ServiceNow Security Operations

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 vulnerabilities continuously target critical business services, IT infrastructure, and users. These incidents and vulnerabilities lack business context, making it difficult to know which ones pose the greatest threat to the organization. Furthermore, manual processes and cross-team handoffs hinder the security team's ability to efficiently respond to attacks or assess and remediate vulnerabilities.

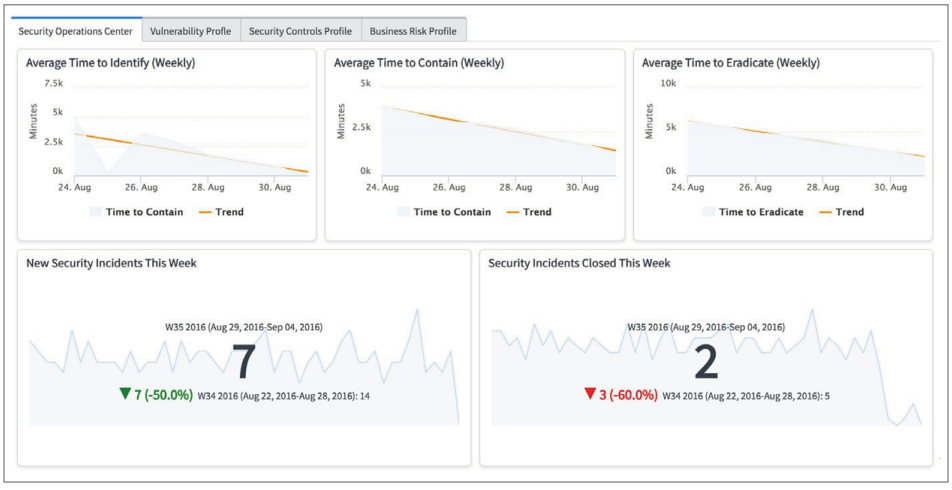
An even more fundamental question for security is: Are we secure, and are things getting better or worse? While there is no simple answer, most organizations struggle to establish baseline metrics for their security posture that they can track over time. Without this understanding, they lack the ability to strengthen the infrastructure and improve their response.

The result? Detection and response times that are measured in months, and missed attacks that could lead to an eventual breach or compromise.

The ServiceNow solution

ServiceNow® Security Operations helps organizations connect security and IT teams, respond faster and more efficiently to threats, and get a definitive view of their security posture. It connects the workflow and systems management capabilities of the Now Platform™ with security data from leading vendors to give your teams a single platform for response that can be shared between security and IT. With orchestration, automation, and better visibility, teams can respond more efficiently, reducing business risk.

The solution leverages the ServiceNow® Configuration Management Database (CMDB) to map threats, security incidents, and vulnerabilities to business services and IT infrastructure. This mapping enables prioritization and risk scoring based on business impact, ensuring your security teams are focused on what is most critical to your business. In addition, visual business service maps show the dependencies of affected systems to minimize change requests and downtime. Because Security Operations is part of the greater Now Platform, this CMDB is maintained by the entire organization, not just security.



Customizable real-time dashboards show security posture.

Connect security and IT

Coordinate response across teams for smoother task handoffs between groups and quicker resolution. Get accountability across the organization and know work is getting done with SLAs.

Drive faster, more efficient security response

Reduce the amount of time spent on basic tasks with orchestration tools. Automatically add threat intelligence to security incidents to speed up remediation and integrate a response platform with your existing security portfolio.

Know your security posture

View your current security status with customizable dashboards and reports backed by quantitative data. Improve processes and team performance through metrics and post-incident reviews.

The Now Platform delivers additional enterprise capabilities that teams can leverage right away, such as built-in service level agreement (SLA) thresholds, skills-based routing, notifications, advanced workflows, and live collaboration. Security Operations also isolates security events from the rest of the system, ensuring that sensitive security data remains confidential.

Security Incident Response application

Security Incident Response 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 email alerts to automatically create prioritized security incidents. Customize security workflow templates to automate tasks and ensure company best practices are followed.

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. This ensures no tasks or decisions are accidentally missed. Security analysts can communicate with stakeholders from within the Now Platform via conference calls or Connect chat to keep everyone in the loop.

To speed up response and allow your security team to spend more time hunting complex threats, Security Incident Response automates basic tasks, including approval requests, malware scans, or threat enrichment when used with the Threat Intelligence application. 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.

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 application

The Vulnerability Response application in Security Operations prioritizes vulnerable assets and adds context to help determine if business-critical systems are at risk. By leveraging the CMDB, it can also easily identify dependencies across systems and quickly assess the business impact of changes or downtime. Vulnerability Response provides a comprehensive view of all vulnerabilities affecting a given service as well as the current state of all vulnerabilities affecting the organization.

Response teams can also leverage the workflow and automation tools in the Now Platform to remediate vulnerabilities faster. When critical vulnerabilities are found, a workflow can automatically initiate an emergency patch approval request. Once approved, orchestration tools can apply the patch and trigger an additional vulnerability scan to ensure the issue has been resolved.

For non-urgent patches, simply click a button to create a change request and send the relevant information to IT. This results in a coordinated remediation strategy for vulnerabilities across services and assets that can address the most critical items quickly.

“

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

Configuration Compliance application

Improperly configured software puts organizations at risk of compromise. Configuration Compliance prioritizes and remediates vulnerable misconfigured assets from third-party security configuration assessment scan data. It leverages the CMDB to determine which items are most critical. Workflows and automation enable quick action against individual assets or groups for bulk changes.

Easily coordinate with IT in a single platform to address changes and updates. In addition, Configuration Compliance data can be fed into the continuous monitoring feature of ServiceNow® Governance, Risk, and Compliance to further mitigate risk.

Threat Intelligence application

Security Operations includes a threat intelligence application to help incident responders find Indicators of Compromise (IoC) and hunt for low-lying attacks and threats. It automatically searches threat feeds for relevant information when an IoC is connected to a security incident and can send IoCs to third-party sources for additional analysis. The results are reported directly in the security incident record for the analyst to review, saving valuable time. ServiceNow supports multiple threat feeds, as well as STIX and TAXII, to incorporate threat intelligence data from a variety of sources.

Trusted Security Circles application

Share threat intelligence data with industry peers, suppliers, or a global circle of ServiceNow customers with Trusted Security Circles. Send an anonymous query containing security observables to other users and receive a sightings count automatically. With this data, security analysts can determine whether suspicious activity may be part of a larger attack.

Users can set sightings count thresholds to automatically create a security incident if the observable count limit is exceeded. Participating in Trusted Security Circles can serve as an early warning of attacks targeted at common groups.

Performance Analytics for Security Operations

Create advanced real-time dashboards and reports with the addition of Performance Analytics. It includes built-in key performance indicators (KPIs) and allows creation of additional custom KPIs to track the metrics that are most important to your organization. Use historical data to find bottlenecks, refine response processes, and identify tasks for automation. Get improved visibility and confidence in your security posture with trusted data.

“Security Operations includes a threat intelligence application to help incident responders find Indicators of Compromise and hunt for low-lying attacks and threats.

servicenow