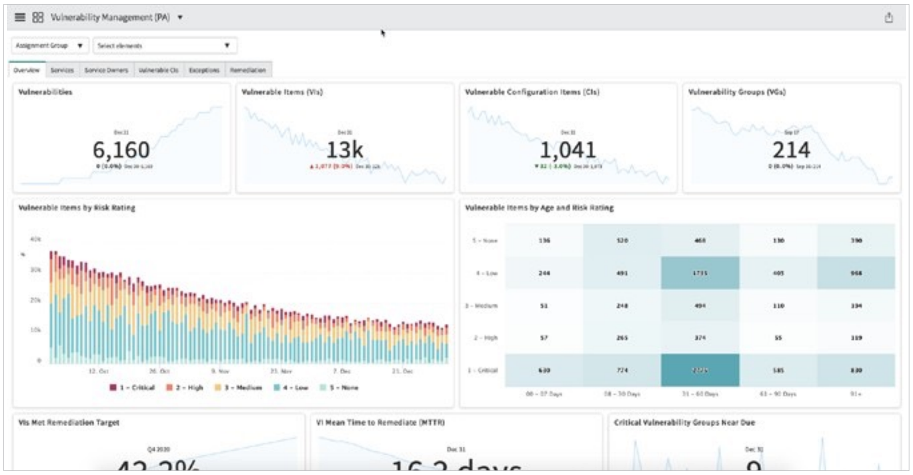
Software Exposure Assessment

Security workflows need to leverage IT assets, operations, and security teams—do it all on the Now® Platform.

The key to handling any vulnerability is to know how widespread it is and then remediate it as quickly as possible. That may be easy enough with a single vulnerability, but when you're managing tens, hundreds, or even thousands each day, true speed comes from operating as a proactive team within IT. Then, you have a clear picture of your assets up front and a platform helping you automate your security procedures across IT with workflows. Security Operations is the concerted effort from both the security and IT operations teams to work closer together to secure systems and data. Building workflows that encompass security, IT, and even the asset management facets of the equation can greatly strengthen your Security Operations procedures.



When vulnerabilities can't wait

It's a familiar story that we've all seen many times: a new, high-risk vulnerability has started to be exploited in the wild and is making headlines. Your CIO expresses concern and wants to reassure the executive team that your organization is not vulnerable to the exploit. This is the point when the security team would go into fire-fighting mode, right? Typically, the next thing that happens is a full vulnerability scan of the environment to understand the risk exposure, but that can take days – or even weeks! That is far too slow, and the longer it takes, the greater the risk.

We have great news for ServiceNow customers who leverage the Now platform with both Vulnerability Response and Software Asset Management (SAM). Together, these two products help your organization quickly find and remediate vulnerable systems in minutes or hours, not days or weeks.

Armed with deeper software estate insights from Software Asset Management and remediation management from Vulnerability Response, Vulnerability Managers can search for exposure to vulnerable software by providing the relevant information— like publisher, product, and version—and associate the findings without requiring a Common Vulnerabilities and Exposures (CVE) ID. Then, the Vulnerability Manager can create tasks for IT that include everything IT teams need to know to remediate them.

> “
>
> 79% of the companies that experienced a security breach indicated that it could have been avoided with a patch or configuration change.
>
> – Market Snapshot / Secure Operations Automation, Voke

IT Asset Management and the Now Platform
ServiceNow ITAM solutions leverage the strength of the Now Platform with its single data model and architecture, so you can:

- Stop maintaining numerous brittle integrations
- Have a consistent user experience across IT workflows
- Leverage predictive intelligence and AI
- Quickly develop apps leveraging all your data

When you deploy ITAM in your ServiceNow environment, it builds on the Now Platform by:

- Extending the amount of data within your CMDB
- Keeping data clean and in sync
- Normalizing and reconciling data, so it's trusted and easier for all systems to use

Security Operations and the Now Platform
Security Operations solutions also leverage the power of the Now Platform. These solutions add intelligence and security procedures to workflows and systems, including:

- Security incident response
- Configuration compliance
- Threat intelligence
- Performance analytics

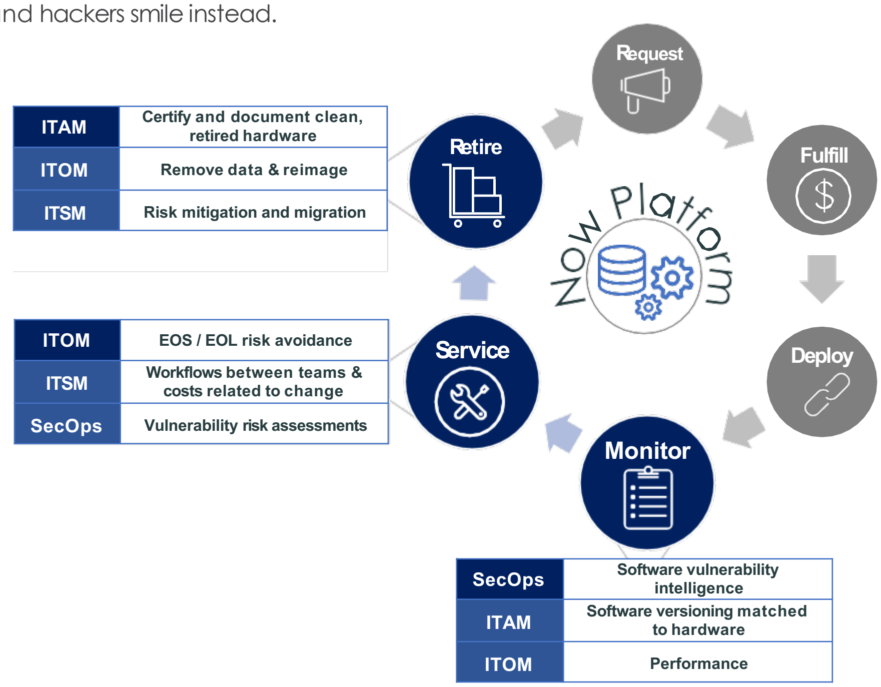
Security is a team sport

Security requires everyone's help across the company. IT asset management (ITAM) professionals can flip the script to be proactive with security. Your team can be the one that proactively notifies security via a workflow about the breadth of the risk and where it exists in your organization, so Security Operations can start the remediation process with a better idea of what it will take. When Security and IT operation teams work with a deeper understanding of the issue and have automated workflows to remediate, everything happens faster. That way when the CIO asks for a status update about the high-risk vulnerability, everyone involved can say, "Already taken care of." Your CIO breathes a sigh of relief and you flash a quick, confident smile. If you're not proactive about managing your software, vulnerabilities mount, tensions grow, and teamwork suffers, and hackers smile instead.

ITAM lifecycle automates more lines of defense

The bigger picture view for reducing attack surfaces is when you can implement additional safeguards within your ITAM lifecycle discipline. It's best to create security checks within your Monitor, Service, and Retire stages of the ITAM lifecycle. Then, integrate those security checks with Security Operations best practices and workflows, which is easy to do with the Now Platform.

Finally, track vulnerabilities from discovery to remediation and close the loop through automated processes in your IT management workflows. That way, everyone can verify that the vulnerability or breach has been correctly dealt with. The following graphic highlights areas within the asset lifecycle where ServiceNow workflows help enhance security:



ITAM	Certify and document clean, retired hardware
ITOM	Remove data & reimage
ITSM	Risk mitigation and migration

ITOM	EOS / EOL risk avoidance
ITSM	Workflows between teams & costs related to change
SecOps	Vulnerability risk assessments

SecOps	Software vulnerability intelligence
ITAM	Software versioning matched to hardware
ITOM	Performance

Workflow for quick vulnerability remediation

There are many ways you can workflow a vulnerability assessment across multiple teams. The following is one such example:

1. A Vulnerability Manager learns from a workflow alert routed from the SAM team that a zero-day vulnerability involving three different versions from a major software vendor is running on 73 laptops, including the CFO's device. He starts up Software Exposure Assessment within Vulnerability Response and sees attributes such as Publisher, Product, Version, and Edition. This verifies the intelligence provided by the SAM team is real and needs immediate corrective action.
2. Vulnerability Manager quickly creates records for each vulnerable asset called Vulnerable Items and combines them together into a work task called a Vulnerability Group. All of this took only a few minutes.
3. The Vulnerability Group is automatically assigned to IT staff or software application owners, who will remediate the affected assets—the workflow will help track the remediation activities as they are completed for the Vulnerability Manager.
4. IT pushes out an immediate patch and schedules a patch for production systems.
5. The vulnerability has a high enough priority, so an alert is created in case other devices come onto the network later and the vulnerability can be patched automatically.
6. Security Operations closes the case and updates a knowledge article for future vulnerability assessments.

For more information about the ServiceNow Platform and how it can help speed up your IT workflows using IT Asset Management, visit servicenowcom/itam

SNC-ITAM00201 102020 ASC-XX-SM.