themissinglink®
An Infosys company

Managed detection and response

24/7 protection with clarity, insight and action

Contents

Managed detection and response

Proactive protection, powered by people and precision.

Cyber threats are relentless and getting more sophisticated by the day. That's why simply having security tools in place isn't enough. You need real-time detection, expert analysis, and rapid response from a team that lives and breathes cybersecurity.

The Missing Link's Managed Detection and Response (MDR) Service monitors your environment around the clock, using best-in-class technology to collect, normalise, and analyse logs, user behaviour, system activity, and patching hygiene across your infrastructure.

The service gives you expert-led threat detection and response, advanced security visibility across your entire environment and peace of mind that nothing slips through the cracks.

Key services include:

- Centralised Log Management
- Real-time Event Correlation
- Integrated Threat Intelligence
- Threat Hunting
- Scheduled Reporting

Our Managed Detection & Response (MDR) service is built to give your organisation a trusted partner to manage and maintain your detection and response capability end to end. For a fixed monthly fee, you gain access to a dedicated team of security specialists who proactively identify and contain threats before they become breaches.

By implementing MDR, your organisation will gain:

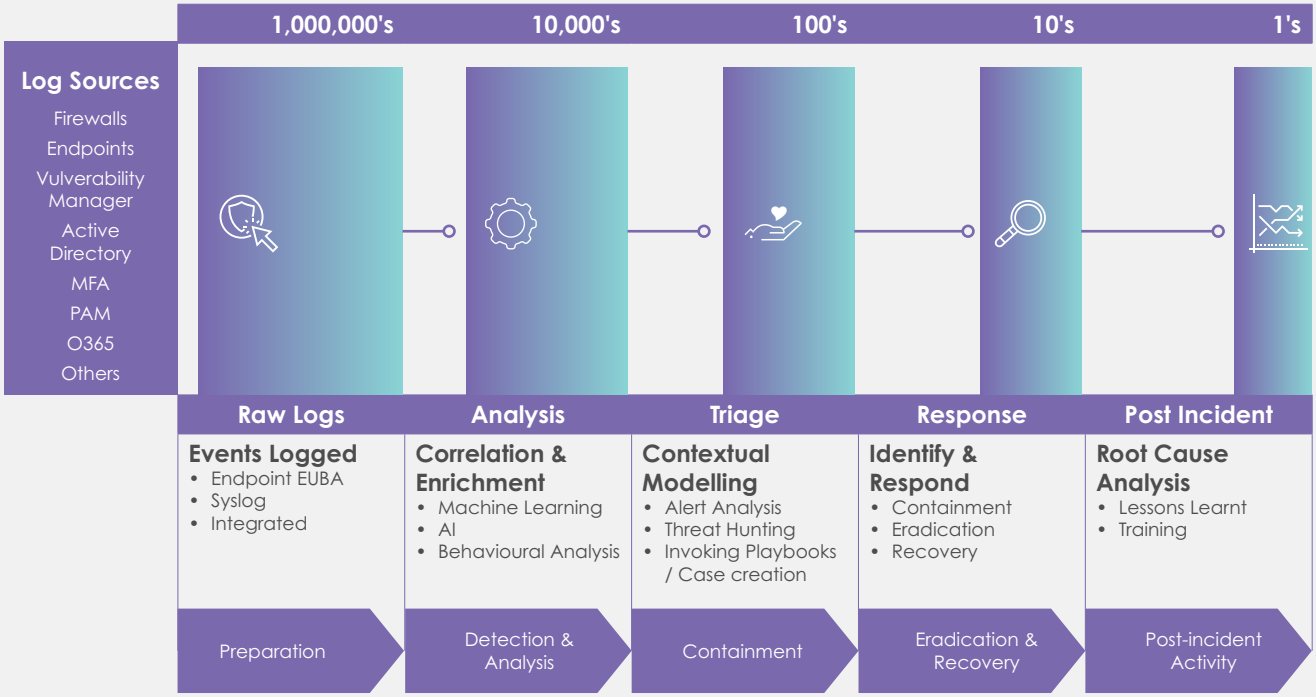
- A single pane-of-glass view across all security event logs from supported devices.
- 24 x 7 Security Monitoring, Analysis and Alerting.
- Enhanced value of your existing security controls through analysis of events by a trained expert.
- Improved efficacy of detection rules through trend analysis and optimisation.
- Reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to security threats emerging across the environment.
- Reduced operational overhead related to responding to alerts from many systems.
- Improved Asset Visibility and Threat Detection.
- Accelerated incident response times and assist in conducting thorough investigations.
- Support for containment or preventative actions, such as Asset or User containment.
- Strengthened compliance with ISO and similar frameworks.
- Improved Cybersecurity Reporting (Operational reporting and Trend Analysis) and Continuous Improvement Recommendations.

Services workflow and deliverables

As part of The Missing Link's MDR Service, all alerts generated by the SIEM Technology are categorised and triaged in real time by our on-shift Security Analysts. If an alert meets the threshold for further investigation, it is escalated and assigned a priority level (P1-P4) based on severity and potential impact.

This structured workflow ensures that genuine threats are identified quickly, actioned appropriately, and communicated clearly, minimising risk and maximising response efficiency.

Log and event workflow



In the event of a P1 or P2 severity alert, the team will contact the relevant stakeholders as defined in your Onboarding Checklist.

P3 alerts may be escalated if additional context or information is required to complete analysis.

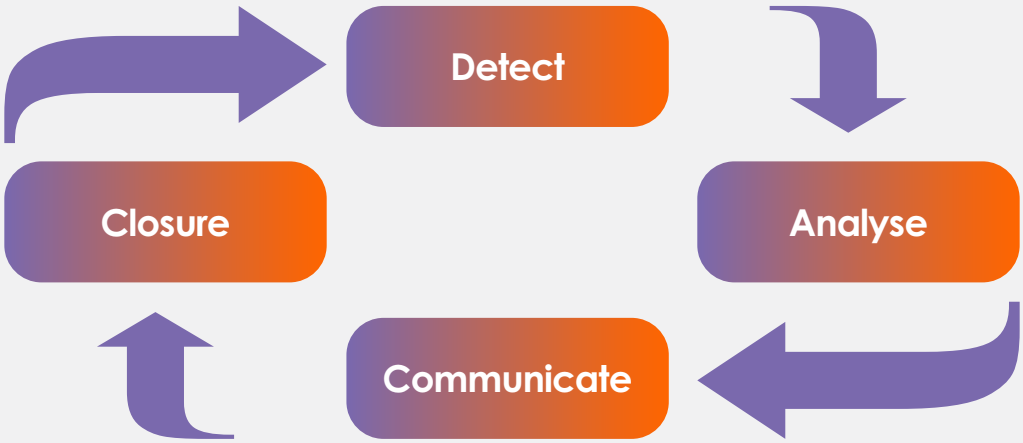
All alerts are reviewed and summarised in your regular reporting cycle (typically monthly), providing a clear view.

1. Detect

Our GSOC team leverages proactive event analysis and rule correlation to detect and investigate potential suspicious activities within your environment. This, combined with our various threat intelligence feeds and proactive threat hunting, allows our team to identify both known and unknown threats before they can cause material impact.

2. Analyse

Once an alert is triggered, our GSOC Analysts investigate and validate it based on multiple factors. These include current threat intelligence, alert type, organisational context, and previous detected activities. By combining adversary threat intelligence with our in-depth knowledge of your environment and IT operations, we can assess the risk and potential impact of each incident. This also enables our team to provide actionable guidance with tailored recommendations to support your team in our joint containment and eradication efforts.



3. Communicate

Every validated alert is assigned a severity if further investigation is required. For critical or high severity (P1, P2) alerts, our analysts will also make direct phone contact with the nominated stakeholders.

When appropriate, we'll issue a Security Alert Report, which is shared through your configured ITSM integration or agreed upon communication channels.

This report summarises the incident with detailed evidence of the threat, recommended containment actions, remediation guidance, and mitigation recommendations.

Distribution lists for these reports are established as part of the Onboarding Checklist and reviewed regularly throughout the engagement.
Our analysts are also always available via email or phone for further discussion.

4. Closure

Following the initial communication, our analysts will confirm receipt of the alert, assist you with any follow-up investigation requests you may have and ensure all necessary context and analysis has been delivered.

Incidents will remain open until we receive confirmation of closure from your security team. Our analysts review all findings to ensure no investigative paths are left unexplored, giving you full assurance the incident has been resolved.

Standard MDR Service

Our standard MDR services are consistent no matter what technology is used. They are delivered through a blend of proven GSOC processes, deep technical expertise, and technology-aligned best practices.

Out of the Box Detections (OOB)

Every SIEM technology has its own OOB detection rules created and maintained by the technology vendor. These are based on industry-recognised data sets and are effective at providing a quick return on investment and visibility into your monitored environment.

However, no two environments are the same. At The Missing Link, our GSOC team has extensive experience in tuning and optimising these detections to suit your environment. We work proactively to reduce false positives, refine rule logic, and maximise accuracy.

Custom Detections

While most SIEM platforms offer a solid foundation of out-of-the-box (OOB) detection rules, there are always gaps. That's why custom detections are a critical part of any effective MDR strategy.

The Missing Link's GSOC team has a proven track record of creating, tuning, and responding to custom detections that reflect the unique behaviours and risks of each client environment. We take the time to understand your IT and security landscape, your critical assets and business processes.

As part of our Continuous Service Improvement (CSI) process, we'll also proactively recommend areas where custom detections can add value, improving visibility and sharpening your overall threat detection capability.

Our GSOC team will continually manage and tune all applicable alerts in your environment to ensure you're always getting the most accurate results.

Threat Scout

The Threat Scout role is a rotating role assigned daily to different analysts. Their mission is to search for threats that could impact your organisation before they reach your environment.

Using a curated collection of industry-recognised threat intelligence feeds, our Threat Scout team reviews emerging vulnerabilities, attack campaigns, and exploit trends.

When an applicable threat is identified, it is verified by a senior or principal analyst for its potential impact on your environment. Where the impact is deemed to be high, an Advisory Notification is sent complete with details of the threat and known remediation or mitigation strategies. Customised threat hunts may be initiated to determine if your environment has already been affected.

Where appropriate, new detection rules will be created in collaboration with your team to detect new attack attempts, and where applicable, threat feeds or access lists will also be updated.

Where historical evidence of the threat has been found, we work with your team to understand the impact and advise on steps to mitigate or reduce the risks.

Threat Hunting

Threat hunting plays a crucial role in monitoring a secure environment. At The Missing Link, we apply three key methods to identify threats:

▶ Anomaly Led

Many security platforms provide well-established "standard" threat hunting searches. These proven searches are designed to detect well-known attack paths, techniques, and behaviours, often focusing on user behaviour anomalies or patterns linked to known threat actors.

▶ Intelligence Led

When new threats emerge, they're accompanied by a published list of Indicators of Compromise (IOCs) and known attack paths. Our analysts use these IOCs to perform intelligence-led threat hunting across your monitored environment, looking for past or current threats. These IOCs are also used to create custom detections, helping ensure continuous monitoring for known threats while threat intelligence feeds are kept up to date.

▶ Hypothesis Led

This method is based on hypothetical or theoretical circumstances and not used as often. While this is not included in our standard MDR service, you can get in touch to explore how we can support hypothesis-led hunts in your environment.

MDR Threat Hunting - Standard

Intelligence-Led	Anomaly-Led	Hypothesis-Led
▶ Critical Vulnerability ▶ Security Advisory Publication ▶ Threat Actor Profiling	▶ Abnormal Authentication Activity ▶ Abnormal Application Activity ▶ Insider Threat Profiling	▶ Threat Actor Research ▶ Absence of Normal, Presence of the Abnormal ▶ Targeted ▶ CTI Managed Service Required
Requirements ▶ Conventional IOCs ▶ Known/Signature TTPs	**Requirements** ▶ Baselining & Behavioural Modelling ▶ Query Library	**Requirements** ▶ Organisational Context ▶ Data Modeling

MDR Threat Hunting - Advanced

Our standard MDR service includes both anomaly and intelligence-led threat hunting methodologies.

Where there is suspicious user behaviour or insider threats, you can request ad-hoc threat hunts, and our GSOC team will investigate and provide feedback on results.

In addition, our GSOC will also hunt for new or novel threats as soon as they're published. Our Threat Scout monitors a curated threat intelligence feed twice daily, identifying relevant updates and feeding them into the GSOC for investigation and threat hunting.

If needed, the Missing Link GSOC will also create new detection rules to monitor activity over a fixed period, typically 2 to 4 weeks, ensuring no threat goes unchecked.

SOAR Playbooks

While not all SIEM technologies include a Security Orchestration & Automated Response (SOAR) capability, where this feature is present, the GSOC team can assist in developing this function.

Our GSOC team will work closely with your team to design and develop a strong SOAR capability, leveraging their deep knowledge of the technology, your specific environment and processes, and proven expertise from real-world incident response.

Some default type SOAR playbooks may include:

- Isolate/ un-Isolate an endpoint
- Disable / Enable a User
- Clear Access Tokens
- Quarantine Files

However, more advanced SOAR functions may include (integration dependent):

- Enrich indicators (e.g. URLs, IP addresses, file hashes) using OSINT tools for deeper analysis.
- Advanced actions like password resets or trigger password reset workflows (where supported by policy).
- Use communication platforms like Slack or Teams to provide feedback and drive decisions within the SOAR playbook.
- Raise tickets or action items in ITSM tools to engage other teams.
- Automatically close well-known and established false positive alerts to reduce alert fatigue when detection tuning is not an option.

Dashboards & Executive Reporting

Dashboards and reporting are essential to understanding how your security environment is performing both in the moment and over time. They provide the visibility needed for planning, improvement, and demonstrating measurable progress.

At The Missing Link, we have a proven track record of delivering clear and actionable reporting across our monitoring services. We deploy a set of "Custom dashboards" within all client environments that provide detailed views, including key telemetry within your environment.

These dashboards form the basis of all reports used by both our customers and the GSOC team. We also work with your team to develop service-related dashboards as part of our standard GSOC service.

Service Level Agreements

Alert Priority

At The Missing Link, our GSOC team collaborates closely with leading industry vendors and threat intelligence organisations to fine-tune detections and ensure they are continually refined for accuracy and relevance. Besides optimising alerts to reduce alarm noise, every alert generated by our systems is assigned an internal priority level based on its potential impact and fidelity.

Alerts flagged as Critical or High, those most likely to indicate malicious activity, are highlighted for expedited triage and investigation. This ensures that real threats are acted on quickly, minimising attacker dwell time and reducing the risk of compromise.

At the same time, this prioritisation model helps our GSOC team avoid wasting resources on benign activity or false positives, keeping the focus on the threats that truly matter.

Alert Validations

Before any alert is escalated, our GSOC team carefully assesses its criticality during the investigation process. The severity can't be determined until we've fully understood its scope and potential impact within your environment.

We define validation as the point at which The Missing Link's GSOC Team has completed initial triage and investigation and can confidently determine that the event is non-benign and requires customer communication.

Response SLAs and Definitions

The agreed Service Level Agreements (SLA) between The Missing Link and our clients are based on the incident definitions outlined below.

Each incident ticket is assessed using a priority rating matrix that considers organisational impact and urgency.

As part of our response commitment, we take the following actions:

- Acknowledgement of the alert
- Initial triage and severity classification
- OSINT enrichment
- Appropriate Response actions
- Client notification as per agreement

Incident Definitions

To classify an incident, our team must first understand two key factors: the required level of urgency and the impact of the event on the organisation. Once understood, the two elements are tied together to determine an incident's priority.

The following outlines the criteria used to define and prioritise incidents:

- Urgency is used to measure how quickly a resolution of the incident is required
- Impact is used to measure the degree of impact on a client's ability to provide services to their customers
- Priority is the output of the urgency and impact rating and determines the response and restoration timeframes
- Major Incident (P1)

	Impact	Critical	High	Medium	Low
Urgency	Critical	P1	P2	P3	P4
	High	P1	P2	P3	P4
	Medium	P2	P2	P3	P4
	Low	P2	P3	P4	P4

Impact Matrix Definitions

Impact is the measurement of the effect that a decision, event, or situation has on a business. The following table shows each impact level, the factors considered, and examples of incidents that align with each level.

Impact	Description
Critical	Confirmed breach, directly impacting key client services, loss of critical site The whole organisation or multiple business groups are affected.
High	High chance of impact on client critical systems, which is time-critical Business group (department) or branch of business systems users are affected.
Medium	Indirect impact on client systems or the environment, which is not time-critical Multiple business systems or users are affected, with other support staff active.
Low	A non-critical business system or user is affected.

Urgency Matrix Definitions

To determine the priority of an incident, each of the urgency and impact components must be understood. Urgency definitions are as follows:

Urgency	Definition
Critical	Urgent and important. Critical systems are impacted.
High	Urgent, but there is time to respond. Primary work functions are impaired.
Medium	Important but not urgent. Inconvenienced but not impacted.
Low	Not urgent and not important.

Service Level Definition

Priority#	SLA	Response	Description
P1	As per the Service Level Agreement	Critical	Confirmed breach, directly impacting critical operations and users. Immediate action required
P2	2 x P1	High	High probability of breach or risk to critical business operations. Urgent action required.
P3	2 x P2	Medium	Default criticality. Can be escalated to P1 or P2. Respond within business hours.
P4	2 x P3	Low	Service or project requests, email communication, unless specified at a higher criticality.
P5	As per the reporting SLA	Informational	Reporting

Under our Co-Managed Service Options, all device uptime remains the responsibility of the client.

Service Reports

The Missing Link provides ongoing reports that offer visibility into GSOC activities, including metrics and context around analyst investigations, technology health summaries and key findings and threat observations.

These reports serve as an at-a-glance overview of GSOC activities.

Your dedicated Service Delivery Manager will walk through each report with your stakeholders during scheduled calls to help reduce risk over time. The frequency of these reviews is defined in your Service Level Agreement. In addition to the scheduled service reporting, we also provide ad-hoc reporting when required.

Threat Intel Report/Security Advisories

When highly critical vulnerabilities are released and/or detected, The Missing Link will issue a Security Advisory.

This advisory is designed to keep you aware of the latest high-risk threats in the wild, provide you with guidance on how to locate them in your environment, and recommend the most effective remediation methods.

Security Research Reports (ad-hoc)

Our security division regularly conducts research across all facets of cyber security, from highly technical security research in Active Directory to comprehensive tooling reviews. While our research is often published publicly, managed service clients receive early access to these insights.

This ensures you're equipped with timely, actionable information ahead of the broader market, giving you a clear advantage when responding to emerging threats or evolving security practices.

Example of a security alert report

Security Alert Reports

Once an alert reaches stage 3 of the analysis workflow, our team issues a Security Alert Report. This report is delivered to the distribution list defined in the onboarding process, which may vary depending on the nature of the alert and the actions already taken, or those that may still be required by you or your service providers.

At a high level, these reports include the following information:

Situation
What is the current situation?

Impact
What is the impact to the client?

Action
What has been done?
What do we recommend being done?

References
Supporting information to aid the technical teams in remediating the Incident

Managed Threat Intelligence Feeds

While many cybersecurity tools promote built-in threat intelligence integrations, their real-world application often results in excessive false positives or misleading severity ratings, especially when they don't consider the customer's geographic region or industry context.

To provide more relevant intelligence, The Missing Link encourages all customers to subscribe to the ACSC CTIS Feed and establish an MISP (An Open-Source Threat Intelligence Feed platform) infrastructure.

The Missing Link integrates trusted threat intelligence feeds directly into our MDR service to enhance detections and response activities. This intelligence is contextualised based on your industry, geography, and risk profile, and we work with clients to incorporate relevant sector-specific and client-provided feeds where appropriate.

Playbook Examples

At The Missing Link, we continuously expand our library of playbooks, each one built on real-world experience and investigations. All playbooks are developed and formatted according to internationally recognised standards, ensuring consistency, clarity and effectiveness across our GSOC operations.

Some of our most-used playbooks cover the following areas:

Malware Outbreak

Phishing
(Please note that forwarding logs from the Email gateway is highly recommended and may require additional licensing to achieve).

Data Theft

Virus Outbreak

Denial of Service

Unauthorised Access

Elevation of Privilege

Improper/ Abnormal System Usage

themissinglink®

An Infosys company

Ready to take the next step in proactive defence? Let's talk.

The Missing Link's Managed Detection & Response (MDR) service is built for one purpose: to give you confidence in your security operations, 24/7, with real experts, real insights, and real outcomes.

Whether you're looking to reduce risk, improve visibility, or strengthen your response capability, our team is here to help you achieve it with clarity, consistency, and a deep understanding of your environment.

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.