servicenow

Automation antidotes for the top poisons in cybersecurity management

How orchestration and collaboration tools can provide a healthy defense against the most serious threats

Introduction

It's a venomous cyberworld out there, but there's a reliable antivenom

No matter what your organization's size or industry focus, cyberthreats are more imminent and dangerous than ever in terms of their persistence and severity. The volume keeps growing too, with the number of breaches rising 15.1% from 2020 to 2021.[1] The costs per breach are also increasing–jumping 24.5% between 2020 and 2021, from $3.35 million to $4.17 million.[2] It's no wonder that almost 50% of CIOs are concerned that their cybersecurity isn't on par with their digital transformation efforts.[3]

A recent ThoughtLab study revealed the top cybersecurity challenges that are top-of-mind for IT leaders. This ebook will discuss how those challenges can poison your ability to protect your business why automating security operations is the antidote, and why 80% of organizations that use automation say they can respond to vulnerabilities in a shorter timeframe.[4] You'll understand how security automation can:

- Deliver visibility of the entire IT estate
- Provide 24/7 monitoring and drive collaboration with other IT teams
- Improve operational efficiency, reduce incident response times, and streamline processes
- Enable AI for continuous improvement
- Address skills gaps, freeing security analysts to do more impactful and interesting work for greater job satisfaction

POISON 1

External pressures make cybersecurity even harder

The rise of newer technologies, greater supply chain vulnerabilities, and increasing government mandates can create chaos in – and be fatal to – your cybersecurity efforts. Risks emerge from misconfigurations in emerging technologies (such as IoT, cloud, and mobile), shadow IT via remote employees, and unpatched third-party software.

These unwitting weaknesses allow pathways for hackers; in fact, 62% of breached organizations were unaware that they were vulnerable.[5] And with limited awareness of these risks until after breaches occur, it's difficult to provide audit trails to comply with the ever-changing regulatory environment.

THE AUTOMATION ANTIDOTE

You need to accelerate the pace of automation to orchestrate risk monitoring, discovery, data collection, change management, playbooks, and remediation. With automation, you can:

- Work with the IT operations team to automate discovery and tracking of new technologies and their maintenance needs for complete visibility of the IT estate and vulnerabilities.
- Collaborate with GRC team to automatically assess risks then prioritize vulnerabilities based on business impact; share risk data with IT teams that implement changes or remediations.
- Rapidly and comprehensively assess cyberrisks from vendors and partners; track, update and remediate risks based on schedules or changes reported by monitoring services.
- Seamlessly collect, monitor and report regulatory compliance data without relying on spreadsheets.

SAS
Scandinavian Airlines

SAS shows how to secure a digital first airline

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

servicenow

Accelerating security operations with automation

To avoid manual, spreadsheet-driven processes, ServiceNow leverages its automated, integrated tools for visibility, alert processing, handling phishing email reports, and authentication failure checks. This allows security analysts to focus on investigating and prioritizing issues for fast, then orchestrate remediations. It also creates a more fulfilling experience for the team, allowing the company to attract and retain the best security talent.

LEARN MORE

"We can't just hire more people. We need to get the most out of our existing team and automation lets us do that."

Security Incident Response team leader at ServiceNow

6X

faster alert processing

50%

increase in number of incidents handled per analyst

$5.7M

hours saved annually

POISON 2

Cybersecurity doesn't get the attention it deserves

About 30% of organizations say cybersecurity isn't high enough of a priority in the enterprise, most likely due to a lack of executive attention and squandering of budget.[6] The allocation of IT spend on cybersecurity – currently about 14.2% [7]—has been rising in recent years, with some IT leaders devoting about 2% more on it in 2022 than they did in 2021.[8] And that means fewer funds for innovation projects. So just throwing more money at cybersecurity won't cut it; IT decision makers must lead the charge in getting the most out of the budget.

THE AUTOMATION ANTIDOTE

Automation can simplify risk reporting and benchmarking to not only justify additional investment in cybersecurity, but also to ensure you get the greatest ROI on what you're spending on it. Additionally, you can facilitate process orchestration and MITRE ATT&CK analysis to focus budget on the highest-impact risks. With automation, you can:

- Quickly spot threats on the attack surface as well as rapidly orchestrate activities across over-extended teams and the tools they use.
- Expose and prioritize the most critical vulnerabilities based on MITRE ATT&CK recommendations to ensure the greatest possible business impact.
- Take actions based on the greatest potential disruptions to operations and the biggest risks to your data.
- Streamline and tailor communication about threats and resolutions for IT leaders and board members so they have full visibility of activities and advocate for more security budget.
- Gather, evaluate and maintain data on trends, risks, and security operations success to show value of investments.

POISON 3

Organizations are too siloed to see risks, evaluate them, and respond rapidly

About 30% of organizations struggle to identify key risks, detect incidents and respond to them, due to a siloed culture and technology set that impedes effectiveness. That's no surprise because only 37% of organizations say they work collaboratively across functions to address security issues.[9] In fact, 76% of organizations have no common view of assets and applications across security and IT.[10] That happens when security and IT teams don't plan ahead to understand shared interests or talk to each other. Without a common view of data across the organization, these teams are deprived of the information they need to make the right decisions—and make them fast.

THE AUTOMATION ANTIDOTE

Automated monitoring, assessments, scoring, prioritization and playbooks using data from multiple teams will provide the visibility, fast and thorough remediation, continuous improvement, and governance to address this challenge. With automation, you can:

- Incorporate and enhance data from various IT tools for all teams collaborating on security to make better decisions and take the most appropriate actions.
- Collect extensive data about asset usage and evaluate asset vulnerabilities to identify and monitor the assets most at risk.
- Leverage data across teams and AI-driven analytics to identify and investigate both common and unique threats;
- Integrate policies, SLAs and reports into IT workflows, then apply them to continual cyberthreat defense activities.
- Enable continuous governance to reduce time to discover the low-hanging fruit of vulnerabilities; easily compile ongoing proof of compliance to senior executives and governance stakeholders who are on the hook for cyberbreach consequences.

Wellstar HEALTH SYSTEM

Wellstar delivers patient care with quality and confidence

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

YOKOGAWA

Yokogawa Electric significantly shortens threat response and 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

POISON 4

Staffing and training shortfalls

Organizations suffer from a shortage of skilled cybersecurity professionals and ineffective cybersecurity training programs. In fact, 82% of employers report lack of cybersecurity skills among IT staffers, who should be cross-trained and constantly educated.[11] So it makes sense that human error is the biggest source of corporate security breaches, whether it's about employees falling for phishing attacks—or overworked staff pushing a button to say "YES" before enough checks are done. Mistakes aren't the only dangers of too few staffers with the right abilities – sometimes things just don't get done. A whopping 56% of organizations say things slip through the cracks due to manual response processes. [12]

THE AUTOMATION ANTIDOTE

Automation can drastically reduce workloads, implement best practices, prevent mistakes, enable accuracy, ensure compliance, and free up staff to focus on optimizing processes. With automation, you can:

- Reduce workloads by eliminating manual steps and empowering security analysts to work on more strategic tasks.
- Use playbooks with built-in policies and timely, comprehensive asset, threat, and vulnerability data to minimize learning curves
- Place cybersecurity controls and processes in functionality for email, browser, chat, and mobile applications to help employees easily avoid and report suspicious activities or communication

Conclusion: Automation saves time, but it takes time to automate

Companies with fully deployed, automated security solutions save an average $2.5 million per year by preventing breaches.[13] We've seen automation reduce triage time by 50% and investigation time by 40% with our own customers.[14] Despite this, only 17% of organizations have invested in security orchestration, automation, and incident response.[15] Security teams are frustrated at the slow adoption of automation considering it has proven its value; success from automation yields exponential results.

Dramatic results from automating cybersecurity

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.[16]

To accelerate automation in security operations and vulnerability management, you can lean on proven workflows, integrated applications on a single platform, orchestration playbooks, libraries with simple tasks, low-code development to easily create workflows, and other tools to streamline processes. According to the Thoughtlab survey, IT security leaders recognize this and plan to attain a higher level of automation maturity within 2 years.[17]

Top use cases being automated:[18]

- Brute force/failed login
- Data loss/exposure to loss
- Insider threat management
- Major security incident management
- Malicious network traffic
- Malware and ransomware
- Phishing
- Privileged access monitoring
- Rogue server/service and incident case management
- Suspicious web access
- Threat hunting
- Vulnerability management executed efficiently.

servicenow

The numbers don't lie[19]

46%

tickets handled via automation

74%

improvement in time to identify threat (year over year)

8,700

hours saved annually via automation

ServiceNow can guide you on your security automation journey

No matter where you are in automating security operations, ServiceNow will help you scale faster, smarter, and more efficiently. Our Security Operations solution enables that critical connection of data and process between IT, security, and risk to rapidly address and remediate threats. It brings in security, IT asset, and vulnerability data from your existing tools and uses intelligent workflows, automation, and a deep association with IT to streamline security response.

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 Vulnerability Response, Security Incident Response and IT Asset Management tools. We use them to patch assets, 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.

Discover today how to leverage the power of the Now Platform® to reduce cybersecurity risk and drive cyber resilience.

LEARN MORE:

ServiceNow and Security Operations Center (SOC) Modernization Security Operations Use Case Guide

Referenced items:

1, 2, 3, 6, 7. 8, 9, 15, 17: "Cybersecurity Solutions for a Riskier World," Thoughtlab, 2022

4, 5, 10, 11, 12, 13: "Costs and Consequences of Gaps in Vulnerability Response," Ponemon Institute Survey

14. "Five ways to safely weather cybersecurity storms," ServiceNow ebook, 2022

16. "The Total Economic Impact™ Study of ServiceNow Security Operations," Forrester Consulting

18. "The 5 stages of security automation maturity and why they matter," ServiceNow ebook, 2022

19. Now on Now case study: "Accelerating Security Operations," ServiceNow, 2022

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**.

servicenow.com