NDA REQUIRED FOR DISTRIBUTION

CHEAT SHEET

Kenna Risk Scoring

Kenna Security Risk Scoring

Risk Score Guide for Kenna.VM

Kenna Security has the ability to manually adjust scores/factors based on active findings and research. IMPORTANT: The scoring model outlined in this document is subject to change as our scoring methods advance and are applied to our Data Science.

Vulnerability Scoring

CVE – SCORE (0-100)

The context behind this scoring model is that Kenna Security provides more information about a CVE and its use in the wild than NVD does when they provide a CVSS. **All scoring begins at 25** and specific factors increase that score from our threat and intel reference feeds.

- a "**weaponized**" exploit is a scripted exploit rather than a Proof of Concept (POC) exploit and is openly available. (+25)
- a "**breach**" is an event of an individual attempting to exploit through a CVE in the wild either through malware or a firewall (+25)
- a "**popular target**" is the 10% decile of prevalent CVEs out there (+2.5)
- the **CVSS** boost is how Kenna takes a categorical distribution (CVSS) and turn it into a pseudo-continuous distribution from 0-100
- as shown below, base-exploitability subscore is the part of the CVSS v2 Base score equation, while base score is the total value (+12.5 *prediction scale applied)
- each CVE has CVSS vectors published from NVD analysis
- "**pre_NVD_chatter**" is defined as a known (pre-NVD) vulnerability that has been discussed anywhere online in three or more sources at a frequency of five or more times. This boost is applied for as long as it is considered "recent" from the RF threat intelligence. (+12.5)
- "**zero day**" vulnerabilities provided by the Exodus Intelligence platform are scored as vulnerabilities that are not weaponized, do not have a breach event, but do have a POC exploit.
- malware reversal data indicates the presence of an exploit that caused the intrusion as well as a breach event. It is scored as both.

```
CVE_BASE_RISK ||= 25
 Breach?         + 25
 Weaponized?     + 25
 Exploit?        + 12.5 * prediction scale (possible values: 12.5, 12.375,10, 7.5)
 Popular target? + 2.5
 Pre-NVD exploit chatter + 12.5

* CVSS boost ((CVSS v2 base-exploitability subscore + base score) / (average of all CVE,
CVSS v2 base-exploitability + base scores))
```

Note: The prediction scale is based on Kenna's confidence quantiles of c = 100% (there is an exploit already), c is greater than 90%, c is greater than 75%, and c is anything less than 75% will scale by 1, .99, .8, and .6 respectively.

Asset Scoring (0-1000)

An asset has a base score of the highest scored vulnerability. This vulnerability is multiplied by the "asset priority" (1-10) and will receive a score bump of +200 if the asset's IP is externally exposed. Some scanners will provide additional mitigating factors such as "internal application" or "behind authentication" in which each will receive a *.875 score influence.

```
BASE_ASSET_SCORE       ||= highest scored vuln
asset priority?          * priority (0-10, defaults to 10 if nothing is set)
internal application?    * .875 (a field provided by some scanners)
behind authentication?   * .875 (a field provided by some scanners)
externally exposed IP?   + 200 (we include those defined by RFC 1918 by default,
clients can specify additional internal facing ranges of IP addresses)
```

Risk Meter Scoring (0-1000)

A Risk Meter is a group of assets. It is specifically a query of Elasticsearch terms that groups a set of assets + vulnerabilities and allows Kenna to track and report on that set.

The score here is simple:
Average of matched, active assets with a score (the sum of asset scores matching query / number of matched assets in the set)
(A possible score range of 0-1000)

Note: Kenna filters out assets scored 0 (zero).

Example:

```
I have a risk meter that matches on tag:Windows and has 4 assets, the scores of
which are 0, 600, 600, 750.

The total risk meter will be scored as such:

  (600 + 600 + 750) / 3 = 650 the average across matched assets
```

If an asset leaves the group or becomes inactive, this affects the group's score. For example, if the 750 asset is decommissioned, the score reduces to 600 ((600+600) / 2)

Similarly, the addition of new assets in a risk meter affects the score.