Five ways to safely weather cybersecurity storms

How to automate security incident response to bridge the gap between IT and security

Introduction

The global pandemic created a perfect storm for cybercrime. With so much of the world now working remotely, the playing field for cyberattacks has never been bigger. And how companies respond to security incidents has never been more important.

Obstacles in your way

But 28% organizations still can't prioritize incidents quickly.[1] And 41% of them say that manual processes and siloed data often hinder response times[1] Both obstacles can deprive security and IT teams of the information they need to make the right decisions—and make them fast.

Automation clears the path

In this eBook, we'll discuss five ways you can navigate the choppier waters of cyberthreats. You'll discover why it's critical to automate security incident response (SIR), how automation helps security and IT teams to collaborate on combatting ever-increasing threats, and how ServiceNow® Security Incident Response can help your organization respond more efficiently and effectively than ever before.

The "perfect storm" created by the global pandemic:

100K+

pandemic-related domains registered in 2021 (50% more likely to be malicious) [2]

775%

increase in Microsoft Teams monthly users over the last year [2]

667%

increase in pandemic-related phishing emails since start of pandemic[2]

76%

of organizations have no common view of assets and applications across security and IT [3]

56%

of organizations say things slip through the cracks due to manual response processes [3]

62%

of breached organizations were unaware that they were vulnerable [3]

82%

of employers report lack of cybersecurity skills [3]

1. Gain visibility into critical incidents

The first way to protect your organization is to empower yourself to identify high-impact threats in real time, and at scale. And that capability starts with visibility. You must continually monitor and accurately assess security incidents across your entire organization—which includes remote workers.

Pulling the data together

It might be tempting to deploy a whole ecosystem of security products—which might include detection tools, and security information and event management (SIEM) systems, as well as vulnerability and threat intelligence solutions. But you might end up with more notifications and alerts than your security team can manage. To see all the changes in your IT estate that can potentially threaten your business, you need to pull all that data together.

Single system of record

With the average enterprise using 75 security tools in their SOC, having a single system of record to hold everything from the related path to notes and attachment helps drive prioritization, cyber resilience, and collaboration. With ServiceNow Security Incident Response, a scoped application, companies need to require separate access permissions—so you're always respecting the data.

Manage incidents anywhere

ServiceNow Security Incident Response drives data from all the various vendors and tools into a single platform. This lets you put incidents in context and ensures you're analyzing and employing the data in the best way possible. To maintain visibility, security analysts need to stay connected to the security operation center (SOC) at all times—whether they're working remotely or just stepping out for coffee. With the Security Incident Response mobile app, security analysts can view and manage incidents anytime, anywhere. After all, cybercriminals probably don't take coffee breaks.

> **"Companies with fully deployed automated security solutions save an average in $2.5 million per year by preventing breaches.[3] Driving cyber-resilience and operational efficiencies is really important in this new normal."**
>
> – Karl Klaessig, cybersecurity expert, ServiceNow

2. Prioritize security incidents quickly

With tens of thousands of incidents happening at any given moment, knowing where to focus your team is another essential way to address cyberthreats. Combining visibility with context will allow you to prioritize events by business criticality and make better decisions. It's key to assign tasks to responders based on areas of expertise and bandwidth, then align the right data with the right people for remediation.

Working at machine speed

You should also automate this prioritization and assignment process, so it happens at machine speed. Manual SIR processes, which are often done in silos, can take hours, days, or even weeks—from the initial alert all the way through to post-incident review and manual enrichment. These processes are also error prone. Automating processes within this workflow reduces manual handoffs, decreasing the chance of errors while bridging the gap between security and IT. It allows you to identify dependencies across the system, which aligns the response across teams and ensures a timely response. You also gain a better understanding of how you can improve your organization's resiliency against threats.

Results of automating SIR

At ServiceNow, we've seen automation reduce triage time by 50% and investigation time by 40% with our own customers. In fact, according to Forrester, companies using the ServiceNow® Security Operations platform saw a 45% increase in security incident response, and their tier-2 security analysts were able to respond to 50% more incidents.[4]

80%

of organizations that use automation say they can respond to vulnerabilities in a shorter timeframe.[3]

3. Accelerate response time with collaboration

Threats today move faster than ever, so speed is a crucial way to successfully remediate cyberattacks. Orchestrating and automating actions and insights across teams will allow you to improve both performance and productivity. By doing this, you standardize best practices to create consistent and repeatable cross-functional workflows. You become proactive, not reactive.

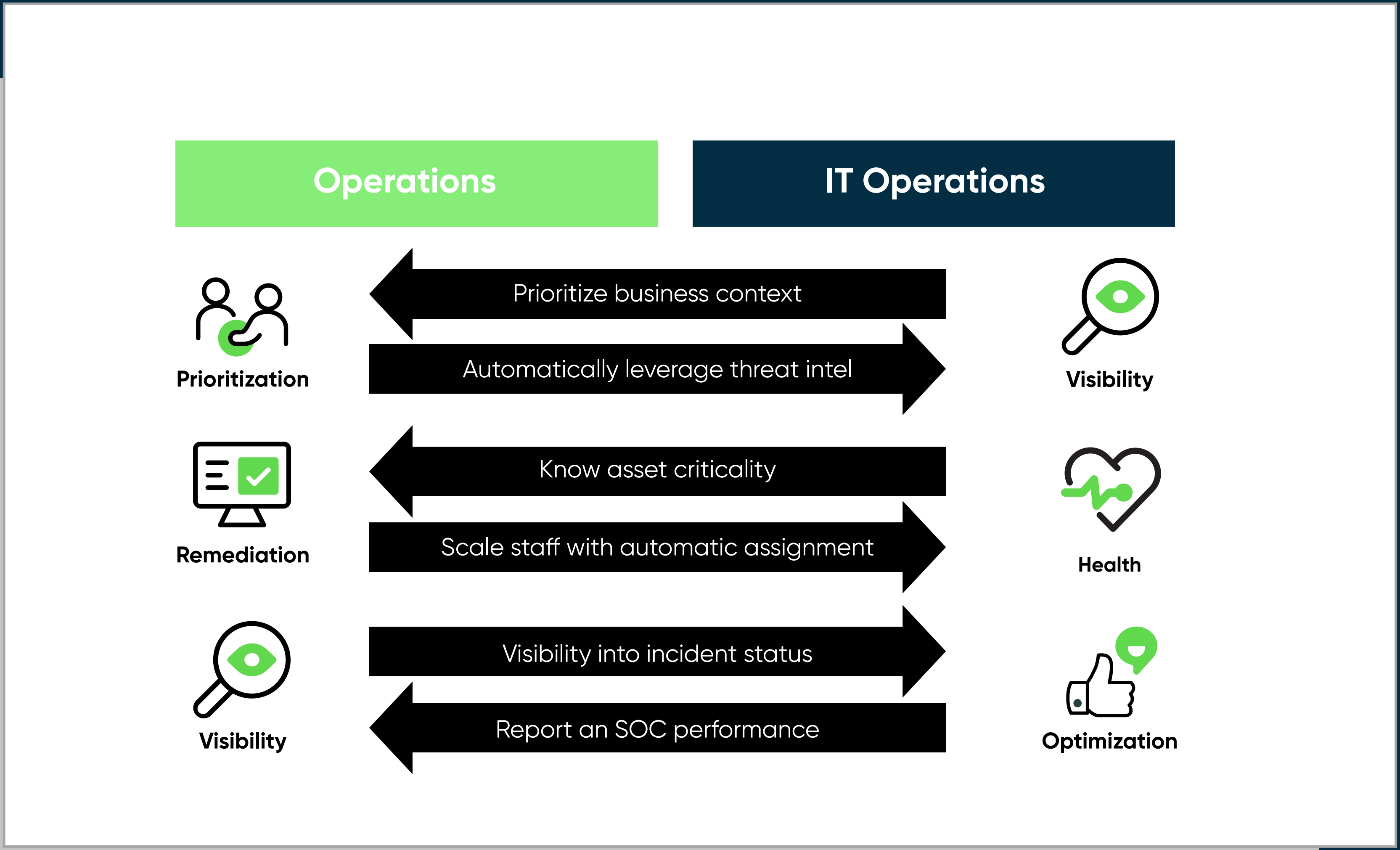
The ServiceNow Security Incident Response tool features dynamic dashboards that support easy cross-team communication and collaboration. You can even use it to remind those assigned to tasks to complete their work on time. This helps maintain SLA thresholds and ensures that nothing falls through the cracks.

Routing work seamlessly between security and IT teams helps you:

- Accelerate resolution with automated workflows
- Automate incident assignment
- View real-time incident status and track remediation processes
- Centralize data and reporting

4. Share data across teams

At the end of the day, sharing the responsibility of security across the organization—along with the data each team collects—is another essential way to thwart cyberthreats. This allows you to track and update workflows, eliminate gaps in visibility and accuracy, and then focus on and respond to the highest-impact incidents quickly and accurately. Making these workflows effective for all the teams involved is vital to not only continuing to do good work, but also to improving processes, increasing efficiency, and getting out in front of more threats.


Operations
IT Operations
Prioritization
Prioritize business context
Automatically leverage threat intel
Visibility
Remediation
Know asset criticality
Scale staff with automatic assignment
Health
Visibility
Visibility into incident status
Report an SOC performance
Optimization

How security and IT teams can share data for mutual success.

5. Report, review, and plan for success

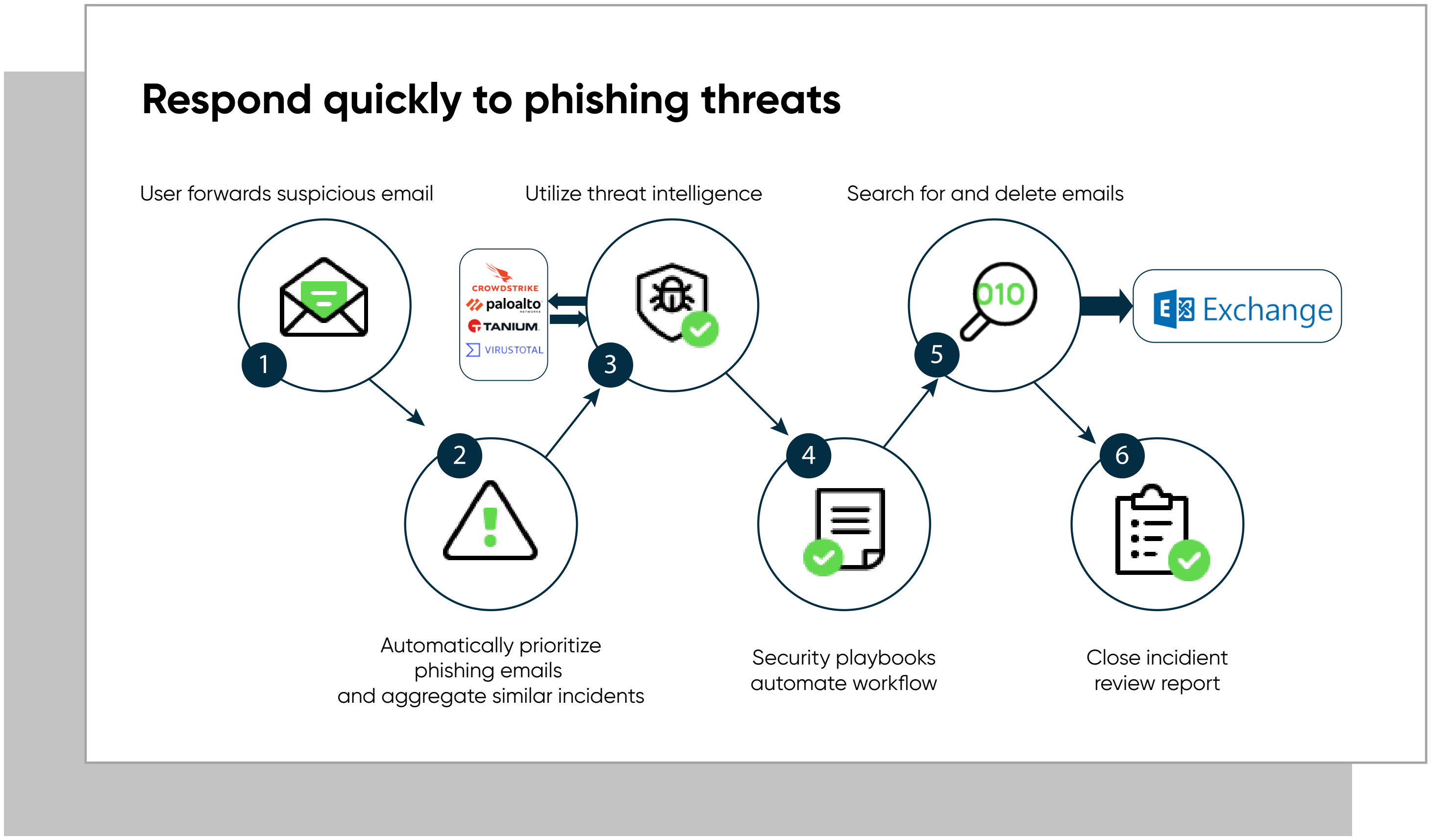
One last way to manage cyberthreats continuously like a boss is understanding and utilizing outcomes. The ServiceNow Security Operations efficiency dashboard shows your teams how they're doing, how your SOC is performing, and where you're facing challenges. You can review analyst efficiency metrics in general or over specific time periods, such as when you know an intense attack occurred. This helps to identify skill gaps, bottlenecks, and roadblocks so you can evaluate and develop both detection and response processes. The ServiceNow Security Incident Response application automatically generates a post-incident review, which also enables ongoing assessment and improvement.

Use case: suspicious email

Let's look at how you could deal with an email phishing threat using the ServiceNow Security Incident Response tool.

1. First, your users e must be able to forward the email—for example, through a macro you would create in Outlook.
2. Next, you'll automatically parse the contents of that email, such as the IP address and payload URL. Sprinkle in some threat intelligence— we can recommend some great sources to work with—to enrich the incident and make a verdict.
3. Then you can use the ServiceNow security playbook to automate the workflow and ensure the correct process is followed, including assignment to the right responder.
4. Your orchestration then takes the correct action—for example, searching for and deleting emails.
5. Finally, you close the incident and review the report to evaluate the efficiency of your response.

The more you repeat this process, the better your response will become.


Respond quickly to phishing threats
User forwards suspicious email
Utilize threat intelligence
Search for and delete emails
1
CROWDSTRIKE
paloalto
TANIUM
VIRUSTOTAL
3
010
5
Exchange
2
4
6
Automatically prioritize phishing emails and aggregate similar incidents
Security playbooks automate workflow
Close incident review report

Neutralizing phishing threats with ServiceNow

How we use our own solutions

At ServiceNow, we drink our own champagne. Just like our customers, we've realized tremendous savings by deploying our ServiceNow Security Incident Response solution. We use it to prioritize alerts, automate digital workflows, enhance data and intelligence, and accelerate security processes. Increasing the efficiency and productivity of our teams allows us to redirect that time towards other valuable priorities and enables us to keep up with the ever-rising volume of threats.

Our results speak for themselves:

46%
tickets handled via automation[5]

74%
improvement in time to identify threat (year over year)[5]

8,700 hours
saved annually via automation[5]

Conclusion

With ServiceNow Security Incident Response, you can effectively manage evolving cyberthreats to your business—even when malicious opportunists up their game during trying times. Rely on us to:

- Proactively manage exposure with visibility into high-impact threats, so you can make sound and fast decisions.
- Ensure cyber resilience with a real-time view into your security posture to quickly prioritize security incidents.
- Drive efficiencies and accelerate reaction time with insights across teams to effectively orchestrate and automate actions.

References

[1] Cybersecurity Solutions for a Riskier World, Thoughtlab, 2022

[2] TechRepublic

[3] Ponemon Institute Survey, "Costs and Consequences of Gaps in Vulnerability Response"

[4] Forrester Consulting: The Total Economic Impact™ Study of ServiceNow Security Operations

[5] Now on Now: Accelerating Security Operations

Dig deeper into SIR

Download a solution brief

Access our security operations use case guide

Sign up for a demo

Visit our website

About ServiceNow

ServiceNow (NYSE: NOW) is the fastest-growing enterprise cloud software company in the world above $1 billion. Founded in 2004 with the goal of making work easier for people, ServiceNow is making the world of work, work better for people. Our cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity for more than 6,200 enterprise customers worldwide, including approximately 80% of the Fortune 500. For more information, visit **www.servicenow.com**.

© 2022 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, Now Platform, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.