text 'os: "Windows Server...'. At the bottom, there is a 'GROUPS' section with a 'Group Name' input field and a 'Save' button.

The screenshot shows the 'Settings » User Roles » New' page in KENNA Security. The page has a dark blue header with the KENNA Security logo and navigation links: Home, Dashboard, Explore, AppSec, and Connectors. The main content area is white and contains the following form fields:

- Name:** A text input field containing 'Server Remediation Team'.
- Apply To:** Radio buttons for 'read-only' and 'read/write'. The 'read/write' option is selected, and a red circle with an arrow points to it with the text 'Select Access Level'.
- Group(s):** A multi-select field containing 'Servers' and 'Database Servers'. A red circle with an arrow points to the field with the text 'Define Applied Groups'.

Below the 'Group(s)' field, there is a note: 'Grant access to objects that belong to any of these group(s)'. At the bottom of the form, there are two buttons: a green 'Save' button and a blue 'Cancel' button.

Success Checklist

Category	Implementation Functional Requirements	Description
Integration	Ingest vulnerability data from third party scanning vendors	Qualys, Tenable, Nexpose, other
Integration	Ingest 3rd party threat intelligence feeds	Correlate external active threats, exploit and zero day intelligence against assets and vulnerabilities
Integration	Platform scalability	Ingest vulnerability data for x assets with no measurable impact to platform performance
Integration	Integrate with workflow / ticketing tools	ServiceNow, Jira
Integration	API	Ability to ingest asset information from various sources (pen test, CMDB)
Reporting	Vulnerability Risk Reporting	Report asset and vulnerabilities and relative risk based on threat, exploit and local environmental context
Reporting	Generate reports based on logical groups, associated data, dates/times	Asset and vulnerability risk reports based on business context (unit), region, IT support org, asset owner, platform technology, date
Reporting	Generate reports to track exceptions and SLA	Asset vulnerability exception reports on a per host, per vulnerability, or per business basis: set exception expiration dates and SLA
Reporting	Generate historical trending / progress reports	Report asset, vulnerability metrics over time: risk score, active assets, open vulnerabilities, avg time to remediate
Workflow	Track and group assets / vulnerabilities by functional IT group	Create risk meter groups for the following teams: Windows Server, Unix / Linux, Desktop
Workflow	Prioritize vulnerabilities / patches	Prioritize based on vulnerability risk and likelihood of exploit and recommend most effective (risk reduction) patch
Workflow	Track / manage vulnerability exceptions and false positives	Custom fields to capture exception / FP context: business justification, exception expiration, status
Workflow	Track / manage vulnerability SLAs	Automatically set SLA dates based on vulnerability severity / environmental context. Manually set SLA dates
Workflow	Create tickets with grouped vulnerability / patching actions	Create ServiceNow / Jira ticket with remediation actions (group by asset, business context, functional group, platform technology)
Security	Role Based Access Control	Grant / restrict access to asset / vulnerability data based on user role)
Alerting	Automatic Email Notification	Option to generate email notification for risk and vulnerability state changes: risk score change, vulnerability exploit change

Kenna Security

350 Sansome Street Suite 500
San Francisco, CA 94104

Phone: **(855) 474-7546**

Email: **hello@kennasecurity.com**

Web: **www.kennasecurity.com**

Team Up On Risk

© COPYRIGHT 2019 KENNA SECURITY, INC. ALL RIGHTS RESERVED.