servicenow

Thwart cyberthreats with security operations + AIOps

- A new cyber security strategy for Australia
- Resiliency through security
- Automating the operational landscape
- Real world example: Department of Industry, Science & Resources
- Real world example: USAA agency
- Real world example: AMP
- Secure government with AIOps

7 minutes
on average where Cybercrimes are reported

- Australian Cybersecurity Centre Annual Cyber Threat Report 2022

A new cyber security strategy for Australia

Australia has the mandate for change. Worldwide, the number of security breaches has risen 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. After a series of high-profile hacks on Australian companies in 2022, the resolve to secure the nation permeates government, boardroom and citizens' agenda. Rising to the challenge, worldwide, almost 50% of CIOs are concerned that their cyber security isn't on par with their digital transformation efforts.[1] Sophistication and preparation is needed as Australian citizens are demanding easy access to their data and at the same time, absolute confidence that their data is safe. Cyber security must be improved across government, business and community.

The need for collaboration driven by automation

Cyber security is not just the domain or responsibility of a few select agencies. All levels of Federal, State and Local governments, must effectively maintain resiliency and service performance from both an operational and security perspective. A unified approach using a powerful Artificial Intelligence (AI) and Security Operations-driven programme can help all government entities monitor and detect threats, predict outages and security issues, and increase performance and resiliency.

Recent changes such as the expansion of coverage of the Security of Critical Infrastructure (SOCI) Act 2018 means businesses need to understand their data flows and how they manage it. Compliance with changing regulations means giving government agencies full visibility into IT and operational technology assets on their networks, complete awareness of vulnerabilities and their ability to respond to threats quickly and effectively. In turn, security operations for government need to be able to leverage Artificial Intelligence (AI) & Machine Learning (ML) to make sense of a overwhelming number of signals, indicators, alerts to effectively combat critical information leaks or security breaches that can cause irreversible damage.

Most compromises identified by the ACSC used relatively simple tradecraft which could have been prevented by enhanced cybersecurity

– Australian Cybersecurity Centre Annual Cyber Threat Report 2022

The challenges facing IT and security teams in Government

Our Federal Government wears many hats: cyber security policy maker, major incident response coordinator and caretaker to vast amounts of data which impacts citizens, economy and national defense. Securing and defending a nation's data is a responsibility across all of Government and not just a designated department or team. It is a thankless and daunting responsibility: the sheer volume of data both new and old, its distribution across the nation and the wide span of types of data, such as personal data to top secret information, makes cyber security a never-ending mission.

To ensure we can prevent, detect and respond to cyber threats, laws are in place to govern our data and information security. But that is not enough. To constantly evolve and protect against new threats, we need to have proactive measures to strengthen the cyber security infrastructure, introduce new regulations and ensure there is a framework for co-ordinating cyber security efforts across all levels of Government. Clear roles and responsibilities across all levels of government is essential to ensure we avoid vulnerabilities of the past and can effectively respond to threats of today and beyond.

Resiliency through increased security

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

- Proactively monitor and respond to technology risks, despite increasing attack surface complexity, threat volumes, and skills shortages.
- Gain real-time, actionable insights to react to risks and potential threats.
- Reduce breaches and data loss.
- Implement Essential Eight mitigation strategies and achieve compliance with new security regulations and mandates.

Drive Savings and Citizen Services

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 prioritise incidents. Research shows that with fully deployed automated security solutions companies can realize AUD $5.05 million average cost-of-breach savings.[3]

ACSC's Annual Threat Report:

$98m

increase in financial losses due to business email compromise

76,000

cybercrime reports were made via ReportCyber

34%

of security incidents were Government

Threats move at machine speed

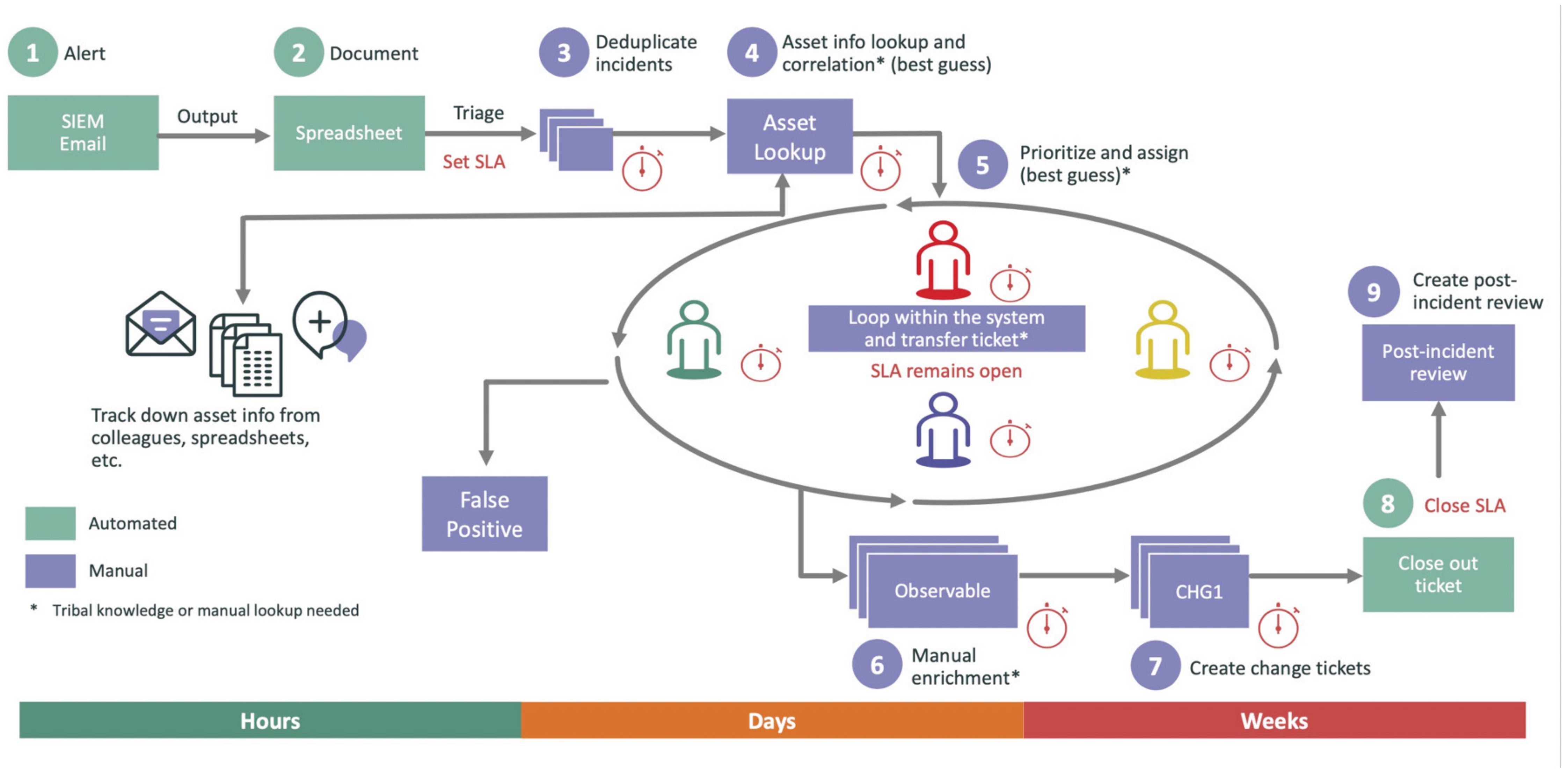
With manual security incident response, typical incident response time can take days or weeks— much slower than the threats to your department. Once an alert has been triggered, it needs to be documented and assets correlated to render a "best guess" as to how to prioritise the event and assign a response 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 Federal, State or Local teams 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
2. scale The ability to quickly prioritise 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 data layer that makes remediation decisions easier. You can immediately understand everything tied to a state actor, specific citizen services or national infrastructure 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.

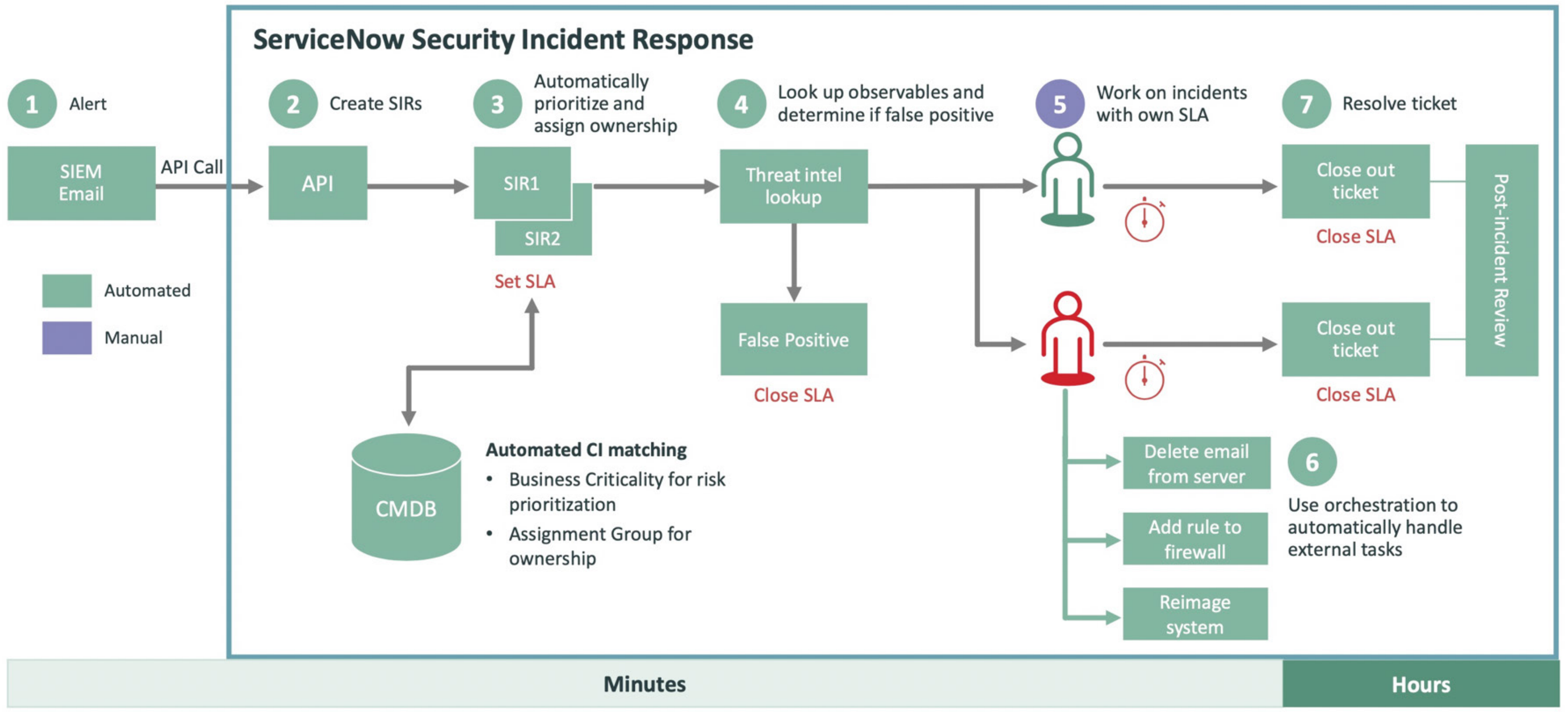
The payoffs of proactive workflows

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 mean time to response (MTTR)
- Improve efficiency and optimise 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 prioritises 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.


ServiceNow Security Incident Response
1 Alert
SIEM Email
API Call
2 Create SIRs
API
3 Automatically prioritize and assign ownership
SIR1
SIR2
Set SLA
4 Look up observables and determine if false positive
Threat intel lookup
False Positive
Close SLA
5 Work on incidents with own SLA
7 Resolve ticket
Close out ticket
Close SLA
Close out ticket
Close SLA
Post-incident Review
Automated
Manual
CMDB
Automated CI matching
• Business Criticality for risk prioritization
• Assignment Group for ownership
Delete email from server
Add rule to firewall
Reimage system
6 Use orchestration to automatically handle external tasks
Minutes
Hours

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

AUD $5 million
Average cost savings associated with fully deployed security AI and automation.

Providing visibility into all resources

ServiceNow received IRAP certification for Australian Government and has served over a hundred Government agencies for more than a decade. ServiceNow for Government has capabilities that will allow you to 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 for you. 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 prioritised 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 prioritises 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
- Centralising 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:

Department of Industry, Science and Resources (DISR)

Automating enterprise service management with ServiceNow Protected Platform.

- **6 months from procurement to implemtation**
- **Services to over 4,000 employees**

All data, all people, all support, in Australia

DISR is the first Australian Government department to use the ServiceNow Protected Platform, which was built to meet Australian data security and sovereignty requirements for government and regulated industries. The major federal Australian department procured and implemented the platform in less than 6 months.

ServiceNow replaced a variety of systems and processes, including IT software that was nearing end of life, while other teams had used a mixture of tools to manage requests. The new platform consolidates the functions into a single portal, giving employees one place to make requests and to access a range of corporate services.

"In our work with more than 100 Australian state and federal agencies, we see them facing increasing demands to deliver more with less, while needing to adapt to increasing security and data sovereignty obligations. Using the ServiceNow Protected Platform, DISR can access the full power of the Now Platform with in-country support and embedded security, to be compliant with IRAP requirements for government data handling at the PROTECTED classification level," said Eric Swift, Vice President and Managing Director ANZ at ServiceNow.

> "
>
> **By using one platform to manage complex tasks and requests, we have improved our automation and streamlined a range of administrative tasks.**
>
> **Steven Stirling**
> **GM, ICT Operations, DISR**

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**

Serving global Federal Governments with unified incident response and 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, personalised services. The organisation prides itself on the ability to provide world-class experiences. Traditionally, USAA has not utilised 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.

Modernising 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 modernise 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**

Prioritising and automating dramatically cut incident response time in private sector

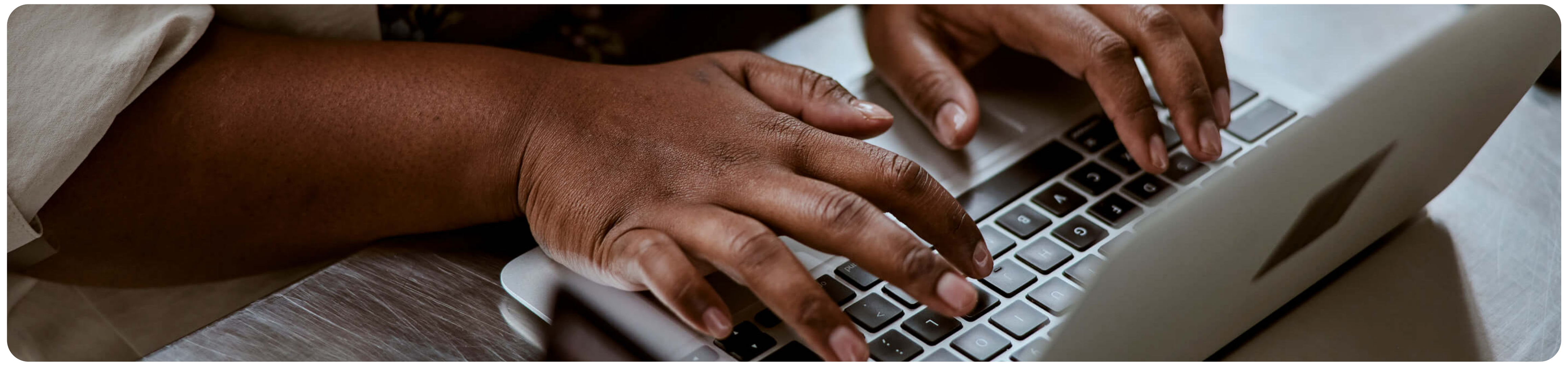
AMP, the Australian financial services company, was struggling to keep pace with new cyberthreats. It was relying on a manual system of emails, spreadsheets, phone calls, and text messages to respond to security events. Response time was averaging 12 weeks and the company knew that wasn't good enough. 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, prioritise 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.

AMP is now 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 workplaces have shifted to accommodate more remote workers, their challenge has been 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 organisation.[7]

Drive resilient government operations

With the ServiceNow platform, you already have the foundation for resilience. Using our Security Operations solution and AIOps on the same platform for threat intelligence and remediation is the best way to prioritise 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, categorisation, routing, assignment, root cause analysis, and remediation is a game changer for security response, security and IT teams, and the overall business.

Secure government with AIOps and an automated response playbook

Government, businesses and citizens benefit 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 citizen 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 governement.

Learn more:

Information security is paramount in ServiceNow. Our cloud and platform meets rigorous standards and compliance for security assurance. For more information visit ServiceNow Trust.

References

1. Cybersecurity Solutions for a Riskier World, Thoughtlab, 2022

2. Australian Cyber Security Centre Annual Cyber Threat Report 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 digitise and unify organisations 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.

servicenow®

The world works with ServiceNow™.

For more information, visit: www.servicenow.com.