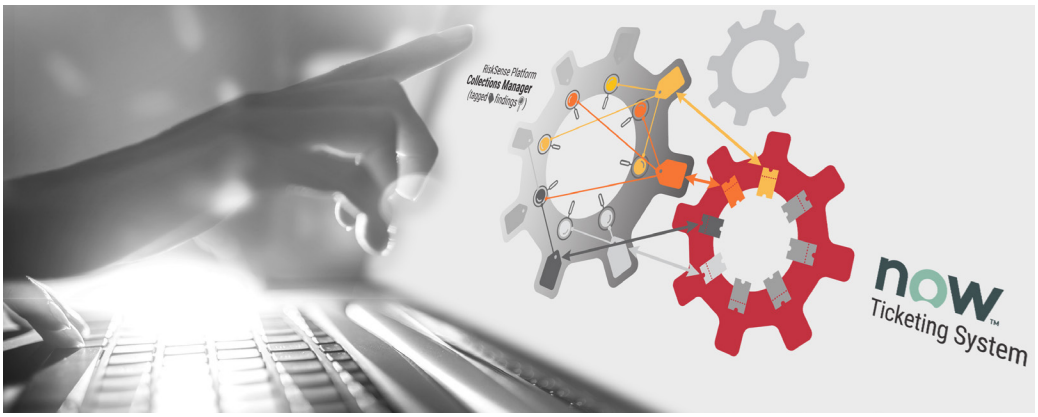
TECHNOLOGY BRIEF
ServiceNow Service Request

ServiceNow Service Catalog Enhanced with Flexibility and Prioritizes Remediation Efforts with RiskSense Integration

SERVICENOW SERVICE CATALOG

ServiceNow makes work better across the enterprise. Keep employees productive by ensuring business continuity with streamlined IT services and operations. ServiceNow Service Catalog automates workflows and approvals to enable organizations to improve the customer experience, accelerate service delivery and reduce operational costs. Gain operational efficiency with accurate information, speedy process execution, and no more duplicated effort.



THE CHALLENGE

Distributed and diverse groups manage IT infrastructure and the policies that define assignments, workflows, and change approvals. Vulnerabilities found across an organization's infrastructure, critical ones to regular security hygiene, requires workflow and remediation assignment flexibility. Vulnerability remediation activities have to be accepted, verified, and tracked. A diverse set of actions, information, and collaboration occurs between IT and security teams. Organizations have to continuously shift resources to keep focus on what matters the most. However, complexity, changing risk levels, and lack of clarity on vulnerability remediation projects hinder resource effectiveness and efficiency in addressing cyber exposure.

RiskSense makes it easy to integrate into the powerful ServiceNow Service Catalog. Organizations can create their service request items with the necessary fields and workflows and have RiskSense bi-directional vulnerability priority and status automatically update these tickets. One service request type cannot solely address the unique workflows needed for vulnerability management across an enterprise organization. RiskSense has integrated with ServiceNow to enhance the flexibility of Service Catalog to address the needs for vulnerability prioritization and resource management. From within RiskSense, a service request ticket can be created that spans multiple types of assets, groupings of vulnerabilities, or based on asset ownership and project initiatives. Customization is easy ensuring that the business focus and IT flow requirements are followed. RiskSense connector configuration allows parameters for what data should be constant and what data can be automatically updated by RiskSense, working within the business set of pre-defined fields to conform to the templates and workflows needed for each service request ticket type.

Flexibility is achieved through the use of RiskSense tagging that allow multiple system findings to be grouped to match your security remediation goals and service request ticket operational models. These tags can be locked to a set of vulnerability findings or set to active groups allowing for additional assets to be added to an open service request as new vulnerabilities are found. The unique aspect of the integration is the ability to have the current status of vulnerability projects automatically updated within ServiceNow.

The combined solution provides Prioritization of Remediation Efforts

USE CASES

Predicting the Most Likely Threats to Prioritize

RiskSense provides the capability of assessing the vulnerabilities within your environment that have weaponized exploits or malware, and capable of remote code execution. Beyond vulnerability management, this risk prediction hones in on the threats that are most likely and capable of causing cyber exposure to your business. From the built-in RiskSense filters and ServiceNow Service Request integration remediation projects can be quickly created to align to IT sprints and workflows. Projects can follow an agile methodology, allowing them to be updated with new vulnerability remediations that have come to light and identify prsistent issues that were not addressed. These projects continually reflect on what RiskSense identifies as the highest risks and highlight the ever-changing threat nature. Updates on the progress of the remediation are reflected within ServiceNow.

Workflow for Closed-Loop Verification for Security and IT

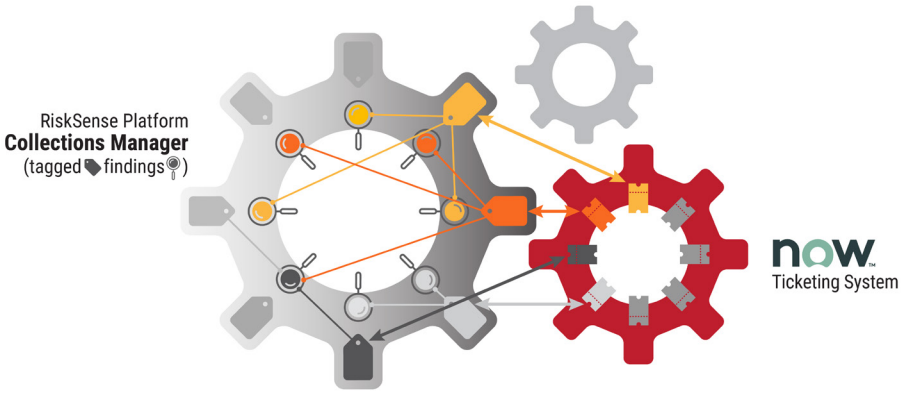
With vulnerability management a multi-step verification process is necessary, ensuring that the IT activities are completed for the remediation and then a security assessment or scan performed for confirmation. With RiskSense, security teams can use tags to create ServiceNow Service Requests as defined by the organization. The flexibility of RiskSense integrated with Service Request provides the ability to:

- Create a Service Request with multiple assets that have similar security remediation tasks by creating a tag group within RiskSense Collections Manager
- ServiceNow Service Request automatically routes the work to the appropriate teams
- Bi-directional updates allow both Security and IT teams to see current status on the number of vulnerabilities and percentage of activities completed
- ServiceNow can be configured to open a Service Request related sub-task for a rescan or security assessment of the associated assets for the ticket
- RiskSense updated with the latest scan data will automatically track and update the vulnerability assessment risk. Security teams can easily verify and confirm remediation and close the ticket

The combined solution provides Prioritization of Remediation Efforts

Active Continuous Security Updates to a Single Service Request

The integration between ServiceNow and RiskSense provides the ability to update a single Service Request with new vulnerability information. Use this feature to allow for a single focus on the most important remediation efforts or set up active workflows based on asset types, business units, risk levels of vulnerabilities or other filtered criteria. As new assets or vulnerabilities are uncovered that meet the set criteria, they can be tagged within RiskSense and automatically added to open Service Request tickets for this focus. Updated status on the work effort completed and number of vulnerabilities resolved can be seen in either RiskSense or within ServiceNow. Effectiveness can now be measured based on remediation effectiveness and not just to number of tickets closed.



RiskSense platform integration with ServiceNow Service Request allows many ways of defining remediation tasks, associating asset vulnerability findings, and directing ticket assignment to the appropriate stakeholders:

- Remediation teams can create tickets for one or more findings giving them the flexibility to group based on organizational needs and priorities
- Users can create and manage tags from the RiskSense Collections Manager and then open corresponding Service Request ticket types
  - Assets can have multiple types of tags allowing for flexibility to address multiple vulnerability remediation types
  - Tags can be associated with multiple selected criteria to best align to IT workflow and security remediation goals
  - Tags can be locked to allow for a specific set of vulnerabilities to be associated with the creation of a Service Request ticket
  - Tags can be active allowing for the continuous update of an open Service Request ticket to reflect the most up to the moment vulnerability findings indicated by Security teams

RiskSense and ServiceNow Service Request integration takes collaboration between security teams and IT teams to the next level, enhancing the investments of your IT service platform and your vulnerability scanner technologies. The outcome enables the most efficient use of resources for end to end security and IT and a more effective way to address cyber risk and vulnerability management across complex organizations.

The combined solution provides Prioritization of Remediation Efforts

ABOUT RISKSENSE

RiskSense®, Inc. provides vulnerability prioritization and management to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense.

RISKSENSE®

Contact us today to learn more about RiskSense

RiskSense, Inc. | +1 844.234.RISK | +1 505.217.9422 | risksense.com

CONTACT US | SCHEDULE A DEMO | READ OUR BLOG