ServiceNow Vulnerability Response

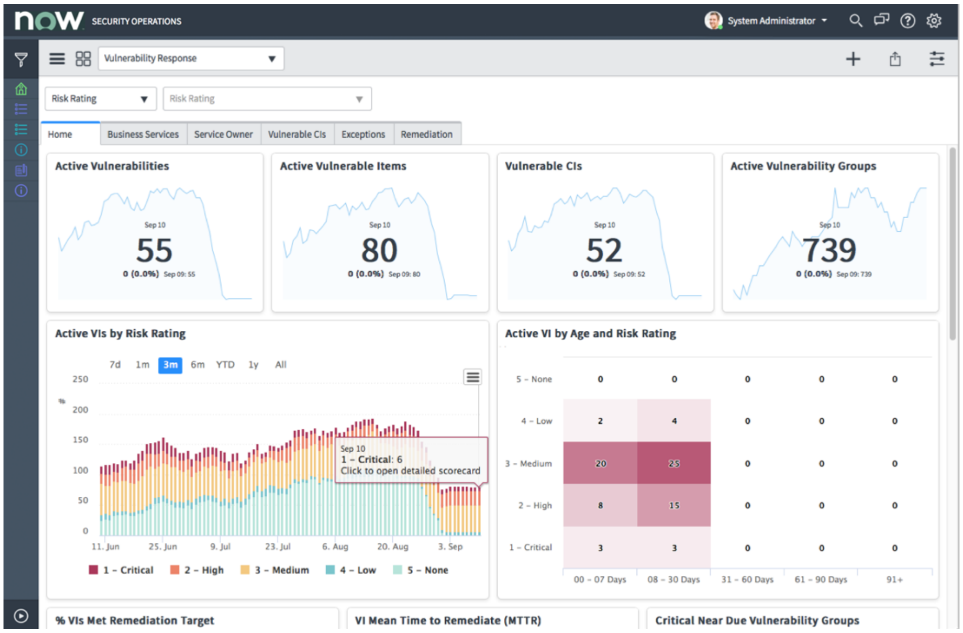
The vulnerability challenge

Vulnerabilities don't often get the same amount of notice as phishing attacks or advanced persistent threats, but when a critical vulnerability is exploited, organizations can suffer major damage. A study conducted by ServiceNow and the Ponemon Institute found that nearly half of organizations surveyed had been breached in the past two years. For many of those, the breach was due to a vulnerability for which a patch existed. However, many organizations have more vulnerabilities than they can effectively keep up with.

In addition to the sheer quantity of vulnerabilities, many organizations also struggle with coordination between security and IT to manage prioritization and patching. The survey showed that an average of 12 days are lost coordinating across teams for every vulnerability patched.[1] When vulnerability response is handled via spreadsheets and email, it's hard to get up-to-date visibility on the organization's current risk exposure.

The ServiceNow solution

ServiceNow® Vulnerability Response is an application that helps organizations respond faster and more efficiently to vulnerabilities, connect security and IT teams, and provide real-time visibility. It connects the workflow and automation capabilities of the Now Platform® with vulnerability scan data from leading vendors to give your teams a single platform for response that can be shared between security and IT.



Sep 10
1 – Critical: 6
Click to open detailed scorecard

	00 – 07 Days	08 – 30 Days	31 – 60 Days	61 – 90 Days	91+
5 – None	0	0	0	0	0
4 – Low	2	4	0	0	0
3 – Medium	20	25	0	0	0
2 – High	8	15	0	0	0
1 – Critical	3	3	0	0	0

The Vulnerability Response dashboard highlights the current status and associated risk of active vulnerabilities in your organization.

[1] Ponemon Institute, Today's State of Vulnerability Response: Patch Work Requires Attention, 2018

Benefits

Connect security and IT

Coordinate response across teams for smoother task handoffs between groups and quicker resolution. Get accountability across the organization and know work is getting done with remediation targets.

Drive faster, more efficient security response

Reduce the amount of time spent on basic tasks with orchestration tools. Automatically prioritize and respond to vulnerabilities with workflows and automation.

Know your security posture

View your current vulnerability status with customizable dashboards and reports backed by quantitative data. See which business services are impacted by critical vulnerabilities.

Vulnerability Response provides a comprehensive view of all vulnerabilities affecting a given asset or service through integration with ServiceNow® Configuration Management Database (CMDB), as well as the current state of all vulnerabilities affecting the organization. When used with the CMDB, Vulnerability Response can prioritize vulnerable assets by impact, using a calculated risk score so teams can focus on what is most critical to your business. The risk score can include multiple factors in its calculation, including the CVSS score of the vulnerability and whether the vulnerability can be easily exploited, using data from the vulnerability scanner and Shodan®.

In addition, you can see dependencies or pending changes against an asset for greater context and to reduce downtime. Additional Now Platform capabilities included with Vulnerability Response include skills-based routing, notifications, and live collaboration tools. Remediation targets can be leveraged across teams to improve overall accountability.

Proactive management

Vulnerability Solution Management in Vulnerability Response correlates your vulnerability exposure with solutions to show the most impactful remediation activities for your organization and orchestrates their completion. It works by matching vulnerability scan data against Microsoft's solution database to recommend which ones to deploy based on supersedence. If the preferred solution isn't practical to deploy, you can view alternate solutions to find a hotfix option.

Easily monitor solution deployment to track progress and identify any issues. Solution options are visible to both security and IT to enable teams to choose the best options for a specific environment.

Respond automatically

When critical vulnerabilities are found, Vulnerability Response can automatically initiate an emergency response workflow that notifies stakeholders and creates a high-priority patch request for IT. Once the patch task has been completed, Vulnerability Response can initiate a follow-up scan with your vulnerability management system to confirm the fix. This results in a coordinated remediation strategy for vulnerabilities with the added benefit of visibility across teams.

Not all vulnerabilities are urgent, however, so Vulnerability Response also includes exception handling. Groups of vulnerable items can be deferred until a selected date. When the deferment window expires, the group automatically becomes active again and team members are notified.

Vulnerability Response also improves visibility through reports and dashboards. With ServiceNow® Performance Analytics you can easily see which services are impacted by critical vulnerabilities and which service owners are accountable to better understand your vulnerability risk in terms of your organization's operating structure. Dashboards for the vulnerability manager provide visibility into the organization's risk posture and team performance to quickly identify issues. Trending and predictive analytics can forecast future performance. For the remediation specialist, a separate dashboard displays task prioritization to work on the items that are critical or provide the greatest benefit first.

ServiceNow Security Operations

Vulnerability Response is part of ServiceNow® Security Operations, a security orchestration, automation, and response engine built on the Now Platform. Designed to help security teams respond faster and more efficiently to incidents and vulnerabilities, Security Operations uses intelligent workflows, automation, and a deep connection with IT to streamline security response. Security Operations consists of five applications: Vulnerability Response, Configuration Compliance, Security Incident Response, Threat Intelligence, and Trusted Security Circles.

To learn more about ServiceNow Security Operations, please visit:
www.servicenow.com/sec-ops

servicenow.

SN-DataSheet-ServiceNow-Vulnerability-Response-052919