Vulnerability Response Success Map

An overview of how to implement, maintain, and get maximum value from Vulnerability Response

Success Foundations | Implement | Run | Optimize and Expand

servicenow

Success Foundations

Critical inputs for successful implementation and maintenance

Vision and value

VR outcome – Align business context with risk and threat intelligence for faster, more efficient vulnerability management.

Sample KPIs

- Active vulnerable items per remediation team
- Vulnerable items risk score
- Age of critical vulnerable items
- Critical vulnerable Items closed

Foundational ServiceNow apps

Implement before or with Vulnerability Response.

CMDB | Third-party integrations

Implementation roles

General

- Executive sponsor
- Platform owners (business and technical)
- Process owners → **Trained in Security Operations products:** VR process owner
- Project manager
- VR analyst
- Technical resources (sys admin, developer, tester, architect) → VR technical admin

Governance

Special roles added to governance team

- **CMDB owner –** Owns CMDB access, use, and maintenance
- **VR Manager –** Makes VR process decisions
- **VR technical admin –** Technical maintenance and support for third-party VR applications

OCM and enablement

Owners and end users of the VR application are informed and provided an enablement plan.

now Skills and expertise

- CMBD, Security Operations, and VR
- Sources: Now Expert Services, Now-certified Security Operations partner, Now-certified internal employees (We recommend a combination.)

Project planning

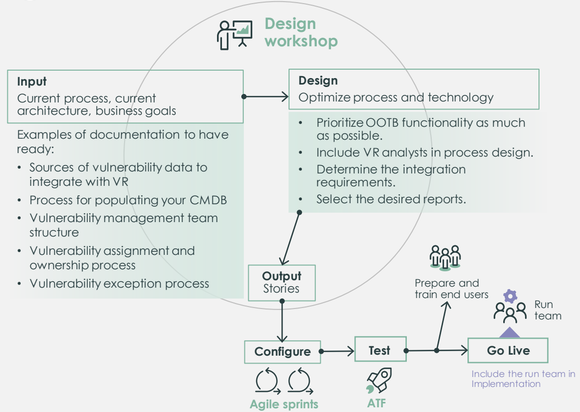
- Prepare for an agile approach
- Review the VR Quick Start Guide
- Use the VR implementation checklist
- Plan for the target value from VR

Implement

Implementation activities and best practices

Use Now Create to execute your implementation.

Before implementation, confirm your CMDB is set up and familiarize yourself with key VR features such as automated vulnerability assignment and service-aware risk scoring.



Run

Plan and execute Now Platform® maintenance

Run roles

- CMBD owner
- VR process owners
- VR technical admin
- Platform owner

Platform health

- **Daily –** Review the error logs.
- **Weekly –** Review the Performance Analytics dashboard.
- **Monthly –** Review VR's effectiveness and attend CAB the meeting.

Demand management

Have a process to intake and prioritize new integrations and Security Operations services to offer.

Enhancements

Check for new Security Operations-related offerings released via the Now Store.

Upgrades

- Prioritize OOTB options to ease upgrades.
- Stay current on releases (N-1).

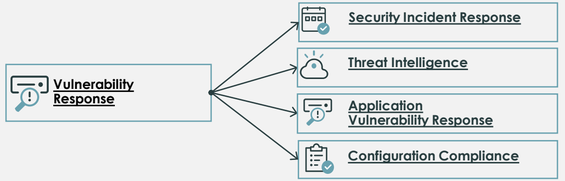
Assess value

- Are vulnerabilities mitigated faster?
- Are there fewer deferred critical vulnerable items?

Optimize and Expand

Maximize value from your Security Operations licenses—increase value from the Now Platform®

Consider which Security Operations applications to implement next.



Consider which Now Platform product suites to implement next.

VR → IT Operations Management (ITOM)
Resolve issues faster using ITOM data to automatically prioritize vulnerabilities.

VR → Governance, Risk, and Compliance
Improve vulnerability response with continuous monitoring and automated exception handling.

VR → IT Service Management (ITSM)
Automate vulnerability remediation workflows with ITSM Change and Release Management.

Click here for print version