ServiceNow Security Incident Response

The security challenge

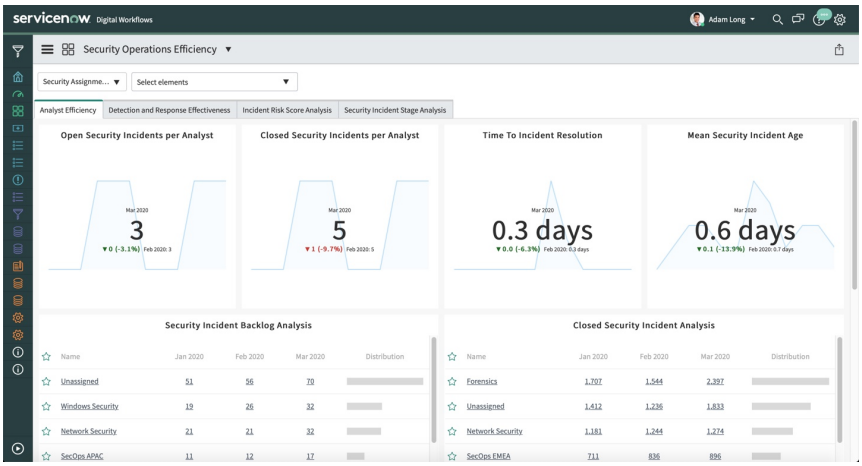
Security teams today are inundated with alerts and information from a growing number of siloed point solutions. In parallel, attacks via both known and unknown threats continuously target critical business services, IT infrastructure, and users. Without business context or a means to organize clear, coordinated workflows, analysts struggle to prioritize threats and organize relevant teams for swift and comprehensive security response. Furthermore, manual processes and cross-team handoffs hinder the security team's ability to efficiently respond to attacks and formulate a more proactive remediation strategy.

An even more fundamental question for security is: Are we secure, and are things getting better or worse? While there is no simple answer, most organizations struggle to establish baseline metrics for their security posture that they can track over time.

Without this understanding, they lack the ability to strengthen their infrastructure and improve their response. The result? Detection and response times that are measured in days or weeks, and potentially missed attacks that lead to a breach or compromise.

The ServiceNow solution

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. Customize security workflow templates to automate tasks and ensure company best practices are followed. This helps organizations connect security and IT teams to respond faster and more efficiently to threats, as well as gain a definitive view of their security posture. 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 based on business impact, ensuring your security teams are focused on what is most critical to your business.



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.

Drive proactive and fast security response

Prioritize threats by business context and automate required actions to triage and remediate incidents quicker. Leverage easy-to-follow workflows and Predictive Intelligence to reduce incident backlog.

Connect security and IT

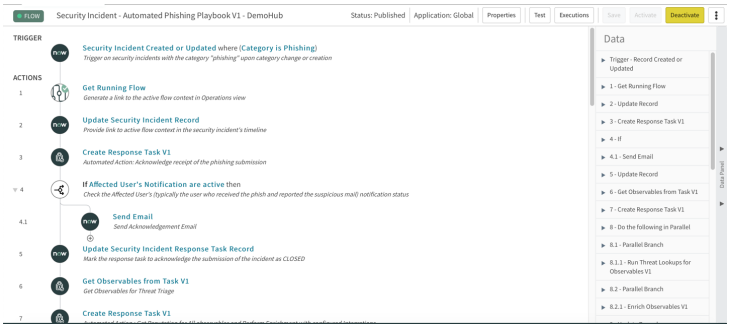
Coordinate response across the organization and standardize task assignment. Ensure frictionless collaboration between Security and IT for discovery, identification, and remediation activities.

Understand your response strategy

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

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.



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

Security Incident Response achieves swift prioritization and incident triage 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. This serves to cut down the incident backlog and dramatically improve operational efficiency for security teams.

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.

ServiceNow Security Operations

Security Incident Response is part of ServiceNow Security Operations, a security orchestration, automation, and response (SOAR) engine built on the Now Platform. Designed to help security teams respond faster and more efficiently to incidents and vulnerabilities, Security Operations uses intelligent workflows, automation, and a deep connection with IT to streamline security response.

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

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

servicenow