

AI Cyber Monitoring as a Service

AI-powered, Human-led.

A Security Operations Centre for your business, delivered by IT Integrity.

By combining human expertise with AI-assisted monitoring, IT Integrity provides an approach that is both scalable and responsive, ensuring that no critical event is missed during periods of high alert volume.



Why Your Organisation Needs a Continuous AI Cyber Monitoring Service

Cyber threats do not sleep. Your protection should not either.

Modern cyber attacks run continuously. They target staff accounts, cloud apps, devices, networks and data, often without any visible warning. Traditional IT support models provide reactive help, but not real-time detection or the specialist analysis required to respond to advanced threats.

IT Integrity's Cyber Monitoring-as-a-Service provides your organisation with a Security Operations Centre that watches your environment 24 hours a day, identifies threats in real time and guides your response.

You gain enterprise-level protection without the cost or complexity of building an internal SOC team.

What is an AI-driven SOC?

An AI-driven SOC (Security Operations Centre) uses machine learning, behavioural analytics and threat intelligence correlation to help identify suspicious activity more quickly and accurately. The technology looks for patterns, anomalies and deviations from normal behaviour across endpoints, cloud systems and networks.

AI does not replace human analysts, but it dramatically improves their efficiency by highlighting the events most likely to indicate a genuine threat.

Example:

Instead of analysing thousands of raw logs, our analysts are presented with prioritised alerts that have already been grouped, correlated and scored by AI for risk. This makes investigation faster, more consistent and less prone to human oversight.

AI + human analysis = faster detection, fewer false positives and better protection for your organisation.

Extended Capabilities

Protect your organisation with an AI-driven Security Operations Centre, delivered as an ongoing, fully managed service for an easy flat monthly fee.

Our Cyber Monitoring-as-a-Service combines three essential capabilities:

- 1 Advanced monitoring platform**
Collects security events from endpoints, servers, Microsoft 365, cloud applications, and networks. Utilises behavioural analytics and multiple threat intelligence feeds to validate alerts and remove false positives.
- 2 IT Integrity security analysts**
Our Australian-based specialists handle incident response, assess risk and provide practical remediation guidance.
- 3 Continuous monitoring and improvement**
Your environment is monitored 24 hours a day, supported by structured reporting, incident escalation and maturity uplift recommendations.



**EVERYTHING A TRADITIONAL
SECURITY OPERATIONS CENTRE
PROVIDES, DELIVERED AS A
PREDICTABLE MONTHLY SERVICE.**

Coverage: What the Service Monitors

Comprehensive visibility across your digital environment

01



Endpoint Protection Monitoring

- Ransomware and malware detection
- Unusual process or behaviour monitoring
- Suspicious activity and privilege escalation attempts

02



Cloud and Microsoft 365 Security Monitoring

- Compromised account indicators
- Unusual login patterns
- Mailbox rule manipulation and privilege misuse

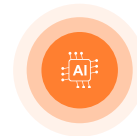
03



Network and Perimeter Monitoring

- Firewall events
- DNS anomalies
- Unusual outbound connections

04



AI-driven Intelligent Threat Correlation

- Multi-source threat intelligence
- Machine learning and behavioural analytics to highlight suspicious patterns, reduce false positives.
- Detection of exploits, vulnerabilities and zero-day activity

05



Incident Containment & Response Support

- Real-time escalation to IT Integrity
- Actionable containment instructions
- Optional hands-on remediation

06



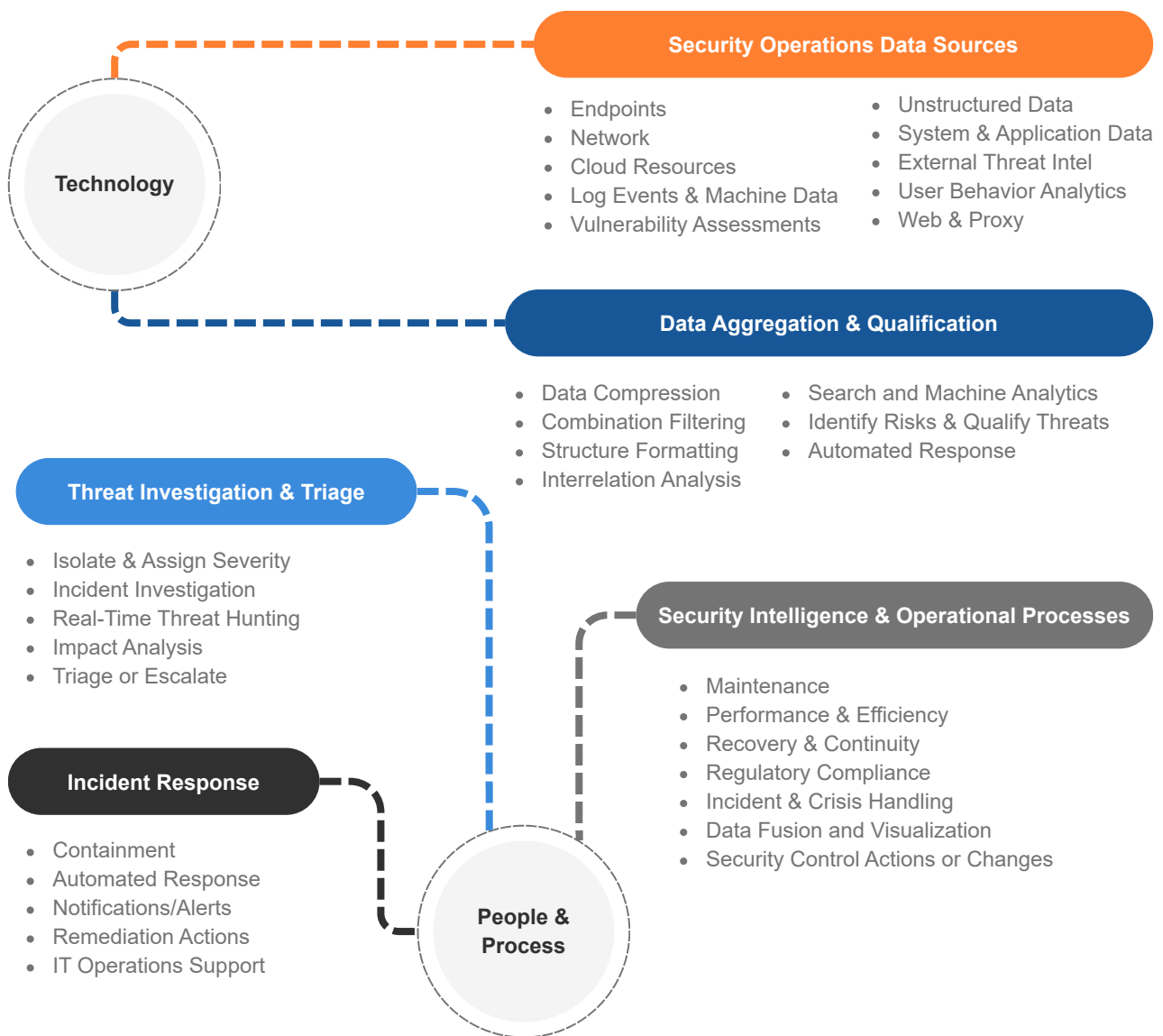
Governance and Reporting

- Monthly SOC reports
- Executive summaries
- Evidence aligned to ISO 27001, GDPR, NIST and Essential Eight
- Audit-ready insights

Advanced Security Defence with our 24/7 Managed Security Operations Centre (SOC)

Yesterday's security is no match for the evolving threats and attack methods used by today's cybercriminals. You need to build a comprehensive security defence using proactive strategies and advanced security controls to dramatically improve your security posture, enabling you to confidently protect your business-critical systems and data.

Our fully managed SOC-as-a-service solution leverages the power of people, processes and technology to quickly detect and remediate threats or breach events, thereby ensuring a more preventative approach to cybersecurity. Our SOC-as-a-Service Framework is below:



- ✓ 24/7 X 365 Monitoring and Response
- ✓ Continuous Vulnerability Checks

- ✓ Operational Performance Analytics
- ✓ Event Tracking Records for Compliance

The Value of Cyber Monitoring-as-a-Service

24/7 Protection

Continuous monitoring ensures threats are detected as soon as they occur.



Trusted Technology

Our monitoring platform provides enterprise-grade detection capabilities across your environment.



Plus Human-led Analysis

IT Integrity security analysts ensure alerts are understood, validated and actioned correctly.



Cost Efficient

Removes the need for internal SOC analysts or security operations staff.



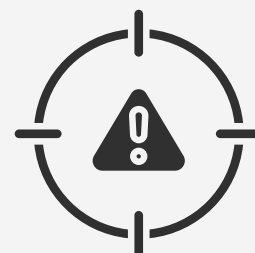
Part of a Wider Partnership with IT Integrity

Findings integrate directly into your Client Partner engagement and managed services.



AI-supported detection

Behaviour analysis and machine learning to identify unusual activity more efficiently, improving signal-to-noise ratios for our human analysts.



Supports Compliance

Helps meet regulatory and audit obligations across multiple frameworks.



How it Works

Simple to deploy, powerful in practice

01



Deployment and Configuration

- Lightweight agents installed on endpoints
- Integration with Microsoft 365, servers and firewall logs

02



Real-Time Monitoring

- Event ingestion in real time
- Behavioural analysis and AI/machine learning
- Threat intelligence correlation

03



Alert Triage and Validation

- IT Integrity analysts assess severity
- Noise and false positives removed
- Clear, practical advice provided

04



Incident Isolation & Response

- Escalation of confirmed incidents
- Containment and remediation advice
- Optional hands-on support, under your managed services or ad hoc service agreements

05



Reporting and Improvement

- Monthly reporting
- Executive dashboards
- Recommendations to strengthen resilience

Who is this Service For?

Ideal for organisations that:

- ✔ Need 24/7 threat visibility
- ✔ Do not have internal cybersecurity analysts
- ✔ Must meet compliance or audit standards
- ✔ Operate with remote or hybrid workforces
- ✔ Rely heavily on cloud applications
- ✔ Want confidence and visibility in their cyber posture

Investment Model

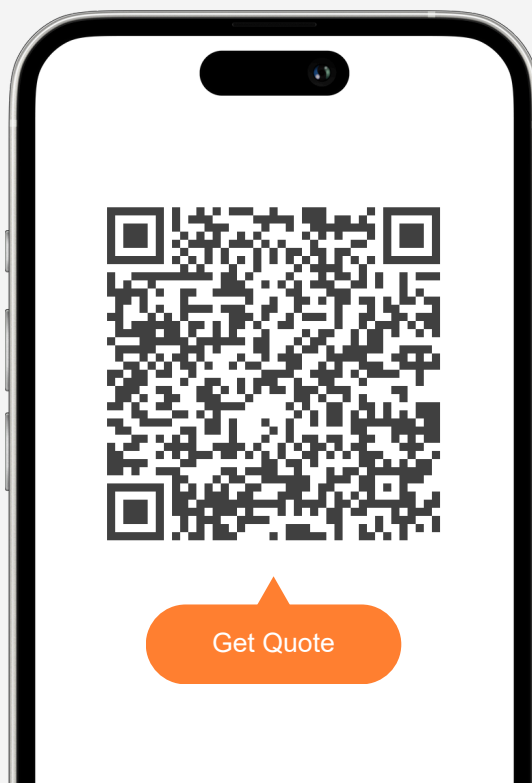
Cyber Monitoring-as-a-Service is delivered through a fixed monthly subscription, priced per monitored user, device or environment.

Cost is determined by:

- Quantity of endpoints
- Required integrations
- Optional incident response or on-site support

Initial set up fee applies.

**TO GET A QUOTATION,
BOOK A CALL OR EMAIL
INFO@ITINTEGRITY.COM.AU**








About IT Integrity

IT Integrity is an Australian ICT integration and cybersecurity provider with more than 20 years of experience supporting organisations across Australia.

We combine advanced monitoring technology with real human expertise to provide continuous protection and peace of mind.

Solution Portfolio

 Technology Strategy & Advisory	 M&A Enablement	 Modern Workplace & Collaboration	 Managed Services & Operations
 Cybersecurity & Risk Management	 Infrastructure & Physical Solutions	 Data, Reporting & Insights	 Project & Program Management

Who We Support

Protect your business while you sleep.

IT Integrity

Trusted ICT Integration & Security Partner



Let's Chat