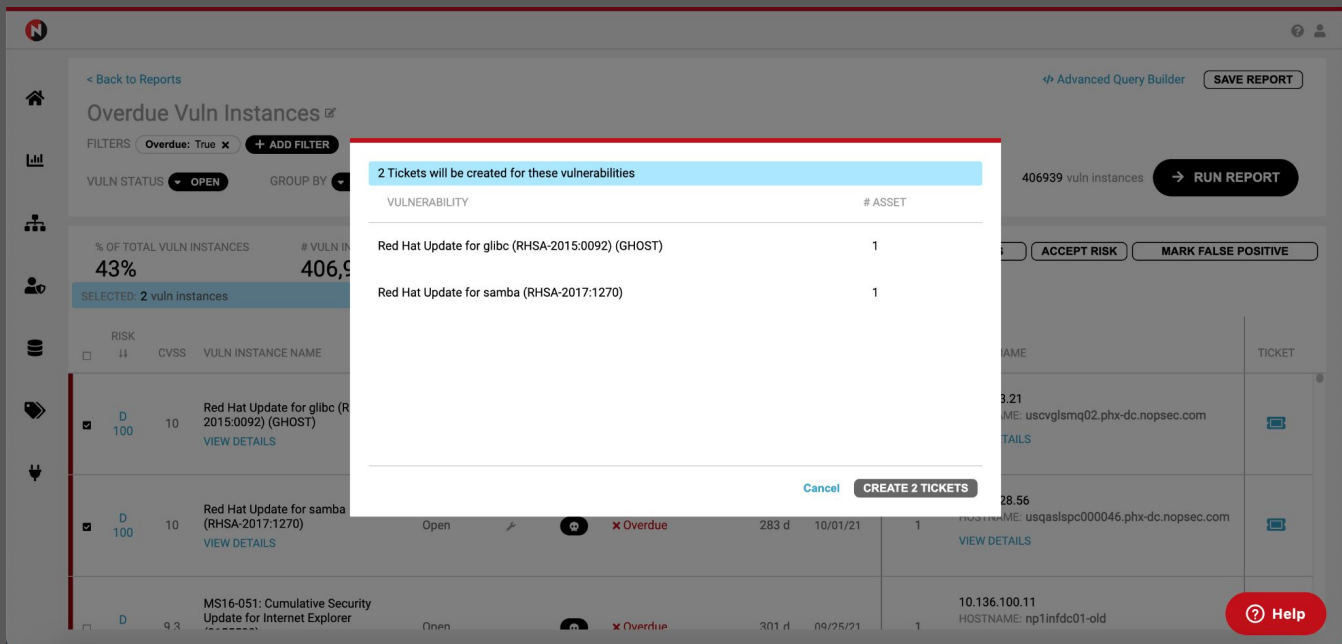


Vulnerability Remediation Workflow Automation

Aligning Security and ITOps Workflows

Unite the efforts of your Security and ITOps teams. Relying on emailed lists or tickets created manually in your ITSM is inefficient and error-prone. NopSec enables you to design and manage vulnerability processes from identification through remediation and automatically push remediation tickets through to your orchestration systems. NopSec UVRM's workflow automation also assigns SLAs based on the NopSec risk score, alerts key stakeholders when critical SLA dates are missed, and enables you to track remediation performance by business line, product, or platform.



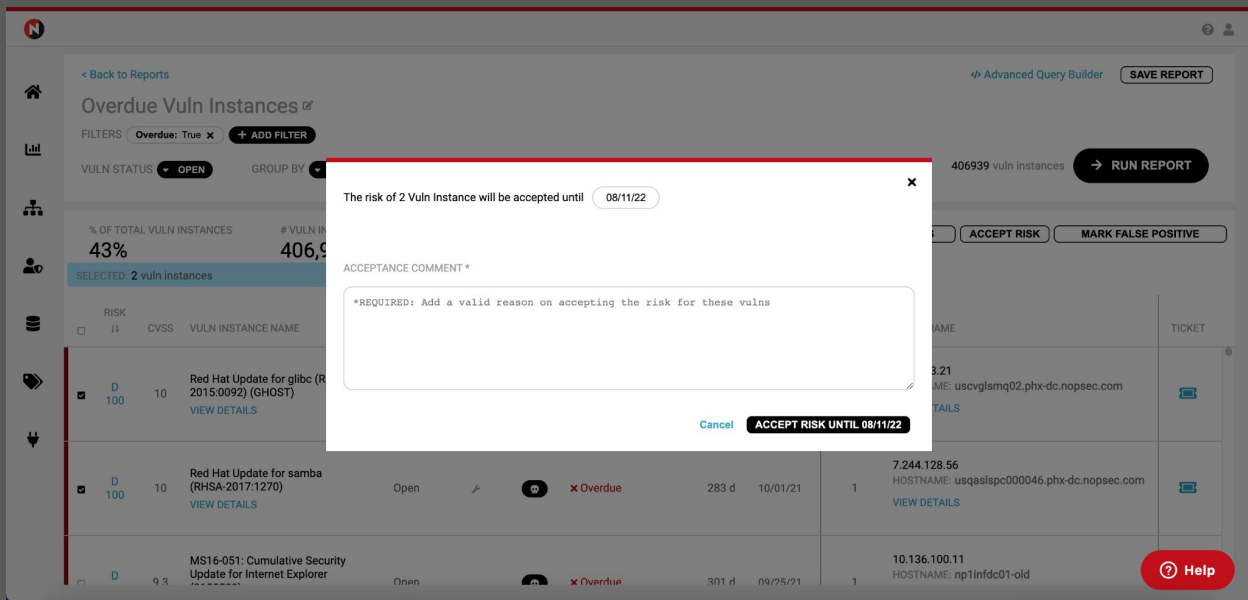
The screenshot displays the NopSec interface with a modal window titled "2 Tickets will be created for these vulnerabilities". The modal contains a table with the following data:

VULNERABILITY	# ASSET
Red Hat Update for glibc (RHSA-2015:0092) (GHOST)	1
Red Hat Update for samba (RHSA-2017:1270)	1

Below the table, there are "Cancel" and "CREATE 2 TICKETS" buttons. The background interface shows a list of vulnerability instances with columns for RISK, CVSS, VULN INSTANCE NAME, and a "TICKET" column. A "Help" button is visible in the bottom right corner.

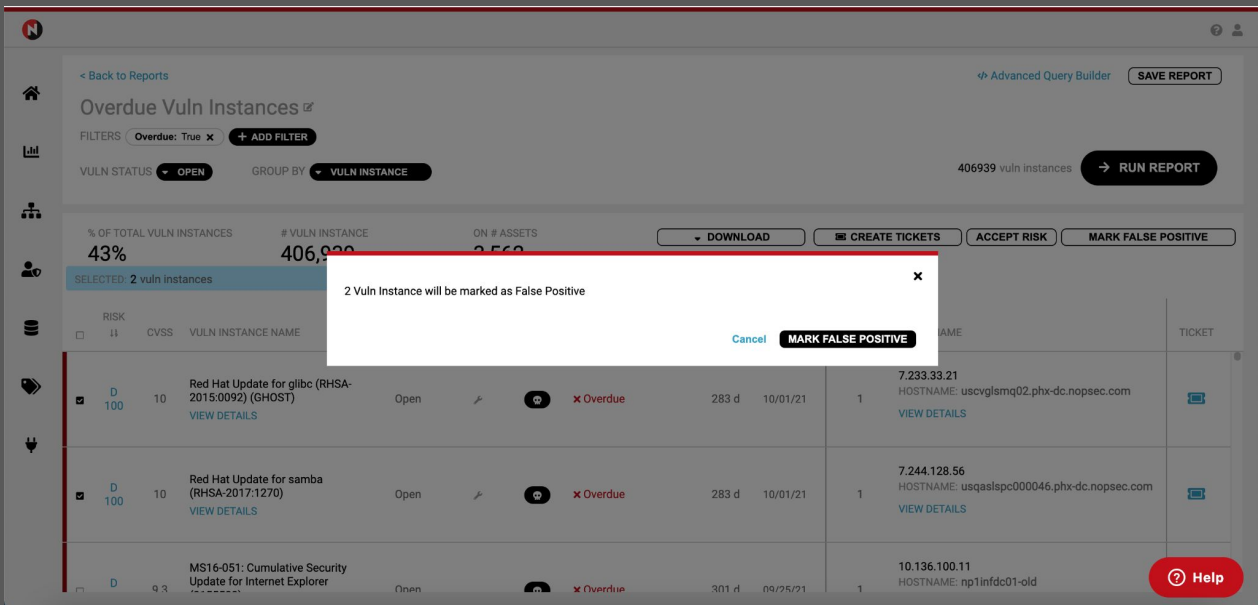
Automatic Ticket Creation

Unified VRM eliminates the need to use spreadsheets and email for manual remediation communication. Once integrated with your ITSM, Unified VRM enables Security team members to create remediation tickets automatically within the platform. The ticketing integration is a bi-directional sync that also enables automatic ticket closer when all associated vulnerability instances have been reported as remediated by your vulnerability scanner.



Risk Acceptance

Unified VRM offers the capability to mark vulnerabilities as Accepted Risk. When doing so, an accepted until date is required that will trigger a reminder notification. This feature prevents vulnerabilities that don't have available patches today from falling through the cracks later.



False Positive Designation

You can apply false positive designation within the Unified VRM applied when a vulnerability is identified as such. Once marked as a false positive, Unified VRM will push this designation back to the scanner source to be reconciled in future scans.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions. NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.