Built-in Automation in InsightVM

Leverage automation workflows to accelerate vulnerability management and empower your team

Given the dynamic nature of modern IT environments, your vulnerability assessment needs are changing. Since you can't protect what you can't see, having complete visibility across your ecosystem has become exponentially more critical. It's no longer enough to just scan the corporate network quarterly, even monthly for vulnerabilities; organizations now need to ensure that vulns, once detected, are remediated or contained quickly—before they're exploited by attackers.

With so much work on your security team's plate and the sheer number of manual steps and processes that need to be executed just to get a vuln from discovery to remediation or containment, it's no shocker that a single vulnerability is enough to incite audible groans from security and IT. InsightVM automates a number of manual processes traditionally required for effective vulnerability assessment, such as the tedious steps encompassed in patching and containment.

Simplify your vulnerability assessment processes

By leveraging the automation workflows available in InsightVM, your team gets back time in their busy days, freeing up the resources needed to scale your vulnerability management program and even expand the number of devices your team can effectively manage.

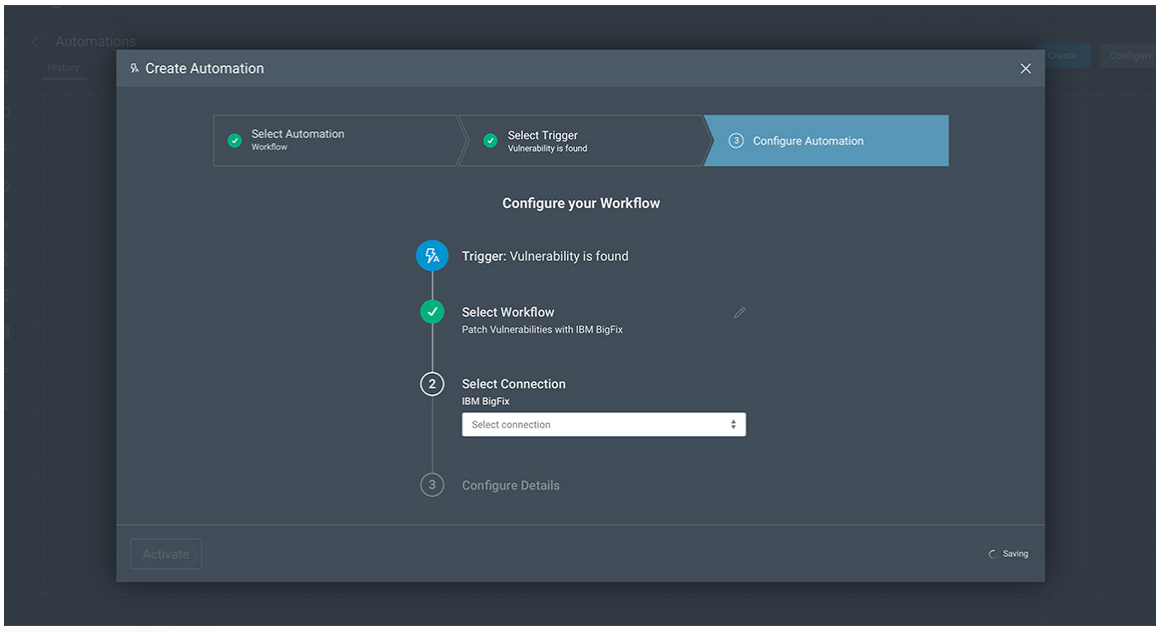

Figure 1: Automation-assisted patching workflow configuration in InsightVM

Accelerate remediation with Automation-Assisted Patching

InsightVM's Remediation Projects enable you to work with your IT team's tools so you can break down the silos between Security, IT, and Development and assign and track remediation duties seamlessly across teams. By using their existing systems and workflows—such as integrations with leading ticketing solutions like Jira and ServiceNow—you can automate the process of handing off remediation duties between teams and validate that fixes are in place.

Additionally, automation-assisted patching through tools like IBM BigFix and Microsoft SCCM lets you streamline the mundane stuff while giving you (or IT) the autonomy to make key decisions in your patching process. Automate the steps of aggregating key information, retrieving fixes for identified vulnerabilities, and ultimately—when appropriate or approved by a sysadmin—applying the patches. Upon completion, your team can elect to have InsightVM automatically re-assess impacted assets to verify patching was successful.

Implement compensating controls with Automated Containment

It's the hard truth: You can't remediate every vulnerability you find immediately—or maybe ever. With Automated Containment, you can decrease exposure from these vulnerabilities by automatically implementing temporary (or permanent) compensating controls via your Network Access Control (NAC) systems, Firewalls, and Endpoint Detection and Response tools (EDR) like Palo Alto PAN-OS, Cisco FirePower, and Carbon Black Response.

With Rapid7, your team can focus on more strategic and demanding priorities. Instead of being bogged down and inundated with manual tasks, your team can make measurable and purposeful progress towards reducing your organization's risk.

About InsightVM

Rapid7 InsightVM is vulnerability assessment for the modern environment. Inspired by our award-winning Nexpose product, it leverages the latest in analytics, endpoint technology, and automation to provide constant intelligence to discover vulnerabilities, pinpoint their location, prioritize them for your business, and confirm your exposure has been reduced.

See what automation can do for you: www.rapid7.com/get-started-with-automation

Support

call +1.866.380.8113

Customer Portal

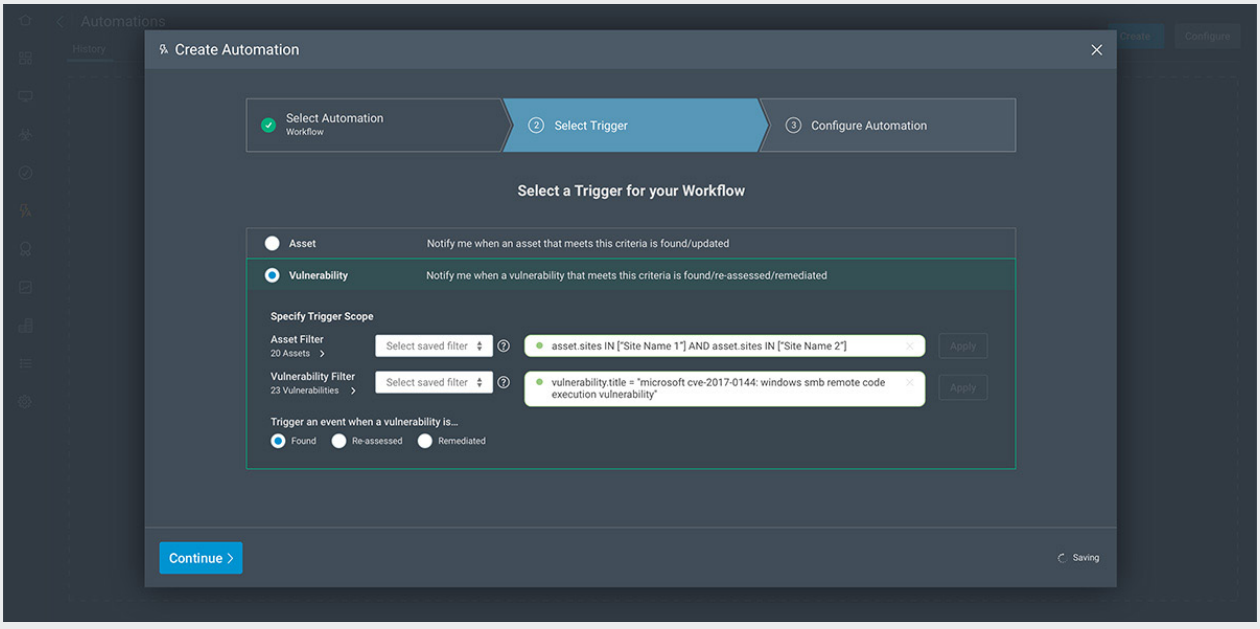

Figure 2: Automated action triggers in InsightVM

©RAPID7 2018