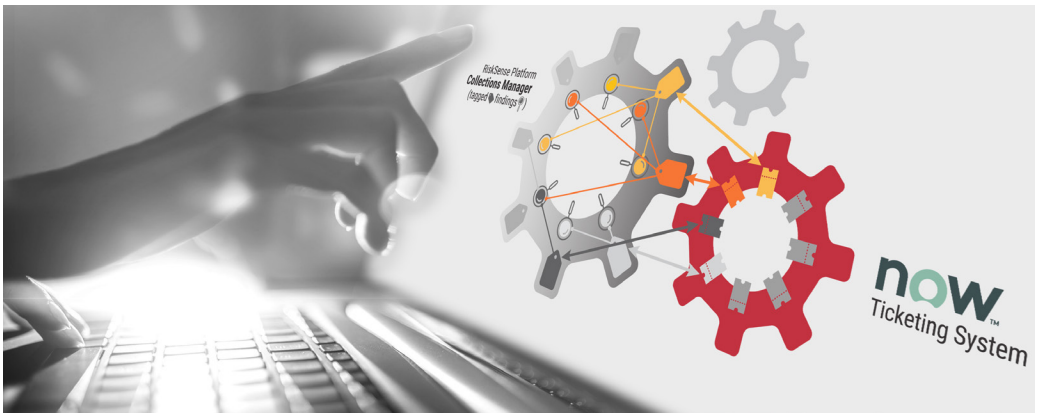
TECHNOLOGY BRIEF
SeviceNow Incident Management

ServiceNow Incident Response Enhanced with RiskSense's Prioritization to Focus Findings for Fast Vulnerability Remediation

SEVICENOW INCIDENT MANAGEMENT

ServiceNow makes work better across the enterprise. Keep employees productive by ensuring business continuity with streamlined IT services and operations with ServiceNow Incident Management. Create incident tickets, use actionable information and proven practice workflows to resolve issues quickly. Also improve transparency and satisfaction with easy end-user access to bi-directional communications, status, and work-related activities. Getting complex multi-step tasks completed can be painless.



THE CHALLENGE

Remediation is hard enough, especially when the volume of work continues to expand because incident tickets have been traditionally focused on assigning efforts toward individual systems. Looking at vulnerabilities and remediation priorities from the viewpoint of what is affected vs. organizing them based on the most effective way to coordinate IT efforts. It's not uncommon to encounter multiple required remediation actions on a single system, or a single remediation action that spans hundreds of systems. It's no longer effective to consider vulnerability findings individually and create corresponding incident response tickets. Vulnerability management needs a smarter way, beyond just integrating and opening incident tickets, to help IT resources keep focus on what matters most. They need the most useful information at hand and want the removal of administrative overhead that can slow them down.

RiskSense has integrated with ServiceNow to provide a smarter way Security and IT teams can collaborate on the management of IT. The RiskSense platform and ServiceNow Ticketing System integration is bi-directional giving updates throughout the remediation process. Users are informed within their preferred system (whether it be the RiskSense platform or the ServiceNow interface).

Workflow focus is achieved through the use of tags that allow for multiple system findings to be grouped to match your security remediation goals. This results in intelligent workflows that make IT and Security more efficient and effective at addressing remediation priorities. Organizations can now group and create incident tickets based on how their teams are structured, or on the importance of the remediation efforts, or the potential operational impact of the remediation activities. They can customize the best way for them to approach and resolve cyber exposure. Details about vulnerabilities, patches, severity, and available exploits can be easily accessed with status updates from remediation activities.

Any number of items can be associated with a RiskSense tag and then subsequently used to create a ServiceNow Incident ticket. This allows asset findings to be involved in more than one incident ticket which is a current common constraint of simple integrations.

The combined solution platform provides industry leading accuracy to the findings.

USE CASES

Expedite workflow for critical assets

A user can create one ticket, assign it to the team responsible for the critical assets, and associate all of the findings for each of these assets. The workflow is focused on critical computing infrastructure, spanning multiple systems and the IT team now has access to the detailed information with all of the findings for the systems involved in RiskSense. Remediation is confirmed when the ticket is closed out and verified with the next vulnerability scan. No chance of delaying or missing critical remediation efforts when work can be consolidated into a single incident ticket.

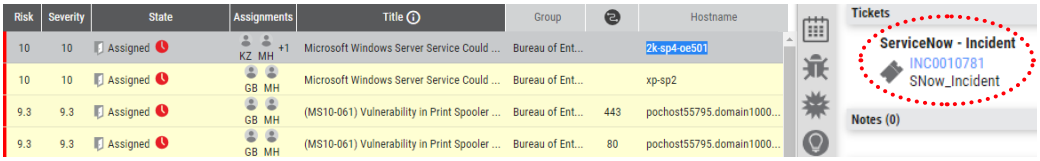
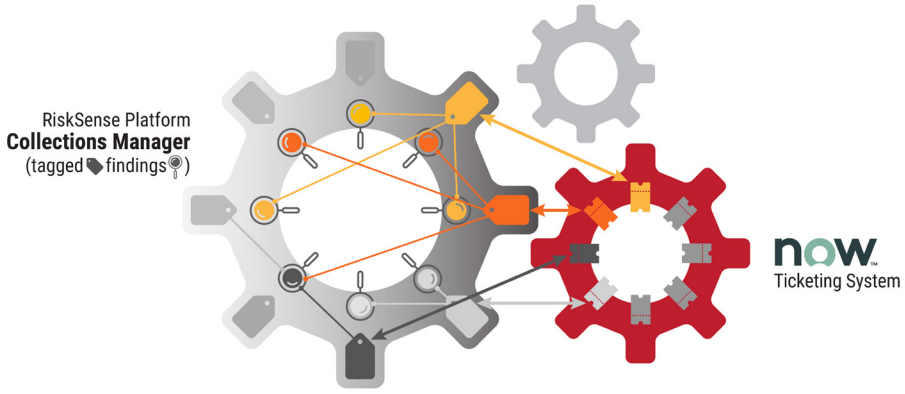


Figure 1. Easily filter and select across multiple assets with various risk rankings to include into one ServiceNow Incident Ticket

Mass remediation across infrastructure

Occasionally a single vulnerability finding needs remediation across a large volume of assets within an organization. The RiskSense platform has a flexible method of selecting and assigning incident tickets by tag which allows asset vulnerability findings to be associated with any number of tickets in ServiceNow. Any asset can be associated with multiple tags from the RiskSense Collections Manager. This many to many relationship removes the constraints of vulnerability management allowing it to adapt to real-world IT workflows. When widespread vulnerabilities occur dedicated project teams can tackle the remediation and easily manage within the incident ticket having a single focus on all of the affected assets.



The combined solution platform provides industry leading accuracy to the findings.

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 Incident Ticketing 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 persistent 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 can be quickly viewed in ServiceNow.

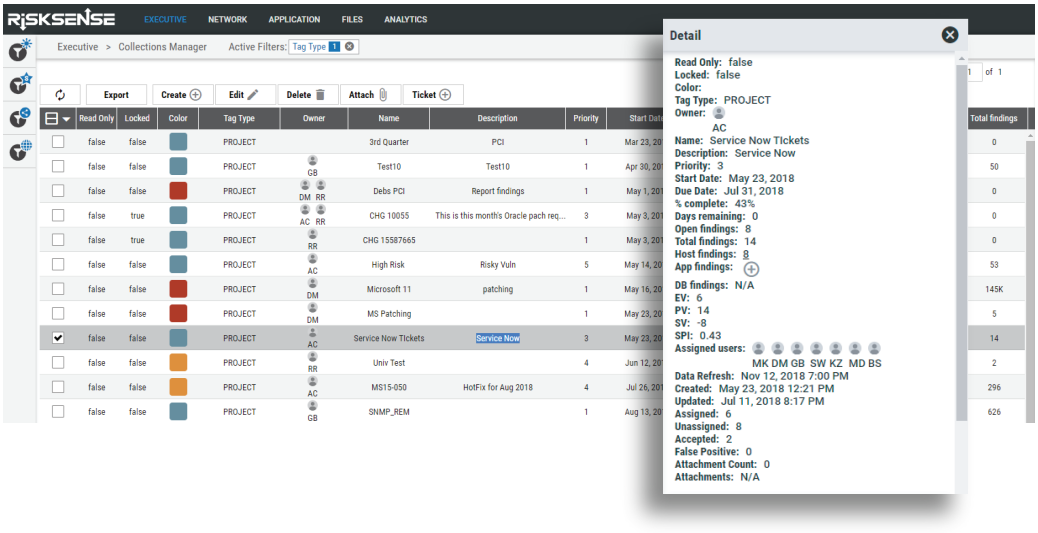


Figure 2. View vulnerability status and remediation completion of Service Now Tickets within RiskSense platform

The combined solution platform provides industry leading accuracy to the findings.

RiskSense platform integration with ServiceNow Incident Ticketing system 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
- Define and manage tags from the RiskSense Collections Manager and then create corresponding incident tickets for ServiceNow
- Users can create incident tickets directly from the RiskSense Findings page, Asset page, or Collections Manager

Responding to incident tickets shouldn't be structured based on how vulnerability management platforms integrate with IT service management systems. RiskSense and ServiceNow Incident Ticket 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 a quicker response to the highest priorities for vulnerability management and in a way that makes sense for your organization.

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