

ServiceNow SecOps Vulnerability Response Module Implementation and Remediation Management

Overview

The client, a premier US-based Property and Casualty (P&C) insurer, encountered significant hurdles with timely vulnerability management due to manual vulnerability tracking and lack of standardized remediation processes. By incorporating Qualys, ServiceNow SecOps, and CMDB into a comprehensive Vulnerability Management Program (VMP), facilitated by Tech Mahindra's expertise, the insurer fundamentally enhanced its IT security posture. This overhaul resulted in over a 50% reduction in vulnerability mitigation time, marking a substantial improvement. The achievement was propelled by streamlined data migration, customized workflow management, and improved tracking and prioritization of threats.




Client Background and Challenge

The client was using a manual excel and email-based approach for tracking system vulnerabilities and remediation, leaving its assets susceptible to external threat for longer times. This resulted in absence of:

- ▶ Vulnerability dashboards which provide real time security posture.
- ▶ Active remediation tracking with the right asset owners leading to longer mitigation time.
- ▶ Standard images to be patched across systems.
- ▶ Grouping of assets and prioritization of vulnerabilities.

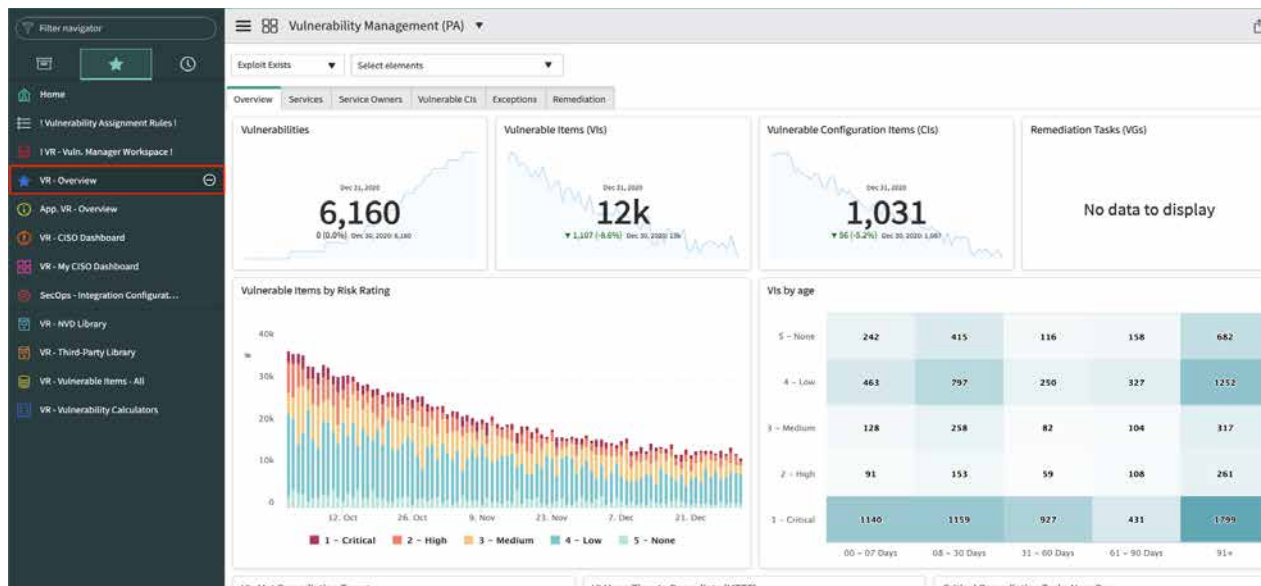
Furthermore, the IT teams needed to be trained in vulnerability understanding and how to prioritize and patch the same.

Our Approach and Solution

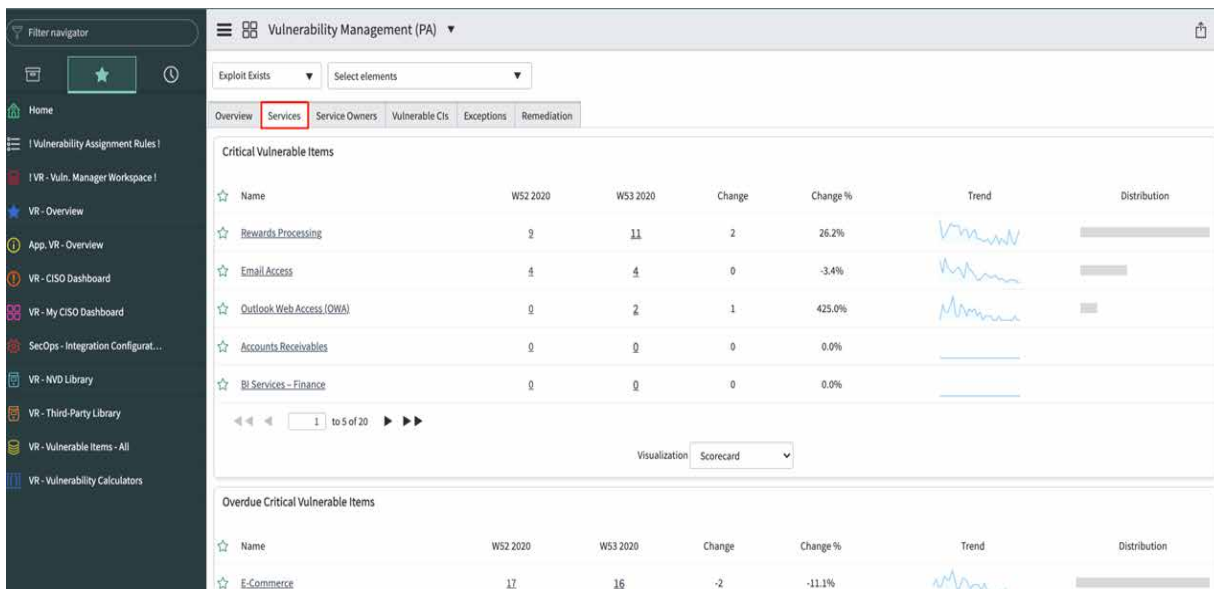
-  TechM has established an end-to-end vulnerability management program which involved Integration of Qualys (Vulnerability scanner tool), ServiceNow Secops module and CMDB (Configuration Management Database) along with the deferred GRC process.
-  Existing vulnerability data from a SharePoint was Integrated with Secops module for better data migration.
-  Customized workflow management was developed with an established remediation process.

Dashboard Images

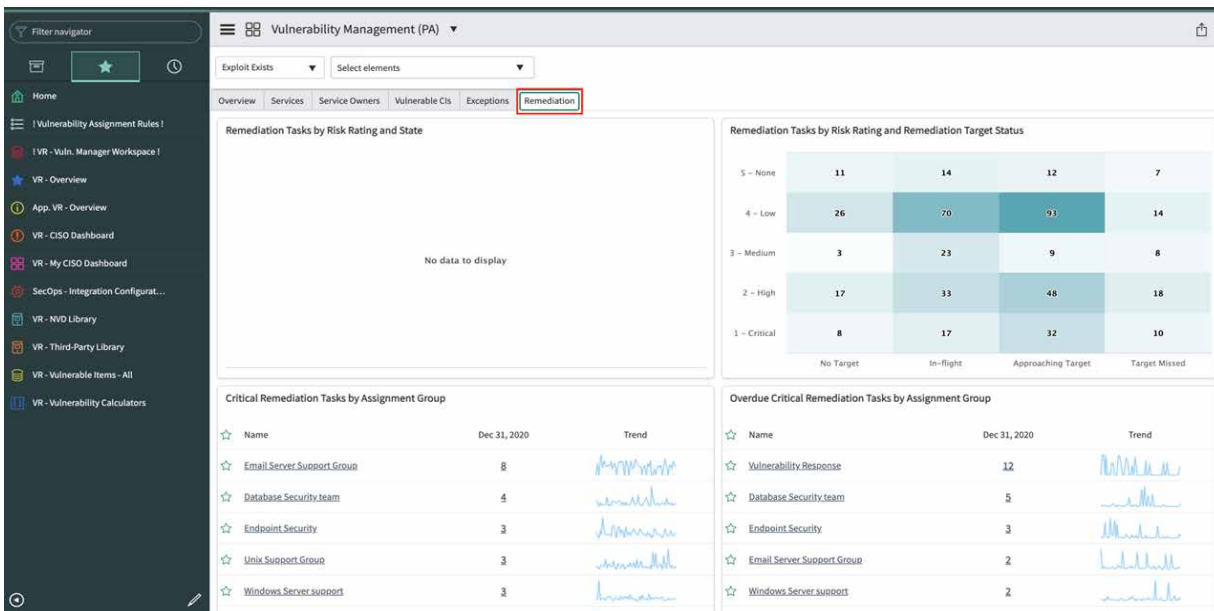
Vulnerability Response Overview



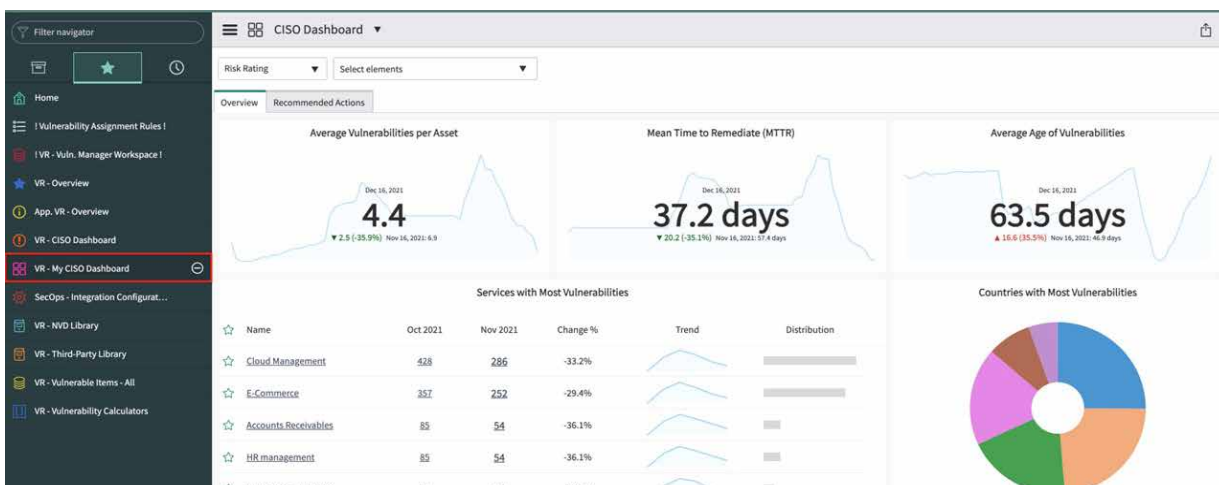
Dashboard Services

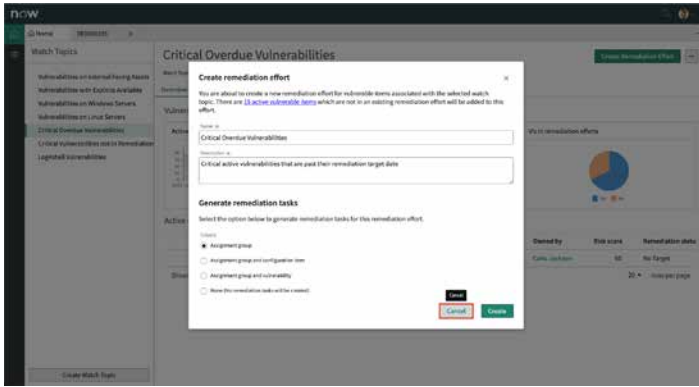
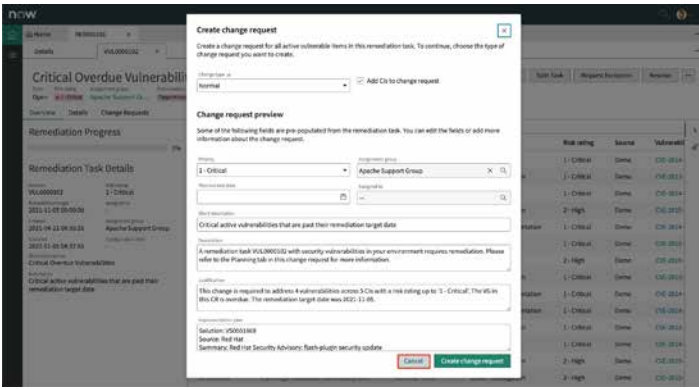


Dashboard - Remediation



Dashboard - CISO





Business and Community Impact

The new VMP reduced Mitigation time for vulnerabilities by 50% through:

- ▶ Fine tuning of scanner ruleset for lesser false positives.
- ▶ Effective tracking of identified vulnerabilities through comprehensive dashboards.
- ▶ Automated prioritization, grouping and assignment of vulnerabilities to respective asset owners.
- ▶ Support provided to asset owners with appropriate patch recommendations.

TECH
mahindra



www.youtube.com/user/techmahindra09
www.facebook.com/techmahindra
www.twitter.com/tech_mahindra
www.linkedin.com/company/tech-mahindra
www.techmahindra.com
mktg@TechMahindra.com

Copyright © Tech Mahindra 2024. All Rights Reserved.

Disclaimer. Brand names, logos and trademarks used herein remain the property of their respective owners.