SAAB

CYBER SECURITY SOLUTIONS

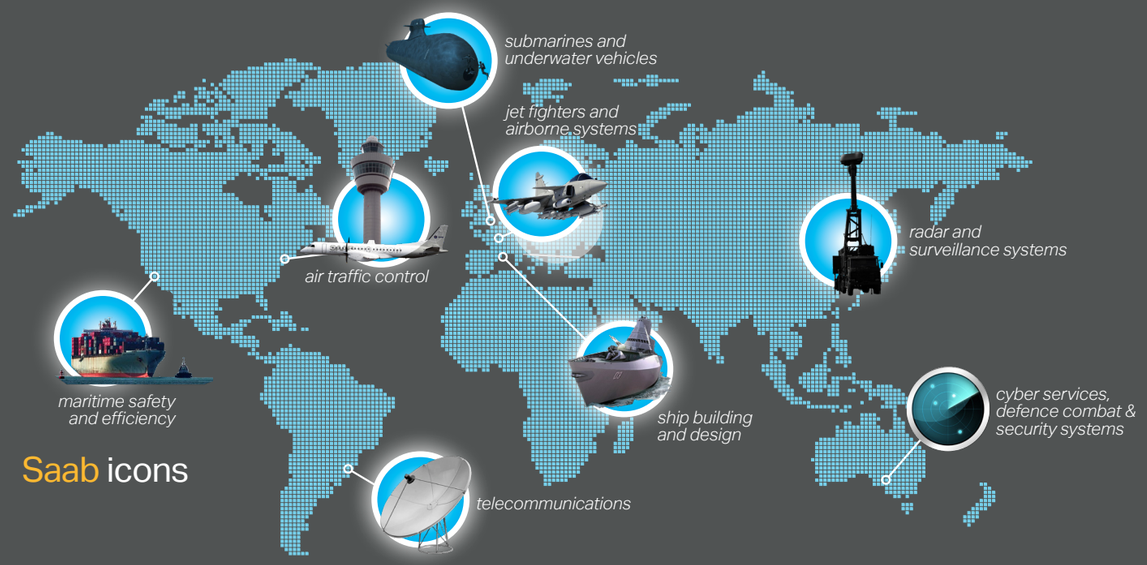
Capability Statement

Keeping people, society and information **safe**

Saab's led defence, aviation and security technology for more than eighty years.

As government, business and military reliance on information, networks, and communication has increased significantly over the past decade, so to has the frequency of advanced, coordinated cyber attacks.

As a trusted, world-leader of defence technology, we've got the 'thinking edge' on leading the fight to combat the cyber threat.



Saab icons

Our story

Saab is a high-technology, defence and security business-to-government and business-to-business organisation with 17,000 employees worldwide.

No other technology company designs and builds submarines, aircraft, underwater vehicles, missiles, torpedoes, radars, camouflage, security systems, plus everything in-between, to **keep people and society safe**.

Our information and cyber security risk management consultancy is built on Saab's primary values —trust, expertise and drive. Always ahead of technology. A reputation for integrity. Committed to our core philosophy of safety ... we're passionate about **keeping information and systems safe.**

Capability and capacity

Saab Australia's information and cyber security capability was built upon the need to protect our own intellectual property and systems, as well as that of our clients. As an organisation developing military and civil systems to defend our national interests and safeguard our critical infrastructure and public safety, protecting that information is absolutely critical. Saab was one of the first defence companies in Australia to achieve **ISO 27001 certification** for its information security management system.

As well as protecting our own systems, we build resilience into the products and systems we develop for our customers. We make sure our products and systems are 'cyber hardened' to withstand the demanding environments in which they operate.

Over many years we built our in-house experience to support Saab's systems worldwide and build a professional security and risk consulting business which offers a comprehensive suite of information and cyber security services.

We built our information and cyber security team through careful design - selecting the best professionals with highest level of experience and knowledge. Our consultants can lead your information and cyber security project from inception through to completion, giving you complete continuity. Our team are skilled communicators with defence and government security clearances.

Our security risk advisors, assessors, analysts and information technology specialists are trusted and respected by federal, state and local governments nation-wide. Our experience spans the defence, government, communications, utilities, health, education, law, finance and hospitality sectors.

Our information and cyber security offer

The framework and systems protecting Saab's information assets are independently audited and certified to the internationally recognised ISO/IEC 27001:2013 standard. We follow these same principles in our information and cyber security consulting work.

IRAP assessments & preparedness

An IRAP assessment is the first stage towards achieving accreditation to process, store or communicate government or nationally sensitive information. Our IRAP program is led by our IRAP assessors who are certified by the Australian Signals Directorate (ASD). We can also assist your organisation prepare for an IRAP assessment or accreditation, by advising on and implementing appropriate security standards, requirements, controls, and recommendations in accordance with the Australian Government Information Security Manual.

Governance, risk and compliance

We will review your organisation's controls, policies and procedures to determine your level of information and cyber security maturity and ability to manage risk. These activities typically align to industry standards and frameworks such as ISO 27001, ISM, PSPF/DSPF, CPS 234 and NIST. For example CPS 234, a mandatory regulation issued by APRA which requires regulated entities to boost their information security capabilities commensurate with the evolving size and extent of threats to their assets.

Product cyber resilience engineering

Whether implementing a new system, upgrading existing or legacy systems, we will work with your organisation to develop or enhance your cyber resilience. By employing a systems security engineering approach we provide the necessary guidance to navigate cyber resiliency to ensure deployed products or systems survive confronting threats.

Defence Industry Security Preparedness accreditation

We will work with you to enhance your information and cyber security maturity in order to comply with the new Defence Industry Security Program (DISP) requirements at all levels (Entry through to Level 3).

Penetration testing

We perform objective-based penetration tests to identify vulnerabilities in your organisation's infrastructure, services and applications. We assess potential risks by then attempting to exploit those vulnerabilities. Tests can be conducted as an anonymous user seeking to exploit weaknesses in the systems and services visible on the internet or as an internal user attempting to elevate privileges or exfiltrate data.

Security architecture

We will determine whether the controls within a network/communications environment are effective and appropriate for your current business. These should align with vendor and industry best practice recommendations. If not, we'll recommend a course of action to keep your information and systems safe.

System configuration and security reviews

These reviews assess your server and IT system configurations against industry and vendor best practices. They typically cover security configuration, password strength testing, software maintenance, firewalls, and network infrastructure—tailored to your needs.

Incident response

This on-demand service supports you through an incident or unpredicted crisis. It involves a full discovery and attempt to recover from an information or cyber security-related breach or significant event such as a business email compromise or data spill.

Training and awareness

We develop and deliver tailored security awareness programs relevant to your workforce. Most security breaches are a result of human error or social engineering. It can be something as innocent as clicking a link, or downloading a malicious file. We'll also help you create policies and procedures to establish a clear framework for developing your information and cyber security culture and governance. We can provide either technical or practical education, training and awareness packages to suit individuals' or organisations' responsibilities.

Supply chain risk management

Managing the supply chain is an important piece of an organisations approach to risk management. Knowing where and how the supply chain interacts with your organisation is critical in ensuring business continuity for your organisation and implementing security best practice. We will work with you to develop or enhance your knowledge of your systems and understanding of your supply chain to identify the inherent risks that arise throughout the supply chain process. We will then help you develop appropriate mitigation strategies to effectively manage your supply chain risk.

We develop and deliver reliable, innovative and cost effective information and cyber security solutions.

OUR CLIENTS

Education institutions (public & private)

Defence & defence industry

Financial bodies

Federal & state government agencies

Electronics & technology/automation production industries

Saab Group and its defence & security customers

Work snapshots

For the most part, a lot of the work we do is focussed on building resilience for our clients in order to protect them from the ever evolving information and cyber security threats. We act with integrity and confidentiality to protect the privacy of every client.

CASE STUDY

Not for profit organisation

As well as its own operational data, this organisation stored the personal information of its workforce and its tens of thousands of donors, supporters and members. Saab performed a series of internal and external penetration tests of their network to determine how safely the systems were managing this data. We detected a critical vulnerability, which if left untreated, could have made all of the personal identity information they stored to be breached, causing enormous reputational damage and ultimately threatening the ongoing viability of their organisation. Saab provided the appropriate advice and guidance for the organisation to mitigate this risk.

CASE STUDY

Business email compromise

We helped a small to medium enterprise interrupt the theft of almost $1,000,000 through the compromise of their email system. When the company discovered the problem and engaged Saab to manage their incident response, we were able to quickly construct an attack timeline and capture and catalogue email and computer accounts involved in the incident. Tracing the initial phishing email that lead to multiple account compromises revealed the steps the attackers took to inject themselves into the client's email chain and coerce them into sending money to a fraudulent bank account. Using this information we established mitigation strategies to prevent further compromise and developed an education program for the business to maintain. Saab was able to provide valuable information to the client which was then used by the authorities to further their investigation, ultimately identify the perpetrators and disrupt the BEC operation.

CASE STUDY

National defence organisation

Keeping our national defence agencies' data safe is a critical element of maintaining our nation's security. Saab reviewed the organisation's information management systems and structure to create a new management framework to meet Information Security Registered Assessors Program accreditation. Saab developed system overview documents, system security plans, incident response plans, security risk management plans, statements of applicability and a suite of policies and procedures.

CASE STUDY

Saab Australia

Saab has been a trusted supplier of advanced military and civil security system for more than thirty years. The relentless trend of managing and sharing information online has exposed Saab and its business partners' systems to possible information theft or disruption. To further enhance our own information and cyber security posture we implemented our own information security management system obtaining ISO/IEC 27001 certification for our Australian operations. A complete framework with structured plans, national cyber security policies, procedures, work instructions and an ongoing employee awareness scheme was developed, initiated and is now in rolling review. Saab is now adopting the model globally for international security management and accreditation.

Our principals

Supporting their industry experience, our consultants hold defence and government security clearances, as well as the following information security credentials: Information security management (ISACA CISM) // Technical information security (ISC2 CISSP) // ISO/IEC 27001 Lead Implementer // Technical security auditing and assessment (EC-Council CEH) // Information security risk management (ISACA CRISC) // Security compliance and auditing (ISACA CISA).

Marc Tapping

Division head & Chief Information Security Officer

Marc's career as an information systems, security and ICT specialist spans 25 years. He is highly sought after for advice as a thought leader and trusted advisor on all matters of information security and risk management. His extensive hands-on technical capabilities with networks, web applications and system architecture is a valuable complement to his strategic consulting and auditing experience.

As a certified IRAP assessor for the Australian Signals Directorate (ASD) Marc leads Saab's IRAP program in conducting risk assessments, penetration testing, compliance and consulting activities for State and Commonwealth government agencies as well as various defence and industry clients. Marc is also a guest lecturer for the Masters of Cyber Security course at the University of South Australia.

Ben Cornish

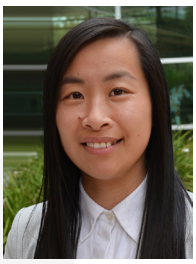
Strategic engagement & project management lead

Ben is a highly experienced negotiator and navigator of the information security space. He has led engagement programs to increase the awareness of sophisticated threats targeting government and industry.

Working across industry, government and critical infrastructure, Ben has led investigations, assessments and the development of strategies for identifying and mitigating threats across the information, cyber, physical and personnel security domains.

Vanessa Wong

Governance, risk & compliance lead



Vanessa is recognised for her problem solving skills and ability to rapidly explore and convey both business and technical concepts with audience for all levels.

She has a demonstrated background in complex analysis and design outcomes for large scale systems in state and federal government, particularly with Defence and law enforcement agencies.

Vanessa leads organisational governance, risk and compliance projects; establishes policies, standards and process frameworks to manage information security risks; and develops defensible security architectures; achieving the highest levels of information systems accreditation for her clients.

Vanessa holds a Bachelor of Applied Science in Mathematical and Computer Modelling, and recognised competencies in implementing information security management systems with world-leading risk management assurer, SAI Global.

Luke Smith

Information and cyber security technical lead

Luke's information security credentials are backed by his solid network architecture, system administration and software development experience.

Respected by clients and his team for an asymmetric approach to testing and auditing, Luke is most celebrated for his effective remediation and mitigation strategies that have saved or forearmed many clients.

Luke is an ISO 27001 Lead Implementer, has a diploma in Information Technology (software development), ITIL foundation Certificate in IT Service Management and is a Cisco certified network administrator (CCNA).

Geoff Stephens

Cyber worthiness / product assurance lead

Geoff brings over 25 years of Software Engineering, Systems Engineer and Defence industry experience to the Professional Services Team. Geoff has worked across a variety of roles, domains and technologies, including as Saab Australia's Head of Discipline (HOD) for Software Engineering and as a Design Approval Engineer, providing an excellent mix of technical, managerial, leadership and customer relations skills.

Geoff has a keen interest and significant experience in developing and implementing cyber security product assurance and evaluation programs.

Geoff has a Masters of Engineering - Military Systems Integration, a Bachelor of Science (Computer Science), a Diploma in Project Management, is a Certified Scrum Master and a member of the Adelaide University Advisory Board – Software Engineering.

SAAB TECHNOLOGIES SAAB