

Strengthen Cyber Resilience with CMDB & Vulnerability Response

CMDB MasterClass Part 9

Chris Padmore, Isaiah Levreau & Christine Morris | July 30, 2025



Agenda

Welcome & Introduction

1. Vulnerability Response Overview

Integrations

Lookup Rules

VR Ticket (VIT) Creation

VR Workspaces & Lifecycle

Reports & Dashboards

2. Vulnerability Response & the CMDB

3. Q&A





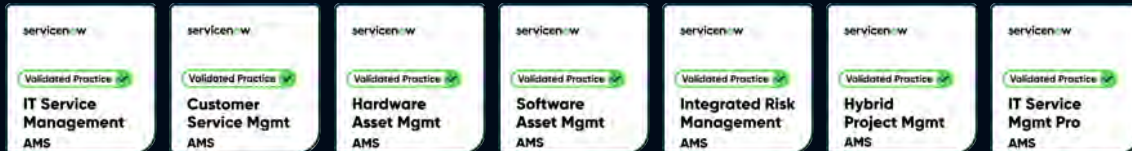
Cask NX is with clients for what comes next – on the platform and in their business.

4.65

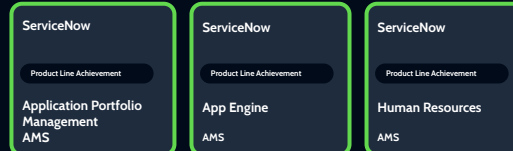
Customer
Satisfaction Rating

5.4K+

Certifications &
Accreditations



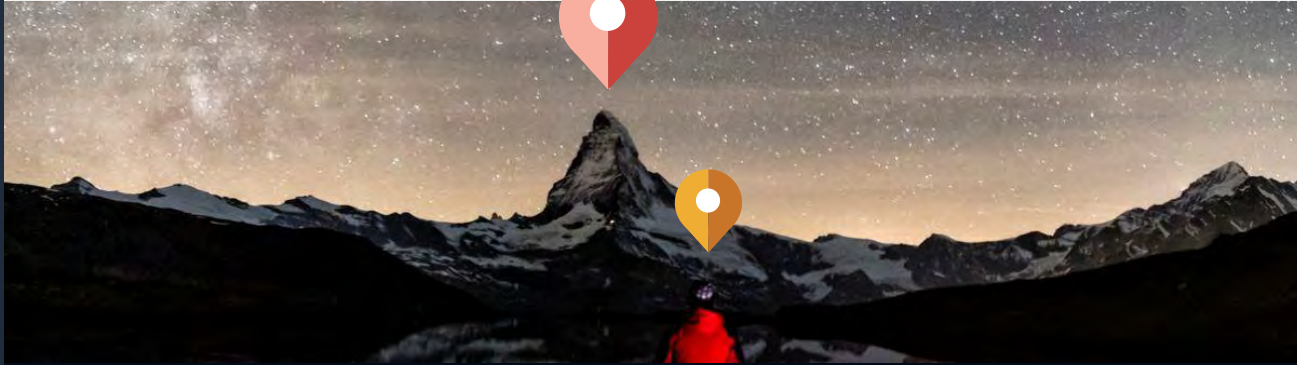
VALIDATED PRACTICES



+3 PRODUCT LINE ACHIEVEMENTS



Cask NX is the only pure play ServiceNow partner with dedicated, fully certified practices across the platform.



IT SERVICE
MANAGEMENT



IT OPERATIONS
MANAGEMENT



IT ASSET
MANAGEMENT



STRATEGIC
PORTFOLIO
MANAGEMENT



EMPLOYEE
WORKFLOW



CUSTOMER
WORKFLOW



SECURITY
& RISK



APP ENGINE

STRATEGY

Strategic Roadmapping

Advisory Consulting

Platform Strategy &
Governance

Demand Management

TRANSFORMATION

App Modernization

UX & UI Design

Product Management

Org Change Management

Testing & Quality Engineering

Program & Project Management

Agile Transformation w/SAFe

IMPLEMENTATION & APP DEVELOPMENT

Product Implementation

Platform Engineering

Data Management &
Integrations

App Development

OPERATIONS & ENHANCEMENT

Continuous Cloud Innovation

Platform Architecture &
Engineering

Functional Process Execution

Cask Reserve

Introductions



Christine Morris
Director, Platform &
Service Management
Cask



Chris Padmore
Solutions Architect,
ITOM Practice Lead
Cask



SPECIAL GUEST

Isaiah Leveau
Sr. Business Consultant,
Cask

Join the Conversation: Using Zoom

Turn on Video

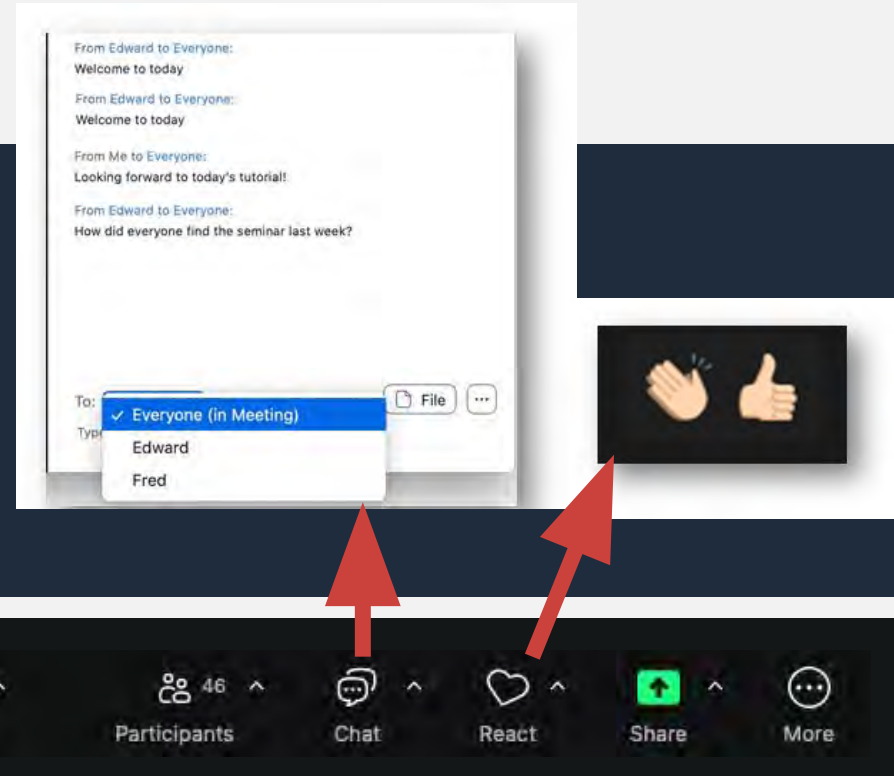
Let's get interactive and enjoy ourselves!

Unmute – Click the microphone icon to unmute and participate

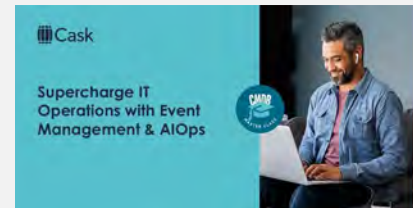
Chat – Message everyone or just one person

Get Help – Use Chat

Show Captions - Click on MORE, click Show Captions



Catch Up with Parts 1-8 of our CMDB MasterClass Series!



Find recordings, resources & more here! <https://casknx.com/cmdb-masterclass-intro/>

AUDIENCE POLL

**How confident are you
in your CMDB's ability
to support vulnerability
remediation?**

- A** Rock solid. Our CMDB is basically a vault of truth.
- B** Fairly good, but there's room for cleanup.
- C** It's trying, bless its little heart.
- D** CMDB? You mean that thing we meant to fix last year?

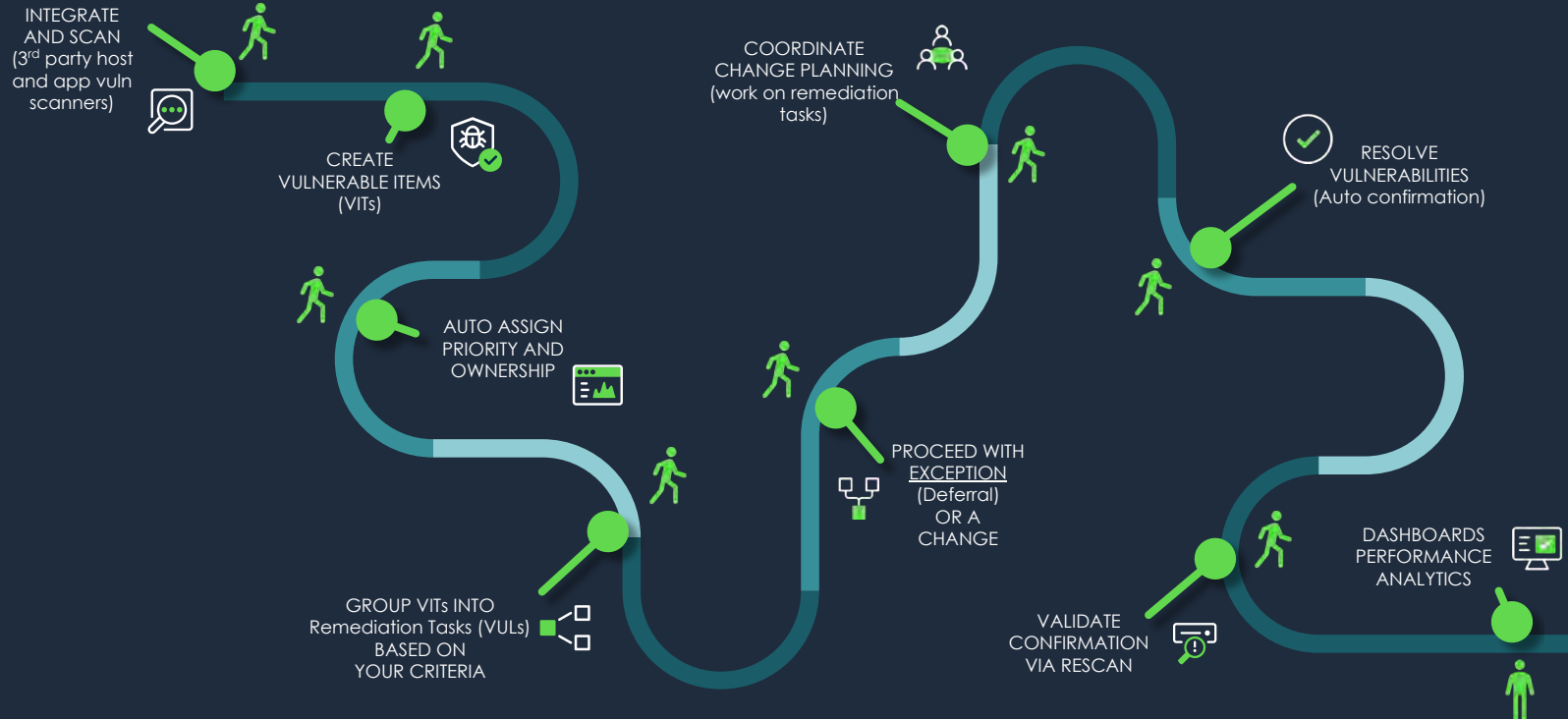


Vulnerability Response Overview



Vulnerability Response Overview

Vulnerability Response High Level Process



AUDIENCE POLL

What tool are you currently using to manage Vulnerability Response?

- (A) ServiceNow – We like our vulnerability data smart, centralized, and automated.

- (B) Tenable, Qualys, or Rapid7 – We scan hard, then spreadsheet harder.

- (C) Excel and hope – It's held together with tabs, macros, and willpower.

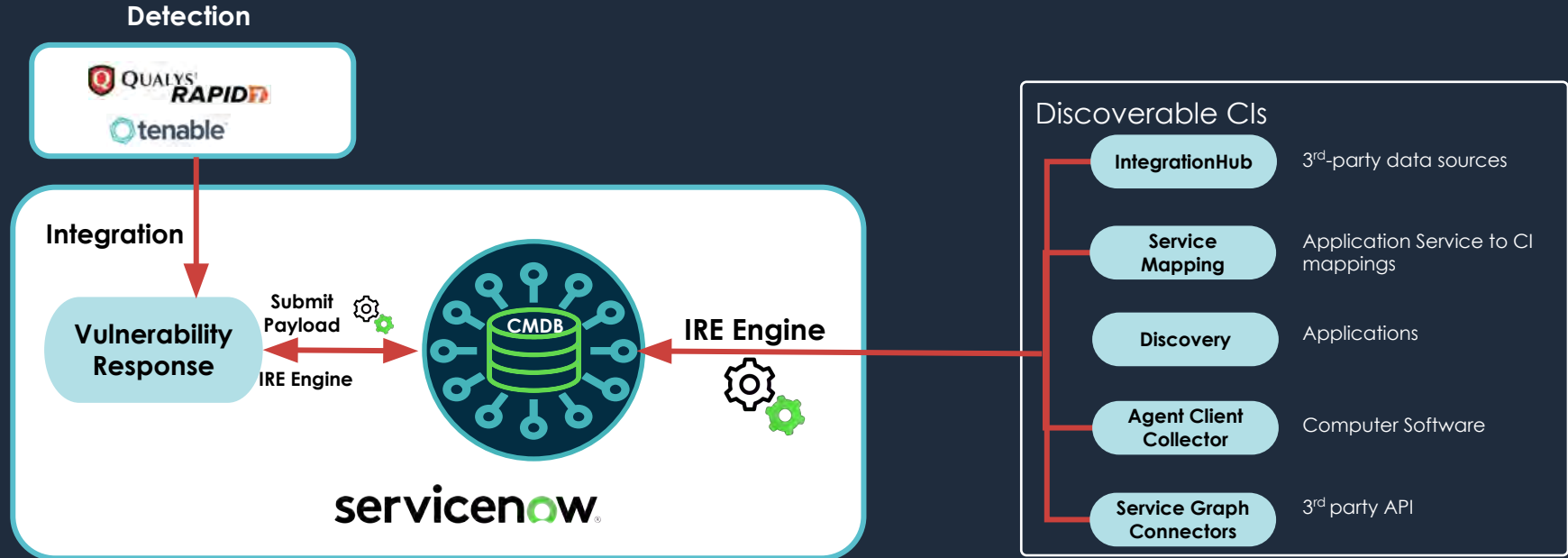
- (D) Other – Tell us what magical chaos you're using.

Vulnerability Response & the CMDB



Vulnerability Response Overview

High Level VR and CMDB



Vulnerability Response automatically uses integration data to search for matches in the CMDB. It does this using **Lookup Rules**. These rules identify applications for the application vulnerable item (VI) record to aid in remediation.

Vulnerability Response & CMDB

Situation – Complexities – Questions – Recommendations (SCQR).

Situation

ServiceNow Vulnerability Response connects external scanners (e.g., Qualys, Tenable) to the CMDB to auto-generate and group vulnerability tickets by fields like “Owned by” or “Supported by” for targeted remediation.

Complexities

- Messy CMDB: Missing/incorrect ownership or relationships lead to mislinked vulnerabilities and wrong assignments.
- Scanner Noise: Unfiltered, low-risk findings flood the system and overwhelm teams.
- Bad Reporting: Misassigned tickets skew SLAs, audit prep, and executive metrics.

Question

How can organizations keep vulnerability data accurate, actionable, and aligned with remediation workflows?

Recommendation(s)

CMDB Alignment:

- Normalize ownership
- Fix relationships
- Integrate discovery
- Ensure “Owned by” / “Supported by” fields are consistent

Scanner Optimization:

- Suppress low-priority vulnerabilities
- Filter false positives
- Scope scans by asset/severity

Smarter Assignment:

- Use dynamic rules
- Trust CMDB data for group filters

Clean Reporting:

- Build KPIs around accurate grouping and assignment
- Ensure dashboards reflect true risk and remediation progress

AUDIENCE POLL

When a vulnerability alert hits your team, what happens next?

- (A) It's instantly routed, triaged, and assigned—like a well-oiled machine.

- (B) We gather in a war room, argue over CI ownership, then punt to another team.

- (C) Someone screams, “Who owns this server?!” and it goes into a black hole.

- (D) Nothing. It becomes one with the backlog... forever.

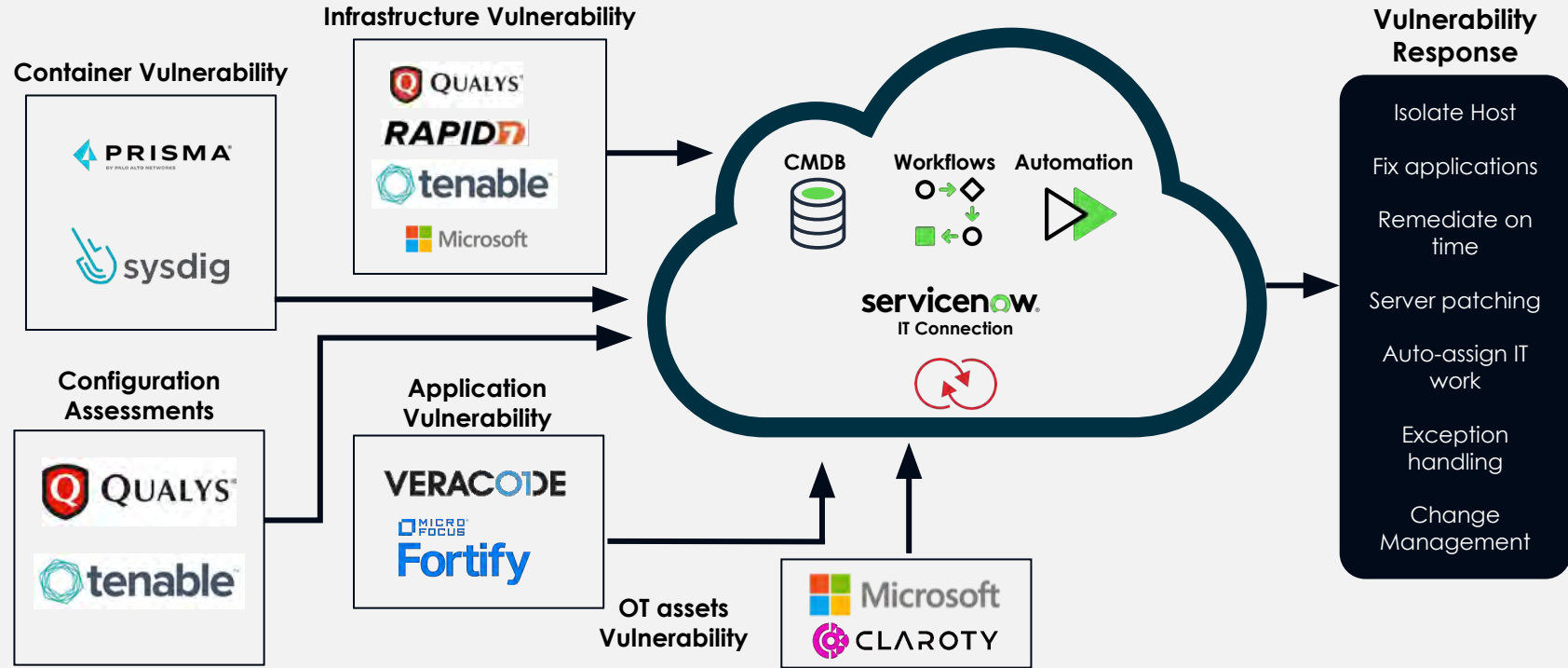


Integrations

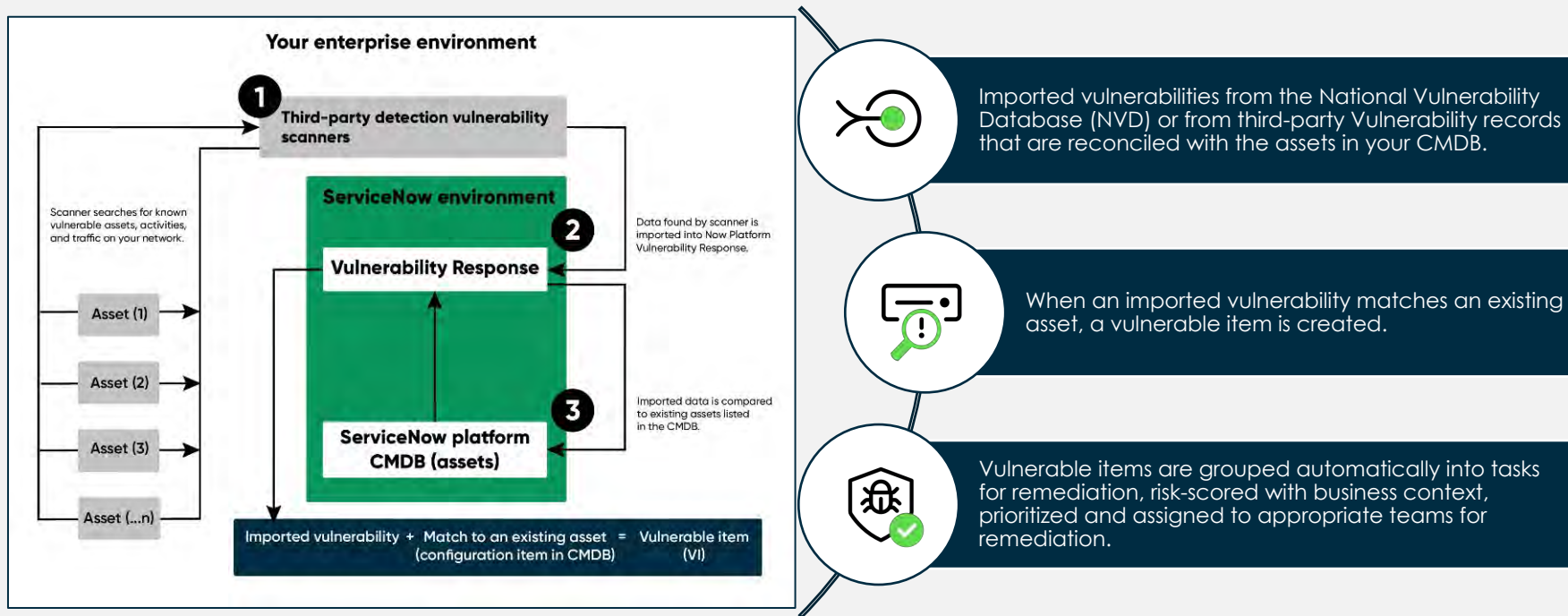


Vulnerability Response Overview

ServiceNow Vulnerability Integration Architecture



Third-party Integrations Process



Vulnerability Response Integrations

Integrations

Vulnerability Response includes support for third-party integrations

- Setup one or many integrations for VR
- The input you provide populate the integration jobs and determines their schedule
- More advanced control and tuning is provided in the integration jobs

Functionality	Integration
Vulnerability Enrichment	<ul style="list-style-type: none">• NVD• Shodan• CISA Known Exploit Vulnerability• First.org EPSS
Infrastructure	<ul style="list-style-type: none">• Qualys• Rapid7• Tenable• Microsoft Defender TVM
Patch Orchestration	<ul style="list-style-type: none">• HCL BigFix• Microsoft SCCM
Solution Management	<ul style="list-style-type: none">• Microsoft• RedHat



More
information



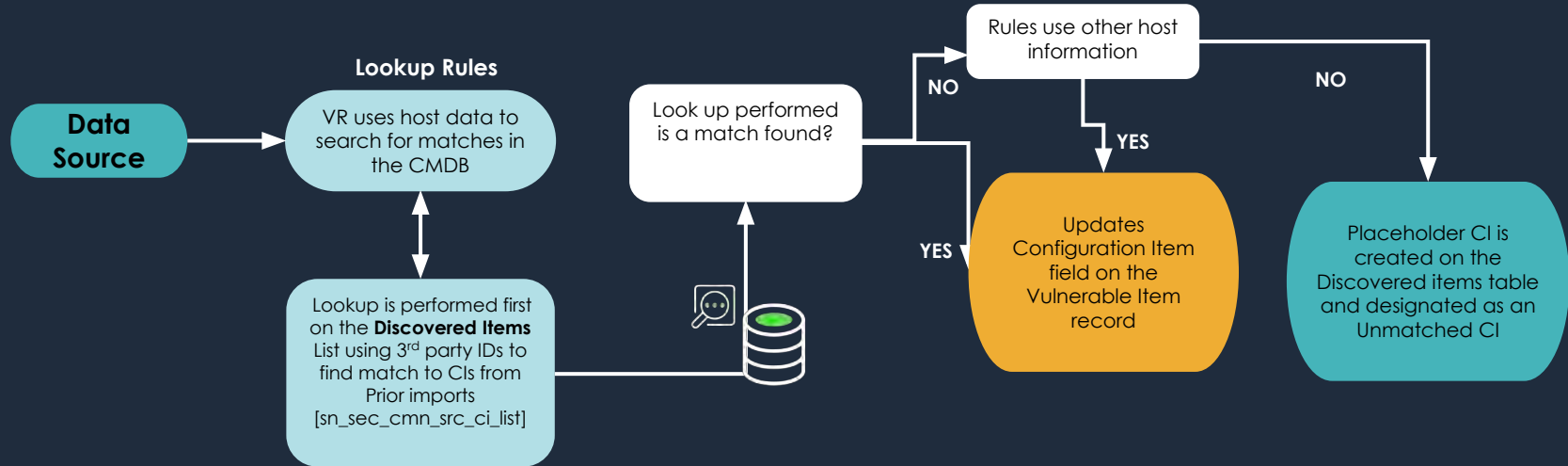
Lookup Rules

Discovered items, Vulnerable items, CI Matching



Vulnerability Response Lookup Rules

Identify Vulnerable Items



Unmatched CIs

Configuration items (CIs) are automatically matched to CIs in the Configuration Management Database (CMDB) when they are imported. By default, the Security Operations > CMDB > Discovered Items module lists those configuration items without a match.

If the Identification and Reconciliation engine (IRE) is activated, the reclassify option from discovered items is not supported.

- Review these records to identify patterns and adjust your CI lookup rules accordingly.
- Consider creating new CIs or updating existing ones to better represent your discovered item

AUDIENCE POLL

How would you describe your current vulnerability response process?

- A "It's tight! We catch threats before they blink."
- B "We do our best and patch fast-ish."
- C "It's chaos. Tickets rain down like glitter at a toddler's birthday party."
- D "Vulnerability response? Oh, is that what we should be doing?"

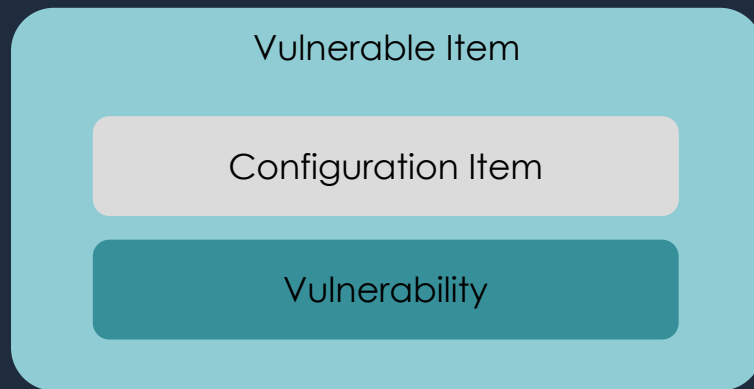
VR Ticket (VIT) Creation



Vulnerability Response Vulnerability Items (VIT's)

Vulnerable Item (VI)

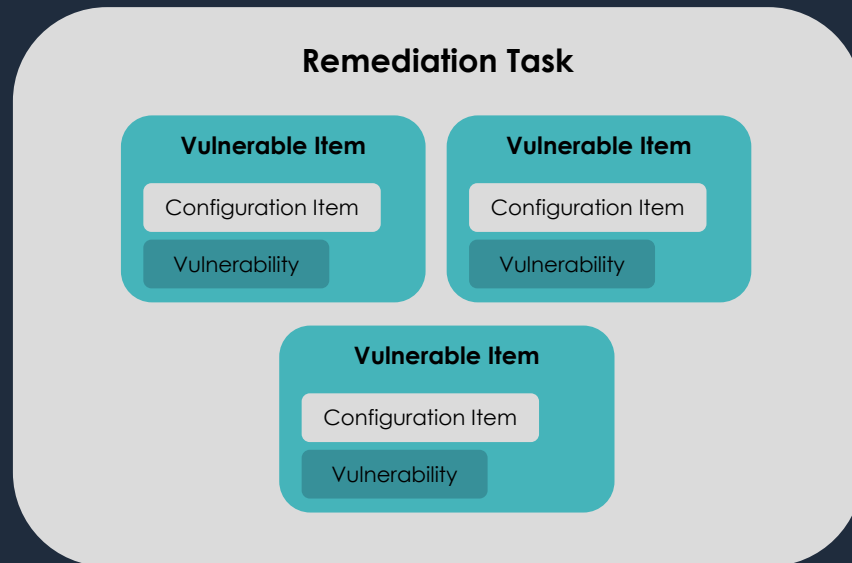
- Identified vulnerabilities discovered by a vulnerability scanner/management tool loaded into ServiceNow's Vulnerability Response application creates Vulnerable Item records
- A **Vulnerable Item (VI)** represents a **Vulnerability** paired with a **Configuration Item**
 - The **Vulnerability** is the finding from a particular third-party vendor (Rapid7, Qualys, Tenable, etc.)
 - The Configuration Item will be the asset (host or application) that the vulnerability was found on



Vulnerability Response Remediation Tasks

Remediation Task (RT)

- As Vulnerable Items are created in ServiceNow, they are strategically grouped into Remediation Tasks (formerly Vulnerability Groups) based on common elements that they share
- A Remediation Task is a single unit of work for a Remediation Owner, commonly a collection of Vulnerable Items with the same vulnerability assigned to an assignment group



Vulnerability Response Remediation Types



Manual Process

- Grouped into a task
- Assigned to a remediation group
- Change request s may be created
- Deliberately patched

Manual patching - Does not scale



Automated Patching

Automated patching is done by IT:

- Microsoft Patch Tuesday
- *nix routine patches

VIs are detected, and imported, all but the most critical are left to be automatically patched.

- Monitoring and manual work for exception cases
- Matches IT workflow



Zero-Day and Company Initiative

- High Priority Emergencies
- Internal company initiative or new regulation, guideline or standard compliance
- A set of VI are targeted for high priority remediation
- Tasks are created
- Remediation process is driven and closely monitored by analysts



Intelligent Patching Remediation

A vulnerability is analyzed before patching to see if there is actual risk in the environment – if settings or a firewall neutralize this vulnerability, the VIs may be deferred indefinitely

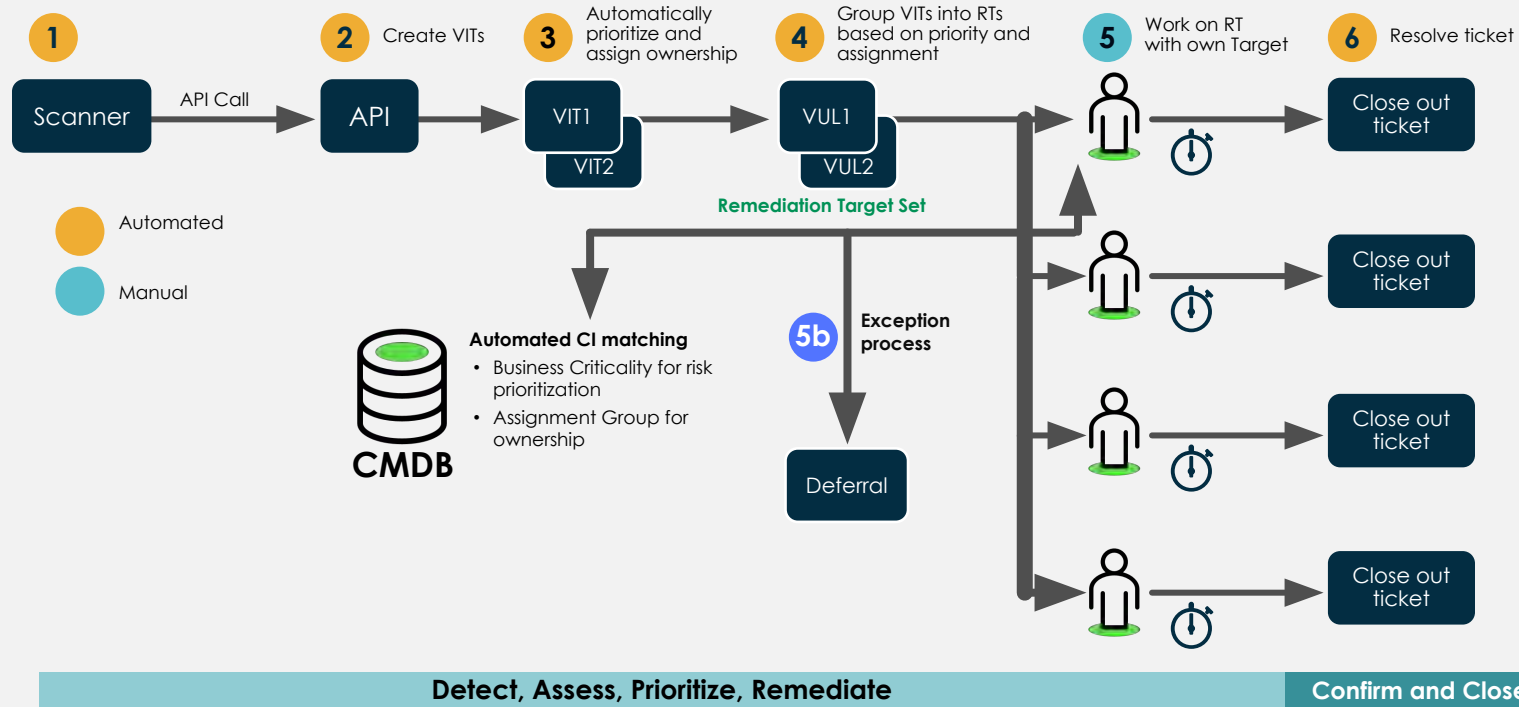
Available with
higher level
licensing

VR Workspaces & Lifecycle



Vulnerability Response Remediation Ticket Lifecycle

Response and Remediation Task Process



Real-time reporting for vulnerabilities, patch status, etc.

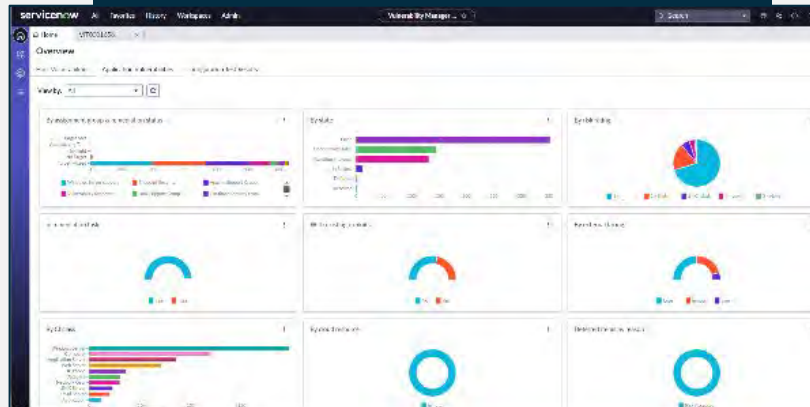
Vulnerability Response Workspaces

Workspace Experiences

“Let’s decide what to remediate”

Vulnerability Manager Workspace

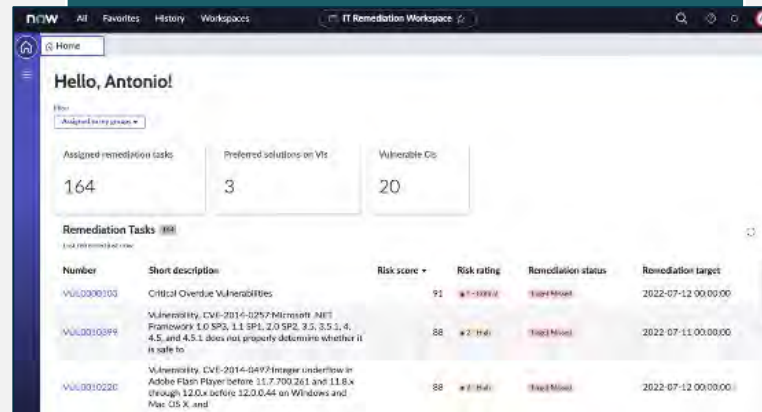
- **Watch Topics:** Enable Vulns Managers to monitor vulns/test results care about
- **Remediation Efforts:** Decide strategically which Remediation tasks to send to IT to work on



“Just tell me what I need to do”

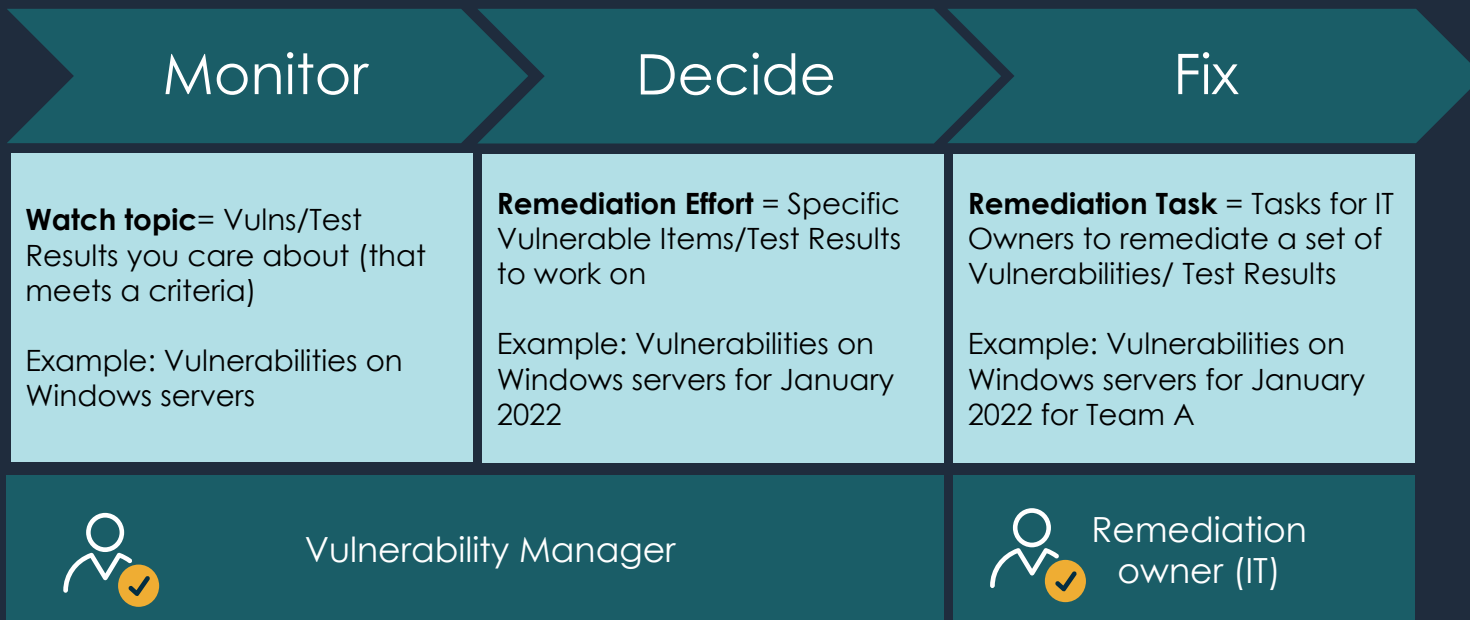
IT Remediation Workspace

- **Remediation Tasks:** Assigned tasks highlight IT-centric information (Solutions, CIs). Assign to IT Teams
- Easy actions for IT (Change, Exception, Rescan)



Vulnerability Response Options/Paths

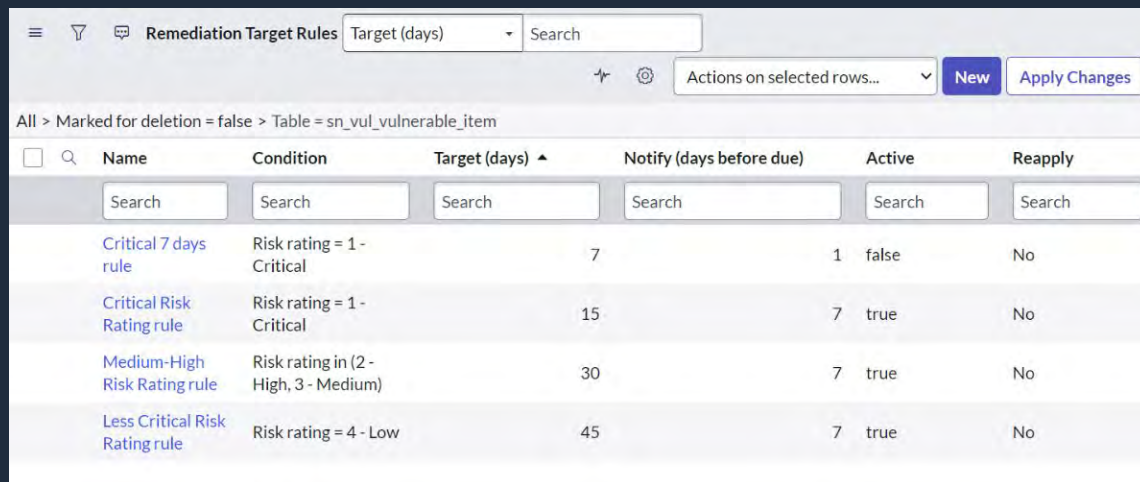
Workspace Workflow



Vulnerability Response Remediation Targets

Deadlines: Remediation Targets

Remediation Target rules are used to define a **Remediation Target** for a Vulnerable Item. The nearest date on the Vulnerable Items in the Remediation Task determines the Remediation Task's Remediation Target date.



The screenshot shows the 'Remediation Target Rules' management interface. At the top, there's a header with a menu icon, a filter icon, a chat icon, the title 'Remediation Target Rules', a dropdown menu set to 'Target (days)', and a search bar. Below the header, there are icons for a refresh and a settings gear, followed by an 'Actions on selected rows...' dropdown, a 'New' button, and an 'Apply Changes' button. The main content area shows a table with the following columns: Name, Condition, Target (days), Notify (days before due), Active, and Reapply. Each column has a search input field. The table contains four rows of rules:

Name	Condition	Target (days)	Notify (days before due)	Active	Reapply
Critical 7 days rule	Risk rating = 1 - Critical	7	1	false	No
Critical Risk Rating rule	Risk rating = 1 - Critical	15	7	true	No
Medium-High Risk Rating rule	Risk rating in (2 - High, 3 - Medium)	30	7	true	No
Less Critical Risk Rating rule	Risk rating = 4 - Low	45	7	true	No

These rules are created by the VM/implementation teams usually determined by compliance requirements

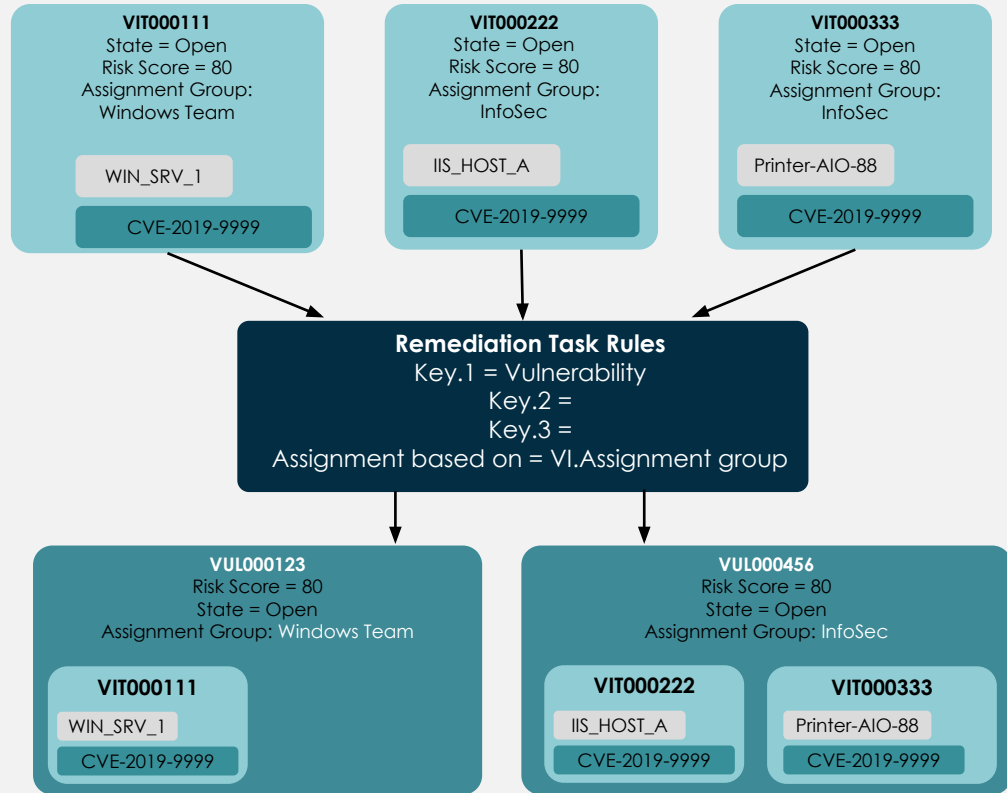
Vulnerability Response Remediation Tasks

Remediation task rules

Remediation Task Rules define how VIs are automatically grouped together as they are imported

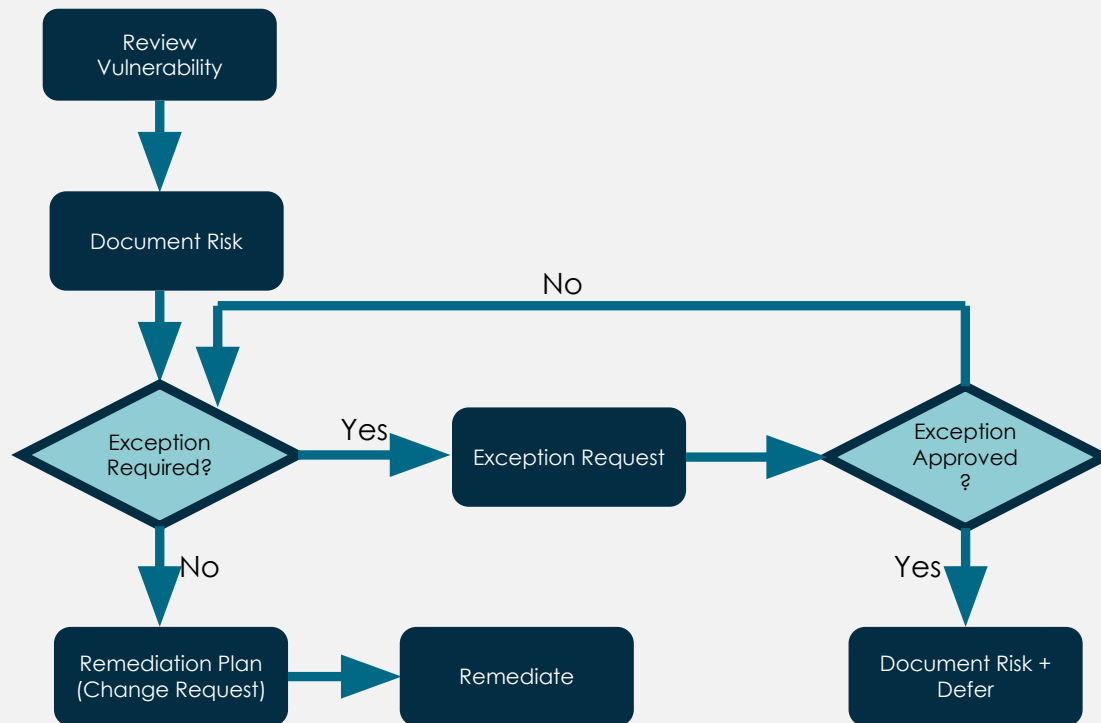
The vulnerable item (VI) assignment group is used in addition to the Group By Keys to group vulnerable items

Define your rules so that all vulnerable items in a remediation task are remediated by the same team, same remediation action, and within the same timeframe, based on your configuration item (CI) environment (ex. production vs. test servers)



Vulnerability Response Change Management

Change Management + Remediation



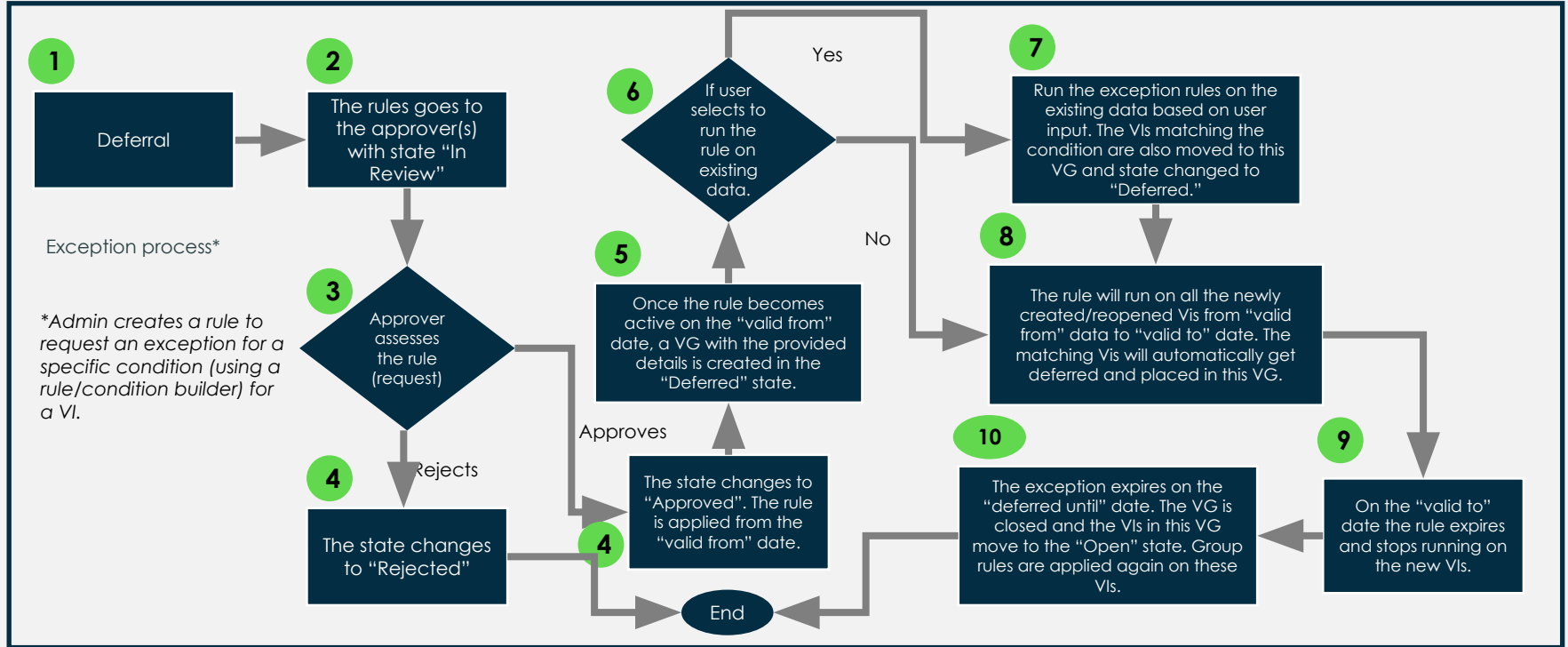
Recommended Actions and Remediation Plans are expressed in *Change Requests*.

Changes are initiated against Remediation Task, not Vulnerable Items.

Vulnerability Response Approval Rules (Exceptions)

Deferral (Exception) Process

Remediation Specialist

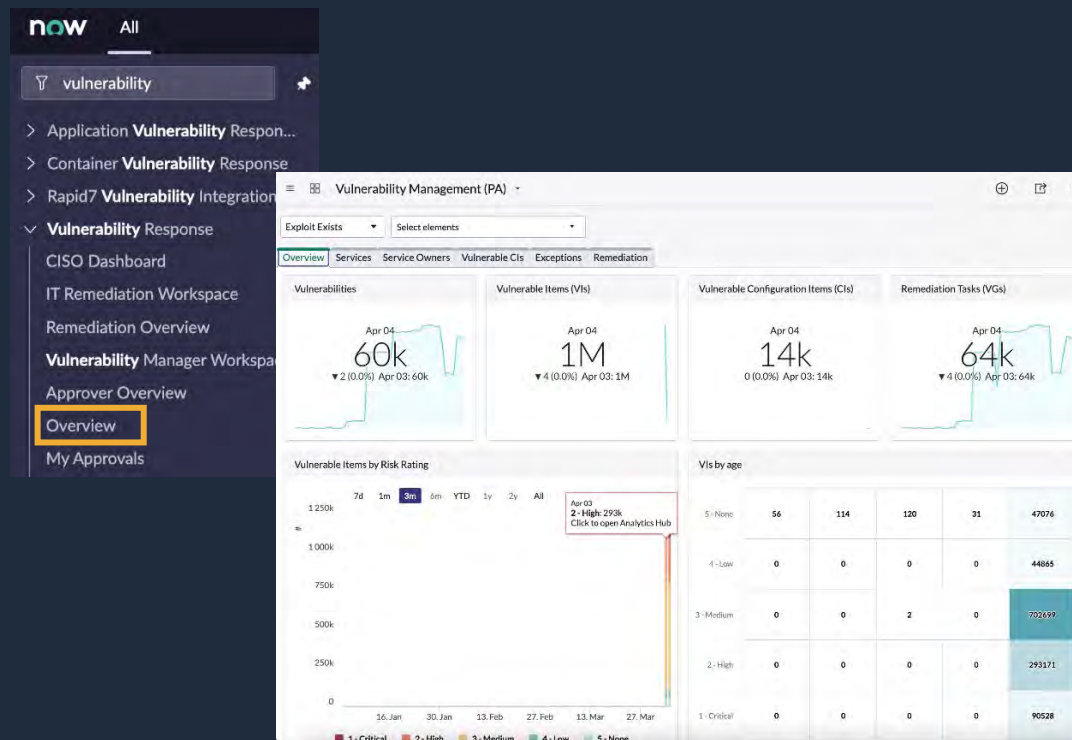


Reports & Dashboards



Vulnerability Response Performance Analytics

Performance Analytics (PA) Reporting (PAR)

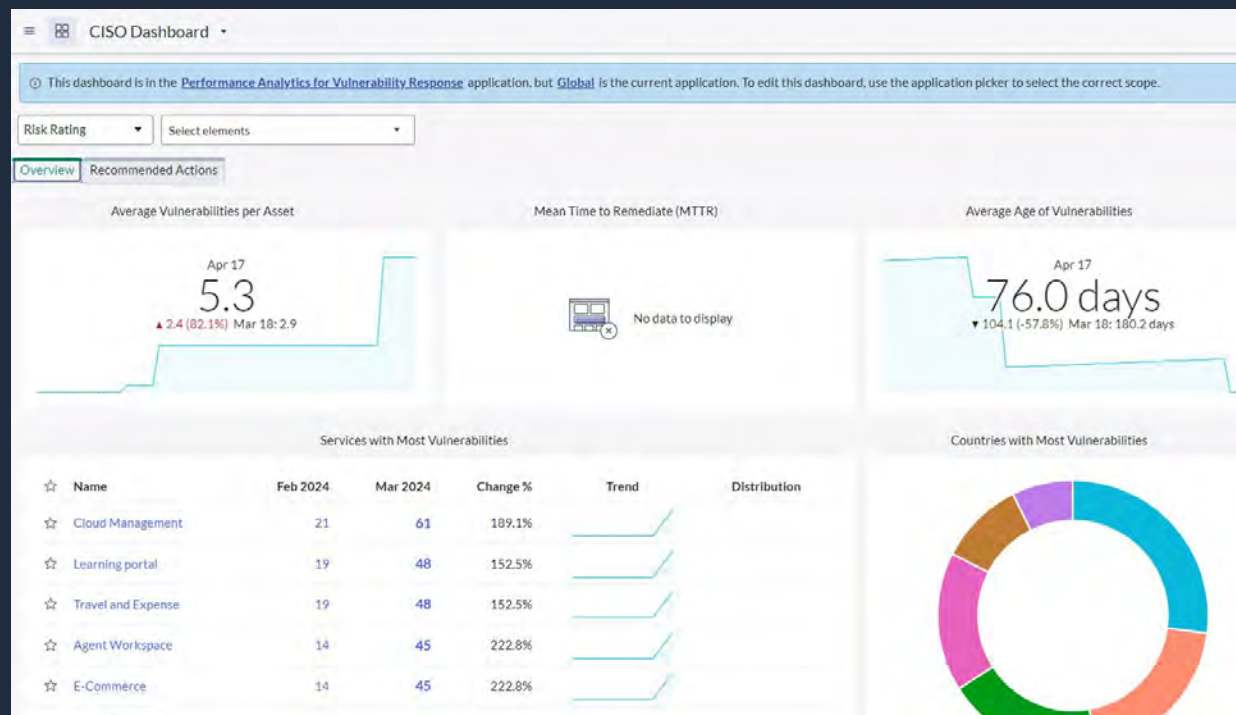


Provides and OOB Vulnerability Management dashboard for trending and analysis for:

- Analyst
- Manager
- C level reporting

Vulnerability Response Dashboards

CISO Dashboard



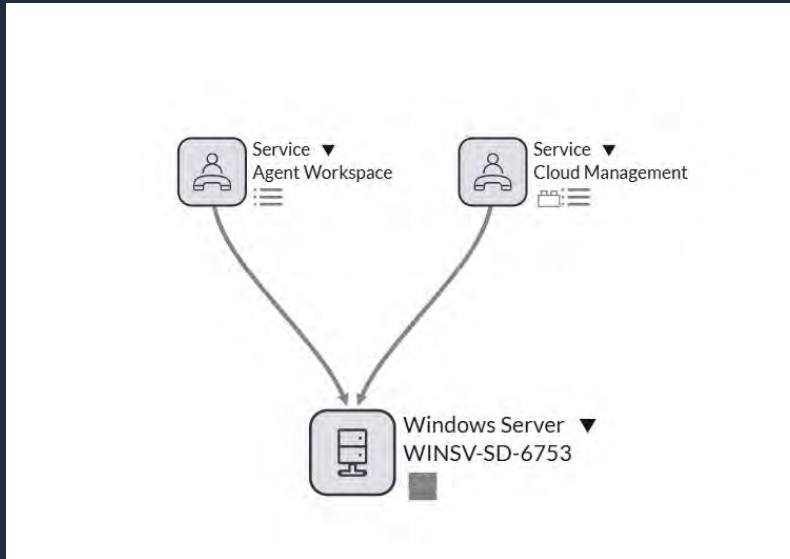
With the Vulnerability Management CISO dashboard, view data such as Key Performance Metrics (KPIs) for vulnerability remediation, see the highest risks, verify scan coverage, and learn how to lower risks

Use the top-level filters to filter reports by Risk Rating, Age Range, or Internet Facing. Some reports display trending data over a period.

Configuration Item (CI) Impacts



Impacts on Related CIs



Use the Dependency View to determine configurations items up and downstream from vulnerable items to determine total impact.

Impacts to Services


The screenshot displays the ServiceNow SAP Administration interface. At the top, there's a navigation bar with 'SAP Administration' and a 'Now' button. Below this, a timeline shows dates '2025-07-09 16:28' and '2025-07-16 15:20'. A central diagram shows a service map with components like 'QA-ORCLE-SD', 'LINUX-DAL-43', 'DEV-LINUX-ATL', 'MYSQL-SD-68', 'DEV-MYSQL-A', 'ORCLE-DAL-21', and 'DB-CH-17'. A 'Properties' panel on the right shows details for 'Application Service', including 'Operational status: Operational', 'Created: 2019-02-02 02:20:12', and 'Name: SAP Administration'. At the bottom, a table lists 'Vulnerable Item' details.

Number	Summary	Configuration Item Name	Risk score	Risk rating	State	Remediation target	Remediation status	Assignment group	Assignee
VIT0002964	The crypto.generateCRMRequest function ...		100	1 - Critical	Open	2025-07-31 05:21:08	In-flight	Vulnerability Response	Kevin
VIT0003058	NDProxy.sys in the kernel in ...		75	2 - High	Open	2025-07-31 05:21:08	Target Missed	Database Security	Henr

If Service Maps exists, you can view the impacts of vulnerable items across your IT landscape to determine business impacts

Support Data Completeness

Most Vulnerability Tools can send data to the CMDB as a Discovery Source, allowing for better data reconciliation as well as additional CI Verification

Preview Data			
 Attribute	CMDB Value	ACC-Visibility ▼	SG-Tanium
Name	mysql-server01	mysql-server01	ip-172-31-81-116
Host name	mysql-server01	mysql-server01	mysql-server01
Created by	midserver	midserver	
Updated by	midserver	midserver	
Firewall status	Intranet	Intranet	
CPU name	Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz	Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz	Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz
CPU type	Intel(R) Xeon(R) CPU E5-2686 v4	Intel(R) Xeon(R) CPU E5-2686 v4	GenuineIntel
Hardware Status	installed	installed	installed
Object ID	i-003b33d0b13de3a42	i-003b33d0b13de3a42	i-003b33d0b13de3a42
Category	Hardware	Hardware	

Getting Started Is Easy!

We can meet you where you're at in your Event Management journey.

Want a quick CMDB assessment
and rapid remediation?



CMDB
LAUNCHPAD

Need to implement CMDB and
see value fast?



CMDB
ESSENTIALS

Ready to get started with
Vulnerability Response Essentials?



VR
ESSENTIALS

Tell us what CMDB topics you
want to learn more about!

Look for a survey following this session

CMDB MasterClass Part 10:
Your CMDB Foundation for AI
scheduled for September 10.

Look for an invite soon!



CMDB & AI

Your CMDB
Foundation for AI



Join our next **ITAM MasterClass**
in September!

Questions?





Thank you!

Questions? Email: inbound@casknx.com

