Managed Security Services

Cyber Defence Services

Enhance your cyber resilience against cybersecurity threats through our comprehensive suite of Managed Security Services (MSS) and Security Operations Centre (SOC) services. AI enabled and delivered from state-of-the-art cyber fusion centre's, these services are tailored for organisations lacking the necessary capacity, expertise, and experience to manage these aspects internally.

Managed Services

Our MSS encompasses day-to-day security administration and operational tasks related to your organization's security solutions. We offer complete outsourcing to our MSS team or supplemental support via Security Support Services (SSS) for organizations with their own security teams. Key domains covered include:

Endpoint, Server and Mobile Device Protection

Securely manage, monitor, and report on security controls for workstations, servers (virtual and physical), and mobile devices. Services include Advanced Endpoint Security, Endpoint Detection and Response (EDR), Mobile Device Management (MDM), and more.

Network Protection

Manage and monitor network security controls (e.g., firewalls, intrusion prevention) associated with network perimeters and infrastructures. Offerings include Unified Threat Management (UTM) Security, Secure Email Gateway (SEG), Secure Access Service Edge (SASE), Distributed Denial of Services (DDOS) and more.

Identity Protection

Manage user and access associated with user identities and authorised access to information resources. Services include Identity and Access Management (IAM), Privilege Access Management (PAM), Multi-factor Authentication (MFA), and more.

Data Protection

Manage data security for data at rest, in transit, and in use. Offerings include Data Leakage Prevention (DLP), Information Protection, Disk Encryption on endpoints, and related services.

Cloud Protection

Manage security for those using cloud services. Services include Cloud Access Security Broker (CASB), Secure Service Edge (SSE), Cloud Infrastructure Security Assurance, and more.

Application Protection

Manage security associated with applications. Services include Web Application Firewall (WAF), Secure Email, and related solutions.

Infrastructure Protection

Manage security associated with the overall infrastructure. Services include Vulnerability Management, Configuration Management, Wireless Security, and more.

Managed Security Services

Cyber Defence Services

Security Operation Centre Services

Our 24 x 7 x 365 SOC services include managing technology platforms such as Security Incident and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Managed Detection and Response (MDR), and Managed Extended Detection and Response (MXDR) delivered as a service or on-prem. This enables real-time event monitoring, threat hunting, incident management, and automated incident response supported by AI. Service options include:

SOCMonAlert

Incident alerts are directed to relevant customer teams for mitigation, with the Liquid C2 SOC teams providing guidance and incident response assistance.

Managed Detection and Response (MDR)

For organizations with Endpoint Detection and Response (EDR), we provide Managed Detection and Response (MDR) as a service, to mitigate server and endpoint attacks as incidents occur. Liquid C2 SOC teams are actively involved in remedial actions and automation in accordance with industry leading Service Level Agreements (SLAs).

Managed Extended Detection and Response (MXDR)

Ingest, monitor and analyze events from various security controls (endpoint & server, network, identity, data, cloud, infrastructure, and applications) to mitigate against attacks within the overall landscape. Liquid C2 SOC teams are actively involved in providing threat intelligence, remedial actions and automation to enable proactive defences.

Managed SOC

Design, build and operate a turnkey 24/7 Managed Security Operations Center (SOC) customized to meet your specific business needs, delivered remotely or on-premise. Our experts work with you to understand your requirements, developing a managed or co-managed SOC solution model that reflect today's dynamic threat environment and operating constraints – including threat monitoring, incident management and response as well as threat intelligence and human-led threat hunting.

Threat Intelligence Services

Augment threat intelligence with external attack surface monitoring, providing comprehensive insights into threat actor activities relevant to your organization. This includes brand intelligence, attack surface intelligence, identity intelligence, third-party intelligence, and more, gathered from various sources such as social media, dark web, and payment platforms.

Incident Response Services

Respond swiftly to security incidents or breaches with our expert incident response team. We conduct analysis, identify root causes, mitigate threats, contain impacts, eradicate sources, and provide guidance to prevent future incidents.