How does my CMDB impact Vulnerability Response?

Questions addressed:

Page 1:

- What is ServiceNow Vulnerability Response?
- Why is CMDB integration critical to using ServiceNow VR?

Page 2:

- What are best practices for populating and maintaining a healthy CMDB?
- How do I ensure accuracy when matching CIs with vulnerabilities?

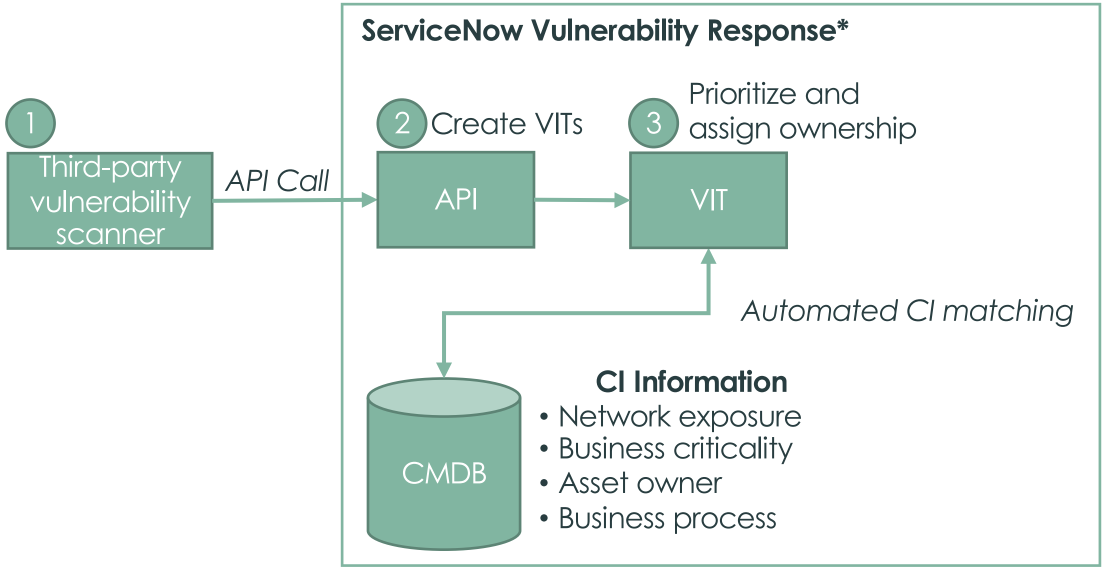
If you have any questions on this topic or you would like to be a contributor to future ServiceNow best practice content, please contact us.

What is ServiceNow Vulnerability Response?

ServiceNow® Vulnerability Response (VR) helps security teams manage significant amounts of vulnerability data and helps operational teams to perform actions to remediate these vulnerabilities. VR does this by integrating with leading third-party vulnerability tools (e.g., Microsoft Threat and Vulnerability Management, Qualys, Tenable, Rapid7) to bring identified vulnerabilities into ServiceNow and use the ServiceNow workflow capabilities to manage and automate the vulnerability response process.

Why is CMDB integration critical to using ServiceNow VR?

ServiceNow VR uses information from configuration items (CIs) in the ServiceNow CMDB to add business context to vulnerabilities. This information helps prioritize and assign ownership for remediation of that vulnerability. Here are the steps in the vulnerability response workflow relevant to understanding the criticality of the CMDB integration:



1. **Scan –** Third-party scanner detects vulnerabilities.
2. **Create Vulnerable Items (VITs) –** Built-in API workflow pulls detections from the scanner and creates separate Vulnerable Items (VITs) for each system impacted by a specific vulnerability.
3. **Prioritize and assign ownership –** Automated CI matching accesses the CMDB and matches the configuration item to the system listed in the VIT. Using information in the CI, it helps prioritize and assign ownership.

*This workflow diagram is limited to the steps necessary to understand CMDB integration. For the full ServiceNow Vulnerability Response workflow see page 5 of Now on Now: Our Vulnerability Response Journey.

How does my CMDB impact Vulnerability Response? (Cont.)

What are best practices for populating and maintaining a healthy CMDB?

Since CMDB and CI matching are key to the effectiveness of ServiceNow VR, it's critical to properly populate your CMDB and keep your CMDB up to date and healthy. To accomplish this:

- ❑ If you're setting up your CMDB for the first time as part of your ServiceNow VR implementation, the first step is to plan your CMDB deployment.
- ❑ Populate and maintain your CMDB with ServiceNow Discovery (you can also import CI data from system configuration software such as Microsoft Systems Center).
- ❑ Use the CMDB health dashboard to monitor your CMDB and take action to address problems.

How do I use CI lookup rules to ensure accuracy when matching CIs with vulnerabilities?

If the vulnerability scanner finds a system that's not yet in the CMDB, an extended CI is created that must then be reconciled and brought into the CMDB as a permanent CI. To make sure you're not adding duplicate CIs to your CMDB (and adding extra work for yourself) during reconciliation, create and refine the CI lookup rules that define what fields have matching data in the CMDB. As a starting point, you can use this three-tier matching process:

1. **Scanner ID –** If you can find the scanner ID—either a host ID or agent ID that your vulnerability scanner assigns a system—you know you have an accurate match.
2. **Name –** If you cannot match the scanner ID, look at the name (FQDN, hostname, or DNS).
3. **IP address –** Then look at the IP address, though only if it's an infrastructure-type device, not an endpoint.