MOORE

CLOUD TRANSFORMATION

Elevate Your Business with Cloud-Powered Advantage

Moore Hong Kong

WHY MOORE?

At Moore, it's not about us. It's all about you. When it comes to providing personalised and commercially astute audit, accounting, tax and business advisory services, it simply can't be anything else.

With over 30 directors and a team of over 300 staff, we offer a wide range of audit, assurance tax, and advisory services to our clients. Our global family of 30,000 professionals in more than 110 countries allows us to share expertise, knowledge, and best practices to ensure our clients receive the highest quality of service, no matter where their work takes them.

As your genuine professional partner, we will not only advise you but also challenge you to meet your goals and objectives for the future. With our team's personal qualities, skills, and experience, we are confident in our ability to support your group's development.

Cloud transformation

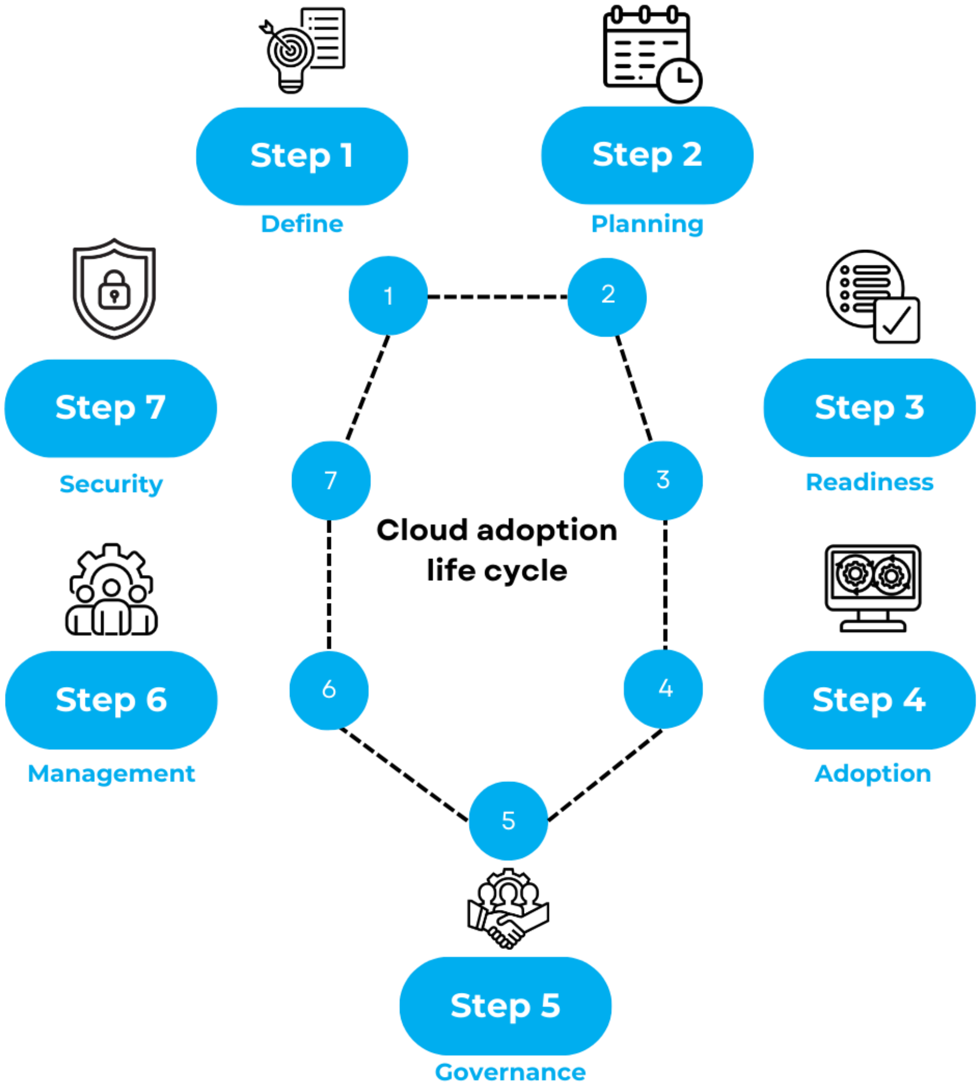
Elevate your business with cloud-powered advantage

The cloud, once known as the panacea for scalability and efficiency, has now become a prime target for malicious actors seeking to exploit vulnerabilities and compromise sensitive data. From distributed denial of service attacks to insider threats and data breaches, the cybersecurity landscape has become increasingly treacherous, with cyber threats constantly evolving. In particular, the emerge of zero day threat could pose a daunting challenge for global businesses in the cloud environment, resulting in increased vulnerability, operational disruption and non-compliance. Ultimately, costly investments in cloud infrastructures does not translate to the achievement of business objectives.

According to the 2024 Cloud Security Report, the top five cloud security priorities are as follows:

1. Threat detection and response
2. User education and awareness
3. End to end visibility and monitoring
4. Cloud governance and risk management
5. Data security and privacy

These priorities indicate that businesses are placing a greater emphasis on securing the assets and infrastructure within their cloud environment to harness the full benefits of cloud transformation. Our IT & Cybersecurity team can help you to secure your digital future in the cloud environment through a comprehensive cloud adoption life cycle.



Define: We conduct a comprehensive assessment of your current cloud infrastructure and strategies. This assessment will involve evaluating your cloud environment from multiple perspectives, including business, financial, and technical, to identify strengths, weaknesses, and areas for improvement.

Planning: We assess the accuracy and completeness of your IT inventory list for the cloud environment, ensuring that all inventory items are accurately mapped to the corresponding cloud-based assets. This mapping exercise will enable us to conduct a thorough cloud rationalisation process that will help you plan and prioritise your migration efforts.

Readiness: We conduct comprehensive risk assessments to identify potential security vulnerabilities, threats, and risks that should be addressed within the landing zone deployment and configuration. We then review and validate the security-related configurations, and the robustness of the security controls implemented in the landing zone reference implementation, ensuring alignment with your organisation's security policies.

Adoption: We help you ensure the security and compliance of the modernised cloud workloads. Our team conduct thorough vulnerability scanning and assessments on the adopted cloud workloads and services to identify any potential security vulnerabilities. Also, we collaborate with responsible teams to establish robust identity and access management controls for the adopted cloud workloads to reduce the risk of unauthorised access.

Governance: We ensure the roles and responsibilities of your cloud governance team are clearly defined and aligned with your overall security policy, involving the evaluation of the integration between your cloud governance processes with the organisation's incident response plan.

Management: We review and evaluate the classification of each workload in terms of its criticality and business value, then conduct an impact analysis to validate that business value aligns with strategic objectives.

Security: We help you establish a security-centric approach to cloud adoption through providing effective security awareness training programmes for cloud environments, empowering your cloud stakeholders in maintaining the security and resilience of the cloud environment.

Data driven cybersecurity

Elevate your approach with data-backed insights

Data driven approach

1 Data collection

- Assessment of data collection processes and tools
- Review of data sources and quality
- Evaluation of data storage and retention policies

2 Data analysis

- Examination of data analysis methodologies
- Review of data analytics tools and techniques
- Assessment of threat intelligence

3 Implementing solutions

- Audit of security control implementation
- Review of incident response procedures
- Assessment of patch management processes
- Evaluation of security architecture and design

4 Monitor and adapt

- Review of continuous monitoring practices
- Assessment of security metrics and KPIs
- Evaluation of continuous improvement processes

In today's hyperconnected world, the cybersecurity landscape is in a constant of flux. As IT networks grow more complex, with an ever-expanding web of devices, applications, and cloud services, the attack surface available to malicious actors has expanded exponentially. A Forrester report states that artificial intelligence is expected to be utilised by cyber criminals to increase the scale and speed of attacks, along with the prediction that AI will conduct attacks that no human could ever conceive of.

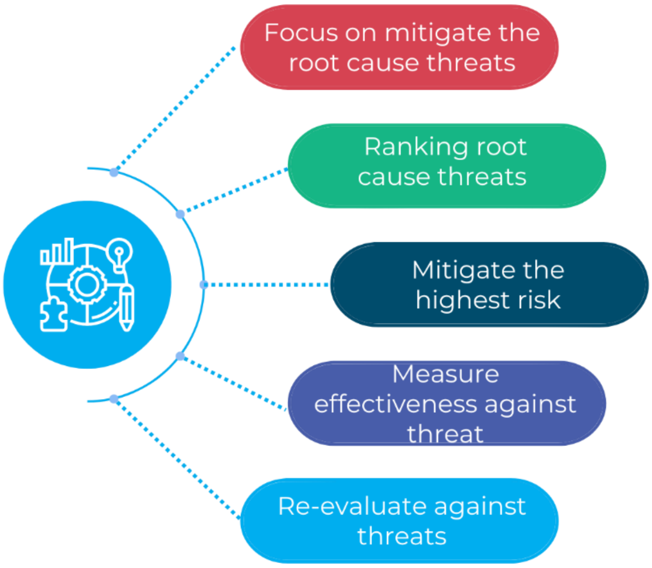
The cascading business impact of such AI-powered cyber-attacks could be catastrophic. Organisations caught flat-footed by these emergent threats face the very real prospect of crippling financial losses from costly data breaches, debilitating operational disruptions, and irreparable reputational damage.

In the face of this evolving, AI-driven threat landscape, a data-driven approach to cybersecurity has become imperative to drive a more holistic cybersecurity strategy. Organisations must establish a robust data driven cybersecurity strategy that could protect themselves against cyber threats with the following principles.

Our IT & Cybersecurity team offers the following services to help your organisation to

build a more robust data driven security posture:

Principles of data driven strategy


Focus on mitigate the root cause threats
Ranking root cause threats
Mitigate the highest risk
Measure effectiveness against threat
Re-evaluate against threats

Green digital transformation

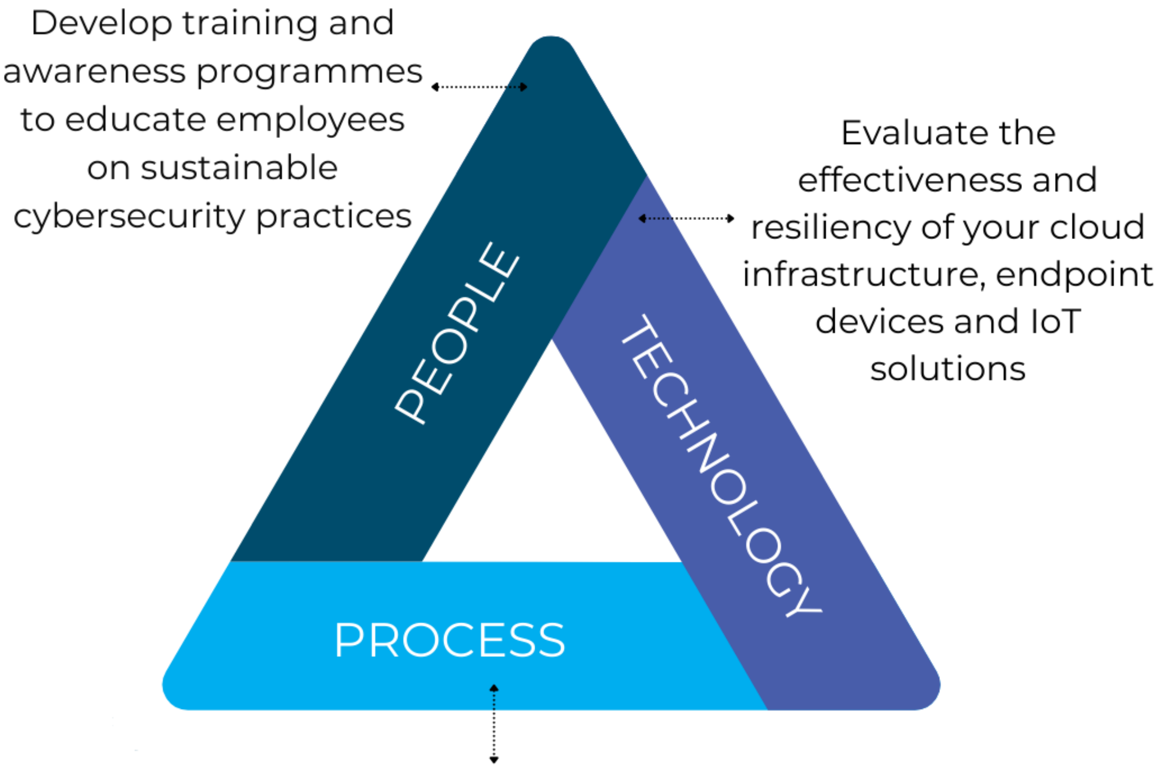
Cyber-powered sustainability: securing a greener, smarter future

In an era of heightened environmental consciousness and stringent sustainability regulations, organisations can no longer afford to overlook the security implications of their green digital transformation efforts. Embracing environmentally responsible practices throughout the people, processes, and technologies that underpin digital initiatives is not just a matter of corporate social responsibility - It is a critical enabler of long-term business resilience and competitive advantage.

According to CEO Insights Report, “Turning Turmoil to Advantage: How CEOs Are Navigating Change to Drive Growth”, sustainability and digital technologies are viewed as the topmost impactful drivers driving growth. Failure in recognising and leverage the linkage between sustainability and digitalisation can significantly slow down an organisation’s progress toward net zero emissions, ultimately failing short of stakeholder expectations.

Our Cybersecurity & IT team possesses expertise that can be invaluable in enabling your successful green transformation through people, process and technology framework:

Successful Green Transformation



Develop training and awareness programmes to educate employees on sustainable cybersecurity practices

Evaluate the effectiveness and resiliency of your cloud infrastructure, endpoint devices and IoT solutions

Align sustainability goals with your organisation's risk management framework, ensuring that your green initiatives are pursued in a secure and compliant manner

Orchestration and automation

Orchestrate your defences, automate your dominance

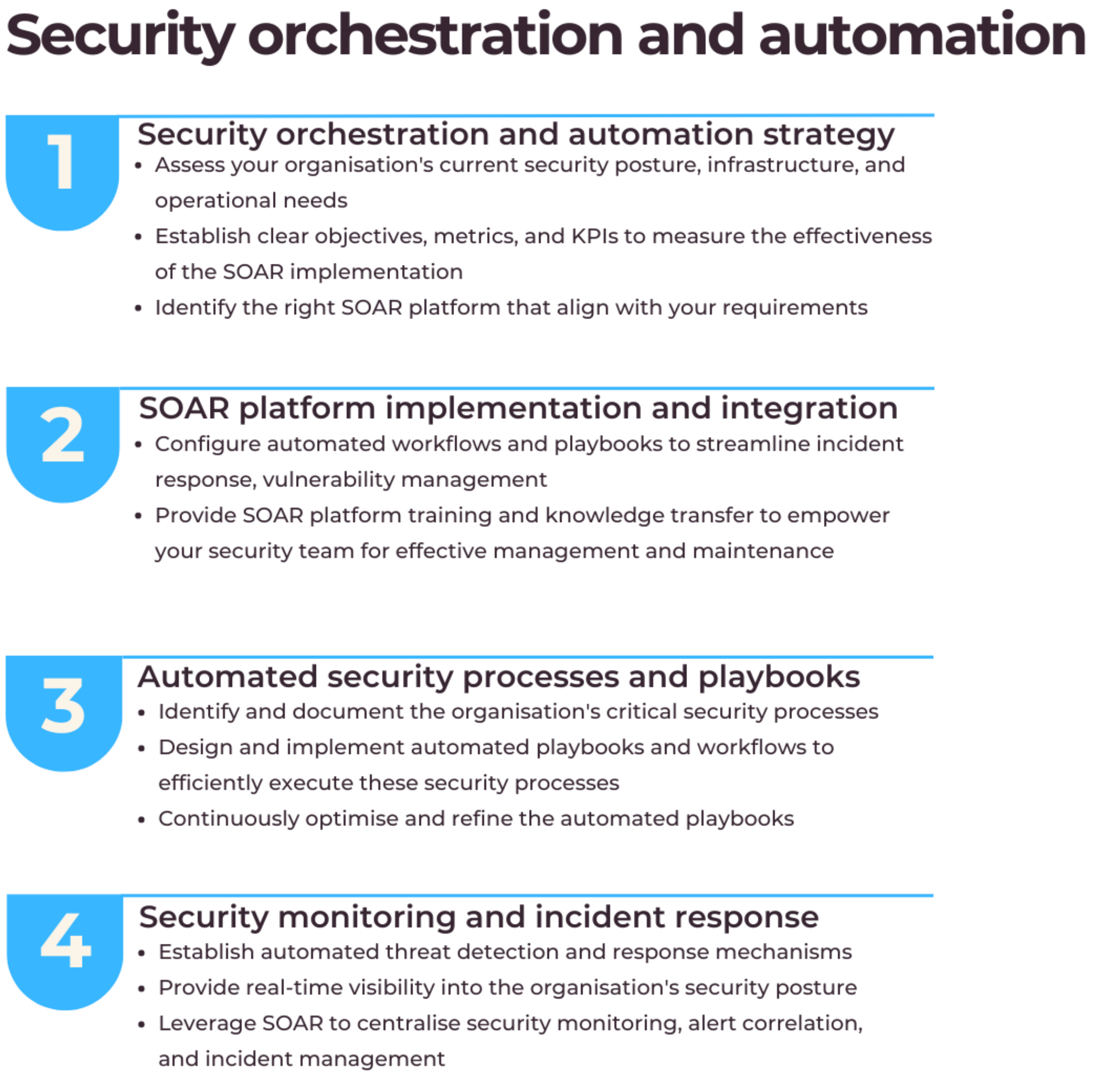
As the threat landscape continues to morph and mutate, the adoption of automation and orchestration in IT cybersecurity has become a strategic imperative. The global security orchestration automation and response (SOAR) market, which encompasses both orchestration and automation capabilities, is expected to grow from $1.2 billion in 2020 to $2.2 billion by 2025, at a CAGR of 13.1% during the forecast period, underscoring the increasing significance of these transformative technologies.

The centralisation of security orchestration creates single points of failure. If an attacker breaches the orchestration layer, they could gain control over security tools and automated processes, paralysing the organisation's ability to defend against subsequent attacks.

A compromised orchestration platform could allow an attacker to disable critical security controls and reprogram automated incident response, exposing the organisation's vulnerable systems while preventing security team coordination.

The heavy reliance on automated security processes opens new attack vectors for cyber attackers. For instance, an attacker could find a way to inject malware into the automated patch management workflow, allowing them to surreptitiously distribute malicious code across the organisation's infrastructure under the cover of legitimate software updates.

Our IT & Cybersecurity team has the expertise to help your businesses leverage the power of security orchestration and automation to enhance your overall security posture, operational efficiency, and stay ahead of the evolving threat landscape:



Security orchestration and automation

1 **Security orchestration and automation strategy**

- Assess your organisation's current security posture, infrastructure, and operational needs
- Establish clear objectives, metrics, and KPIs to measure the effectiveness of the SOAR implementation
- Identify the right SOAR platform that align with your requirements

2 **SOAR platform implementation and integration**

- Configure automated workflows and playbooks to streamline incident response, vulnerability management
- Provide SOAR platform training and knowledge transfer to empower your security team for effective management and maintenance

3 **Automated security processes and playbooks**

- Identify and document the organisation's critical security processes
- Design and implement automated playbooks and workflows to efficiently execute these security processes
- Continuously optimise and refine the automated playbooks

4 **Security monitoring and incident response**

- Establish automated threat detection and response mechanisms
- Provide real-time visibility into the organisation's security posture
- Leverage SOAR to centralise security monitoring, alert correlation, and incident management

CONTACT US

Our IT and Cybersecurity practice offers a spectrum of services that help businesses to achieve a robust IT architecture and security framework through identifying vulnerabilities, threats, and areas for improvement.

For any enquiries, please contact our advisers directly.

PATRICK ROZARIO
Advisory Services Managing Director

T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
IT & Cybersecurity Principal

T +852 2738 4631
E kevinlau@moore.hk

At Moore, our purpose is to help people thrive – our clients, our people, and the communities they live and work in. We're a global accounting and advisory family with over 37,000 people in 558 offices across 114 countries, connecting and collaborating to take care of your needs – local, national and international.

MOORE

An independent member of Moore Global Network Limited – members in principal cities all throughout the world.

The information provided is for general guidance only and should not be treated as professional advice. While we believe the content is correct at the time of publication, we cannot accept responsibility for any loss or inconvenience caused by actions taken based on the information herein. We recommend consulting a qualified advisor to ensure your specific circumstances are properly evaluated before making any decisions.