

MANAGED DETECTION AND RESPONSE

24/7 endpoint monitoring, human-led triage and active containment.

Cyberattacks don't keep business hours, and EDR alerts alone don't stop threats. Our managed detection and response puts certified analysts behind the endpoint tools you already run, 24/7, so a person reviews every alert before any automation acts on it.

BEYOND ALERTS. REAL RESPONSE.



Signal: 24/7 endpoint monitoring

Telemetry from your EDR across process activity, network connections and file access, watched around the clock on workstations and servers.

Triage: analyst-led detection

Behavioral analytics, rule sets and live threat intelligence surface the threats that matter. A certified analyst reviews every alert first.

Action: active containment

Endpoint isolation, process termination and session revocation, applied as soon as an analyst confirms the threat, with Tier 2/3 escalation.

Report: monthly reporting

Executive summaries, root cause findings and a monthly KPI report covering MTTD, MTTR, incident volume and threat types.

WHY DIGITALERA

Works with your EDR

Integrates with CrowdStrike, SentinelOne, Microsoft Defender and more.

Human-reviewed alerts

A certified analyst reviews every alert before any automation acts.

Sevii detection engine

Built for high-fidelity signal in complex, high-volume environments.

Mapped to NIST CSF

Reporting aligns to the framework, so progress is demonstrable.

WHAT YOU CAN EXPECT

- 24/7 coverage without adding internal headcount
- Faster detection and less dwell time across endpoints
- Verified alerts with the context to act on them
- Guided remediation tied to your environment
- Reporting for auditors, insurers and your board

DELIVERED MONTHLY

- ✓ Strategic remediation guidance
- ✓ Incident reports and case logs
- ✓ Monthly MTTD & MTTR reporting
- ✓ Executive and technical formats

Getting started

Read access to your EDR console and a point of contact during 2 weeks of tuning. No new hardware, no agents to deploy.

Right fit if you run EDR but nobody watches it 24/7, or you need documented MTTD and MTTR for a board or insurer.

Something else first if you have no endpoint protection yet (start with Endpoint Protection) or you're mid-incident (call the emergency line).



Talk to an expert

digitaleragroup.com/contact/managed-detection-response

Active incident? Certified responders answer 24/7, no retainer required.

CALL US: 1-786-621-8600