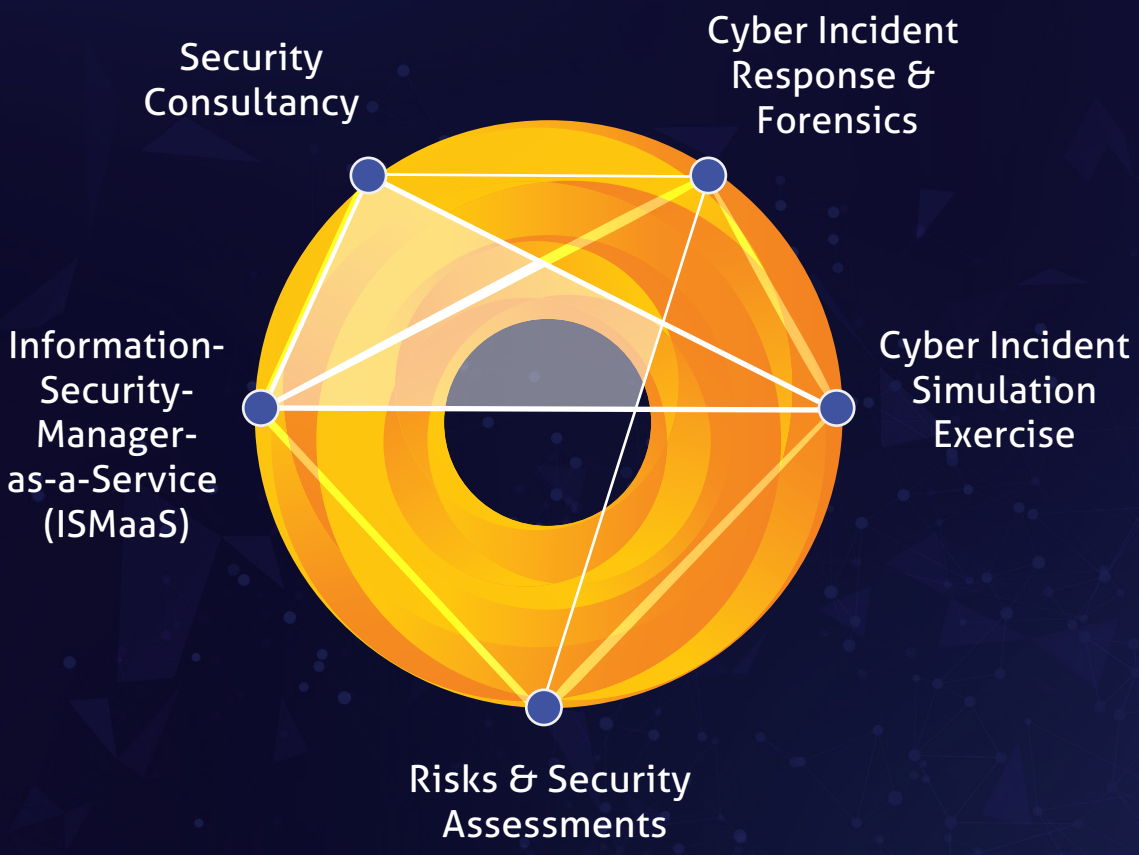
R&TCYBER
Safeguarding your Digital Assets



CYBERSECURITY

Rajah & Tann Cybersecurity is uniquely placed to help secure digital architecture and digital assets, mitigate risks of attacks, minimise cyber-related disruptions, and investigate data breaches.

Comprehensive Suite of Services

We offer end-to-end services that cover the entire risk management lifecycle in our clients' operations and ensure they maintain a robust cyber security strategy.

Professional Domain Experts

Led by highly experienced technical experts in the field of security services and consultancy, we are a market leader in providing comprehensive pre and post incident security services.

Cross-Domain Expertise

Our clientele spans across multiple industries including government, financial, transport, e-commerce, medical, logistics, media and education

OUR SERVICES

Security Consultancy

Assist our clients to attain industry recognised certifications such as Cyber Trust Mark and ISO/IEC 27001 or compliance with industry regulations such as MAS TRMG/BCMG, CEM+HIA certification for healthcare entities, IMDA BCS/TCS Code and etc.

Cyber Incident Response & Forensics

Assist in setting up a Cyber Incident Response System with processes based on ISO standards, and provide staff training and conduct regular table-top exercises and develop a Cyber Incident Response playbook per scenario for each system.

Cyber Incident Simulation Exercise

Designed to be as realistic as possible, participants are engaged through an immersive and engaging exercise to assess the organisation's ability to prevent, detect and respond to cyberattacks, and to also prepare organisations in responding to a cybersecurity incident.

Information-Security-Manager-As-A-Service (ISMaaS)

Engage cybersecurity experts to monitor, detect, and neutralise risks, helping your organisation better manage information security and cybersecurity compliance.

RISKS & SECURITY ASSESSMENTS

Configuration Audit

Assess the configuration of the hardening of systems against industry-accepted security standards.

Incident Response & Investigation

Set up an Incident Response System with processes based on international standards, and provide training for your staff and conduct regular table-top exercises and develop Incident Response playbook per scenario for each system.

Perform post-mortem investigations of security incidents, identify root cause(s) and propose recommendations to recover from and prevent similar incidents from recurring.

Information Security Risk Assessment

Identify, understand and prioritise risks in your IT systems to determine measures to mitigate, reduce, remove or transfer these risks.

IT Architecture Security Review

Improve your security posture to ensure greater confidentiality, integrity and availability of your critical IT services.

Personal Data Protection

Advise organisations using our DEFICIT© framework to more effectively minimise the risk of data leakages from your internal network or from publicly accessible web servers.

Privacy Impact Assessment (PIA)

Identify the effectiveness of your organisation's personal data protection and compliance with privacy laws.

Source Code Security Review

Conduct independent security review of source codes (including Java and .Net) and secure coding awareness training for your development team.

Vulnerability Assessment & Penetration Test

Provision of network, operating system and web application VAPTs, including HTTP / SMTP Distributed Denial of Service (DDoS) assessments.

Pre-Incident

- Threat Modelling and Risk Assessment
- Architecture Review (NIST 800-53r5/CSF/CIS Controls)
- Configuration Audit
- Development of Incident Response Plan and Playbooks
- Vulnerability Assessment
- Penetration Testing (licensed by CSRO)
- Source Code Security Review
- Incident Response Simulation Exercises
- Compliance Review and Advisory (e.g. MAS TRMG)
- Security Operations Centre Monitoring

Post-Incident

- Incident Response (remote and onsite)
  - Forensic Imaging and Analysis
  - Identification, Containment, Eradication
- Malware Reverse Engineering
- Threat Hunting
- Technical Advisory Support for Responses to Regulators
- Lessons Learnt Workshops
- Post-Incident Controls Verification
- Dark Web Monitoring for Post-Mortem Transmission

Rajah &Tann Cybersecurity

INFO@RTCYBER.COM

WWW.RTCYBER.COM