Continuous Managed Threat Response (cMTR)

“Continuous Managed Threat Response for GxP Manufacturing Security”

INTRODUCTION

Manufacturing environments are under increasing pressure from cyber threats: ransomware, supply chain attacks, insider threats, and legacy OT vulnerabilities. The risk is not just to IT, but to product integrity, compliance, uptime, and regulatory standing. Traditional cybersecurity models reactive, tool-centric, fragmented, often fail to deliver the continuous protection and audit-readiness required for GxP & pharma environments.

Continuous Managed Threat Response (cMTR) by xLM, in partnership with Sophos, provides a fully managed, always-on cybersecurity-as-a-service tailored for GxP manufacturing. cMTR integrates detection, response, threat hunting, compliance enforcement, and credentialed access control across IT, OT, cloud, endpoints, and networks. Built to ensure both resilience against threats and alignment with regulatory standards such as FDA Data Integrity and others.

With cMTR, you get:

- **Continuous threat vigilance**
- **Expert incident response**
- **Broader coverage including OT/supply chain/legacy systems**
- **Built-in compliance and audit readiness**

VISION FOR cMTR

Continuous Managed Threat Response (cMTR) by xLM delivers a new standard in cybersecurity for regulated manufacturing. It doesn't just protect; it proactively defends, adapts, ensures compliance, and preserves business continuity in environments where risk has real consequences.

We believe that in regulated manufacturing, cybersecurity must evolve from being a checklist item to a continuous, integrated capability. Key elements of our vision:

- Proactive defense, not just reactive patching detection before damage occurs.
- Continuous visibility across all attack surfaces user, network, endpoint, cloud, OT/legacy systems.
- Compliance built in, not bolted on auditing, data integrity, regulatory alignment being part of every response cycle.

OUR PROCESS

Asset & System Discovery

Automated discovery of all IT/OT/cloud assets; constant inventory updates.

Analytics, Dashboards & Risk Scoring

Dashboards with real-time threat visibility, user risk scoring, compliance status; proactive alerts.

Continuous Monitoring & Detection

24/7/365 monitoring across endpoints, network, cloud; detection using XDR, Sophos tools for anomalous behaviour.

Thread Hunting & Response

Managed Detection and Response (MDR) by experts; threat hunting; rapid incident response; automatic containment.

Access, Segmentation & Zero Trust Control

Zero Trust Network Access (ZTNA); device health / policy enforcement; network segmentation; securing remote and third-party access.

Continuous Compliance & Managed Service

Continuous validation; managed security service with Sophos expertise; evidence and audit trails built-in; supply chain risk, legacy protection, multi-cloud coverage.

INTELLIGENT FEATURES

- **24/7 Managed Detection & Response (MDR)**
  Round-the-clock expert monitoring and response to threats that evade basic defenses.
- **Extended Detection and Response (XDR)**
  Integrates data from endpoints, networks, applications, cloud to deliver unified threat detection and forensic capability.
- **Zero Trust Access & Network Segmentation**
  Enforce strict policy-based access, validate identity & device health, limit lateral movement.
- **Cloud, OT/Legacy & Supply Chain Coverage**
  Protects cloud workloads, legacy systems, and external partners/suppliers; ensures coverage even for difficult-to-patch environments.

VALUE MATRIX

Aspect	Traditional Threat Response	cMTR by xLM	Impact
Time to Detect Threat	Days to weeks; threat often already in play before detection	Near real-time detection with XDR & managed MDR	Reduced dwell time; less damage
Response Speed & Containment	Delayed responses, manual escalation, limited containment	Expert response, automated and policy-driven containment	Lower impact of incidents; faster recovery
Coverage of Asset Risks	Blind spots especially for OT/legacy, remote, supply chain devices	Broader coverage across IT, OT, cloud, third parties	Reduced exposure; more resilient infrastructure
Compliance / Audit Effort	Reactive auditing; manual gathering of evidence; risk of findings	Continuous logging, secure evidence, alignment with GxP & data integrity	Lower audit prep time; fewer non-compliance issues
Insider & User Risk Management	Hard to monitor; often manual review; behavior may go unnoticed	Proactive risk scoring, user behavior analytics, policy enforcement	Reduced insider risks; better policy compliance

ABOUT US

xLM is a trusted managed application provider enabling FDA-regulated organizations to modernize compliance, quality, and IT operations.

With decades of domain expertise and a technology-first mindset, xLM helps companies scale digital transformation without compromising on validation, traceability, or audit-readiness.

Our Other Applications

- Continuous Intelligent Validation (cIV)
- Continuous Predictive Maintenance (cPdM)
- Continuous Environmental Monitoring System (cEMS)
- Continuous Temperature Mapping (cTM)

Our stack incorporates intelligent and responsible AI into all our managed services. From Predictive Analytics to Software Validation, our apps are pre-built with best practices so that they can be deployed within days or hours.

Intelligent Application Provider
All our apps are delivered as managed apps. We do the heavy lifting so that you can focus on building your business

Intelligent and Responsible AI
Through our partnership with IBM, all our AI centric apps are delivered with cLCG (Continuous Life Cycle Governance)

White Glove Service
Our team does more than 95% of the heavy lifting. All we need from you are approvals

Extensive App Portfolio
xLM leverages its robust partner ecosystem to deliver over 15 managed apps and it is growing

Delivered Validated
All our managed apps are delivered “validated”

21 CFR Part 11/Annex 11/FDA CSA Compliant
Ensures all our managed services are compliant out of the box

High Data Integrity Assurance
Our services guarantee accurate, reliable and resilient data across all our managed apps

Get Started