Data Correlation

- Vulnerability Deduplication: How are vulnerabilities caught by a scanner and by the patch management tool correlated?
    - Deduping is done by CVE per asset per port.

> **EXAMPLE**
>
> You have two Tomcat servers on a machine and two vulnerability scanners. Your scanners would show four total vulnerabilities, but RiskVision would dedupe so that it would only show as two vulnerabilities, one for each instance of Tomcat.

- How is the many-to-many CVE-patch relationship managed?
    - We can correlate on a per CVE basis. See previous question.

- Is risk measured at the CVE or patch level?
    - RiskVision scores risk at the vulnerability instance level. A patched risk is equal to the sum of the risks of the vulnerability instances that the patch remediates. Patched risks are not currently displayed in the user interface; however, the data relationships are available to generated this information in reports.

- How are discrepancies managed? For example, the vulnerability scanner says there's a MS17-010 vulnerability, but patch management says it's already been applied.
    - If a Patch Management tool says a patch has been applied and scanner hasn't seen the patch, there are two possible scenarios:
        1. A timing difference (example, no updated scan since the patch was applied). We recommend that the ticket is updated when a patch is applied. However, we don't close the vulnerability or ticket until another scan is run and RiskVision has verified that the vulnerability is no longer present on that host.

        2. The scanner could be erroneously missing the patch. We recommend that you label the vulnerability as a false positive using the **Status** field of the vulnerability, or create a vulnerability exception.

- Are all of the above configurable?
    - Generally, yes. For more information, contact Resolver Support .

- Is manual correlation occasionally required? For example, do I need to update correlation rule sets as new patches/vulnerabilities are released?
    - As long as the data sources that are being sent to RiskVision do not have errors (e.g. CMDB repositories, vulnerability scanners, threat intelligence feeds, etc.), manual correlation should not be required. RiskVision provides two types of automated vulnerability-related correlation:
        1. **By CVE**: Vulnerability scanners typically identify vulnerabilities using their own IDs (e.g. Qualys QID, Nessus Plug-In #). When the source scanner provides CVE cross-references, RiskVision automatically correlates CVE associations with assets. Once RiskVision has asset-to-CVE associations, the system can perform vulnerability instance deduplication when multiple scanners report the same vulnerabilities. This allows RiskVision to infer threats and exploits, both of which are highly useful to automate vulnerability risk scoring. This also facilitates patch-to-asset correlation.

        2. **By CPE**: This is used when RiskVision is aware of a vulnerability definition, but doesn't know which assets the vulnerability applies to. A common scenario where this might occur is a zero-day vulnerability, which by definition will not be caught by any scanner. A vulnerability advisory service would typically indicate which technologies are affected and the steps to exploit the vulnerability. Through CPE correlation, RiskVision can identify the assets affected

by a zero-day vulnerability.

CPE correlation is also valuable when assets can only be scanned on a low-frequency basis (e.g. due to difficulty of obtaining credentials for credentialed scans or due to performance effects on critical assets). Using CPE correlation, RiskVision can take vulnerability definitions from the National Vulnerability Database or another vulnerability advisory service and correlate these definitions to the assets that are affected by the vulnerabilities.