ServiceNow® Security Operations

Resolve security incidents and vulnerabilities fast with prioritization, automation, and orchestration
Security response today is too slow and complex

Is your business secure? It’s a straightforward question that can be difficult to answer. Most organizations today use a variety of different security products, often from different vendors, that don’t communicate with each other. These products generate thousands of notifications and alerts—far more than your security team can investigate. As a result, it’s possible for issues to be missed simply because they were hidden amid the noise.

These challenges lead to long discovery and remediation times when incidents occur. In 2018, the Ponemon Institute reported that it took organizations an average of 197 days to spot a breach and 69 days to contain it. That’s nearly nine months from infection to remediation.

In addition, many organizations track remediation in spreadsheets or via email, which are difficult to maintain and report from. These manual processes add up to lost time, averaging 12 days to coordinate vulnerability response across security and IT.1 A study from the Enterprise Strategy Group also cited coordination across teams as the top incident response challenge.2

How long does it take your team to resolve security incidents on average? This can be difficult to answer with manual methods. What kind of records do you have so you can repeat the process next time something similar happens?

Solving these issues requires a solution that connects security and IT and provides better visibility, in turn helping you deliver faster, more efficient security response.

---

1 Ponemon Institute, Today’s State of Vulnerability Response: Patch Work Requires Attention. March 2018
What would make your security team more efficient when responding to incidents?

• Prioritization by asset criticality
• Spending less time on manual tasks

ServiceNow Security Operations is a security orchestration, automation, and response engine that leverages key strengths of the Now Platform™, including intelligent workflows, prioritization, and a deep connection with IT. It adds capabilities for security incident response, vulnerability response, and threat intelligence.

When Security Operations receives alerts from your existing security products, it can deduplicate events and create security incidents. Before the incident is assigned to an analyst, the affected asset is matched against the ServiceNow Configuration Management Database (CMDB) to determine priority based on how critical the asset is to your business.

In parallel, Security Operations correlates threat intelligence data and automates analysis using orchestration tools to perform additional malware scans or pull running processes from an affected endpoint. This condenses up to an hour of research into just seconds. The security analyst now has a wealth of information available from the very first moment he reviews the incident.

How do you better connect security and IT?

• Have security and IT work from the same platform
• Use service level agreement tracking for accountability

With ServiceNow, security analysts and vulnerability managers better communicate with IT by working from a unified platform. They can easily hand off tasks, such as patching, to IT while still maintaining visibility into the task. Skills-based routing assigns tasks to the correct responders, and service level agreement tracking ensures they are completed on-time.

ServiceNow’s single platform allows security and IT to collaborate faster, but access to sensitive security data is protected through user roles. This means even a ServiceNow admin can’t see security data unless he also has a security role.
How do you know if you’re secure?

• Visual dashboards of incidents and vulnerabilities
• Dynamic trend and performance data

Security Operations uses customizable role-based dashboards and reports to quickly show your overall security posture. Quickly see the latest status of all security incidents and vulnerabilities along with additional context to know whether critical business services are affected. These dynamic dashboards utilize ServiceNow Performance Analytics to track performance over time to know if things are getting better or worse.

Streamline your security operations with ServiceNow. For more information or to request a demo, visit [http://www.servicenow.com/sec-ops](http://www.servicenow.com/sec-ops)