themissinglink®
An Infosys company

Global Security Operations Centre

Your security, managed 24/7

Contents

Global Security Operations Centre (GSOC)

Your security, managed 24/7.

Building and running an in-house Security Operations Centre (SOC) is time-consuming, resource-intensive, and difficult to maintain from a technology and staffing standpoint. Finding the right mix of resources to operate the SOC with diverse levels of expertise in triage, incident response, and threat hunting can be challenging.

That's exactly why our GSOC exists.

The Missing Link has operated in Australia since 1997, providing specialised managed services since day one. In 2014, we responded to a growing demand for specialised cybersecurity services by launching our Security Division. Over the last decade, our GSOC services have matured into a world-class operation designed to evolve alongside your business, and the threat landscape.

Why choose The Missing Link GSOC?

- Access to industry-recognised advice and expertise
- An assigned Service Delivery Contact (Non-Technical)
- A dedicated Principal Analyst/Engineer Contact (Technical)
- Specialised experience and thought leadership across a wide range of security technologies
- A true Partnership (Co-Managed) SOC Service model
- Continuous Service Improvement, planning, and governance

Your new security operations team

The Missing Link Security launched its SOC in March 2018, investing in advanced equipment, innovative software, and a highly certified team. From day one, we've invested in advanced technology, smart automation, and an elite team of security specialists. Operating from secure facilities in Sydney, Melbourne, and the United Kingdom, we deliver continuous monitoring, threat detection, and strategic insight, helping you see more, respond faster, and stay ahead of evolving threats.

Our award-winning security specialists are experts in their field, with extensive knowledge and understanding of all aspects of cybersecurity. We focus on increasing visibility, minimising risks, and providing secure solutions tailored to your organisation. We are also ISO27001-certified, so you can trust that your data and operations are safeguarded by the highest standards of information security governance.

We offer a range of service levels to meet every business requirement, including **24/7 support**, delivered via:

- A **follow-the-sun model** for global reach
- A **sovereign approach** when data residency is essential

The team

Service Delivery Manager

Your Service Delivery Manager (SDM) is your central point of contact, responsible for maintaining a strong working relationship and overseeing the delivery of your SOC services.

Throughout the service, your SDM will keep you updated with regular check-ins, schedule service review meetings, and ensure reporting is timely and relevant. They will also assist you by directing queries to the right resources to contextualise and explain alerts and response requirements. You can also proactively contact your SDM directly at any time. They will be your escalation point for any incidents or concerns.

As part of the GSOC service, The Missing Link will provide metrics and context surrounding the analysts' activities, technology health, and findings summaries. The SDM, jointly with your principal technical contact, will deliver recurring reports on your service. They will also work with you to understand both parties' roles and responsibilities in driving continuous improvement in your service.

GSOC Team Structure

Our GSOC Team is made up of security analysts and engineers, each specialising in core SOC functions including proactive monitoring and alert triage, malware analysis, threat hunting, and threat remediation.

Our team comes from various IT backgrounds, whether desktop and network engineering, penetration testing, or digital forensics. Each discipline provides valuable input into our process, playbooks, and analysis of our client's threat landscape.

Roles and responsibilities in the SOC are clearly defined, with each level of seniority providing operational oversight and mentoring to the analysts in the level below. Our current roles in the SOC are as follows:

- **Defender - GSOC Engineers**
  Responsible for the proactive management, maintenance and incidents involving security solution software and infrastructure.
- **Watcher - GSOC Analysts**
  Triage and investigate alerts from various security solutions, primarily from EDR (Endpoint Detection & Response) and SIEM (Security Information and Event Management).
- **Hunter - GSOC Analysts**
  Conduct regular hunts through security telemetry looking for Indicators of Compromise (IOCs) and Behavioural Indicators of Compromise (BIOCs).
- **Responder - GSOC Analysts and GSOC Engineers**
  Lead or contribute to the progression and resolution of Incident Response scenarios.
- **Head of Security Operations**
  Provides administrative, leadership and strategic direction to the SOC Team and has many years of real-world experience in the field.

The Missing Link invests heavily in the development of its people, and the GSOC Team is no different. From initial onboarding, all our analysts are provided with a bespoke Personnel Development Plan (PDP) based on their previous experience and training. This PDP includes:

- 2 weeks of The Missing Link New Employee Orientation
- 2 weeks of Technology & Vendor Training
- 4- 6 weeks of Client Immersion and Shadowing
- 16 weeks of Operational Ramp-Up

We deliver continuous monitoring, threat detection, and strategic insight, helping you see more, respond faster, and stay ahead of evolving threats.

Ongoing learning is at the core of our culture. Analysts are supported with dedicated time to pursue industry certifications and have full access to The Missing Link's internal learning platforms to support their development.

Below are some examples of typical certifications undertaken by our analysts.

Analyst Tier/Title	Approx. Years	Training Courses/Certifications
Associate Security Analyst	0 – 1.5	CompTIA Network +, CompTIA Sec +, SC 100
Security Analyst (Level 1)	1.5 – 4	CompTIA Sec+, CEH, CEH Practical (12 Hour Exam), SC 200, CCFR (CrowdStrike Falcon Responder), CCFH (CrowdStrike Certified Falcon Hunter)
Senior Security Analyst (Level 2/Triage Specialist)	4 – 8+	CompTIA CYSA+, CHFI, CHFI Practical, SC 300, GIAC Certified Forensic Analyst (GFCA), CCFA (CrowdStrike Falcon Administrator)
Principal Security Analyst (Level 3)	8+	SANS 508, SANS 572, OSCP,

Engineer Tier/Title	Approx. Years	Training Courses/Certifications
Associate GSOC Engineer	0 – 1.5	CompTIA Network +, CCNA, CCSA
GSOC Engineer (Level 1)	1.5 – 4	CompTIA Sec+, ZCSA-IA, CyberArk Defender
Senior GSOC Engineer (Level 2)	4 – 8+	CCIE, CCSE, PNSCE, NSE Level 4, CyberArk Defender & Sentry
Principal GSOC Engineer (Level 3)	8+	CCIE x2+, CCND, NSE 5 / 7, CISSP

Security Operations Training and Certification Plan
Our team operates on a 24-hour-a-day rotating roster to ensure that your systems are always monitored and managed, and that all alerts are triaged and responded to in a time-efficient manner. We also operate a continuous recruitment and training cycle, ensuring we always have the right people in place: skilled, certified, and ready to act.

Visit our website to explore some of our customers' success stories. We are also happy to connect you directly with existing clients who can share their experience with The Missing Link.

Shift Rotation
Monitoring shifts are 12 hours in duration, rotated daily and nightly. Day shifts are from 7am to 7pm and night shifts are from 7pm to 7am.

The Missing Link SOC team consists of multiple functional groups working together to ensure you receive world-class incident detection and response, providing 24/7 monitoring, unsurpassed service, and contextualised reporting that delivers real value.

We pride ourselves on being a true extension of your internal team, providing transparency into our backend systems, clear communication, and direct access to the experts supporting your environment.


Close
100ms
2048mb
Metric
SES-008
enabled
enabled
Static
dd/mm/yy
enabled
ABASE

Additional Members of The Missing Link's Team

A unique value point for The Missing Link's SOC service is the strength and expertise of our employees who work with your organisation to advance your security maturity. Throughout our service, you may encounter our highly skilled team members, which may include:

Account Executives: Your primary point of contact for all pre-sale needs. The Account Executives take the time to understand your business challenges, explain how our technology works to solve them and propose solutions to help accelerate your security maturity.

Project Managers: Our Project Managers oversee technology implementations. They are responsible for ensuring a smooth experience during the deployment stages of a project and manage any issues throughout deployment.

Security Architects: The Security Architects oversee the design process and develop a roadmap for deploying security solutions. They are responsible for defining the scope of work, connecting business and IT needs, and ensuring that security controls adhere to best practices.

Security Engineers: The Security Engineers oversee the implementation and deployment of security solutions. They are responsible for configuring, optimising, and troubleshooting security solutions according to the design requirements.

Security Consultants: Our team of Security Consultants handles Offensive Security Activities. The Missing Link's Red Team is highly respected among our peers and is tasked with identifying potentially vulnerable areas of your technology infrastructure, helping you stay a step ahead of threats that others miss.

Contacting the SOC

The SOC can be contacted 24/7 via email or phone, including access to a dedicated **24-hour hotline** available to our customers.

Every call is managed and tracked so nothing slips through the cracks. We ensure **every request is handled promptly**, thoroughly, and in line with your escalation plan.

Process/Function	Client			The Missing Link			Vendor
	Director of Cyber Security	Manager Cyber Security Operations	SecOps Team	SOC Manager	SDM	TML SOC	Support
Platform & Service Management							
24 x 7 Monday to Sunday Support Hours	A	R	R	R	S	R	R
Ticketing & Remote Telephony Support	I	A	S	S	S	R	
Incident and Problem Management	A	S	R	S	S	S	
Patch and Release Management	A	S	R	S	S	C	R
Emergency & Standard Change Management Requests	A	S	R	S	S	S	R
System Vulnerability Management Remediation	A	S	R	S	S	C	R
Availability & Health Monitoring	A	S	R	S	S	S	R
Asset Management and Usage Monitoring	A	S	R	S	S	S	
Configuration Maintenance & Backups	A	S	R	S	S	C	R
System and Design Documentation	I	A, S	S	C	S	S	
Security Operations Maturity Assessment & Continuous Improvement Strategy	C	A, C	C	R	R	C	
SIEMaaS Monthly Report	I	A, I	I	S	R	S	
Security Alerts & Operations							
Critical Alert SLA (P1)	I	A, S	S	R	S	R	C
Incident Response	C	A, C	S	S	S	R	C
Log management & compliance reporting	I	A, S	R	S	S	R	C
Alert triage & analysis	I	A, S	R	S	S	R	C
Threat monitoring & alerting	C	A, R	S	S	S	R	C
Correlation rule fine tuning	I	A, R	S	S	S	R	C
Threat remediation recommendations	I	A, C	C	S	S	R	C
User dashboards & reports	I	A, C	S	S	S	R	C
Threat intelligence reports & security advisories	I	A, I	S	S	S	R	C
Security research reports	I	A, I	S	S	S	R	C
Remote Incident Response reports							

Example RASCI Matrix

RASCI Matrix

To ensure alignment between your team and ours, we'll work with you to build a tailored RASCI Matrix, clearly defining who is Responsible, Accountable, Supportive, Consulted, and Informed for all key services.

This is part of our commitment to clarity, accountability, and a truly co-managed approach. A sample matrix is shown above.

Onboarding: The first 90 days

Our onboarding process is built to ensure your service is delivered with precision, clarity, and confidence. Across the first 90 days, we follow a model focused on three key phases:

- Technology Deployment
- Transition to Managed Service & Hypercare
- Quality Assurance Testing

Technology Deployment

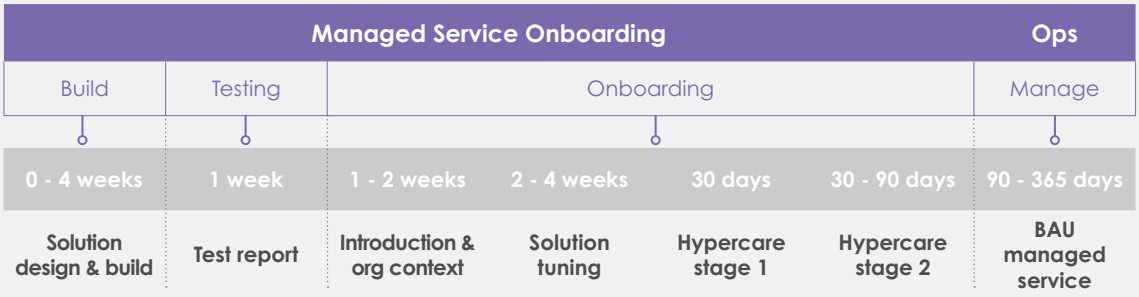
At The Missing Link, we take pride in the quality of our work. We believe in a methodical approach to the deployment of any solution. That's why every project is guided by a detailed statement of work.

While every engagement is tailored to your needs, typical outcomes include:

- End-to-end project management
- Collaborative solution design and build
- Quick Start Services to get you operational quickly
- A Security Maturity Assessment to benchmark your environment
- Seamless transition planning into managed service

Transition to Managed Service

Before transitioning a solution to our Security Operation Team, we complete a series of onboarding checks that span across people, processes, and technology.
The Onboarding process is defined at a high level in the diagram below.



The exact stages and deliverables may vary depending on the service you subscribe to, but our Service Delivery and Project Management teams will provide a tailored project plan and timeline during your project initiation.

As part of the onboarding process, and before the service goes live, The Missing Link team will request key information to be provided. This information is then built into the platform as our standard operating procedures to form a critical part of the service going forward. This information would include but not be limited to things like:

- Organisational Structure, key contacts, high-value targets
- Relevant third-party vendors or service providers
- Environment details like networks, servers and equipment
- Applicable process or procedure details for things like incident response
- Defined response expectations
- Your current ITSM tools and integrations

Continuous service improvement

At The Missing Link, we're committed to continuous improvement. Not just of our service, but of the platforms and environments we monitor, support, and influence.

Through regular technical meetings and reporting, the Service Delivery and SOC teams will help identify potential areas for improvement, which are then tracked and reviewed. These may include:

- Alert logic, triage, and response actions
- Process or procedure enhancements
- Recommending improvements and contributing expertise in areas or technology where we can add value (NGFW, Event Sources, DLP, etc.)
- Security Operations Maturity Assessment (SOMA) Development and Tracking

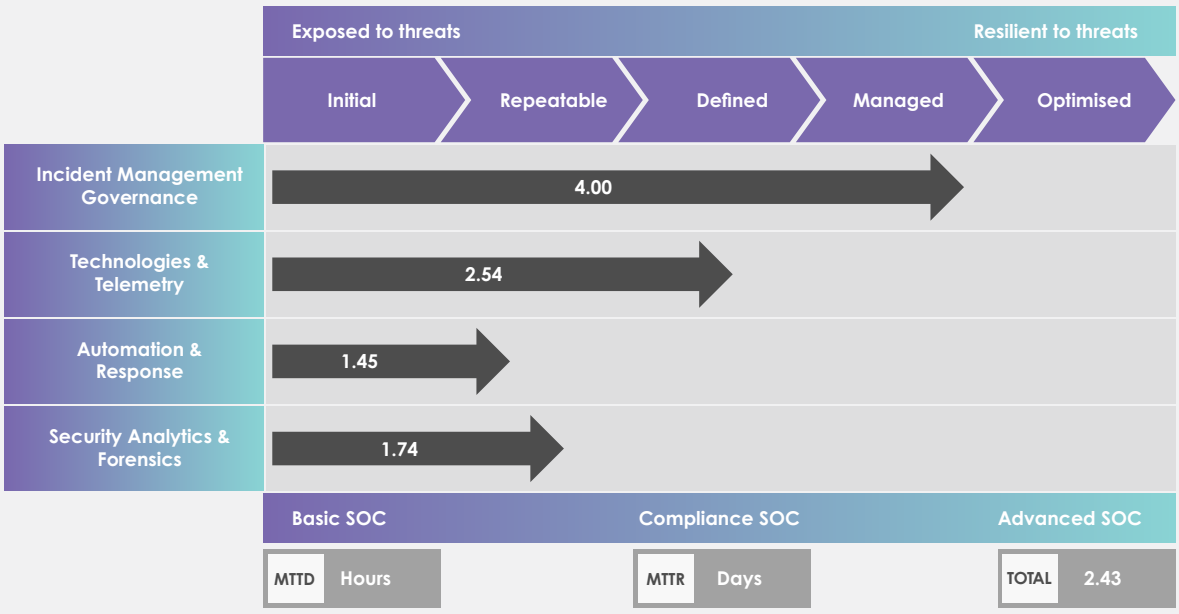
Security Operations Maturity Assessment (SOMA)

Included in your GSOC service, our assessment is a consultative engagement that evaluates your current SecOps program, specifically your people, processes, and technologies.

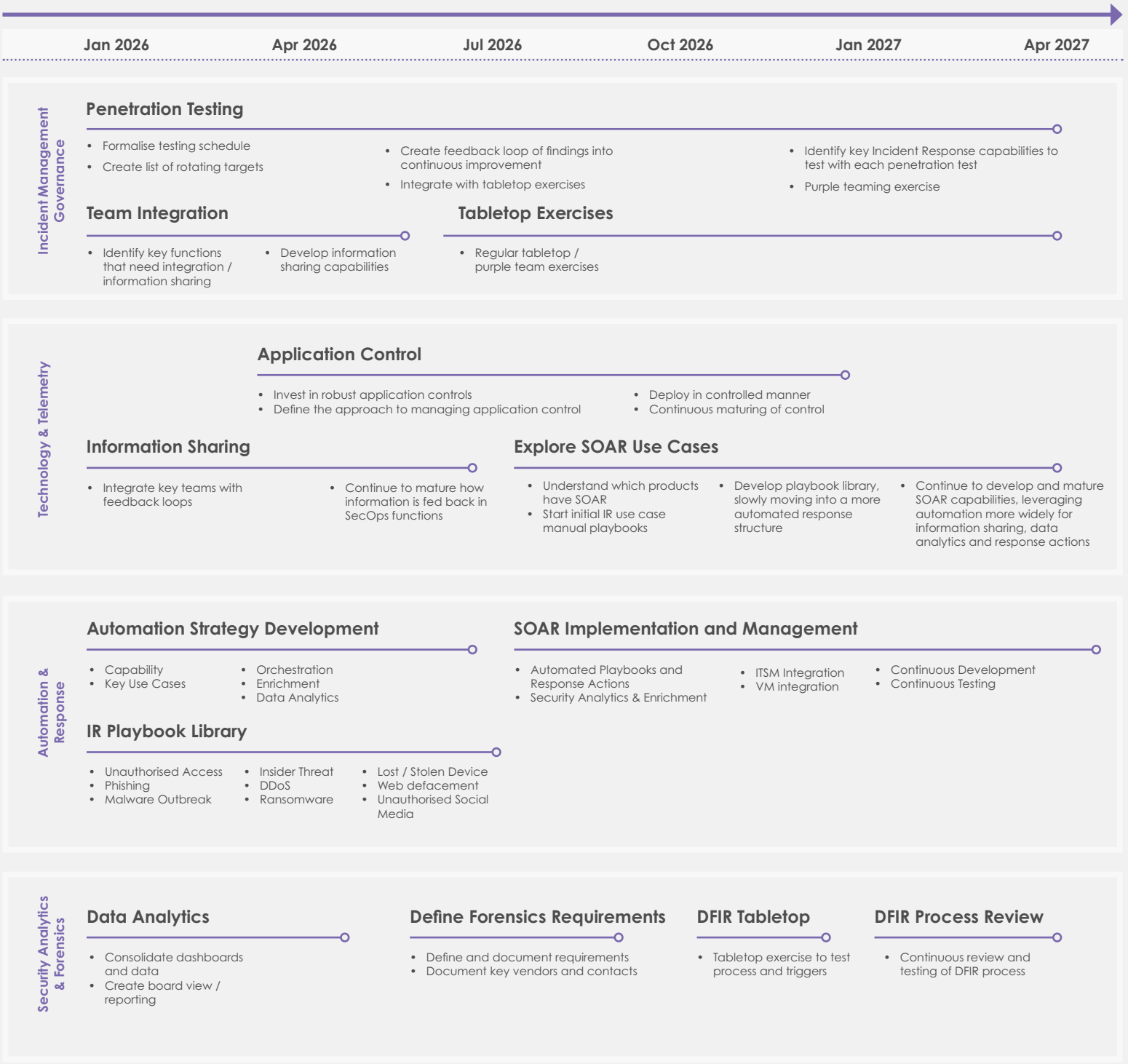
1. Incident Management Governance
2. Technologies and Telemetry
3. Automation and Response
4. Security Analytics and Forensics

The SOMA identifies your current maturity level, uncovers gaps, and provides a phased roadmap with actionable recommendations. This roadmap fuels your Continuous Service Improvement (CSI) program throughout the engagement.

Driven by your SDM, we conduct CSI check-ins at every Service Review Meeting to provide updates on each activity's status, risks, and outcomes.



Example Security Operations Maturity Model



The image above shows an example of a Continuous Service Improvement Roadmap for our customers. Leveraging the SOMA framework, target maturity, and recommendations, our Team will help you drive each activity or initiative. We also assist with technology comparisons, PoC and tech integrations, testing, and deployment.

Our goal is simple: to become your trusted security advisor. Whether you need hands-on support, roadmap delivery, or strategic input, we're here to help you continuously elevate your security operations.

themissinglink®

An Infosys company

Ready to take the next step in building a smarter SOC? Let's talk.

The Missing Link's Global Security Operations Centre (GSOC) service is designed to give you complete confidence in your security operations backed by 24/7 monitoring, expert-led analysis, and a team that acts as a true extension of yours.

Whether you're looking to mature your security posture, gain full visibility, or improve threat response, we'll work with you to deliver outcomes that are tailored, trusted, and built to evolve with your business.

Take the next step towards a more secure future.

themissinglink.com.au
1300 865 865
contactus@themissinglink.com.au

The Missing Link - your partner in cyber security excellence.

Infosys®
Navigate your next

Proudly part of Infosys. Locally delivered, globally backed.
The Missing Link is proud to be part of Infosys - a powerhouse in next-generation digital services and cyber defence. Together, we combine award-winning local expertise with global scale to deliver unrivalled Security and IT Services.