ServiceNow Security Operations

A new cyber risk landscape

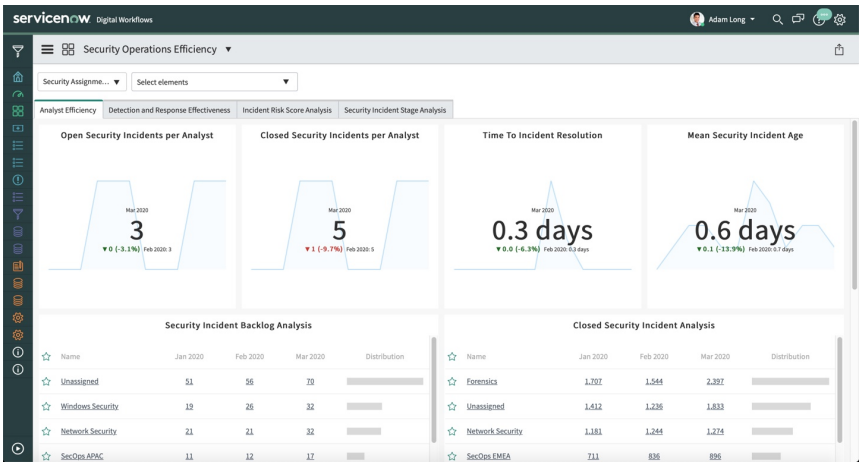
The attack surface has greatly expanded as organizations embrace remote teams, dispersed, cloud-based operations, and software-oriented infrastructure solutions. This has introduced new levels of cyber risk—exposing flaws in existing vulnerability management and security response strategies.

Although organizations have increased their investment in threat intelligence and security products, as many as 60% of them faced a security breach for which they knew a patch was available. [1] This is due to the fact that a majority still do not have comprehensive visibility into applications and services across their security and IT teams, and with IT stakeholders taking an increasing level of security and patching tasks, there exists knowledge gaps in how to respond to and prioritize vulnerabilities and incidents. [1] This can translate to manual incident response processes between IT and Security teams and inconsistent patching refreshes. As a result, costly and time-intensive incident response and vulnerability case backlogs continue to compromise their security posture. Notably, a changing cyber risk landscape exacerbates these existing gaps in security workflows, visibility, and cross-functional coordination.

The ServiceNow solution

ServiceNow® Security Operations is a security orchestration, automation, and response (SOAR) engine built on the Now Platform. Designed to help security and IT teams respond faster and more efficiently to incidents and vulnerabilities, Security Operations uses intelligent workflows, automation, and a deep connection with Security Operations and IT to streamline response. In addition, the solution leverages the ServiceNow® Configuration Management Database (CMDB) to map security incidents to business services and IT infrastructure. This mapping enables prioritization of incident queues and vulnerabilities based on business impact, ensuring your security and IT teams are focused on what is most critical to your business

Within Security Operations, ServiceNow offers two solutions: Security Incident Response and Vulnerability Response.



The Security Operations Efficiency dashboard provides key metrics to know how your SOC is performing and where you need to evolve teams and response workflow.

[1] Source: 2019 Ponemon ServiceNow-sponsored survey, "Costs and Consequences of Gaps in Vulnerability Response"

Connect security and IT

Coordinate response across the organization by standardizing task assignment. Ensure frictionless collaboration between Security and IT to coordinate discovery, identification, and remediation activities.

Drive proactive and fast security response

Reduce the amount of time spent on basic tasks with orchestration tools. Automatically prioritize and respond to vulnerabilities with workflows and automation.

Understand your response strategy

Get a centralized view into security team efficiency by using customizable dashboards and reports. View metrics that help identify bottlenecks and actionable insights into shaping your response and vulnerability management strategy.

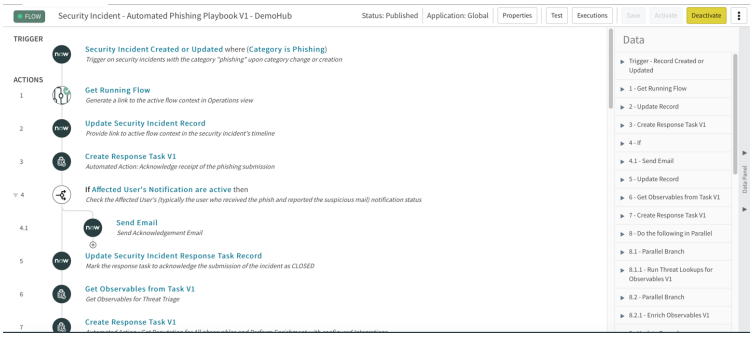
Security Incident Response

ServiceNow® Security Incident Response, a security orchestration and automation response (SOAR) solution, simplifies identification of critical incidents and provides workflow and automation tools to speed up remediation. Data from your existing security tools or Security Information and Event Manager (SIEM) are imported via APIs or direct integrations to automatically create prioritized security incidents.

With Security Incident Response, analysts can easily view and track response tasks that run in parallel. The system will remind assignees if their tasks aren't completed on-time per SLA thresholds, or it can escalate tasks if necessary. Additionally, analysts can also get a centralized view into existing security workflow data using the Security Operations Center (SOC) Dashboard. This helps identify incident trends and can reveal bottlenecks and provide actionable insights.

To speed up response, Security Incident Response automates many tasks, including approval requests, malware scans, and threat enrichment. Orchestration packs for integrated security products facilitate common actions, such as firewall block requests, from within Security Operations. A security knowledge base (KB) adds additional information, and relevant KB articles are automatically associated with incidents for reference.

Security Incident Response simplifies identification of critical incidents and provides workflow and automation tools to speed up remediation.



Using Flow Designer, security tasks and workflows can be easily managed within Security Incident Response.

Security Incident Response achieves swift prioritization and triage of threats through a proactive, data-driven approach. For example, Predictive Intelligence can be utilized for user-reported phishing to help quickly identify suspicious phishing emails, organize your incident queue with built-in classification to pinpoint high-impact cases, and decrease MTTR (mean-time-to-resolve) for phishing incidents.

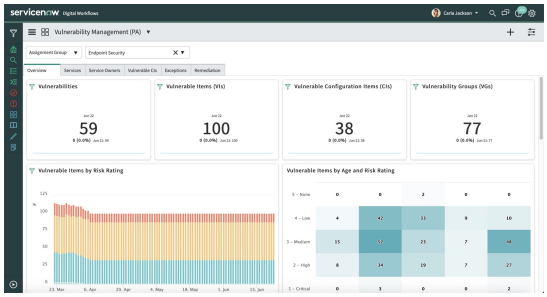
All activities in an incident lifecycle, from analysis and investigation to containment and remediation, are tracked in the platform. Once an incident is closed, assessments are distributed across the team and a time-stamped post-incident review is automatically created as a historical audit record.

Vulnerability Response

ServiceNow® Vulnerability Response helps organizations respond faster and more efficiently to vulnerabilities, connect security and IT teams, and provide real-time visibility. It provides a comprehensive view of all vulnerabilities affecting a given asset or service, as well as the current state of all vulnerabilities affecting the organization. When used with the CMDB, Vulnerability Response can prioritize vulnerable assets by business impact, using a calculated risk score so teams can focus on what is most critical to your organization. The risk score can include multiple factors in its calculation, including the CVSS score of the vulnerability and whether the vulnerability can be easily exploited, using data from the vulnerability scanner and Shodan®.

Vulnerability Response centrally manages both infrastructure and application-level vulnerabilities. In addition to integrating vulnerability scanning data, Vulnerability Response can also assess Dynamic Application Security Testing (DAST) results to track against vulnerable items and coordinate fixes. Within the Now Platform, users can identify, prioritize, and remediate vulnerable misconfigured software in deployment-stage applications using ServiceNow Configuration Compliance. Finally, with Continuous Monitoring, security policies are connected into the vulnerability lifecycle by exchanging data collected from observables and workflows with ServiceNow Governance, Risk and Compliance. This ensures policies across application and infrastructure can be adaptive and stay up to date, and overall dramatically reduces organizational risk.

When critical vulnerabilities are found, Vulnerability Response can automatically initiate an emergency response workflow that notifies stakeholders and creates a high-priority patch request for IT. To ensure accuracy in patching, Vulnerability Response recommends the most impactful remediation activities with Vulnerability Solutions Management. Analysts can also monitor real-time status of patching progress.



The Vulnerability Response dashboard highlights the current status and associated risk of active vulnerabilities in your organization.

Vulnerability Response also improves visibility through reports and dashboards. With ServiceNow Performance Analytics you can easily see which services are impacted by critical vulnerabilities and gain visibility into the organization's risk posture and team performance to quickly identify issues. Trending and predictive analytics can forecast future performance.

To learn more about ServiceNow Security Operations, please visit:
www.servicenow.com/sec-ops

With better visibility, teams can respond more efficiently, reducing both the vulnerability backlog and your risk exposure.

SN-DataSheet-SecurityOperations-091020