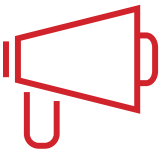
Streamlining Security Incident and Vulnerability Response

servicenow | Use-Case Guide

Table of Contents

Information Security Challenges

Security incident identification and remediation are daunting challenges for security teams. Manual processes, multiple cross-team hand-offs, and the proliferation of security tools hinder a team's ability to quickly assess and remediate vulnerabilities and attacks. A recent CSO study revealed that the average enterprise uses 75 security products.[1] Security admins must manually sift through hundreds or thousands of alerts each day, making it difficult or even impossible to determine which events are the most important. Due to this flood of information, it now takes approximately 201 days for an enterprise to discover a breach.[2]



The biggest obstacles to achieving "incident response excellence" are security and IT tool integration and coordinating incident response, according to a study from the Enterprise Strategy Group.[3] Without automated and integrated solutions, security teams are forced to communicate with IT via email, phone, and complicated spreadsheets. Even if analysts can identify an imminent threat, they may not know whom to contact on another team for remediation.

Relying on inefficient manual processes inevitably leads to a lowered security posture for the organization and could result in an eventual breach or compromise. Choosing an effective security operations solution is essential for combatting these ever-increasing security challenges.

[1] http://www.csoonline.com/article/3042601/security/defense-in-depth-stop-spending-start-consolidating.html
[2] Ponemon Institute, 2016 Cost of a Data Breach Study
[3] http://www.servicenow.com/content/dam/servicenow/documents/analyst-research/analyst-status-quo-creates-security-risk.pdf

Evaluating a Security Operations Solution

The right security response platform will make remediation efforts more efficient, streamline response processes, and provide the ability to visualize the enterprise's security posture.

To accomplish these goals, it must be able to:

- Pull data from multiple sources into **a single system**
- **Prioritize** incident workload
- **Understand the business criticality** of all enterprise assets
- **Route information** to the appropriate teams and people
- Enable IT and security teams to work from the **same system**
- **Automate** all basic tasks and processes
- **Provide intuitive, visual dashboards** that reflect current security posture

Unfortunately, very few of today's security operations solutions can provide all of this essential functionality.

ServiceNow Security Operations

ServiceNow Security Operations meets the requirements of the ideal security incident and vulnerability response solution. It extends the advanced workflow and systems management capabilities of the core ServiceNow platform to give security teams a single solution for managing and understanding the security posture of all critical business services and IT infrastructure. Security Operations helps organizations streamline remediation, accelerate responsiveness, and increase the overall accuracy of incident handling by leveraging collaboration functionality built into the platform.

Security Operations uses the ServiceNow Configuration Management Database (CMDB) to map security incidents and vulnerabilities to business services and IT infrastructure. This mapping enables threat prioritization based on business impact, ensuring that security teams are able to focus on the most critical events first. In addition, a service level view of all security incidents supports **a more coordinated response** that minimizes change requests and downtime, and effectively remediates all open threats.

Security Operations Use Cases

Let's take a closer look at how the solution works in the following three use cases.

Use Case Example #1: Investigating a SIEM Alert

An enterprise has linked its Security Information and Event Management (SIEM) system to ServiceNow Security Operations and has determined which alerts will be automatically imported into the solution. (The set-up process in this example was easy because Security Operations provides built-in integration with Splunk.)

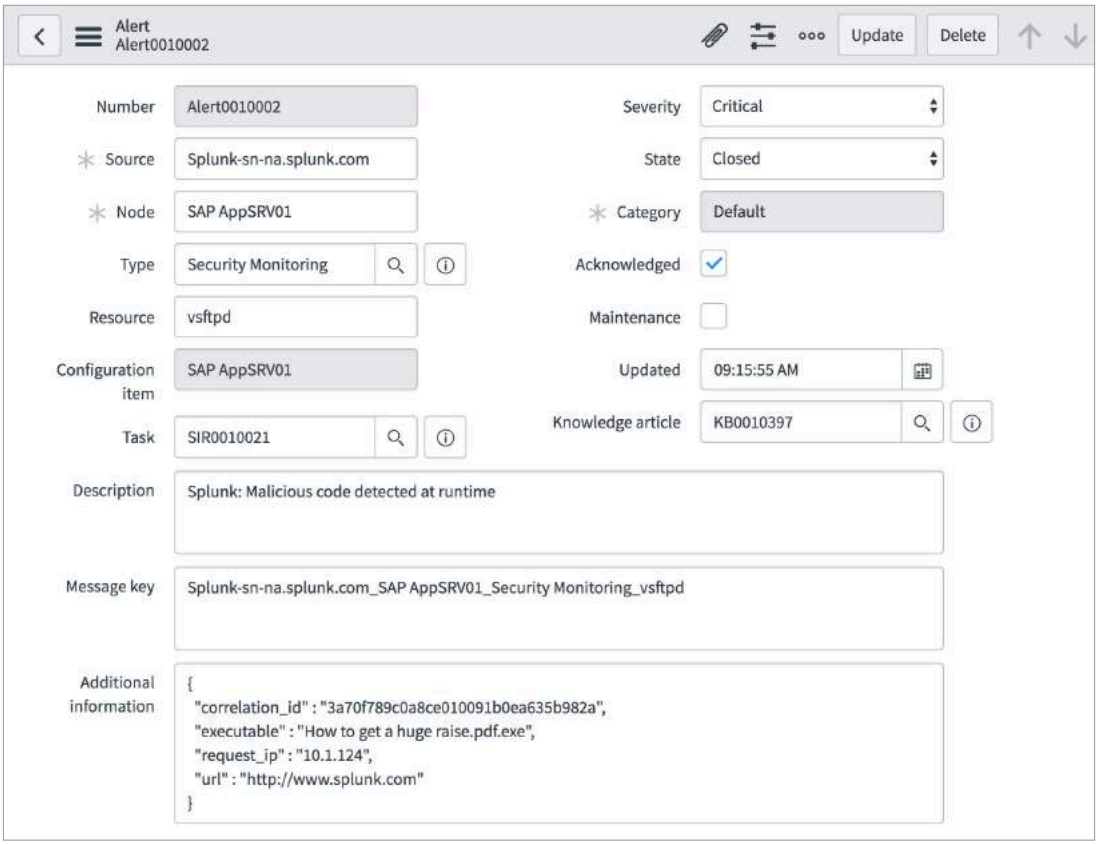


Figure 1: Investigating a SIEM Alert with ServiceNow Security Operations

Splunk generates a malicious code alert in Security Operations, and the data from Splunk is recorded for reference in the alert. Security Operations automatically creates a security incident based on pre-defined rules and links it to any associated knowledge base (KB) articles. Security Operations uses the ServiceNow CMDB information to match the affected hostname or IP to configuration items in the environment. In this case, an SAP server was impacted.

Prioritize Incidents According to Business Criticality

It turns out that this server runs a number of crucial business applications, so the server and incident are prioritized according to built-in business criticality calculators. The security team can easily see system dependencies, along with anything else impacting this item, including known vulnerabilities and open incidents. And finally, automatic prioritization of incidents helps security analysts focus on key issues first.

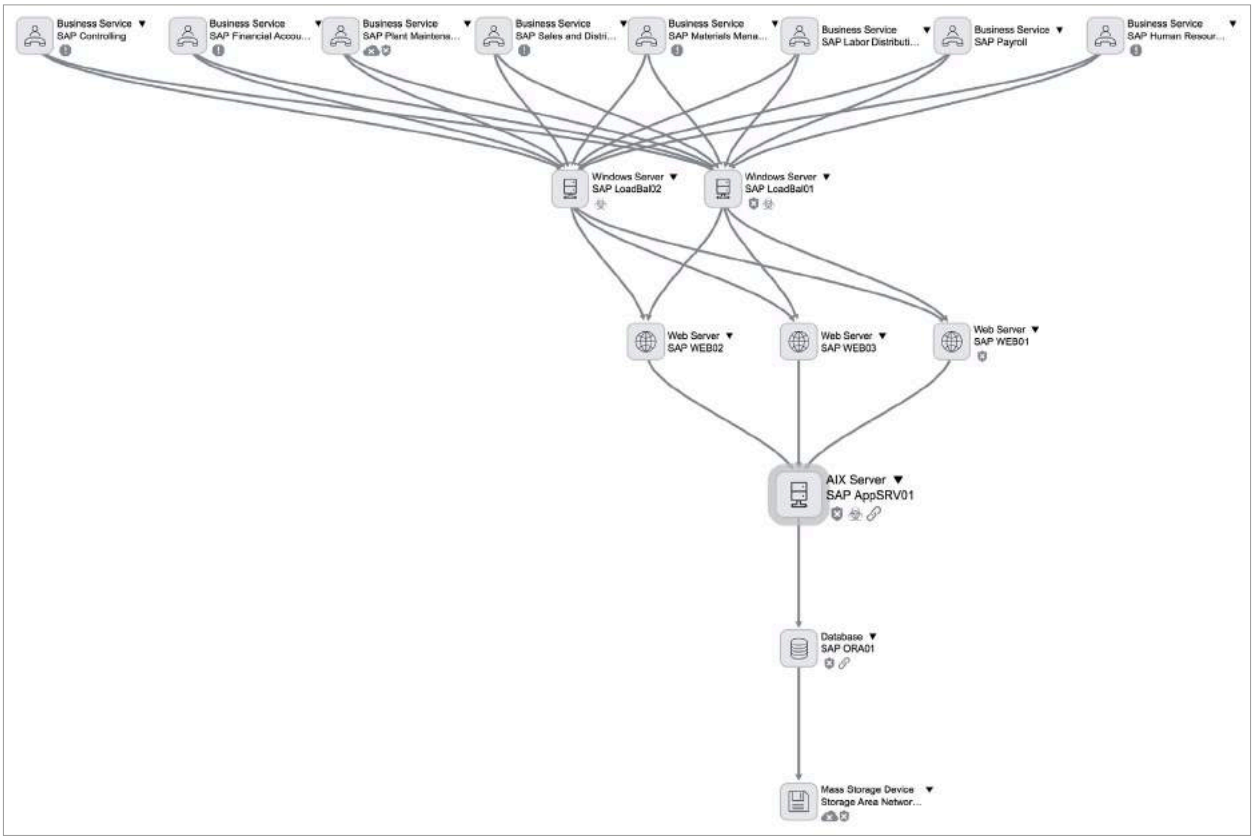


Figure 2: The Business Service Map shows assets that depend on the affected server

Align Workflows to Your Security Runbook

Security Operations uses pre-defined workflows to ensure that the security runbook is always followed. Overall incident response processes follow National Institute of Standards and Technology (NIST) best practices but can be customized to follow the organization's security runbook. Workflows can be customized for each type of incident or affected resource. In this example, the workflow involves a potential breach of sensitive personal information, so legal, human resources, and law enforcement contacts are included, ensuring that all required groups are consulted and decisions documented.

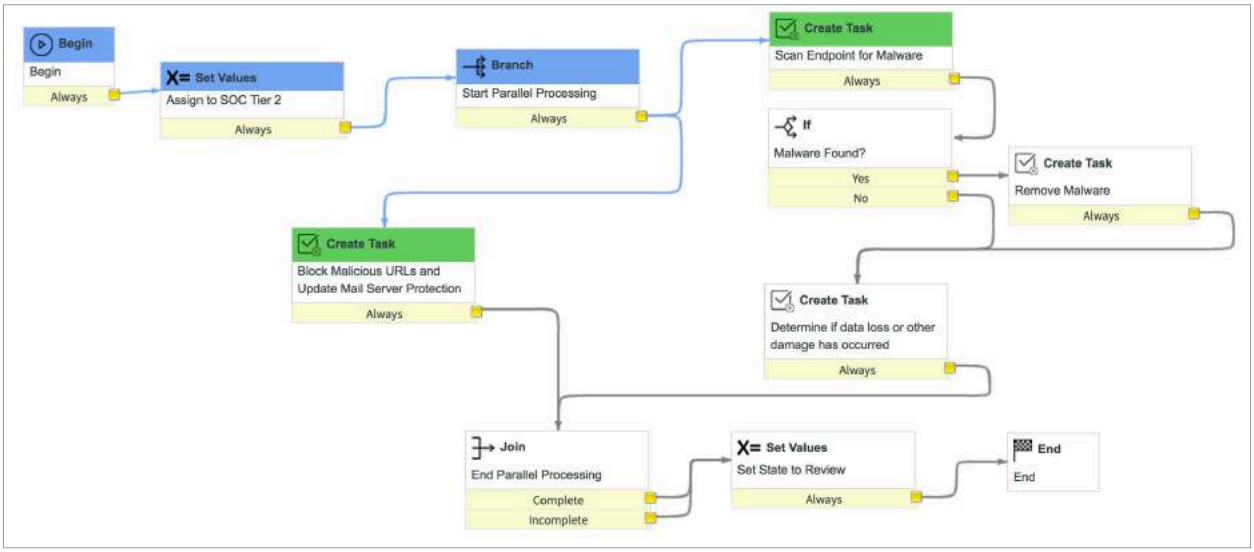


Figure 3: Workflows show all actions of a task. Blue items are complete, and green shows the current step

Search for Indicators of Compromise

Next, the security analyst searches for any Indicators of Compromise (IoCs). Data from Splunk showed a suspicious executable file, and the security analyst pastes the file name into the IoC search field. The system searches against threat intelligence feeds (Security Operations supports both STIX and TAXII standards), and the results show that the file is related to TorrentLocker. Clicking on this information tells the security analyst more about the threat: it is a type of ransomware. The analyst now has the necessary information to remediate the threat—much faster than using manual research and correlation methods.

Security Operations Use Cases

Use Case Example #2: Responding to an Employee-Submitted Phishing Email

An employee forwards a suspicious email to phishing@example.com. A security incident is created, the email attachment is automatically sent to a scanner for analysis, and the verdict is quickly returned. If the verdict is “not malicious,” the incident closes. An automated message informs the user and thanks him for submitting the incident, which encourages repeat participation. If, however, the verdict is “malicious,” the incident is escalated and it automatically triggers tasks for investigation and remediation, reducing the need for manual triage.

Subtasks are automatically created and assigned in the Security Incident Response application and routed to the correct person or team. Pre-defined workflows guarantee that all steps follow the established security runbook. In this case, the security incident workflow includes three subtasks: scanning the user’s endpoint for malware; updating the email server protection; and updating the firewall rules to block traffic to IP addresses the malware is known to communicate with.

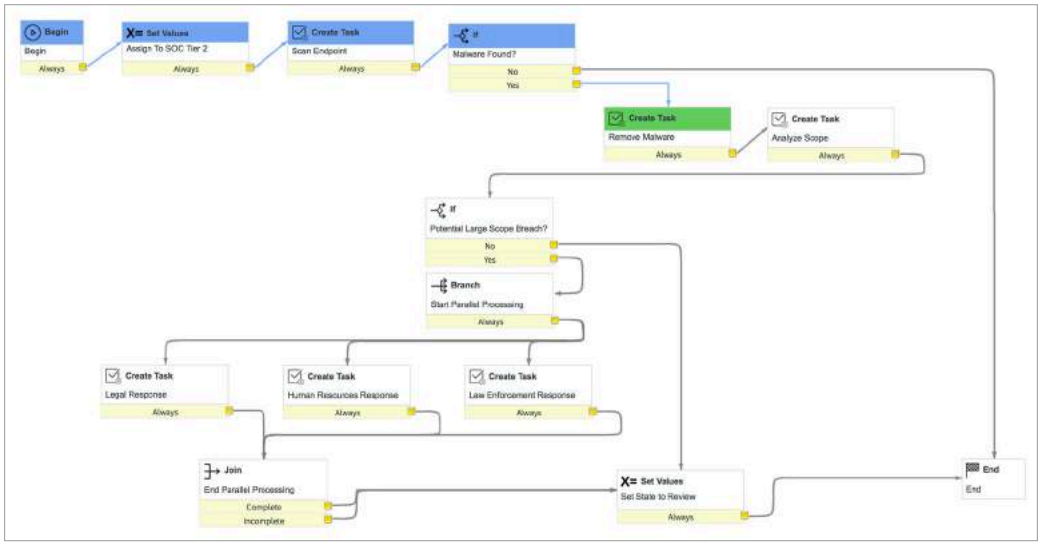


Figure 4: Workflow tasks can run in parallel

Know When Tasks Are Completed

The security analyst is then able to easily see when the subtasks are completed and compare them to SLAs. Tasks can be escalated automatically if the SLA time period is nearly up or passed. All of these processes are configurable by the administrator. When the process is complete, all tasks are shown clearly as “resolved,” eliminating the need for manual follow-up with other team members by phone or email.

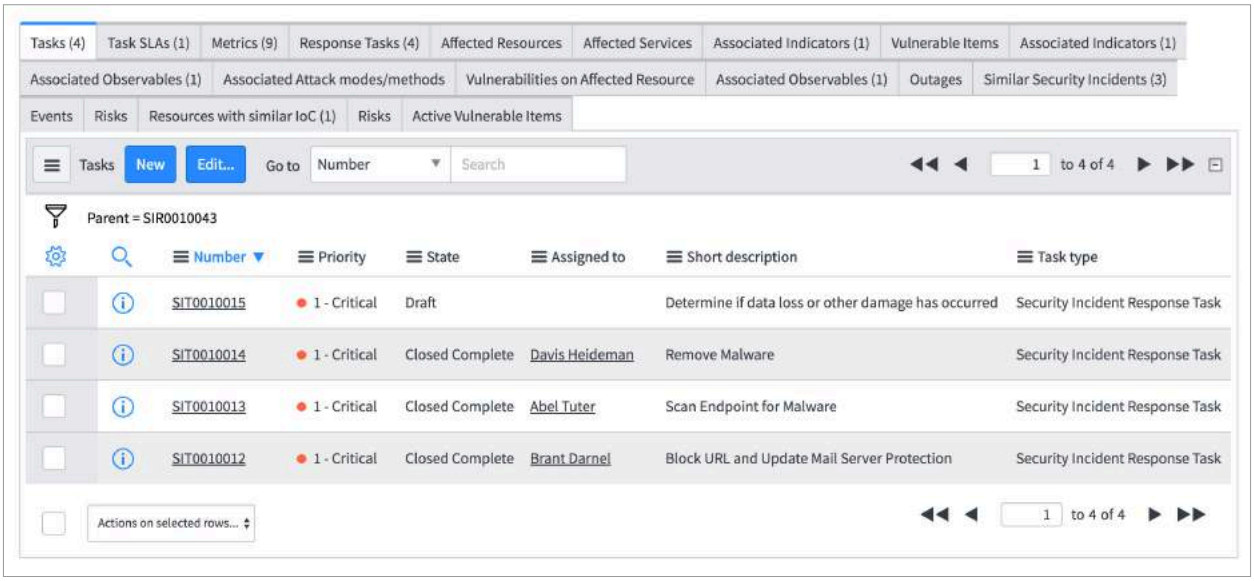


Figure 5: See all related subtasks, assignees, and statuses in one place

Create Post-Incident Reviews

Security Operations tracks all actions and approvals made within the incident. This allows a time-stamped post-incident review to be created automatically with the option to gather additional detail from participants via assessments. This information can then be used to create a knowledge base article to assist with identifying and remediating any similar future incidents. Accurate post-incident reviews are also valuable data for audits.

Security Operations Use Cases

Use Case Example #3: Addressing a High-Profile Vulnerability

A new vulnerability is in the news, and the company's CISO needs to know if the organization is affected. Vulnerability scan data is automatically imported into the Security Operations Vulnerability Response application using APIs. The new vulnerability is determined to be extremely risky (scoring a 10/10), with a complete loss of confidentiality, integrity, and availability if exploited.

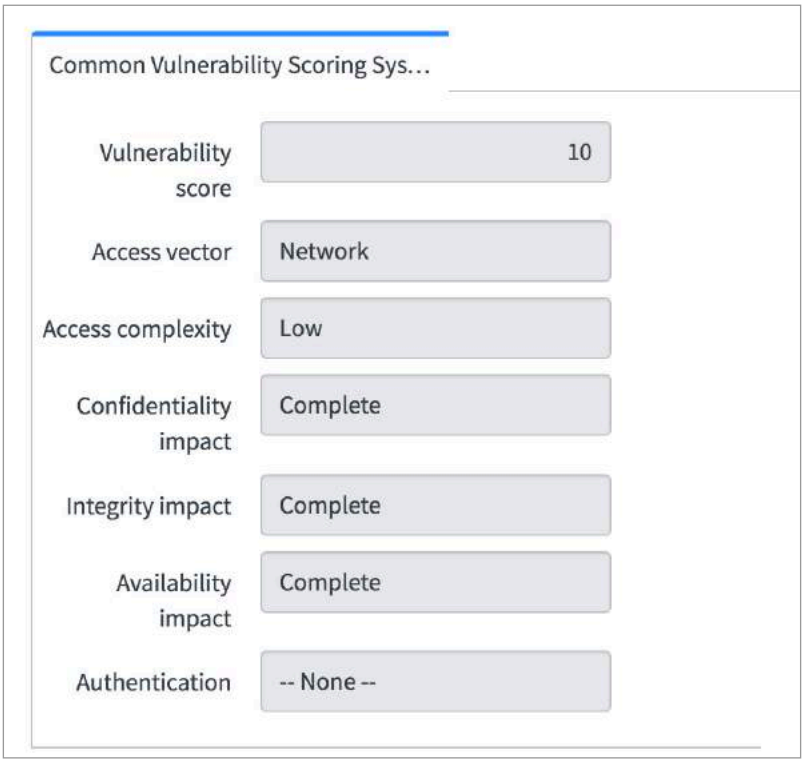


Figure 6: Common Vulnerability Scoring System data is automatically imported, eliminating the need to go back and forth between Security Operations and vulnerability management

All of the information about the vulnerability (e.g., what it is, how it's exploited, and how to remediate the threat) is automatically pulled into Security Operations, eliminating the need for manual research. The solution's configurable dashboards quickly show the organization's overall vulnerability exposure.

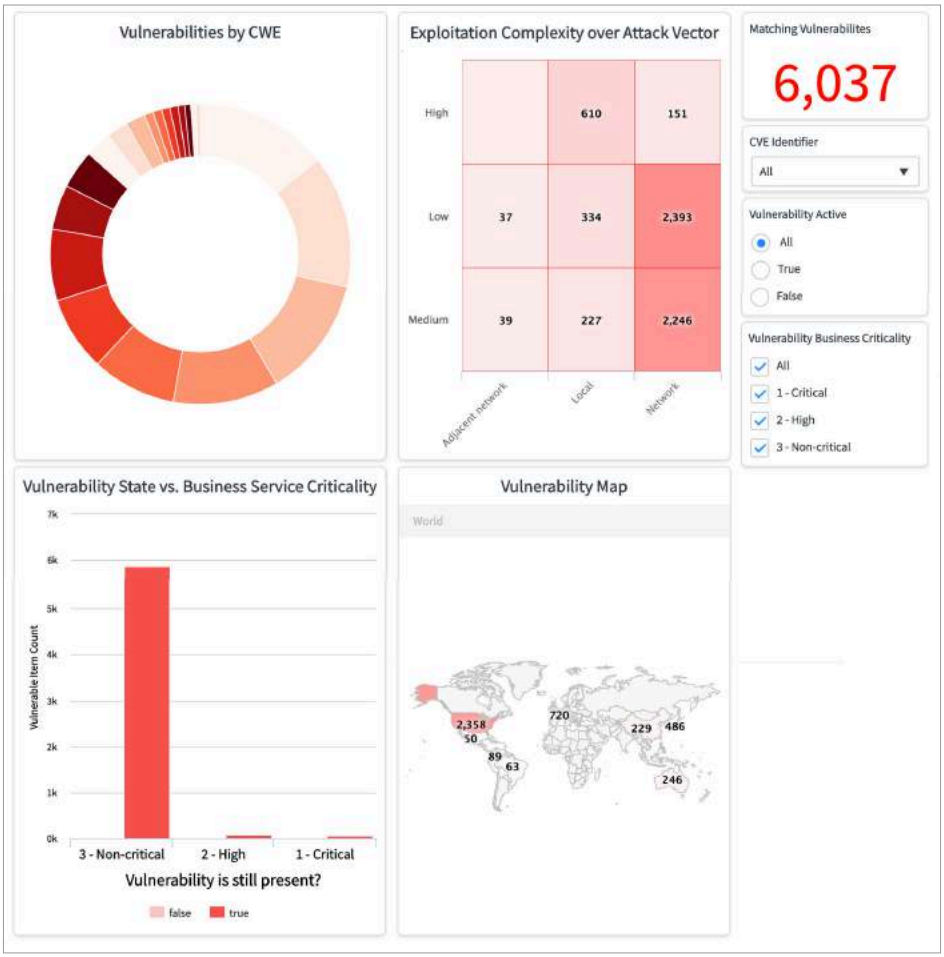


Figure 7: Role-based dashboards are customizable

Find Critical Vulnerabilities Quickly

Vulnerability scan data shows that hundreds of assets are vulnerable. All vulnerable item data is correlated with the configuration management database (CMDB). Business criticality calculators prioritize all vulnerable items based on business service impact, asset criticality, and vulnerability risk score. Luckily, the majority of affected items are considered non-critical.

Security Operations workflows automate several of the next steps. For business-critical vulnerable items, requests to approve automatic patching are sent. (There is no need to search for who's on call or manually decide which items count as "critical.") Upon approval and completion of the patch, a second scan is automatically run to verify the fix. Using prioritization, workflows, and automation, the most critical items are addressed first.

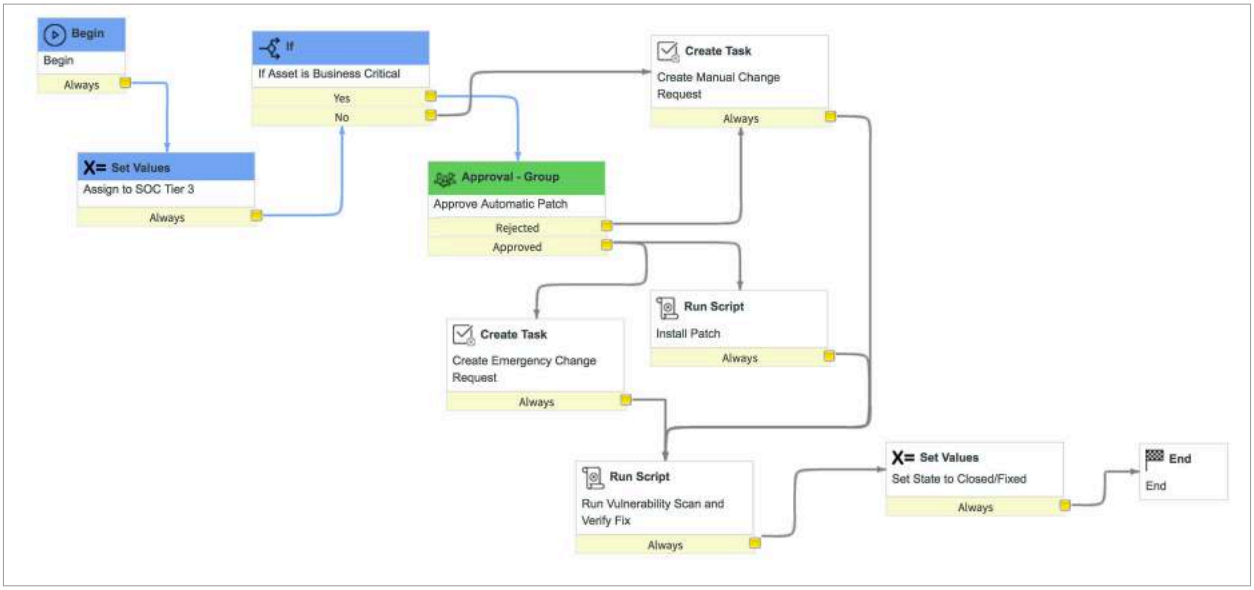


Figure 8: This workflow uses scripts to install emergency patches

Coordinate with IT Using a Single Platform

Since the system seamlessly integrates IT and security, the security analyst is then able to coordinate a plan with IT to address the remaining non-critical vulnerable items from within a single platform. Security Operations can send change requests to IT, only sharing as much security detail as deemed appropriate. (Separate roles can be created to identify who can view security data—providing the ability to limit access as appropriate.) Security Operations workflows automatically route the requests to the right people—eliminating the need to memorize the company's organizational structure. And finally, the CISO can view the Security Operations vulnerability dashboard to see that all critical items have been patched. And since ServiceNow is cloud-based, the CISO can access that information from anywhere in the world.

Conclusion

ServiceNow Security Operations is the most innovative security incident and vulnerability response solution. Security teams can respond faster and more efficiently by reducing the need for manual investigation, and responses are prioritized based on what's most important to the business. Security Operations automates basic tasks and ensures that the security runbook is followed. It tracks all tasks to completion, even through multiple hand-offs. With Security Operations, the security team can now report with confidence, quickly see current exposure via dashboards, conduct post-incident reviews using historical data, and easily track SLAs.

For more information on ServiceNow Security Operations, or to request a demo, visit www.servicenow.com/sec-ops.

About ServiceNow

ServiceNow is changing the way people work. With a service-orientation toward the activities, tasks and processes that make up day-to-day work life, we help the modern enterprise operate faster and be more scalable than ever before. Customers use our service model to define, structure and automate the flow of work, removing dependencies on email and spreadsheets to transform the delivery and management of services for the enterprise. ServiceNow enables service management for every department in the enterprise including IT, security, human resources, facilities, field service and more. We deliver a 'lights-out, light-speed' experience through our enterprise cloud – built to manage everything as a service.

To learn more, follow us on Twitter or visit www.servicenow.com.

SN-WP-SecOpsResponse-082016