ServiceNow Vulnerability Response

The vulnerability challenge

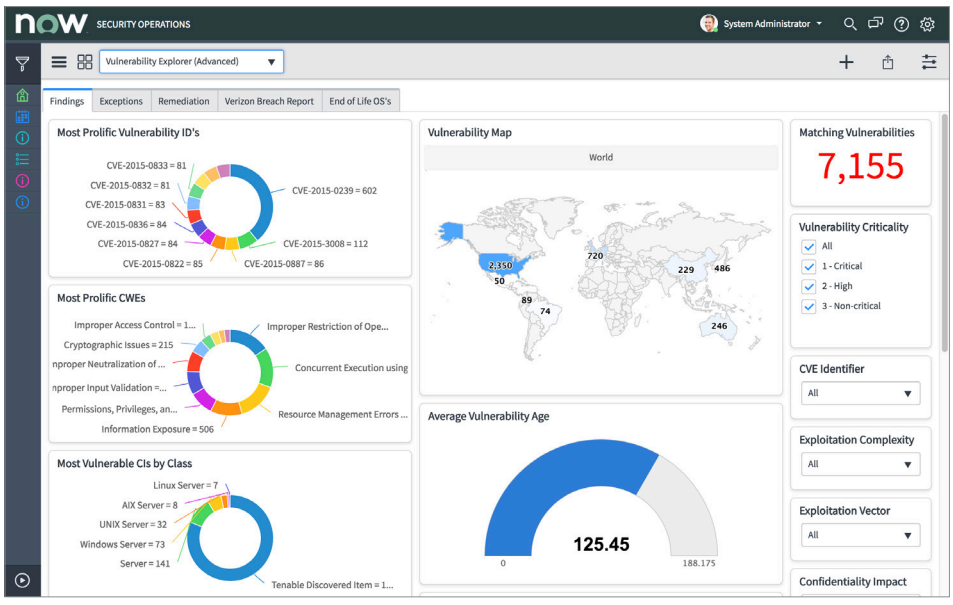
Vulnerabilities don't often get the same amount of notice as phishing attacks or advanced persistent threats, but when a critical vulnerability is exploited, organizations can suffer major damage. The WannaCry ransomware attack targeted organizations around the world by exploiting an existing vulnerability. More than 230,000 unpatched systems were infected, even though the patch had been available for nearly two months before the launch of WannaCry.

This illustrates how organizations are often overwhelmed by vulnerabilities, many of which may never be mitigated. In fact, the 2017 Verizon Data Breach Investigations Report showed that if a vulnerability is not addressed within four weeks of discovery, it's likely never to be fixed.

In addition to the sheer quantity of vulnerabilities, many organizations also struggle with coordination between security and IT to manage prioritization and patching. A recent 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.



The Vulnerability Explorer dashboard shows up-to-date information about active vulnerabilities in your organization.

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.

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

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.

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

Respond automatically

When critical vulnerabilities are found, ServiceNow 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. Easily see which services are impacted by critical vulnerabilities or which assets have older vulnerabilities at greater risk of exploit. With better visibility, teams can respond more efficiently, reducing both the vulnerability backlog and your risk exposure.

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

“With better visibility, teams can respond more efficiently, reducing both the vulnerability backlog and your risk exposure.

servicenow