ServiceNow Vulnerability Response

Protect the growing attack surface

Vulnerabilities pose a serious threat to business reputation and data security. Methods to exploit vulnerabilities are growing more sophisticated, with cybercriminals increasingly leveraging machine learning and artificial intelligence to thwart traditional vulnerability response mechanisms. However, security and IT teams struggle to keep up with the sheer volume of vulnerabilities in an ever-increasing attack surface.

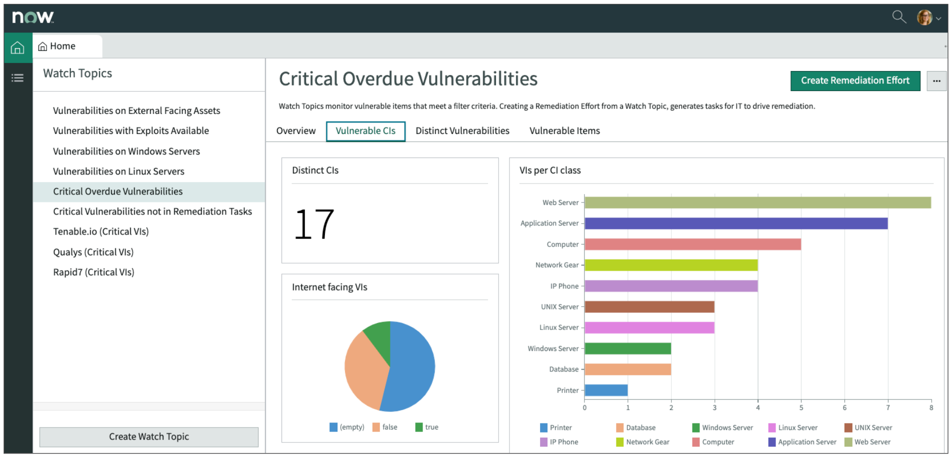
A study conducted by ServiceNow and the Ponemon Institute found that over a third of organizations who suffered a breach already knew they were vulnerable. In many cases, there was an existing patch for the vulnerability which was not applied due to reliance on manual processes and siloed information.[1]

Prioritization, collaboration, and visibility are necessary to focus limited resources where they can have the greatest impact. Having a solution which interlocks security, risk, and IT helps organizations take a holistic approach to vulnerability response and stay ahead of attackers.

The ServiceNow solution

ServiceNow® Vulnerability Response helps organizations focus on the most critical risks, respond faster and more efficiently across 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.

Centrally manage weaknesses in infrastructure, applications, and software configurations with Vulnerability Response. It works with leading scan vendors to find vulnerabilities and assets in your network, then prioritize and coordinate response with IT for remediation. Prioritize vulnerabilities and coordinate fixes with developers in deployed applications with ServiceNow Application Vulnerability Response. You can also identify, prioritize, and remediate vulnerable misconfigured software with ServiceNow Configuration Compliance.



Critical Overdue Vulnerabilities

Watch Topics monitor vulnerable items that meet a filter criteria. Creating a Remediation Effort from a Watch Topic, generates tasks for IT to drive remediation.

Distinct CIs: 17

The Vulnerability Manager Workspace allows you to track vulnerabilities by watch topic to quickly understand status and make strategic remediation decisions.

Focus resources on the most critical risks

Automate prioritization with configurable risk score calculators. Create watch topics to identify and respond to vulnerabilities of interest. Reduce the amount of time spent on basic tasks with orchestration tools

Drive faster, more efficient response across security and IT

Coordinate response across teams for smoother task handoffs between groups and quicker resolution. Provide preferred solutions and integrate with change management for faster patching. Ensure accountability with remediation targets and automated rescans.

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.

[1] Source: Ponemon ServiceNow-sponsored survey, Costs and Consequences of Gaps in Vulnerability Response, 2019

Finally, with Continuous Monitoring, risk policies are connected to the vulnerability lifecycle to identify business risks and manage them in ServiceNow Governance, Risk and Compliance. This ensures policies across applications and infrastructure can be adaptive and stay up to date, dramatically reducing organizational risk.

Proactively reduce risk

Vulnerability Response provides a comprehensive view of all vulnerabilities affecting a given asset or service through integration with the 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 business impact using a calculated risk score so teams can focus on what is most critical to your organization. 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®.

Vulnerability managers can create watch topics to help them quickly identify risky vulnerabilities, such as a high risk score, specific critical CVE, or overdue tasks. This allows for easier monitoring and can be used to create remediation tasks by topic.

You can also easily identify which solutions will have the greatest impact on vulnerability risk reduction with Vulnerability Solution Management. It works by matching vulnerability scan data against Microsoft or Red Hat's solution databases to recommend which to deploy based on supersedence. If the preferred solution isn't practical to deploy, solution options are visible to both security and IT to enable teams to make the best choice for a specific environment.

Respond efficiently across security and IT

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. Analysts can monitor real-time status of patching progress and ensure process visibility across security and IT. It also uses machine learning to identify the most appropriate teams for vulnerability findings and auto-assigning tasks to reduce manual effort. This results in a coordinated remediation strategy for vulnerabilities.

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. Vulnerabilities are closed when a rescan confirms the vulnerability is no longer present to ensure nothing is missed.

In addition, remediation targets define the expected time frame for resolution for each affected asset. These rules can take into account whether an asset has sensitive information and is therefore subject to regulations that define how fast the vulnerability must be fixed. Notifications are sent at a defined reminder time and again if the target date passes. This ensures vulnerabilities are remediated in a timely fashion that can vary by asset or criticality.

To streamline the patching process, IT remediation specialists have a unique workspace to show them prioritized tasks, affected assets, and solution options. It integrates with ServiceNow IT Service Management for change management, allowing IT to create or modify change requests. This provides your IT team the right level of detail for successful remediation while focusing them on high-value tasks.

Understand security posture and performance

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.

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

servicenow.

SN-DataSheet-VulnerabilityResponse-100621