servicenow

Thwart cyberthreats fast with security operations + AIOps

How automated collaboration saves the day

IT operations and security operations are better together

Our world of work continues to change at an ever-increasing pace—amidst more cyberthreats and new security challenges. The volume keeps growing too, with the number of security breaches rising 15.1% from 2020 to 2021. The costs per breach continue to rise—jumping 24.5% between 2020 and 2021, from $3.35 million to $4.17 million. It's no surprise that almost 50% of CIOs are concerned that their cybersecurity isn't on par with their digital transformation efforts.[1]

At the same time, the demand for technology services is exploding, driven by new market opportunities, the quest for efficiency and agility, and emerging trends such as hybrid work. It's an exciting, but challenging time for technology leaders, who are under increasing pressure to deliver applications quickly and securely.

The need for collaboration driven by automation

The only way to maintain resiliency and service performance from both an operational and security perspective—especially in an environment of doing more with less—is with automation and collaboration between IT and security operations teams. Organizations need a unified, automated approach to respond to new security threats.

To meet these new challenges and head off new threats, traditionally siloed IT and security operations departments will need to apply a common, automated approach that connects workflows across the enterprise. With the help of AIOps that combines artificial intelligence (AI) and machine learning (ML) to monitor data and manage incident response, IT and security operations can collaborate to efficiently and effectively secure corporate data assets. They can also work together to prevent threats and breaches from impacting employees and customers.

To meet new challenges and head off new threats, traditionally siloed IT and security operations teams need to come together and apply a common, automated approach connecting workflows across the enterprise.

The challenges facing IT and security teams

The greatest challenge that IT and security departments face is they are forced to be too reactive, especially when it comes to cybersecurity. Other challenges include the inability to prioritize incidents quickly, lack of visibility across the entire IT estate, and the impediment of manual processes, which results in delayed responses. Consider that in a recent report: [2]

83%
of organizations studied had more than one data breach

45%
of breaches were cloud-based

30%
of organizations have no security AI and automation deployed

62%
of organizations are not sufficiently staffed to meet their security management needs

How AIOps helps

Faced with a complex environment, a flood of alerts and manual processes, teams need to:

- Find a proactive approach to incident response.
- Automate responses to reduce threat vulnerability.
- Use a predictable approach to resolve issues.

Big savings from automation

The best strategy to drive cyber-resilience and enable operational efficiencies is to promote collaboration between IT and security teams, using AIOps to automate responses and prioritize incidents. Research shows that with fully deployed automated security solutions companies can realize USD $3.05 million average cost-of-breach savings.[3]

47%
of IT departments with automated IT functions use automation for escalation of security incidents[4]

Threats move at machine speed

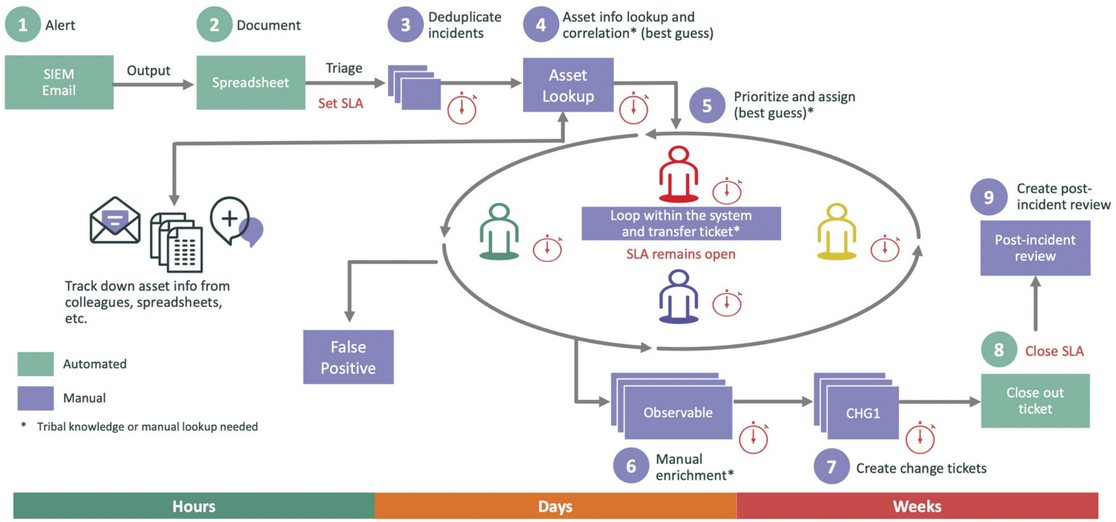
With manual security incident response, typical incident response time can take days or weeks— much slower than the threats to your enterprise. Once an alert has been triggered, it needs to be documented and assets correlated to render a "best guess" as to how to prioritize the event and assign a response team.

Understanding the operational landscape

Before you can define appropriate actions, you need to understand the operational landscape and potential impact. Further delays with a manual process occur as once the trouble ticket is generated, it requires manual, observable data to formulate change tickets to solve the problem.

37%
of IT departments with automated IT functions use automation for ticket creation and routing.[5]

Manual security incident response process



Automating security responses

To move from reactive to proactive threat response requires AI and ML to provide context and automate workflows—in other words, AIOps. Automating security incident response requires three key elements:

1. Visibility into critical incidents to identify high-impact threats in real time, at scale
2. The ability to quickly prioritize security incidents with business context
3. IT and security collaboration in orchestrating and automating the appropriate actions

Simplify remediation decisions

Working from a real-time infrastructure view you can create a business-aware data layer that makes remediation decisions easier. You can immediately understand everything tied to a specific service or asset to focus on troubleshooting efforts. For example, if you are upgrading a server, you have an understanding of all the applications that will be impacted.

Once you understand the business context, you can apply historical data and ML to create an automated response. Insight becomes actionable—you can prioritize incidents and trigger responses using intelligent, automated remediations.

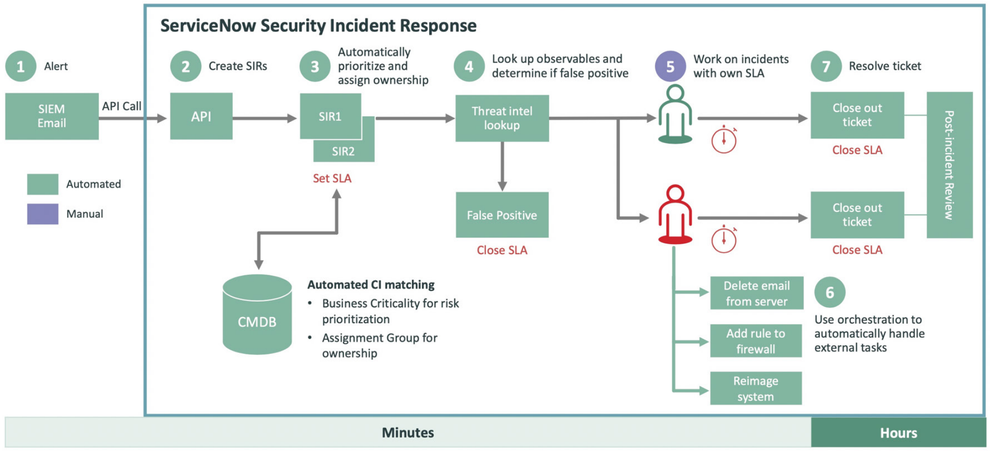
The payoffs of proactive workflows

The result is end-to-end, proactive workflows that span operations, security and service management. Beyond that, you:

- Reduce the number of issues that need to be addressed
- Drive faster resolution and shorten the meantime to response (MTTR)
- Improve efficiency and optimize costs

Automated security incident response process

With automated incident response, processes that used to take days or weeks can be completed in minutes or hours. The alert triggers an automated workflow that prioritizes the incident, matches observables, and then either resolves the issue automatically or provides the data needed to deal with the problem manually. The incident report becomes an essential component with AIOps since it provides the data needed for machine learning to create repeatable, collaborative workflows.



Promoting collaboration between IT and security teams and automating incident response is the best strategy to drive cyber-resilience and promote operational efficiencies.

USD $3.05 million
Average cost savings associated with fully deployed security AI and automation.

Providing visibility into all resources

ServiceNow can discover the entire operations footprint. This includes discovery across both on-premises and cloud-based applications, infrastructure, PaaS services, assets, and TLS Certificates.

Fully map assets

When it comes to security, you want to be sure you can see everything and have relevant context. For example, expired TLS certificates are vulnerabilities that can lead to service outages and data breaches. To prevent this from happening, it's important to have a full mapping of relevant assets along with their criticality. Building on the CMDB, ServiceNow can concretely pinpoint any issues. With Certificate and Inventory Management you can discover and manage the full lifecycle for TLS Certificates—tasks to renew expiring certificates are created, incidents are created for any expired certificates, and all are prioritized based on importance.

Ending a phish tale

Let's walk through how an automated workflow is created to handle phishing emails.

1. The phishing email is forwarded as suspicious.
2. The system automatically prioritizes it and aggregates similar incidents in the database using threat intelligence as part of the assessment.
3. The security playbook then triggers an automated response to search and delete emails, add a rule to the firewall, and reimage the system.

The process takes minutes, and no human interaction is required.

Why AIOPs works

Using AIOps to create security and IT collaboration accelerates response time. How?

- Automating and orchestrating processes
- Assigning ownership
- Providing real-time tracking of incident status
- Centralizing data and reporting
- Applying AIOps to enable shared data and automated workflows speeds resolutions, drives resilience, and promotes operational excellence.

47%
of IT departments using strategic automation believe it can increase the efficacy of the organization.[6]

Real-world example:

ServiceNow

By applying AI analyses and automating operations, ServiceNow was able to recoup 1,800 hours of lost productivity due to recurring VPN outages.

- **1,000 hours of IT/security time saved per year**
- **78% reduction in VPN outages**
- **50% reduction in the meantime to response**

Using our own AI solutions to predict an outage

We understand the value of collaboration and automated incident response since we use our own AIOps technology.

ServiceNow began to encounter productivity challenges due to ongoing VPN outages—a problem that was then magnified with the COVID-19 pandemic. As the amount of VPN traffic increased, the number of outages increased as well, impacting remote employees' ability to access enterprise resources to do their jobs. We were losing an estimated 1,800 hours per year in productivity due to these VPN outages, not to mention adding to employee frustration.

Proactively predicting a VPN outage

Applying AIOps and adopting our own end-to-end visibility concepts allowed IT operations to assimilate, analyze, and correlate data from a wide range of sources. We determined root causes and we were able to identify patterns that would predict a VPN outage. As a result, we were able to create an automated remediation playbook to address VPN outages and save the company thousands of hours in time and resources.

With automated incident response, we were able to reduce VPN failures by 78% and reduce incident response time by 50%. Our customers have been able to achieve similar benefits:

- Beachbody – 90% reduction in service outages
- Lincoln Financial Group – 80% reduction in vulnerability backlog
- AMP – 30% reduction in security response time

Real-world example:

USAA

As USAA continued to push its mobile-first agenda, it found that creating a unified threat management framework could bridge the gap between IT and security and tame an unwieldy incident response system.

- **42% drop in current vulnerabilities**
- **56% decrease in past due vulnerabilities**
- **49% reduction in total vulnerabilities**

Creating a unified incident pipeline as part of mobile-first initiative

USAA has been providing financial services to members of the U.S. military since 1922 and has built its reputation on providing responsive, personalized services. The organization prides itself on the ability to provide world class experiences. Traditionally, USAA has not utilized physical locations on a global scale so innovation has been a part of the story from the beginning. As part of a digital transformation strategy, USAA adopted a mobile-first initiative for products, processes, and experience.

As USAA continues to deliver world class experiences for its members, the pressure to ensure the availability and resiliency of services grows exponentially in importance. The company translates billions of daily downstream monitoring signals into manageable and actionable events. By correlating business context to events, USAA understands the business services being impacted and can configure dynamic priorities into the automation and incident escalation playbook. Impact analysis correlated to change and vulnerability allows USAA to push the bounds of automated remediation capabilities.

Modernizing threat management

Migrating from monolithic services to microservices and deploying workloads to public and private clouds made visibility into the threat landscape even more critical—but previous attempts to modernize threat management resulted in a fragmented system that was unwieldy. Using the ServiceNow incident management and response platform, the USAA AIOps team created an event stream processing pipeline to map business context to events using metadata. This data was then used to power a playbook to drive automated remediation.

The results were impressive. Following a 90-day implementation period, USAA saw a 42% decrease in current vulnerabilities and a 56% reduction in past-due vulnerabilities, as well as a 49% drop in vulnerabilities as a whole. Using AIOps for incident response continues to yield more benefits as USAA finds new efficiencies from its automated framework. By adopting the Now Platform™, USAA has been able to replace its fragmented technology with agile service delivery. Now USAA has a unified threat management framework that is more effective, more efficient, and more importantly, bridges the gap between IT and security.

Real-world example:

AMP

The cybersecurity team at Australian financial services giant AMP saw an opportunity in the convergence of three big things: the deployment of ServiceNow, increased attention to compliance brought on by new regulations, and an urgent need to improve vulnerability response times. With help from KPMG, the AMP IT team has deployed ServiceNow to create an automated and highly effective security operations solution.

- **60% reduction in vulnerability response time**
- **12 weeks to 1 week for incident response**
- **1 CMDB system for a unified view**

Prioritizing and automating dramatically cut incident response time

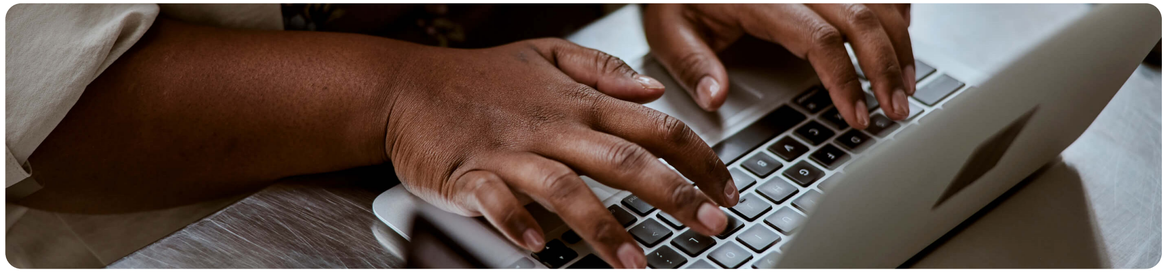
AMP, the Australian financial services company, was struggling to keep pace with new cyberthreats. It was relying on a manual system of emails, spreadsheets, phone calls, and text messages to respond to security events. Response time was averaging 12 weeks and the company knew that wasn't good enough. So, with help from KPMG, AMP implemented a configuration management database (CMDB), a service catalog, and automated service request fulfillment using ServiceNow.

During the initial stages of integrating the ServiceNow platform, the IT team discovered the ServiceNow Security Operations solution. Within six weeks the ServiceNow Security Incident and Response application was up and running as part of the CMDB system for IT. KPMG added business criticality components to core applications which sped up the Security Operations deployment. With the qualifiers in place, when a threat was detected by the FireEye or Nessus scanning systems, the scanned data was ingested into ServiceNow which was in turn able to sift through the noise, prioritize action, and kick off a security incident response.

Better collaboration between IT and SecOps

Integrating IT incident response with security incident response meant IT and SecOps could collaborate on resolutions using a common platform to handle incident visibility and communication. And by linking the security module into AMP's change management application, the response could be automated to mitigate risk—that was impossible using spreadsheets and emails.

Thanks to ServiceNow and AIOps, AMP is automating threat response and other processes, freeing its team for more important tasks.



A new level of security incidents requires faster, automated incident response

As more organizations have had to scramble to accommodate remote workers, they haven't been able to keep up with changes in the enterprise threat landscape. The old tools and techniques just aren't able to cope with the deluge of security threats triggered by work-from-home employees.

Rather than struggling to react to a growing number of security incidents, this is the opportune time to automate threat management and break down the siloes that separate IT operations management and security operations.

32%
of IT departments using strategic automation believe it can enable them to be more compliant as an organization.[7]

Drive resilient operations

Using ServiceNow and AIOps to create a single, common platform for threat intelligence and remediation is the best way to prioritize and respond to threats and vulnerabilities faster. End-to-end workflows and business context can transform operations with actionable insights and intelligent automation. The ability to automate incident creation, categorization, routing, assignment, root cause analysis, and remediation is a game changer for security response, security and IT teams, and the overall business.

Everyone wins with AIOps and an automated response playbook

Everyone benefits when applying AIOps and machine learning to address security threats. By leveraging AIOps in your day-to-day operations, you can:

- Reduce the number of service outages and major incidents that impact employee productivity and customer experience.
- Lower the mean time to response by accelerating analysis to identify and correct incident root causes.
- Get a real-time view of your security posture.
- Shift IT operations and security operations from being reactive to teams that work intelligently for the business.

Learn more:

See how one team kept control of their workday by combining automated workflows for security and IT operations, ITAM, and risk management. Read our ebook, "Same cyberthreat, different story."

References

1. Cybersecurity Solutions for a Riskier World, Thoughtlab, 2022
2. 2022 Cost of a Data Breach Report, Ponemon Institute, 2022
3. ibid
4. Future Workforce Insights: Why Strategic Automation Empowers Employees in IT, September 2022, Author: Angela Salmeron, Research Director, European Future of Work, IDC #EUR149378222, an IDC eBook, sponsored by ServiceNow.
5. ibid
6. ibid
7. ibid

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.