Security Automation: Achieving Digital Resilience

Exploring how executives are leveraging automated security tools to safeguard data and drive innovation, in partnership with Omdia

Content

Executive summary

Context

Telstra commissioned Omdia to research the state of Security Operations (SecOps) in North Asia, assessing security automation maturity across a range of complex technology environments and threats. This paper arms security executives with the insights they need to bolster their organisational cybersecurity resilience and support their ongoing digital transformation projects.

Who did we speak to?

Field survey

250 senior technology decision-makers surveyed in August 2022

Respondent mix

50% were IT Executives (including CIO, CTO, CISO)

50% were senior technology leaders (including technology leads, senior consultants)

Sectors surveyed

BFSI, Transport & Logistics, Retail & Wholesale, Manufacturing, and Healthcare

Organisation size

50% with 100-999 employees.
50% with 1000+ employees.

Domain surveyed

Security automation maturity across the technology stack and end-to-end threat management (NIST CSF)

Purpose

Reveal how organisations can help secure digital transformation through automation

This report confirms that the rate of security automation is relatively low in North Asia, with limited use across the region.

Organisations are forgoing the benefits of using security technology to augment security analyst instinct and experience in complex environments. There is an opportunity to use automation to remove the time firms spend on repetitive, arguably lower-value tasks to help security teams better safeguard vital business operations.

Organisations are investing in additional cybersecurity platforms to overcome rising incidents and breaches, but this has resulted in sprawling toolsets that generate a higher volume of alerts and false positives.

China and Japan experienced the highest number of false alarms in the region. From an industry point of view, manufacturing and transport & logistics suffer more 'noise' from alerts than other sectors across the region.

This paper provides recommendations and a proposed industry maturity step model to drive security automation uplift, helping organisations deal with alert fatigue while increasing their security resiliency.

Key findings

32% of firms have seen attacks increase in the past 12 months across their entire IT stack, with endpoints, networks and operational technology suffering the worst impacts.

66% of organisations that experienced a significant rise in security incidents also saw a surge in breaches.

40% of firms lost revenue due to these attacks, 38% suffered reputational damage and 34% sustained operational downtime.

Security leaders are confident they could reduce nearly 50% of all serious security incidents and breaches with better security automation.

24% of regional organisations are 'advanced' in leveraging security automation.

China has the highest levels of security automation, while Japan has the lowest.

The retail & wholesale sector has the highest proportion of firms with more 'advanced' security automation levels. By comparison, transport & logistics have many firms still at basic maturity levels.

The state of cybersecurity in North Asia

Security is a growing concern and a constraint to digital ambitions

Organisations in North Asia have experienced a significant rise in security incidents

Omdia's research confirms that businesses in this region are being hit hard by an increasing volume of Advanced Persistent Threat (APT) attacks. 32% of firms in North Asia experienced a significant increase in security incidents (Figure 1) across multiple information technology (IT) areas (Figure 2).

The high rate of incidents is a warning for firms in North Asia, demonstrating foundational security shortcomings that will hamper transformation ambitions.

Has your organisation experienced a significant increase in overall security incidents attacking any of the following resources in the last 12 months?

32%
Yes, and it was a serious issue

43%
Yes, and it was a minor issue

24%
No, have not experienced

1%
Don't know

Figure 1. The high rate of incidents is a warning for firms in North Asia, demonstrating foundational security shortcomings that will hamper transformation ambitions

One in five North Asian firms dealt with a breach

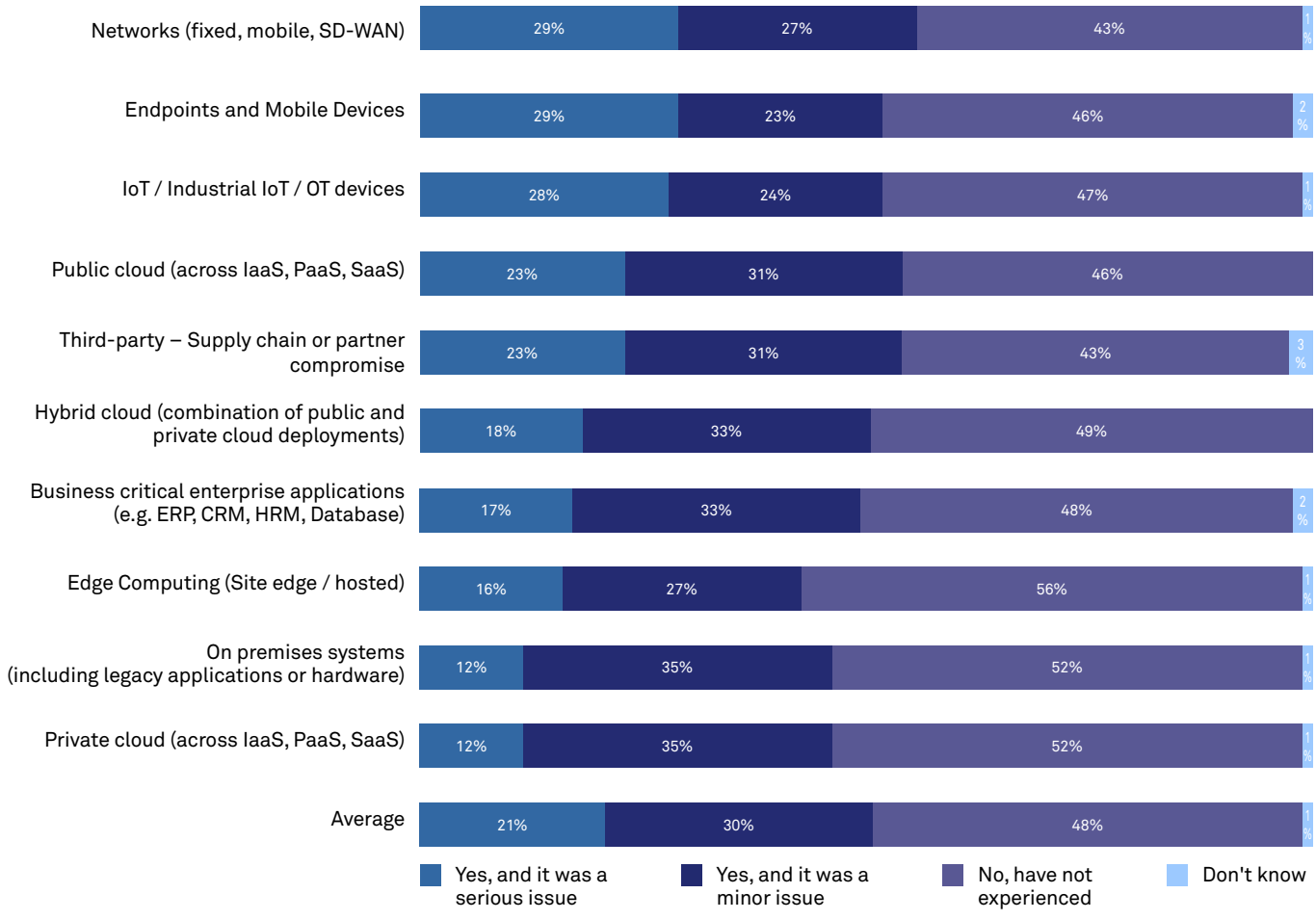
The rise in security incidents is a worrying trend. Worse still, 50% of firms have seen a 'significant' increase in security breaches in the past year. All areas of technology were hit, albeit some more than others (Figure 2).

The most common areas of the attack surface exploited were endpoints, networks, Internet of things (IoT), public cloud and third-party software (including supply chain).

> **We see lots of phishing emails, 3-4000 a day, it's cost effective for the attackers.**
> **Even with multilayer solutions, not all attacks can be blocked.**
> **We have loaded EDR to adapt but it can be tricked if the user lets them in.**

Head of Security at a large banking firm in Hong Kong SAR

Has your organisation experienced a significant increase in security breaches in any of the following areas, in the last 12 months?



n=250

Figure 2. 21% of organisations have seen an increase in serious breaches, especially across endpoints, networks and IoT resources

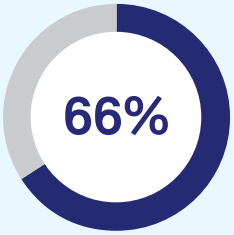
The ratio of security incidents to realised attacks is at a dangerous high

When we compared the rate of security incidents that ended up becoming a breach, the conversion rate was a dangerous 66%.

By technology type, the proportion of incidents that ended up becoming a breach was highest for endpoints (93%), hybrid cloud (91%), networks (75%) and business-critical applications (68%).

Serious breaches through the public cloud and supply chain were also above average across all IT, reflecting continuous exposure resulting from the digitisation of value chains. IoT and operational technology have rapidly risen as a cause for concern, especially in manufacturing and transport & logistics.

When considering the impact of these severe breaches on those organisations, the results are alarming.



of organisations that had a significant increase in serious security incidents also saw a surge in serious breaches.

Breach impacts are far-reaching and material

Over a third of all firms experienced a variety of impacts, varying from downtime to lost revenue (Figure 3).

Any of these negative impacts are sufficient to derail the gains from new technology deployments or draw unwanted attention from the boardroom and regulators.

In the last 12-18 months, what was the impact of the most significant cybersecurity incident or breach on your organisation?

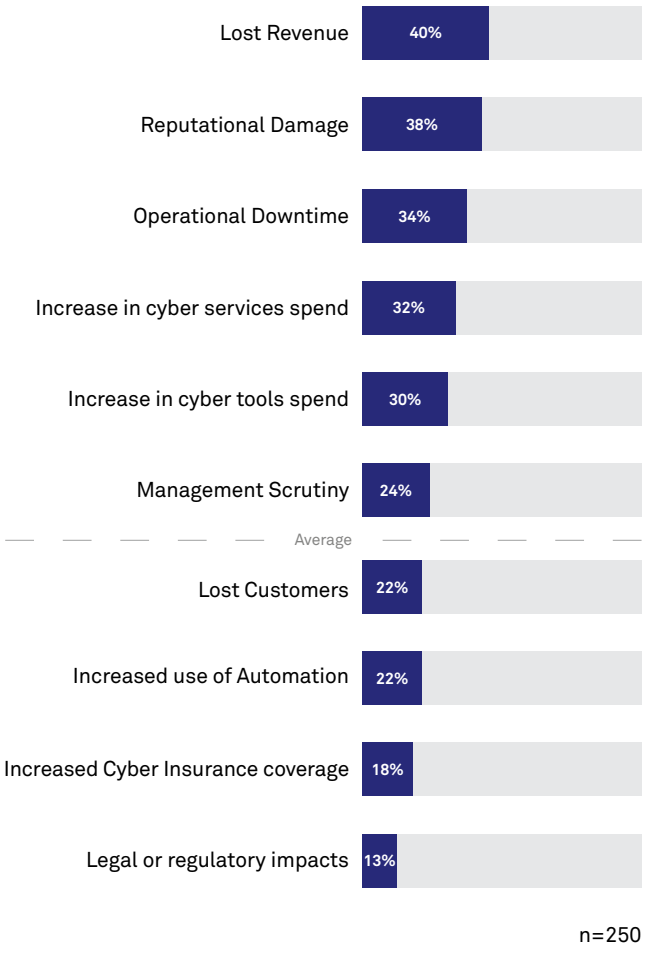


Figure 3. Major impacts from security breaches in North Asia are concerning

There is no shortage of publicly disclosed cases where a security breach has toppled organisations, and far too many to list in this report.

SecOps teams have a fundamental role in preventing and mitigating cyber risks and consequent negative impacts, but their challenges are manifold.

Security Operations staff face increasing pressure

Organisations across North Asia are deploying more siloed tools that are generating more alerts (and false positives). Figure 4 shows that most firms have deployed a wide range of security solutions, but not all are integrated or well-tuned. Worse still, nearly a third of breaches were from unactioned alarms.

Security staff are in short supply and many are overwhelmed by alert fatigue. Security analyst and engineering efforts almost exclusively focused on threat investigation at the expense of prevention and more proactive security efforts, such as the development of a thoroughly documented and maintained response playbook.

> **We have a big talent gap. There is rapid change in security technology, and we don't have the people with the skills to keep up with this.**
>
> Chief Technology Officer at a Hong Kong SAR banking firm

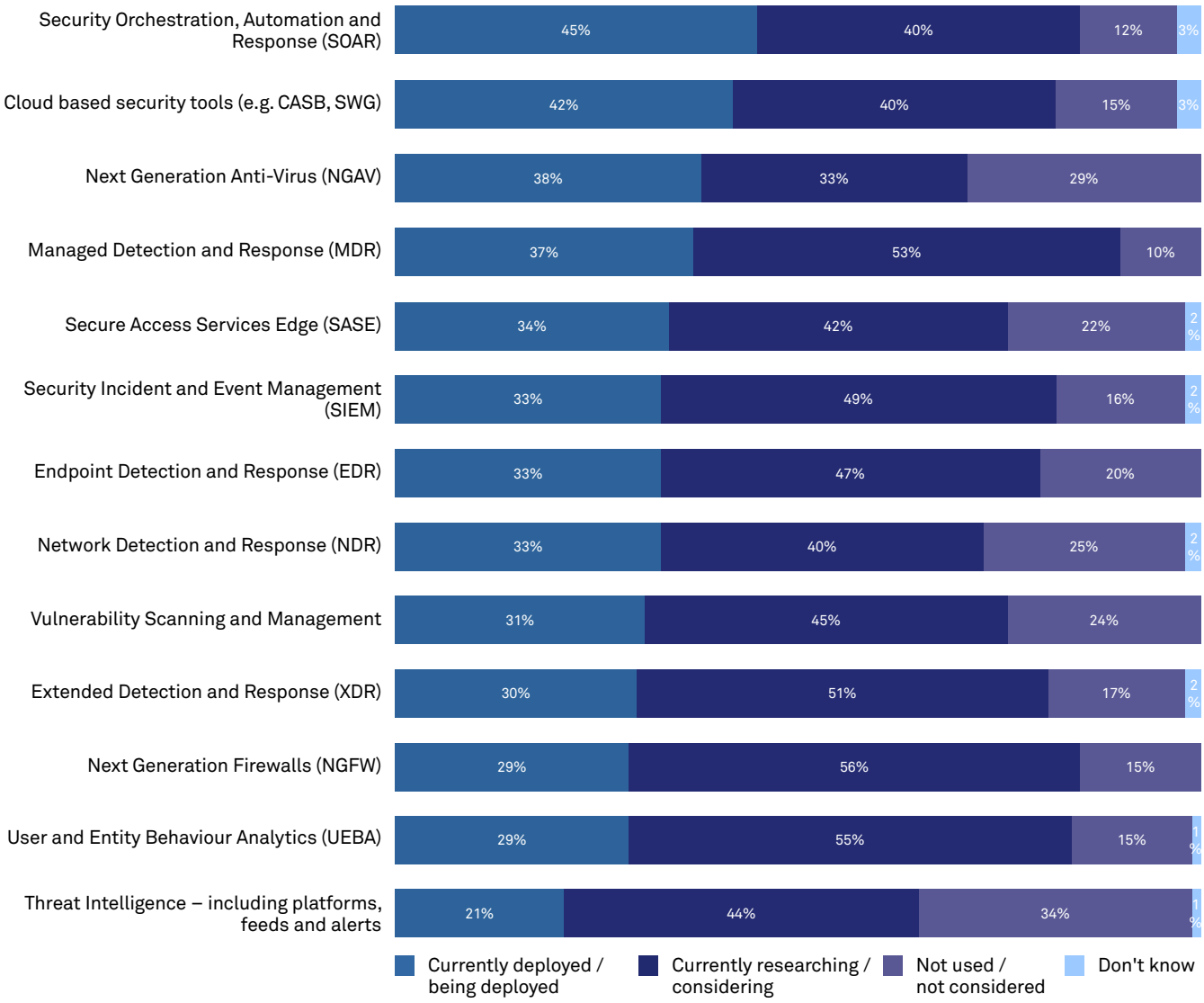
Organisations have more security tools but fewer solutions

As highlighted in Figure 3, firms are investing in more cybersecurity platforms to overcome rising incidents and breaches.

This has resulted in sprawling toolsets for most firms. Siloed and partially integrated SecOps, Incident Response (IR), and Threat Intelligence (TI) technologies now stretch from endpoints, cloud and networks to more sophisticated Security Incident and Event Management (SIEM) platforms.

Figure 4 highlights some investment priorities.

Which best describes the use of SecOps technology in your organisation today?



n=250

Figure 4. Organisations have deployed and are considering a wide variety of security tools, many with limited integration or automation

Most firms have deployed many tools to deal with security across different fronts, with each tool selected to address a specific use case and essential purpose. But Figure 4 shows that over 21% of all 250 respondents have deployed all thirteen categories of toolsets.

Many of these tools are disparate, not always pre-integrated and operate differently. As a result, SecOps, IR and TI teams need expensive security analysts with unique certifications, experience and training across many tools from multiple vendors.

> **We have a SIEM that can input a lot of logs, but it's very challenging to correlate those alerts and find out what's really going on, so up to 50% of current alerts and alarms are ignored because of lack of resources and tool tuning.**
>
> Senior Security Manager of a large Japan based manufacturer

Lagging Mean Time to Detect and Respond (MTTD / MTTR) metrics are exposing firms

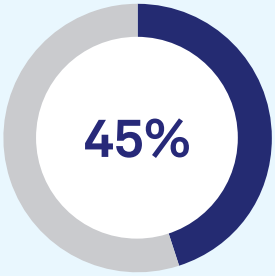
Two key measures of SecOps effectiveness are MTTD and MTTR. MTTD is the average (mean) time it takes an organisation to identify a potential or actual security threat across any resource, and MTTR is the average remediation response time.

47% of North Asian firms say they have an MTTD of within a few hours, while 93% say their MTTD is within days of an indicator of compromise.

Only 35% of firms can respond to the most severe alerts within hours, while 45% need days to react effectively to breaches (Figure 5).

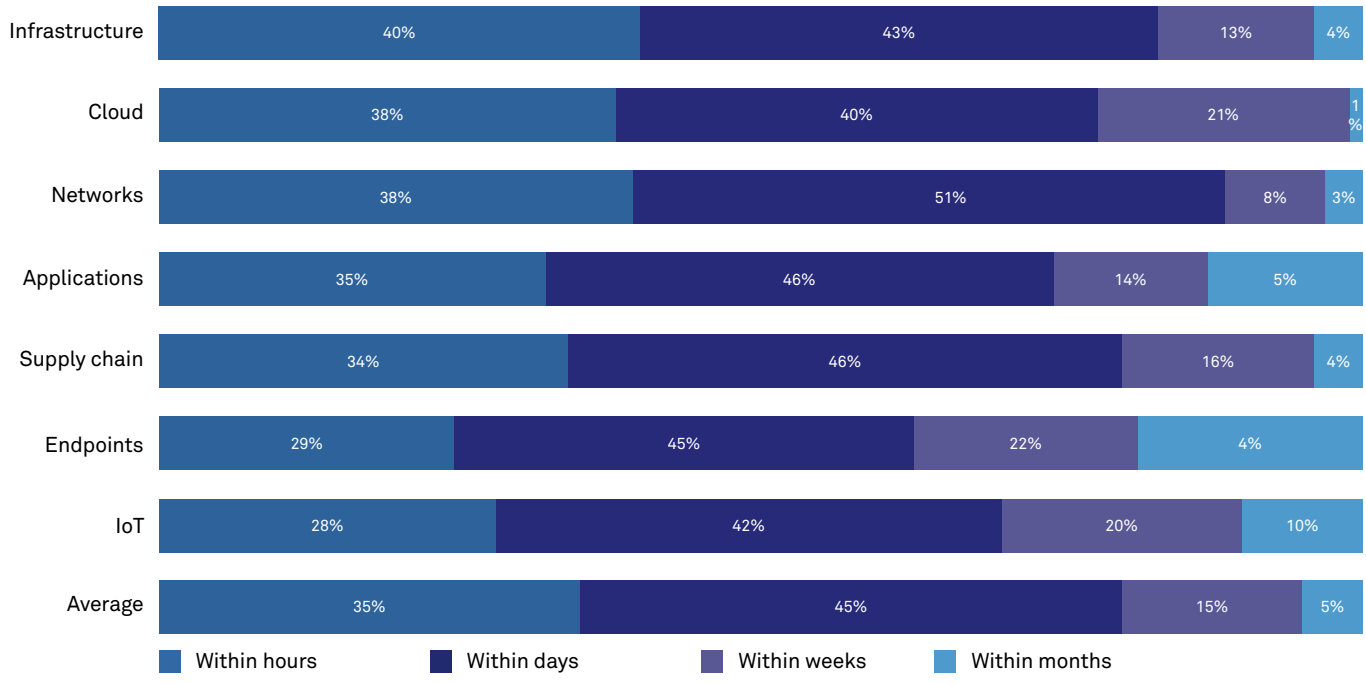
So how long is too long? Attackers only need minutes to launch major assaults using evolving methods such as phishing, ransomware, DDoS or AI/ML-based attacks. Some vendors report that attackers can fully penetrate a complex network in under a day.

Figure 5 shows the MTTR across the IT stack, which also corresponds with the highest number of 'serious' breaches in Figure 2.



of firms need days to effectively respond to a breach.

What was the Mean Time to Respond (MTTR) to a breach in your organisation in the past 12 months?



n=250

Figure 5. MTTR – Only 35% of firms detect and respond to security incidents within the first few hours

Lost in the noise – 42% of all security alerts are false positives

A large volume of threat alerts, alarms, tickets, and possible incidents generated by various security tools are causing headaches for security professionals.

The problem's extent differs by location, with Hong Kong SAR experiencing the least false positives across all security signals, with 39%.

China and Japan face more considerable challenges, where 44% and 42% of alerts (respectively) are false positives (Figure 6).

From an industry point of view, manufacturing and transport & logistics suffer more noise from alerts than other sectors across the region, due to sprawling IT and OT (Figure 7).

Industry executives interviewed during the research project frequently spoke about emerging threats, as manufacturing plants increasingly deploy sensors and other intelligent devices through distribution networks, which are attached to core networks.

Challenges include a dramatic increase in the attack surface as more OT devices become integrated with IT systems, lagging patch and device management across legacy technologies, and a wide variety of non-integrated toolsets flooding security teams with false positives.

In the past 12 months, what percentage of current security alerts are false positives (by location)

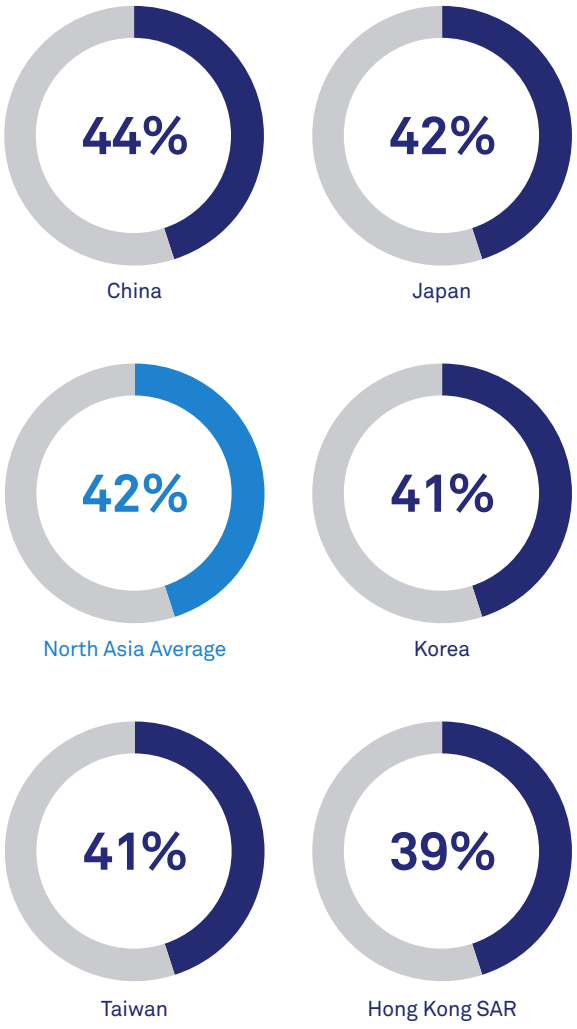


Figure 6. China and Japan endure the highest number of false alarms

In the past 12 months, what percentage of current security alerts are false positives (by sector)

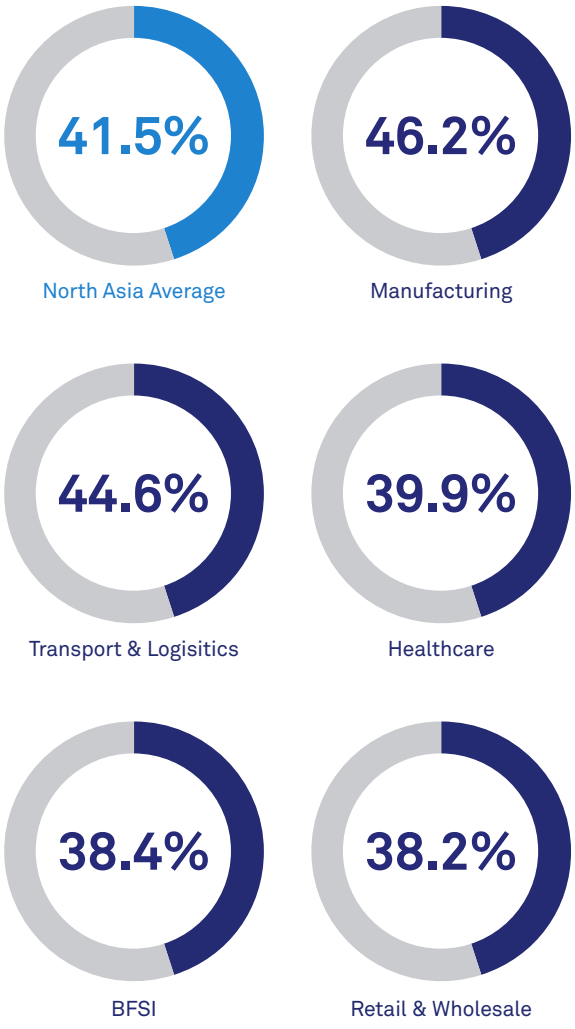


Figure 7. Manufacturing and Transport & Logistics endure the highest number of false alarms across the region

Security automation maturity in North Asia

Leveraging security automation across the threat lifecycle

Conversations with executives in North Asia confirmed that organisations are taking advantage of Artificial Intelligence (AI) in powerful new ways. Examples include automating repetitive tasks in back-of-house processes, enhancing speed and accuracy of decision-making, and improving the customer experience.

In cybersecurity, AI enables automation in systems and software that emulates human actions, especially manual and repetitive tasks. AI and ML harness data science, decision rules and algorithms to make specific recommendations and perform security functions to improve the prevention, detection and management of cyber incidents.

AI-powered bots can gather, analyse, and correlate enormous volumes of structured and unstructured data, including alerts, alarms, rules, and behaviours, to find potentially dangerous and suspicious patterns across multiple attack surfaces and vectors.

Recent developments in cross-platform integration between multi-vendor detection and response tools (including EDR, NDR, SIEM and SOAR) have increased the extent to which manual and repetitive 'swivel chair' SecOps analyst activities can be automated.

A prime benefit of automation is leveraging technology to augment security analyst instinct and experience in complex environments. Removing time spent on repetitive, arguably lower-value tasks can help the security team better safeguard vital business operations.

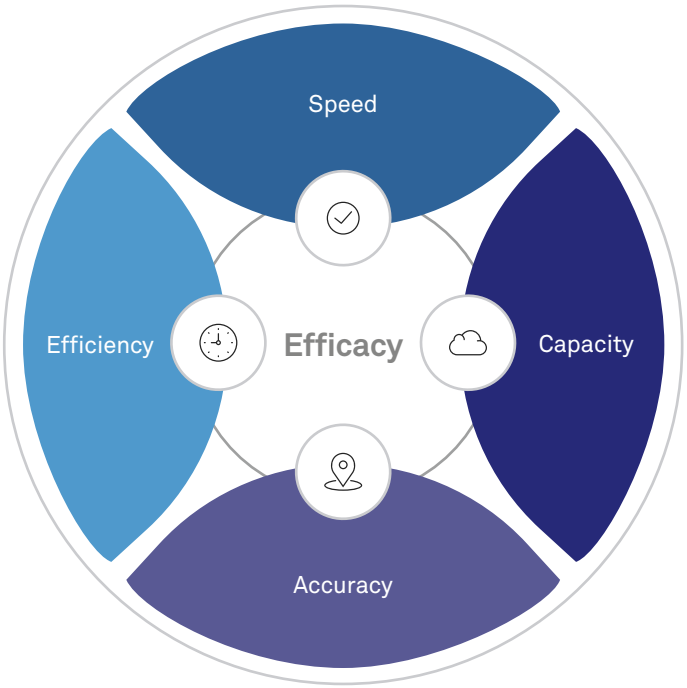
Well architected, implemented, and tuned security automation can dramatically reduce the likelihood and impact of a severe breach. Improvements are realised by decreasing MTTD/MTTR and reducing alert fatigue through the unification of threat intelligence (capabilities and feeds), incident response and security operations functions.

Typical use cases for automation include alert enrichment, phishing investigation & response, endpoint triage (malware), investigation & containment and more complex threat intelligence such as telemetry analysis, correlation, and user entity behavioural analytics.

Security automation allows organisations to harness the unique power of AI and technology to boost digital transformation plans in a stable and secure way.

> **"We put a lot of focus on security automation because we would like to respond to real incidents as soon as possible and as fast as possible as we are in a highly regulated environment."**
>
> Head of Security at a large banking firm in Hong Kong SAR

The four pillars of security automation efficacy



Support digital transformation — secure migration, adoption and deployment of critical technologies such as SWG, IoT, cloud, AI/MI, and edge technologies on which the business runs

Minimise security and enterprise risk — improve compliance, security posture and reporting to manage stakeholders

Balance the budget — leverage security tools to better manage OPEX/CAPEX costs, even as APTs and threat surfaces grow

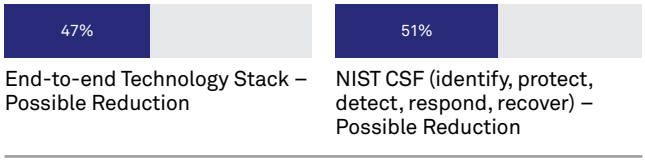
Security team improvements — free up time for value-creating security team activities, supporting new CX-led product developments

Realising measurable benefits from automation

Omdia's survey of 250 security experts in North Asia shows that half of all severe security breaches could have been reduced with effective automation (Figure 8).

Security leaders are confident they could reduce nearly 50% of all serious security incidents and breaches with better security automation. Interestingly, executives see more potential for automation for their threat lifecycle functions (NIST CSF) than from a technology stack (cloud and endpoints to on-premises) perspective.

Of the 'serious' cybersecurity incidents or breaches that impacted your organisation in the past 12 months, what percentage could have been reduced with optimised security automation?



End-to-end Technology Stack – Possible Reduction

NIST CSF (identify, protect, detect, respond, recover) – Possible Reduction

Figure 8. Effective security automation can dramatically reduce the likelihood and impact of a breach

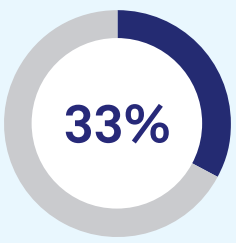
Organisations are underutilising SIEM and SOAR capabilities

Our survey shows more mature security companies are tackling security challenges by leveraging the in-built capabilities of Security Orchestration, Automation and Response (SOAR) and Security Incident and Event Management (SIEM) platforms.

Not to be confused with Robotic Process Automation (RPA) in other security areas such as application development (SecDevOps), advanced SIEM and SOAR tools are purpose-built to collect and analyse vast volumes of security-related log and telemetry data to enable near-real-time detection of malicious security events.

When deployed and tuned well, these tools detect and act on anomalous behaviour and potential security incidents earlier and more efficiently.

However, despite SOAR being around for several years and SIEM even longer, most firms are not taking full advantage of the capabilities offered by these platforms.



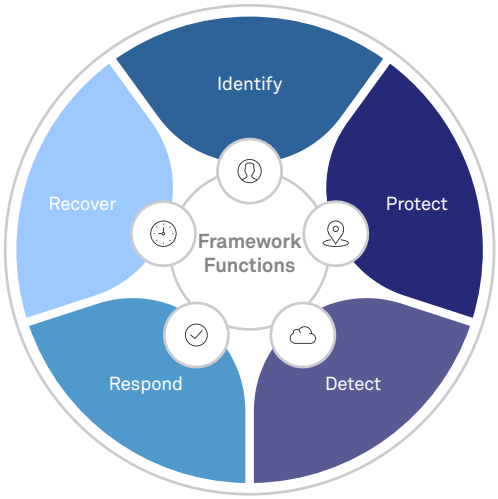
of firms in North Asia have currently implemented SIEM.

Use a framework to assess security automation

Organisations tackle security from different perspectives. To maximise coverage and insight, Omdia framed the research to test and compare the maturity of firms from two perspectives.

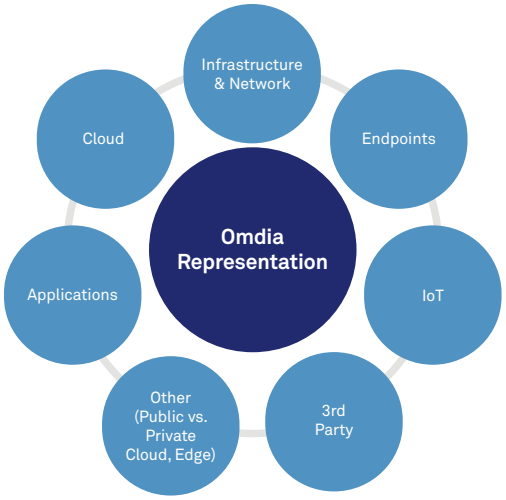
NIST CSF

The widely adopted and accepted National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) threat lifecycle is perhaps the most intuitive choice for integrating security automation concepts into complex technology environments.[1]



End-to-end technology stack

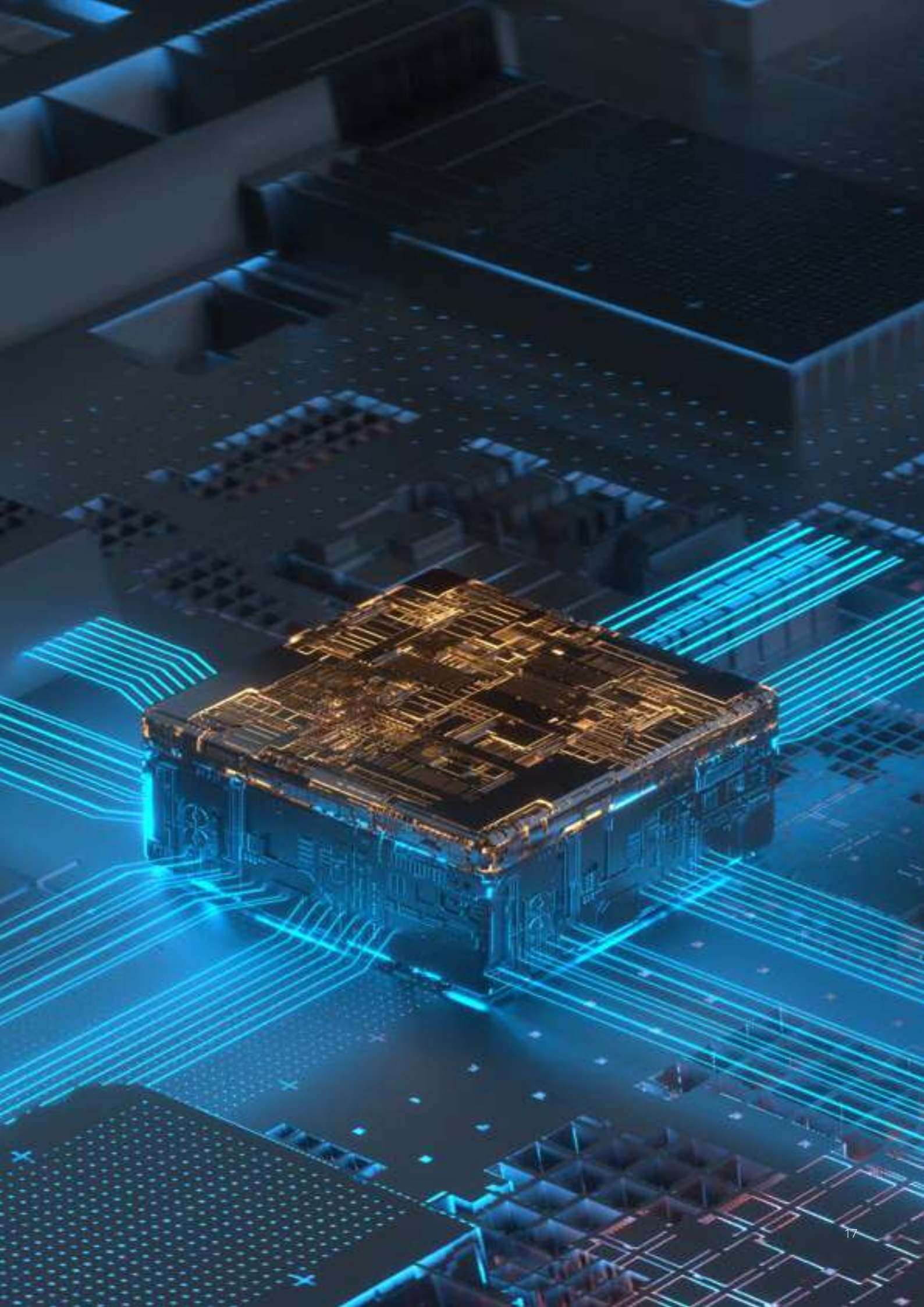
Modern organisations have seen a significant increase in attacks across all technology resources, from the core data centre and cloud through to networks, endpoints and IoT. Business leaders must align their security automation deployments to key business challenges, relevant to their industry, maturity, and technology configuration.



Digital Value Chain: Collective people, process and technology combinations for sustainable competitive advantage in each industry.

Figure 9. A model of security automation maturity assessment for the region

[1] The complete NIST CSF: https://www.nist.gov/cyberframework



Most firms in North Asia are early in their security automation journey

Using the assessment model outlined below, most organisations in North Asia are at operational (level 3) maturity or lower. At this point on a maturity journey, most firms are not harnessing the available benefits of security automation.

How mature is your organisation in using security automation across the cybersecurity attack framework on a scale of 1 to 4?

9%

Level 1

Basic / Nascent – e.g. automation is rarely used, very manual SecOps.

22%

Level 2

Developing – e.g. security automation is used in some security tools, basic processes.

40%

Level 3

Operational Security automation is widespread, integrated, processes and playbooks well defined.

24%

Level 4

Advanced use of automation in security as a key part of SecOps across process, people and technology.

Figure 10. There remain a lot of potential improvements to harnessing security automation across North Asia

The reality is striking. Despite more investments over the years by firms in SIEM, SOAR and single domain solutions tools, less than a quarter of organisations in the region are advanced in using security automation.

At these lower maturity levels, security tools frequently operate as stand-alone and reactive solutions, requiring frequent attention from security analysts to sort through alert/alarm noise.

Many organisations also experienced challenges 'tuning' these tools, with a 'buy, set and forget' mentality becoming a business reality. This is happening under the weight of more alerts (from more tools, sensors, and feeds), as well as skills shortages and the pace of change which COVID-19 cemented across technology and culture.

Apparent industry and location maturity differences across North Asia

There are several differences in the level of security automation maturity across industries (Figure 11) and locations (Figure 12) in North Asia.[2]

Industry view

How mature is your organisation in using security automation across the cybersecurity attack framework on a scale of 1 (basic) to 4 (advanced) ?

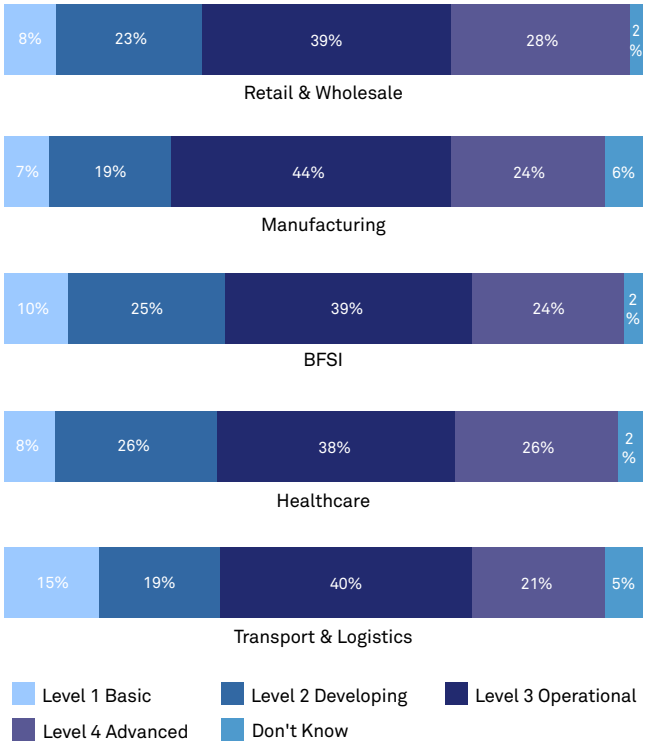


Figure 11. Retail & Wholesale, Health, and BFSI are the region's most progressive in security automation

[2] To avoid any one geography or industry skewing the results, a statistically valid sample – equally distributed across all five locations and industries – was used.

From an industry perspective across the region, retail & wholesale leads the pack with the highest proportion of more 'advanced' (level 4) firms. Manufacturing has the highest ratio at 'operational' capability, but conversely answered 'don't know' more than any other sector. Transport and logistics has the biggest representation of organisations at a basic maturity (15%), and 5% that 'don't know'.

The chart shows vast differences in security automation maturity. Interviews in the region highlight the importance of leveraging tools, people, and processes to overcome industry-specific challenges, including operational technology and IT integration-triggered security issues.

Regulatory scrutiny has forced BFSI organisations to deploy automation to assist with mandatory reporting requirements.

Healthcare has been at the frontline since the pandemic, forcing a sector that traditionally lags in IT investments to improve cybersecurity readiness. Healthcare organisations have put more emphasis on protecting private patient data, as services and information move online and firms invest in intellectual property with medicines and treatments.

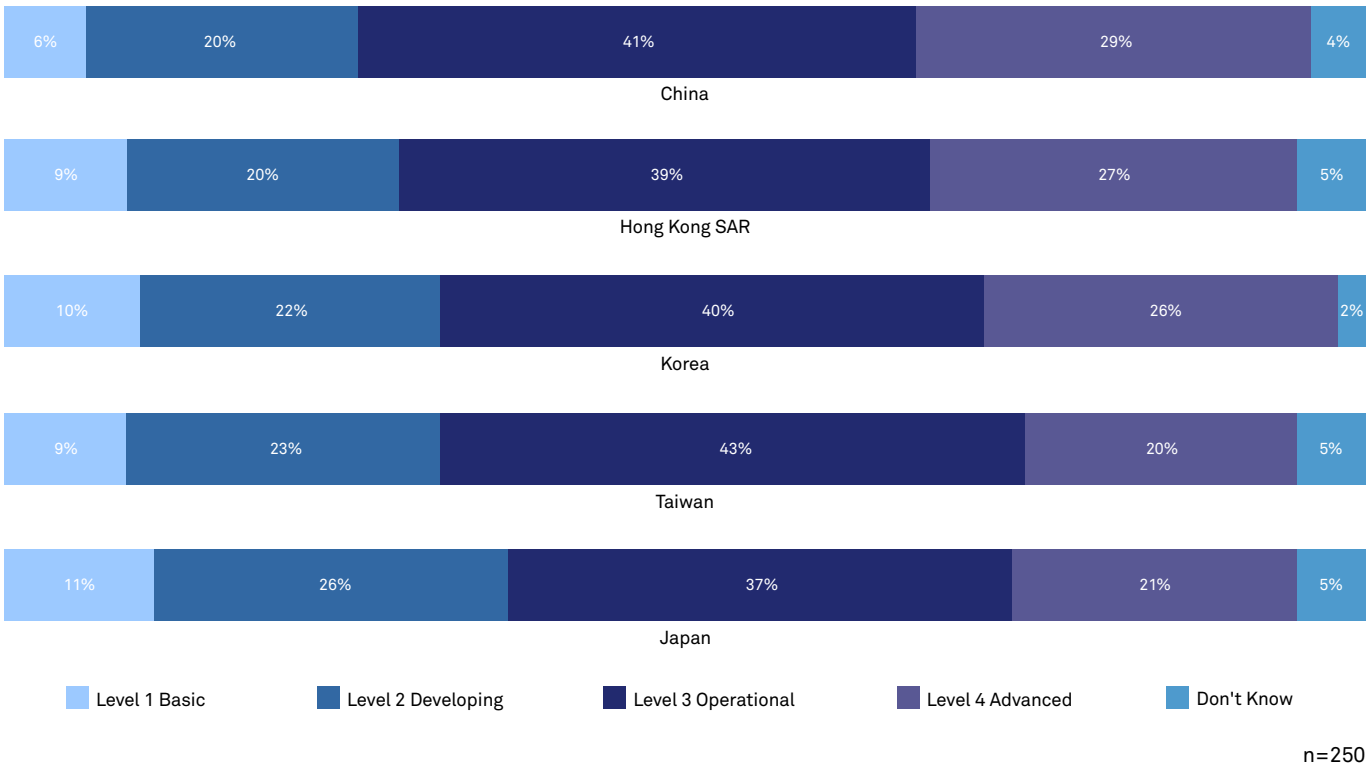
Retail & wholesale have faced similar challenges to healthcare, as the explosion in online commerce has boosted many cloud-native start-ups who more readily use cloud security automation solutions.

Transport & logistics face a substantial challenge with IoT and connected fleets. Automation in this sector must cross the physical and virtual membrane to connect OT with IT across an immense attack surface.

In terms of location, China has the highest percentage of organisations reporting at levels 3 (operational) and 4 (advanced). Japan has the lowest relative level of security automation, despite advanced manufacturing and a history of process invention (e.g. Total Quality Management, Kaizen). Variance in relative maturity across all countries is due to the industry makeup of each location and the embedded use of technology.

Location view

How mature is your organisation in using security automation across the cybersecurity attack framework on a scale of 1 (basic) to 4 (advanced) ?



n=250

Figure 12. China is the most advanced user of security automation

Improving cybersecurity resilience with automation

Automation has the potential to dramatically improve security posture, but every organisation has different requirements. This report aims to help business leaders identify their key automation barriers (challenges) and enablers (drivers), and accelerate adoption through a step-change maturity model.

Figure 13 shows the most significant challenges that emerged during interviews with executives in the region.

Organisations are generally less confident deploying automation across their entire IT stack, preferring to deploy only across their threat lifecycle tools.

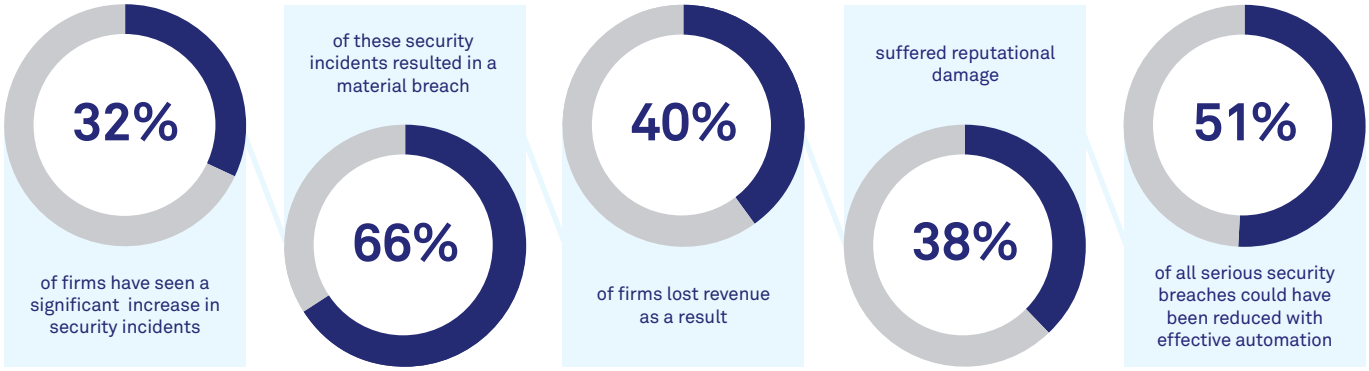
The ever-expanding technology asset base, combined with the multi-vendor skills needed by security analysts, contribute to the issue.

Of note, the top three challenges in using automation in security operations in the last 12 months across the region were staff, trust in tooling, and dealing with the vulnerabilities arising from advanced threats.

> **“The best thing automation could do is free up security analysts' time, so they don't have to investigate (false) alerts.”**
>
> SecOps Director at a large financial services firm in China

Drivers for Security Automation

- Overworked staff with alert fatigue and resulting human error
- Increasing Advanced Persistent Threats
- Growing hybrid IT estates (remote workers, cloud migration & CI/CD)
- Complex security controls for regulation
- Complex attack vectors and vulnerabilities



- Right staff and skills to leverage tools and AI
- Lack of trust in AI and concerns over explainability for consumer and regulatory requirements (black box effect)
- Growing, complex vulnerability that can't be automated easily
- Difficult to demonstrate ROI
- Unclear differences from existing tools

Barriers to Security Automation

Figure 13. The most significant drivers and barriers to accelerating automation

A path forward

Final recommendations

The insights presented in this report serve to coalesce extensive quantitative and qualitative research across North Asia to benefit organisations.

Leading firms surveyed show more progress across integrated security tools and automated playbooks. They're also more likely to engage third parties for consultation and managed security services to augment internal capabilities. However, challenges and constraints to leveraging automation are real and require a robust and holistic strategy.

To help improve security automation maturity, here are four fundamental principles – aligned with a step-change model – for North Asian firms to consider:

> **"In the future, our security automation will focus more on assessment of the event that is happening. We are exploring tools and looking for patterns across threat intelligence in near-real-time."**
>
> SecOps Policy and Chief Risk Officer at a large Indian bank based in Hong Kong SAR

	Level 1 Basic / Nascent	Level 2 Developing / Maturing	Level 3 Operational / Widespread	Level 4 Optimised / Advanced
Tool	○ Automation rarely used and tactical. ○ Most common use is automated threat intelligence feeds, and NDR/EDR alerts.	○ Automation still tactical but more widespread. ○ Multiple threat intelligence feeds, third-party support, and proprietary tools deployed. ○ Basic level integration to foundational SIEM.	○ Automation widespread across security, IT and lines of business. ○ Customised proprietary tools deployed, including SIEM and SOAR.	○ Automation fundamental to all major business operations, including security. ○ Customised and integrated third-party supported tools deployed, including XDR and/or MTDR.
Process	○ Usually overly focused on threat identification. ○ No automated playbooks deployed. ○ Very limited full IT stack telemetry, analysis and prioritisation.	○ Capability may extend into detection and response, although recovery capabilities are limited. ○ Minimal playbook automation. Broader full IT stack telemetry, analysis and prioritisation.	○ Extending capabilities into recovery for major IT assets, databases and applications. ○ Several playbook responses automated within SOAR.	○ All major critical infrastructure, applications, systems and devices incorporate security automation. ○ Growing automated playbook volume.
People	○ Highly labour-intense SecOps for gathering, assessing, prioritising and taking action. ○ Limited understanding and trust in ML/AI.	○ Highly labour-intensive SecOps for prioritisation and action from multiple threat telemetry feeds and alerts. ○ Growing awareness of automation use.	○ Shifting from labour-intense SecOps detection activities to faster response and recovery. ○ Increasing proactive prevention activities. ○ Growing automation understanding and experimentation.	○ SecOps aligned with development teams and innovation. ○ Dramatically reduced burnout and attrition.
Results	○ High staff fatigue, burnout, manual interventions and unplugged technology gaps. ○ High enterprise risk and low upfront cost (higher long-term cost from breach).	○ More alerts causing higher staff fatigue and burnout, with manual interventions required for assessment and prioritisation. ○ Fewer technology gaps but high enterprise risk from blind spots remains.	○ Gradual reductions in attrition and burnout, with a slight shift from reactive to proactive security activities. ○ Lower enterprise risk and greater security performance underpinning business innovation.	○ Measurable reduction in staff attrition and burnout, with better employee wellbeing. ○ Manageable and measured enterprise risk. ○ Solid security performance, boosting business innovation and agility, including partners.

1

Position security as a champion of digital resilience

Poor security constrains digital transformation efforts, as cyberattacks increase across all technology areas. Security leaders must address the material business impacts that can be mitigated with adequate investment in cybersecurity.

Lost revenue, reputational damage and operational downtime are three of many pertinent and tangible consequences of inaction.

2

Define a strategy across the four tiers of security automation readiness

Defining and implementing a change strategy across tools, processes and people is essential for achieving measurable results in cyber resilience. It's important to note that change takes time and organisations require a robust plan to succeed.

Based on insights from leading firms in North Asia, this report outlines a 4-tier security maturity model to enable your security automation strategy.

3

Unlock value from security tools

Security leaders should reassess the value and role of each of their security tools and investigate how to best unify them through automation.

Executives will leverage partners to access skills and expertise, helping them drive better integration between tools, processes and people. This approach can drive SecOps efficiency and better protect business interests against increasingly sophisticated threats.

4

Leverage the right partner for cybersecurity

Cybersecurity skills are scarce and expensive. Leading organisations in North Asia increasingly plan to address security constraints with platform-led automation and more native cloud security, whilst retaining third-party support.

Executives in the region must partner with Managed Security Services Providers that offer high-quality services, always-on reliability and industry-leading expertise to help them scale their automation activities.

Appendix

Omdia was pleased to conduct this research in partnership with Telstra International. The insights and trends within this report reflect the latest experiences of organisations and are based on in-depth fieldwork carried out in the second half of 2022.

We trust this paper will guide security, technology, and business leaders in taking advantage of new security tools, processes, and skilled people to drive sustainable competitive advantage.

Sources

Additional insights and syndicated research in this paper are available to clients. Key sources include: Digital Enterprise Services – https://omdia.tech.informa.com/products/digital-enterprise-services-intelligence-service

Author

Adam Etherington
Senior Principal Analyst, Digital Enterprise Services
adam.etherington@omdia.com

Methodology

To better understand the reality of cybersecurity in North Asia, Telstra International commissioned Omdia to conduct an independent, comprehensive, local market study focusing on China, Hong Kong SAR, Taiwan, Japan, and Korea.

From August through to October, Omdia conducted a direct primary research survey of 250 senior security decision-makers at mid- and large-sized firms across Banking, Financial Services, Insurance, Transport & Logistics, Retail & Wholesale, Manufacturing, and Healthcare.

Small to medium enterprises (>100 to 999 employees) comprised 50% of respondents, while 50% were large (>1000 employees) organisations. 50% of respondents were IT Executives (including CIO, CTO, CISO) and 50% were senior technology leaders (including technology leads, senior consultants).

Omdia also conducted in-depth interviews with eleven senior decision-makers responsible for choosing cloud in their organisations to reveal detailed views of executives' aspirations, challenges, constraints, and service provider partner considerations in security.

Global counterpoints in this research draw on Omdia's global expertise in its digital enterprise services, and cybersecurity intelligence services.

About Telstra

Telstra is a leading telecommunications and technology company with a proudly Australian heritage and a longstanding, growing international business. Telstra has also been operating outside Australia and extensively across the Asia Pacific region for about 70 years.

Today, we operate in over 20 countries outside of Australia, providing services to thousands of businesses, governments, carrier and OTT customers. We provide data and IP networks, network application services, unified communications, cloud, industry solutions and integrated services.

Furthermore, Telstra Purple, our professional and managed services business in Australia, Asia and the UK, brings together people and innovative solutions to define and deliver a clear vision of our customers' transformation journey, network foundation, and the cyber protection they need to thrive.

These services are underpinned by our subsea cable network, one of the largest in the Asia Pacific region, with licenses in Asia, Europe and the Americas, and access to more than 2,000 Points-of-Presence around the world.

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. We offer expert analysis and strategic insight across the IT, telecoms, and media industries through our global base of analysts.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalise on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

Contact your Telstra account representative for more details.

telstra.com.hk

telstraenquiry@team.telstra.com