DELTA LINE INTERNATIONAL

MDR SERVICE BRIEF

Managed Detection & Response

Fully managed, expert-led 24×7 cybersecurity operations — the analysts, processes and integrated tooling to defend your organization, without the cost and complexity of building an in-house SOC.

Vendor-agnostic MDR | **SIEM + SOAR managed** | **24×7 SOC** | **In-house DFIR**

WHY MDR — THE OPERATING GAP

24×7
Always-on monitoring & response from globally distributed SOC teams.

Minutes.
From detection to notification and containment — not hours of dwell time.

72h
Enhanced monitoring stays active after every incident closure.

THE CHALLENGE

Organizations today struggle not with *accessing* security technology, but with operating it effectively around the clock. Modern EDR/XDR platforms generate significant alert noise. **DLI runs the SOC — detection, triage and response — so your internal teams stay focused on business priorities.**

WHAT'S INCLUDED IN OUR MDR

Security Platform Management
Complete management of your SIEM & SOAR, enhanced with behavioral analytics and AI-driven detection. We fill the missing pieces of your stack.

24×7 Monitoring & Response
Distributed SOC teams cover your environment around the clock. Critical incidents are investigated immediately and your contact is notified within minutes.

Pre-Authorized Response
Customer-approved actions let analysts isolate hosts, block malicious activity and contain threats instantly — cutting dwell time to minutes.

Proactive Threat Hunting
With visibility across tens of thousands of endpoints and servers, we continuously hunt emerging attacker techniques and feed intelligence back in.

Guidance & Hardening
Beyond response, our experts deliver actionable recommendations to strengthen posture, reduce attack surface and prevent repeat incidents.

Root Cause Analysis
Every significant incident is broken down: initial attack vector, scope and impact, containment and recovery — with 72h of enhanced post-closure watch.

Executive Reporting
Full transparency into every action taken by our SOC.

- Real-time dashboards
- Incident summaries
- Monthly executive reports
- Trend analysis & remediation

KEY BENEFITS

Intelligence, not alert fatigue
We manage the full alert lifecycle — filtering thousands of alerts down to validated incidents with clear actions to take.

SLA-based fast response
Our SOC rapidly investigates and executes pre-approved containment to limit damage and stop attacker lateral movement.

Flexible delivery
Onsite, remote or hybrid — tailored to each customer's environment, compliance needs and budget.

Unified security stack
A consolidated, managed end-to-end service that reduces complexity and ensures consistent protection across all workloads.

WHY DELTA LINE INTERNATIONAL

1. **Vendor-agnostic MDR**
2. **Compliance covered**
3. **Certified SOC analysts & engineers**
4. **AI & Threat intelligence driven detection**
5. **Rapid, adaptive onboarding**
6. **Advanced automation & playbooks**
7. **In-house DFIR & recovery**

Cyber attackers never stop. Neither do we.

SERVICE TIERS AT A GLANCE

Service Component	Silver	Gold	Platinum FULL DFIR
Onboarding & Deployment	✓	✓	✓
Security Platform Management (SIEM + SOAR)	✓	✓	✓
24×7 SOC Monitoring	✓	✓	✓
Pre-Authorized Response Actions	✓	✓	✓
Expert Recommendations & Hardening	✓	✓	✓
Root Cause Analysis	✓	✓	✓
Executive Reporting	✓	✓	✓
Ticketing System Provision / Integration	–	✓	✓
Proactive Threat Hunting	–	✓	✓
Dedicated Security Account Manager	–	✓	✓
Threat Intelligence	–	✓	✓
Dark Web Monitoring	–	✓	✓
Digital Forensics & Incident Response	–	–	✓
Full eradication & recovery across all systems	–	–	✓

Gold includes all Silver capabilities; Platinum includes all Gold capabilities. Scope tailored per engagement.

ADDITIONAL SERVICES (ADD-ONS)

- **SOCaaS**
- **Cloud Security Posture Assessment** — Azure, AWS, GCP
- **Red / Purple Team** exercises
- **Compromise Assessment**
- **Social Engineering** testing
- **VAPT** — vulnerability assessment & penetration testing
- **Secure Network** architecture review
- **SIEM review** / SOC maturity assessment
- **DLP** assessment, implementation & DLPaaS
- **Privacy & Compliance** assessment
- **Risk Assessment**
- **Business Impact Analysis** (BIA)
- **Disaster Recovery** assessment
- **Business Continuity** management review
- **ISO 27001 / 20000 / 27035, SOC 2, GDPR** — assessment & implementation
- **NCA, SAMA, PDPL, NESA, PCI-DSS, Aramco CCC** & similar compliance
- **HIPA & PCI-DSS Consultancy**

See what your current SOC is missing.

Let's scope an MDR engagement tailored to your environment, compliance needs, and budget.

CONNECT AT
support@deltaline-it.com

24×7 SOC / INCIDENT DESK
soc@dlisupport.com