Data Sheet

# MCL Cyber
# SOC as a Service

## Use Cases

- **Compromised Hosts**
  Detecting and responding to systems that have been infiltrated or taken over by malicious actors.
- **Malware Detection**
  Recognising and mitigating harmful software before it spreads across the network.
- **Unauthorised Access**
  Identifying and blocking access breaches by unauthorised users.
- **Policy Violation**
  Monitoring and enforcing security policies to prevent misuse or non-compliance.
- **Insider Threats**
  Risks from internal personnel compromising data, intentionally or unintentionally.
- **Data Exfiltration**
  Unauthorised transfer of sensitive data outside the organisation.
- **Lateral Movement**
  Preventing attackers from spreading across the network after an initial breach.

## Enhance Your Security with MCL's SOC

MCL Cyber delivers next-generation Security Operations Centre (SOC) services, purpose-built to provide continuous threat monitoring, proactive intelligence, and rapid incident response across modern IT environments. Whether your infrastructure is on-premises, cloud-based, or hybrid, our SOC integrates advanced technologies, expert-led processes, and automation to deliver effective and efficient cyber defence.

Our SOC is staffed by a highly skilled team of analysts with extensive experience in managing and responding to complex cybersecurity threats. They bring a deep understanding of threat landscapes, incident response, and security monitoring, ensuring that our clients benefit from timely detection, thorough analysis, and effective mitigation of potential risks.With deep operational knowledge and years of frontline experience, our team is equipped to handle complex threats, conduct advanced investigations, and deliver actionable insights.

Our services are aligned with a robust compliance roadmap, supporting regulatory and security frameworks including ISO27001, SOC 2, GDPR, Cyber Essentials plus and more. We work with businesses across a range of sectors to enhance their cyber resilience and ensure their security posture meets both operational needs and regulatory expectations.

# Offering

The following core offerings included in our Security Operation Centre, are designed to deliver comprehensive protection against cyber threats.

| | |
|---|---|
| **1 24/7 or 8-8 Monitoring:**<br>Continuous surveillance of your IT infrastructure to identify and respond to security incidents in real-time. | **2 Vulnerability Management**<br>Regular scanning, assessment, and remediation of security weaknesses. |
| **3 Email Quarantine Checks**<br>Review and analysis of flagged emails to detect phishing, malware, and other email-based threats. | **4 Attack Surface Reduction**<br>Expert consultation and advisory to address existing exposure points, supported by targeted recommendations to reduce and harden your attack surface. |
| **5 Open-Source Intelligence (OSINT) & Reputation Analysis**<br>Monitoring deep and dark web sources to identify risks, detect credential leaks, and address reputational threats based on tailored intelligence needs. | **6 Threat Intelligence**<br>Integration of real-time threat intelligence to stay ahead of emerging threats and adversarial tactics. |

## Service Models

### 1. Bring Your Own Infrastructure (BYOI)

Our SOC analysts collaborate with your existing security infrastructure, enhancing your current capabilities without the need for additional investments.

- **Benefits:**

- Seamless integration with your existing tools and processes.
- Enhanced security posture through expert analysis and monitoring.
- Cost-effective utilisation of current assets.

**Technological Capabilities**

**Supported SIEM Platforms:**

- Microsoft Sentinel
- Splunk
- LogRhythm
- ArcSight
- And more..

**Supported EDR/XDR Solutions:**

- Microsoft Defender XDR
- SentinelOne
- CrowdStrike
- And more..

## 2. Turnkey SOC Solution

A comprehensive, fully managed SOC service where MCL Cyber provides the necessary infrastructure, tools, and expertise to monitor and protect your organisation.

- **Benefits:**

  - Scalable solutions tailored to your organisation's growth and evolving threats.
  - Access to the latest security technologies without capital expenditure.
  - End-to-end security management by experienced professionals.

## SOC Delivery Process

**Step 1: Security Assessment & Planning**

- Evaluate existing security posture and identify vulnerabilities.
- Define security objectives and risk tolerance.

**Step 2: Technology & Infrastructure Deployment**

- Integrate with existing security tools or deploy MCL Cyber's SIEM/XDR solutions.
- Configure security monitoring systems and incident response protocols.

**Step 3: Threat Intelligence & Baseline Setup**

- Establish baseline activity patterns for normal user and network behaviour.
- Implement real-time threat intelligence feeds for proactive defence.

**Step 4: Continuous Monitoring & Incident Response**

- 24/7 monitoring of security events with automated alert prioritisation.
- Rapid containment and mitigation of detected threats.

**Step 5: Reporting & Improvement**

- Provide detailed incident reports and security recommendations.
- Conduct regular assessments to refine security strategies.
- Deliver weekly security reports for ongoing visibility
- Provide a comprehensive monthly report and conduct a monthly review meeting