ServiceNow Security Incident Response

Wanted: Cyber resilience under pressure

Security Operations teams continue to show grace under pressure, every day. With ever-greater reliance on digital systems, the job is getting harder, every day. According to Enterprise Strategy Group Research, security and IT professionals continue to struggle with SOC modernization:

- 70% say it is difficult to recruit additional SOC staff
- Nearly 2/3rds are adopting new tech for automation and orchestration
- Top two priorities are integrating security and IT tools and improving collaboration between security and IT staff
- 81% say MITRE ATT&CK® is an important component of their security posture

Transform investigations and response

ServiceNow® Security Incident Response, a security orchestration and automation response (SOAR) solution, helps you rapidly respond to evolving threats while optimizing and orchestrating enterprise security operations. Security Incident Response eliminates the errors and friction natural to manual handoffs across systems, teams and responsibilities. Integrations, playbooks, dashboards, and a common data model for enterprise case management expedite investigation, response, and remediation across IT, Security, and Risk teams to minimize incident impact, data loss, and exposure. This drives maturity of your security operations, and centralizes case management for threats, data loss events, and more.

Automate away the basics to focus on the critical

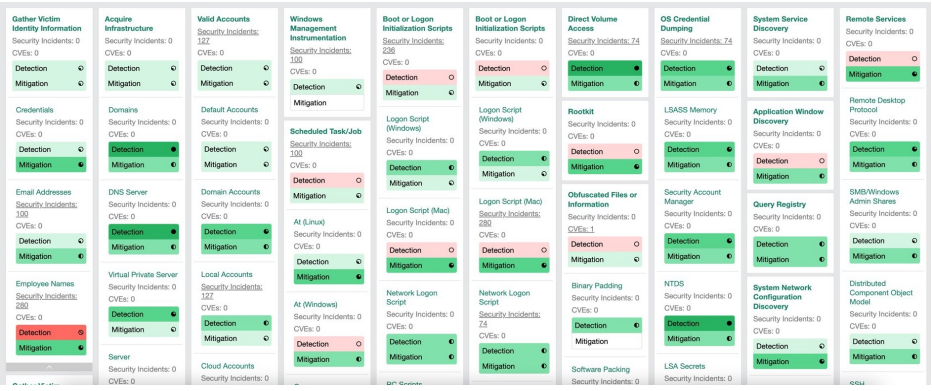
A playbook library gets you started quickly, and hundreds of integrations and apps can be downloaded from the ServiceNow store. Orchestration packs for integrated security products facilitate common actions, such as firewall block requests. For instance, routine phishing and malware response can be fully automated, as well as approval requests and threat enrichment. Within workflows, AI simplifies identification of critical incidents and expedites assignment to the right analysts and responders. A SOC efficiency dashboard provides ongoing visibility into trends and helps identify areas for further automation and risk reduction.

Make your team more satisfied and productive

Automation helps your workforce scale to succeed in a mode of constant change. Security analysts can focus their attention from basic, repetitive duties to more challenging work. At the same time, success and morale go up as integrated intelligence and asset data help prioritize investigations based on risk.

Proactively manage threat exposure using MITRE ATT@CK and threat intel

The MITRE ATT&CK framework is integrated into playbooks and analytics. The latest adversarial and threat insights enable security teams to optimize workflows, tools, and skills against evolving attack techniques to profile and predict active attacker behavior, and guide response. It even tells you where to boost defenses.



Key Features

Major Security Incident Management

Centralize operations to better prepare and respond to high profile security incidents such as ransomware, data breaches, targeted attacks

DLP Incident Response[1]

Integrate DLP Incident Response with your DLP tool to reduce exposure and respond quickly to contain data loss events

CISO Dashboard

Assess exposure, measure and monitor progress against key metrics, and get real-time, actionable insights about changing security posture

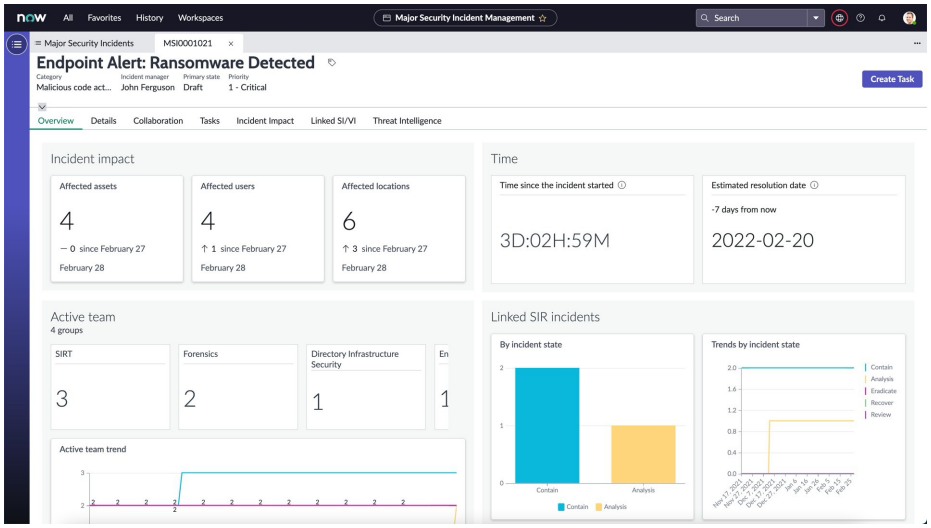
MITRE ATT&CK

Optimize defenses, forecast attack behaviors, predict targets, and define and automate response based on attacker behavior, TTPs, and risk

Proven Playbooks

Scale team capacity and increase expertise with automated playbooks for common events such as phishing and malware

[1]DLP Incident Response is a product within the ServiceNow Security Operations portfolio.



Major Security Incident Management creates a cross-functional command center.

Modernize Your SOC with ServiceNow
To elevate your security capabilities, Security Incident Response incorporates many process and productivity improvements. 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. Incidents are automatically associated with relevant security knowledge base (KB) articles for reference.

Bridge security, risk, and IT to remove friction, risk, and errors
Security teams need to collaborate with IT and risk counterparts for effective investigation, management and resolution of incidents. With Security Incident Response, security teams can access a wealth of contextual information about services, assets, owners, risks, and compliance without extensive integration work. Playbooks pull this information automatically, replacing emails and spreadsheets.

Orchestrate enterprise-wide incidents with ease
Data breaches, ransomware, and zero-day vulnerabilities are just some of the big and breaking problems that trigger crisis response. As regulators shorten disclosure windows, you need to be prepared and ready. With ServiceNow, purpose-built workspaces connect stakeholders from execs to IT to legal to PR in a consistent experience with appropriate data access. This crisis command center supports the collaboration, efficiency, and evidence-handling essential to critical situations.

Adapt actions to changing best practices
As an intelligent workflow platform, ServiceNow provides tools to quickly configure and construct playbooks, without writing code or waiting for IT. This makes it easy to embed policies and preferred practices into activities, shorten learning curves, and avoid problems that often come with ad hoc decisions under pressure.

Visibility and assessment for continuous performance improvement
Maturity is a journey that each organization travels at their own pace. ServiceNow quantifies processes and captures key metrics and indicators to give you visibility into what is happening, what is working, and what could improve your security posture and performance. Built-in analytics drive role-based dashboards and reporting so leaders and analysts can identify trends early and act—tuning playbooks, protections, staffing, and training to meet this dynamic threat evolution.

Accelerate your team's success with the ServiceNow Security Operations portfolio.

> "Security Incident Response allows SAS to manage the lifecycle of security threats. SAS can now understand the nature of security incidents, spot trends, and deal with bottlenecks.
>
> Threats are identified within 1 minute, contained in less than 10 minutes, and analyzed within the hour.
>
> —Scandinavian Airlines

servicenow

SN_DataSheet_SecurityIncidentResponse_02012024