

## MANAGED DETECTION &amp; RESPONSE

# AI-Accelerated. Human-Validated. MDR you can trust.

CRITICALSTART® is the only Managed Detection and Response provider with contractual per-alert commitments, a deterministic-first architecture, and human validation behind every security decision.

See how Critical Start is raising the bar for MDR.

Every MDR vendor will tell you how fast their AI responds. **Ask them what happens when it's wrong.**

4

THINGS TO ASK  
EVERY VENDOR**01** ACCOUNTABILITY · NOT JUST SPEED

**Speed is the table stake.  
Accountability is the difference.**

The market races to show how fast AI can respond. Your real question is: what happens when it's wrong? At Critical Start, every threat alert, low, medium, or high severity, is validated by a qualified SOC analyst.

**96%** of CISOs now own **AI governance & risk management**. The board question is already in the room.

SOURCE: GARTNER CISO SURVEY, 2025

**02** HUMAN GOVERNANCE · AUDIT-READY BY DESIGN

**"Fully-autonomous" is a risk word.  
Not an aspiration word.**

Every one of our AI recommendations carries a full audit trail: what the agent proposed, what the analyst decided, and why.

Gartner estimates **60% of AI incidents by 2026 will stem from governance failure**. Our answer isn't a policy document, it's the architecture itself.

**03** DATA ISOLATION · BOUNDED BY ARCHITECTURE

**Your data stays in your environment.  
Full stop.**

Most AI security platforms treat cross-customer data sharing as a network effect. For regulated industries, that's a data governance risk. Our architecture keeps telemetry inside your environment. Agents operate on your signal, within your Rules of Engagement and never share investigation outputs across customers.

**78%** of CISOs name **data leakage** as their #1 concern with AI in security operations.

SOURCE: GARTNER PEER INSIGHTS, 2025

**04** CONTRACTUAL OUTCOMES · NOT BENCHMARKS

**We put our SLA in writing.  
Ask if your other vendors will.**

Every AI vendor has a benchmark: response in five minutes, triage in seconds, investigation cut by 68%, measured in vendor-controlled environments, against vendor-selected workloads, with no contractual commitment behind them.

Critical Start offers **per-alert SLAs**, audit-ready obligations on how every signal is handled. The question isn't whose AI is fastest in a demo. **It's who will put it in writing.**

Ready to see SOC AI in action?

REQUEST A DEMO →

# From your first signal to a resolved verdict in one flow.

AI accelerates every step. Your analysts and ours validate the moments that matter. The result is a contractual, audit-ready outcome.

## Five agents : one governance model

Every agent **proposes**. A qualified human **approves**. Each one has a tightly scoped charter: what it can do, what it cannot, and what it must hand off.

- 01 TBR Agent**  
Examines false positives in production and proposes new entries to the Trusted Behavior Registry – the deterministic rules engine that has filtered ~99% of events for more than a decade.
- 02 Investigation Agent**  
Accelerates triage by pre-populating investigative workflows, running OSINT enrichment, and suggesting verdicts on alerts for analyst review.
- 03 Case Agent**  
Detects, links, and proposes closure of related alerts during triage so analysts work a single coherent case instead of duplicates.
- 04 Response Agent**  
Suggests existing automations from the catalog to run on true-positive verdicts and proposes new workflows for human review before publication.
- 05 Threat Hunting Agent**  
Runs hypothesis-first proactive hunts against all ingested events to surface threats before they become alerts and suggests new detections for the catalog.

## 02 Detect · Investigate · Respond · Improve

# From your first signal to a resolved verdict - in one flow.

AI ACCELERATED · HUMAN VALIDATED

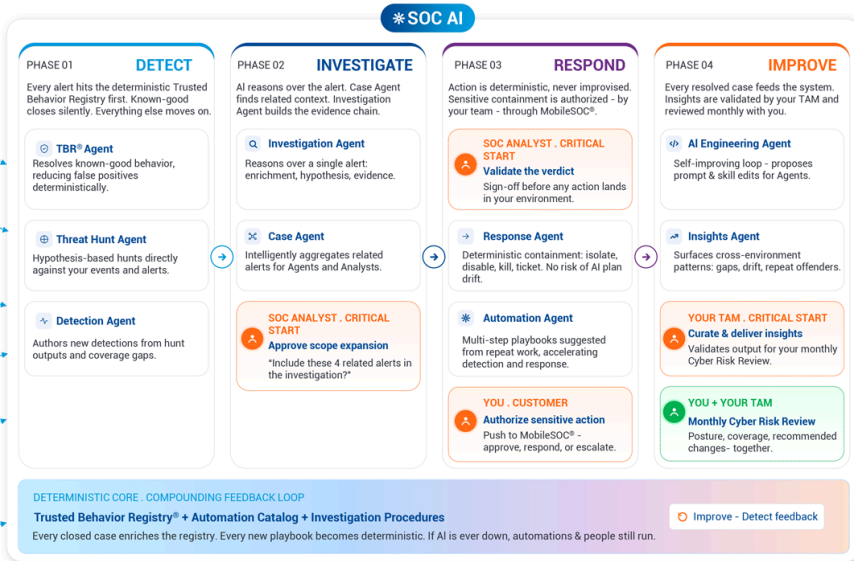
- 1 Your tools send signal**  
Direct integrations stream alerts & telemetry - no broker, no proxy.
- 2 AI triages & investigates**  
TBR®, Investigation & Case agents applied to every alert.
- 3 Humans validate the moments that matter**  
Analysts & you authorize scope, verdicts & containment.
- 4 The platform improves itself**  
Every closed case enriches TBR, detections & automations.
- 5 You get measurable outcomes**  
True-positive close, sub-minute MTTR, zero alert fatigue.

### Direct Integrations

Native connectors stream signal directly into the platform. You keep your stack - we handle the rest

- EDR & ENDPOINT**
  - CrowdStrike
  - SentinelOne
  - Microsoft MDE
  - Cortex XDR
- SIEM & DATA LAKE**
  - Splunk
  - Falcon NG-SIEM
  - Sentinel
  - Sumo Logic
- IDENTITY & EMAIL**
  - Entra ID
  - Microsoft MDO/MDI
  - Proofpoint
  - Abnormal
- NETWORK & CLOUD**
  - Palo Alto
  - Fortinet
  - GuardDuty
  - Microsoft MDC
- ITSM & OTHER**
  - ServiceNow
  - Jira
  - Email
  - XSDAR

DAILY INFLOW  
**2.3M+** events / customer  
All ingested. All addressable. Sub-second



### Your Outcomes

What changes for you, your CISO, and your board - measured, contractual, and visible end-to-end.

- 99.83%**  
TBR Agent False Positive Resolution  
Every signal handled. No silent drops, no triage backlog.
- <60<sup>s</sup>**  
Mean time to respond  
Sub-minute deterministic containment, with human authorization for sensitive actions.
- 0+**  
Alert fatigue on your team  
You see escalations only - every other alert closes with full evidence.
- 24/7**  
MobileSOC® decisioning  
Authorize, escalate, respond from anywhere - full audit trail.
- ∞**  
Compounding coverage  
Every closed case enriches TBR, automations & detections.
- 100%**  
Resilient operations  
If AI is unavailable, deterministic automations + analysts continue without disruption.

■ Detect ■ Investigate ■ Respond ■ Improve ⚠ Human checkpoint (analyst, customer, or TAM)