Transform Enterprise Security

Wanted: Cyber resilience under pressure

ServiceNow Security Operations helps security teams scale faster, smarter and more efficiently, enabling and automating critical collaboration of data and process between IT, security, and risk to effectively respond and remediate threats. It brings in security and vulnerability data from your existing tools and uses intelligent workflows, automation, and a deep connection with IT to streamline security response. ServiceNow Security Operations helps you use the power of the Now Platform to reduce cybersecurity risk and drive cyber resilience.

Transform investigations and response

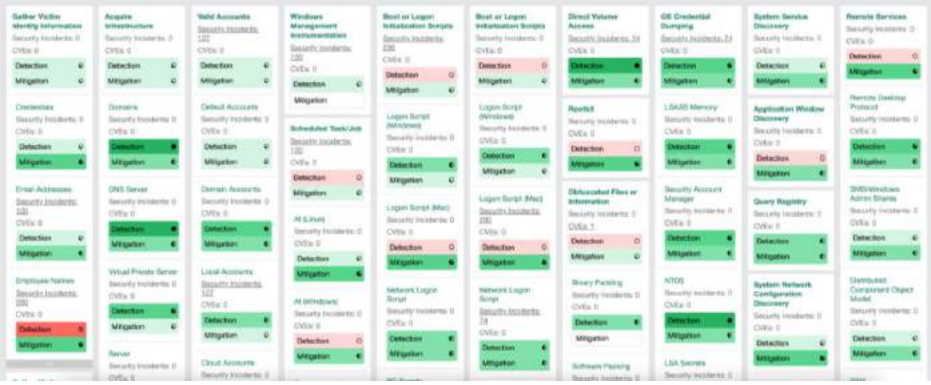
ServiceNow® Security Incident Response, a security orchestration and automation response (SOAR) solution, helps you rapidly respond to evolving threats while optimizing and orchestrating enterprise security operations. Security Incident Response eliminates the errors and friction natural to manual handoffs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

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.

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.



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.

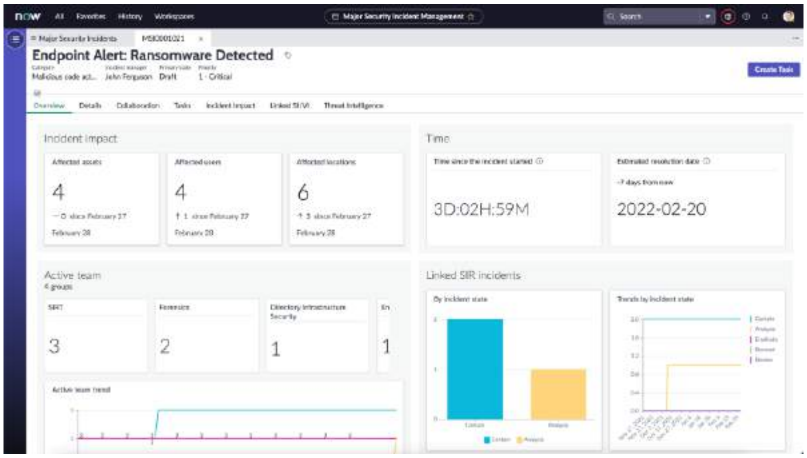
Key Features: Incident Response

- Major Security Incident Management
- DLP Incident Response[1]
- CISO Dashboard
- MITRE ATT&CK
- Proven Playbooks

Key Features: Vulnerability Response

- Modern collab spaces
-
- Expansive visibility
-
- Automation, not backlogs
- Prioritization your way
- Vulnerability Solutions Management
- Performance analytics

[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.

Harden the attack surface exploding across cloud, infrastructure, and applications

According to the Enterprise Strategy Group (ESG) Security Hygiene and Posture Management report, nearly 7 out of 10 respondents admitted to a cyber breach resulting from exploitation of unknown, unmanaged, or poorly-managed internet-facing assets.

Vulnerabilities pose a serious threat to business reputation and data security. Methods to exploit vulnerabilities are growing more sophisticated, with cybercriminals increasingly leveraging machine learning and artificial intelligence to thwart traditional vulnerability response mechanisms.

One of the operational dilemmas for security teams is their dependency on IT teams and tools for scanning and asset data and for actual patching or mitigation of issues. It really takes a team. And almost every organization's security and IT teams struggle to keep up with the sheer volume of vulnerabilities in an ever-increasing, ever-diversifying attack surface.

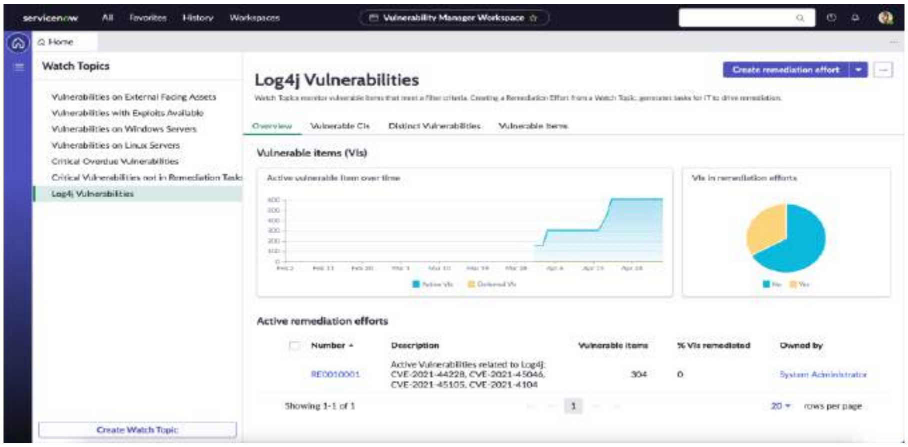
Transform operations with ServiceNow risk-based vulnerability management

ServiceNow Vulnerability Response synthesizes asset, severity, exploit, risk, and threat intelligence insights into automated workflows for fast, reliable prioritization and remediation. App integrations on the store plug in multiple cloud, application testing, penetration testing, vulnerability assessment, OT/IT discovery, and asset management tools for fast time to visibility across your evolving attack surface.

> “
>
> 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

Coordinate with application owners, developers, and the risk team

With broad DevOps and Agile adoption, internal software developers present a special challenge. Our included ServiceNow Application Vulnerability Response unites your processes and teams to improve security at the speed of software development. You can prioritize vulnerabilities and coordinate fixes with developers in deployed applications. You can also identify, prioritize, and remediate vulnerable misconfigured software with ServiceNow Configuration Compliance.


servicenow
All
Favorites
History
Workspaces
Vulnerability Manager Workspace
Home
Watch Topics
Vulnerabilities on External Facing Assets
Vulnerabilities with Exploits Available
Vulnerabilities on Windows Servers
Vulnerabilities on Linux Servers
Critical Overdue Vulnerabilities
Critical Vulnerabilities not in Remediation Task
Log4j Vulnerabilities
Create Watch Topic
Create remediation effort
Overview
Vulnerable CIs
Distinct Vulnerabilities
Vulnerable Items
Active vulnerable item over time
600
500
400
300
200
100
0
Feb 2
Feb 11
Feb 20
Mar 1
Mar 10
Mar 19
Mar 28
Apr 6
Apr 15
Apr 24
Active VIs
Deferred VIs
VIs in remediation efforts
No
Yes

Log4j Vulnerabilities

Watch Topics monitor vulnerable items that meet a filter criteria. Creating a Remediation Effort from a Watch Topic generates tasks for IT to drive remediation.

Vulnerable items (VIs)

Active remediation efforts

□ Number ▲	Description	Vulnerable items	% VIs remediated	Owned by
RE0010001	Active Vulnerabilities related to Log4j: CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104	304	0	System Administrator

Showing 1-1 of 1   1   20 ▾ rows per page

Security and IT teams build trust with a collaboration space for vulnerability, risk, and remediation activities.

Use in-depth IT and asset insights to prioritize and build up an accurate CMDB

In the ESG survey, the top source of prioritization and patching data is vendor products in use, especially those with high-criticality. When used with the ServiceNow Configuration Management Database (CMDB), Vulnerability Response provides a comprehensive view of all vulnerabilities affecting a given asset or service, as well as the current state of all vulnerabilities across the organization.

> “With ServiceNow, Prime has created a highly structured, efficient process. We know exactly where each vulnerability stands and what IT is doing to fix it.
>
> — Prime Therapeutics

Respond efficiently across security and IT when critical vulnerabilities appear

When critical vulnerabilities are found, Vulnerability Response can automatically initiate emergency response workflows that notify stakeholders and create high-priority patch requests for remediation owners.

Vulnerability managers can create watch topics to help them quickly identify risky vulnerabilities, such as a high risk score, specific critical CVE, exploitable vulnerabilities, overdue tasks, and more, allowing for easier, more precise monitoring. Stakeholders can continuously monitor real-time status of patching progress and ensure process visibility across security and IT.

For maximum impact on vulnerability risk, you can also easily identify the most beneficial activities with Vulnerability Solution Management. It works by matching vulnerability scan data against Microsoft or Red Hat's solution databases to recommend which to deploy based on supersedence. Once the best solution is found, use Patch Orchestration to complete the last mile of the vulnerability journey: automating the patching process via 3rd party patch tools.

Transform Enterprise Security

Security Incident Response and Vulnerability Response are part of the ServiceNow Security Operations portfolio. To learn more, please visit: **www.servicenow.com/sec-ops**