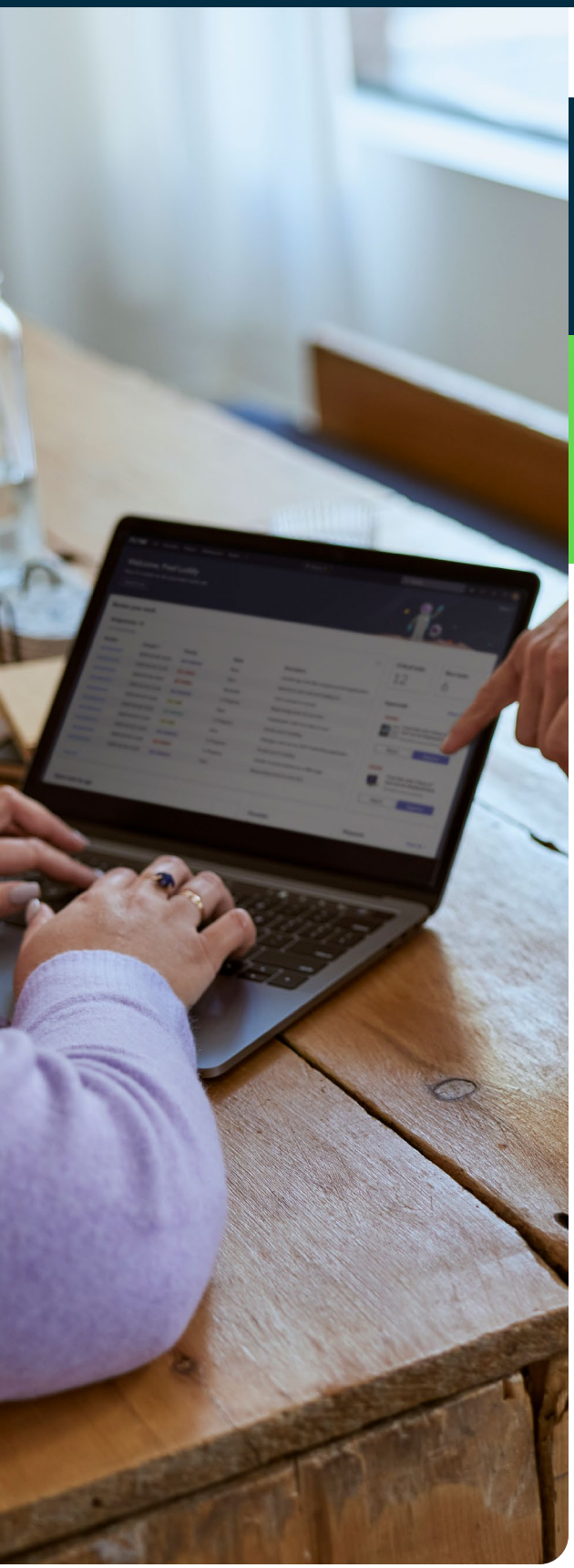
servicenow

Imperative Guide

3 steps to transforming security operations

How to be more agile, effective, collaborative, and scalable



Here's your roadmap for automating processes and data-sharing among IT, security and risk management teams to rapidly remediate threats.

In our technology excellence handbook, we discussed the top four, forward-looking imperatives that are driving business transformation and growth. One imperative that frees up your teams to focus on what's next is transforming security operations. When enterprises like yours can reduce cybersecurity risk and drive cyber resilience, you can confidently support the technology change your organization needs to thrive in uncertain times.

As you rely more on the cloud, new devices, and transformative services, you face growing threat vectors and increasingly complex environments. Today, 277 days is the average time to identify and contain a cyberbreach and each breach leads to an average loss to organizations of $4.35M.[1] That's unacceptable. In this brief guide, you'll get a 3-step roadmap for innovation in security operations that will show you how to rapidly mitigate ever-changing security risks, despite increasing attack surface complexity, threat volumes, and skills shortages. You'll also discover how to take the burden off of overworked and limited staff, as well as free up 8,700 hours annually[2] that you can redirect toward other critical business areas.

Step 1

Systematically harden the digital attack surface with integrated, AI-driven processes

90% of security leaders believe their organization is falling short in addressing cyber risks.[3] Yet many risks are avoidable. For example, using emails and spreadsheets to manage security response processes lets things slip through the cracks—hardly an efficient way to assess and protect your entire attack surface. What you need are optimized and automated workflows that unite security, risk, IT, and asset management—because threats don't care about business silos. Such an approach can improve the mean time to contain breaches—wait for it—by 85%.[4] This approach empowers you with:

- **Data on severity, business context, risk levels, true exposure, and external threat intelligence** for a scoring system to prioritize and drive incident response
- **AI-powered intelligence** to assign mitigations and remediations to the right teams for the most efficient and effective actions
- **Visibility across your digital infrastructure**—including applications, cloud, OT, and services—to uncover assets and their vulnerabilities
- **Automatic patch orchestration** that works with change management systems and the CMDB to avoid disruption and continuously minimize vulnerabilities

REAL-WORLD EXAMPLE

SAS
Scandinavian Airlines

Six systems consolidated into one to speed up responses to cyberthreats

SAS, one of the world's largest airlines, is a global, digital-first business—and a highly attractive target to cybercriminals. Its main priority is safeguarding company and passenger data. With ServiceNow Security Operations, SAS can easily understand security threats, spot trends, and vanquish attacks. It also monitors performance on all business-critical systems.

LEARN MORE

"We're a digital—first airline. Cybersecurity is foundational for our business."

Thomas Widen, Head of cybersecurity and compliance for SAS

>1 minute
to identify a threat

>10 minutes
to contain it

>1 hour
to analyze future risk

Step 2

Optimize and orchestrate enterprise security operations to improve investigations, decisions, and threat responses

More threats, a talent shortage, and mistakes from overworked staff are taking a toll: 84% of cybersecurity professionals are experiencing burnout.[5] You can reduce the workload and boost security analyst efficiency by 300%[6] if you transform and modernize security operations with digital workflows that enhance analyses, conclusions, and actions. Start by using automated, best practice playbooks connected to IT and third-party data, tools, and teams. Other essential tactics:

- **Use security orchestration, automation, and response (the SOAR approach), to scale resources and give your teams more interesting work;** SOAR also reduces errors and friction from handoffs across tools and responsibilities.
- **Connect the security operations center (SOC), network operations center (NOC), and data protection teams** for seamless management, extraordinary efficiency, and close collaboration that will become critical for major incident management.

REAL-WORLD EXAMPLE

YOKOGAWA

How to drastically reduce cyberthreat response and breach recovery times

Yokogawa Electric develops and manufactures measurement and control equipment for oil, gas, and chemical industries, to name a few. Inconsistent IT security management put the company's global operations at risk. With ServiceNow, the company streamlined its security workflows to shorten incident response times by 30%.

LEARN MORE

"ServiceNow ITOM and Security Operations provide visibility of global IT asset management statuses, and automate security breach prevention from serious threats."

Tetsuo Shiozaki, deputy head of digital strategy

35K
global IT assets visible

30%
efficiency gain by prioritizing incidents

1 minute
from threat detection to response, vs. 1 to 3 weeks previously

Step 3

Respond with agility and minimize impact of evolving cyberthreats

It's eye opening: A record 26,448 software security flaws were reported in 2022, with the number of critical vulnerabilities up 59% over the previous year.[7] To avoid attempted exploits, you need to leverage everything in your arsenal: playbooks, automation, intelligence, and integrations with multiple vendor solutions. All of these weapons can trigger throughout the kill chain to reduce delays in response as well as the attacker's ability to succeed. If you're vigilant, you can reduce open vulnerabilities by 80%.[8] But be prepared to:

- **Take control of infrastructure and cloud security configurations** to improve security posture and maintain compliance.
- **Use real-time, adversarial insights** to skillfully beat back evolving attack techniques, predict attacker behavior, and guide your responses to high-profile incidents like ransomware and data breaches.
- **Monitor performance of processes and analysts** for continuous improvement as well as reduced risk and exposure.
- **Take advantage of integrations, playbooks, dashboards, and a common data model** to speed investigations and responses across IT, security, and risk teams and minimize impact on the organization (including data loss and reputational damage).

REAL-WORLD EXAMPLE

Wellstar HEALTH SYSTEM

Security and IT teams collaborate to rapidly remediate vulnerabilities

Wellstar Health System is a regional—but nationally ranked—U.S. healthcare network. To ensure it could continue providing excellent patient care, the company established an efficient vulnerability management system built on the ServiceNow platform. With a clear plan for prioritization, assignment, and grouping, remediation of vulnerabilities is executed efficiently.

LEARN MORE

"Wading through laborious spreadsheets to provide data to meet compliance is now a challenge of the past. Senior leadership has access to performance analytics through one intuitive dashboard with customized reporting."

ITS Partners, which helped implement the vulnerability management system

99%
of vulnerability groups are assigned correctly

92.5%
of all vulnerability items are remediated within SLA targets

100%
of critical vulnerabilities are effectively remediated

Walk the steps confidently with your bright ideas

With a rapidly expanding attack surface and an ever-growing volume of costly threats, the path to transforming security operations for technology leaders like you is clouded with challenges: sharing siloed data, prioritizing vulnerabilities, responding quickly despite manual processes, and burning out your teams, to name a few. But it has never been clearer that AI-driven, automated workflows and intra-departmental collaboration can light your way. Only ServiceNow enables you to bring together security, risk, IT, and asset management on a unified cloud platform to deliver a single source of truth. With ServiceNow, you can gain unprecedented visibility of threats, nimbly cover an expanding attack surface, and drive continual cyber resilience. With these capabilities, you can lead your organization confidently and boldly into a secure future in which the enterprise can thrive.

servicenow

Learn more

about how ServiceNow Security Operations can protect your organization for unimpeded business growth:

SecOps use case guide

SecOps on servicenow.com

References

1. Cost of a Data Breach Report, Ponemon Institute, 2022
2. ServiceNow customer results (technology company)
3. Foundry 2022 Security Priority Study, 2022
4. ServiceNow customer results (global manufacturer)
5. Mimecast, How to Combat Cybersecurity Burnout — and Keep Your Company Secure, 2022
6. ServiceNow customer results (major consulting firm)
7. The Stack, We analysed 90,000+ software vulnerabilities: Here's what we learned, 2023
8. ServiceNow customer results (prominent insurance company)

About ServiceNow

ServiceNow (NYSE: NOW) makes the world work better for everyone. Our cloud-based platform and solutions help digitize and unify organizations so that they can find smarter, faster, better ways to make work flow. So employees and customers can be more connected, more innovative, and more agile. And we can all create the future we imagine. The world works with ServiceNow™. For more information, visit: **www.servicenow.com**.

SN-Security Operations IG-032023