



*Scale Your SOC Ops.
Without Adding Headcount.*

SOC Ops are hard.

Scaling them is even harder.



Staffing



Infrastructure



**Process
Automation**



**Threat
Handling**



Morpheus Lets You Scale SOC Ops...

*Without adding headcount. Without switching tools.
With ROI on Day One.*



100%

Alert Coverage –
never miss an incident



800+

AI-Ready Integrations
– *works with any
stack*



95%

Alerts Triageed in Under
2 Mins. – *Fully automate
L1 & L2 work*



315x

Faster Investigations –
*Outperforms Tier 3/4
Analysts*





Security analyst

Alert Verification & Ticket Logging	10 min
Timestamp Correlation Across Platforms	10 min
Email Content and Header Analysis	10 min
Extraction of Malicious URL from Email	5 min
Firewall Log for Outbound Connections	15 min
Network Traffic Analysis	15 min
Authentication and AAD Sign-In Review	15 min
User Behavior Baseline Comparison	10 min
Threat Intelligence Lookup for URL/IP	10 min
Domain and WHOIS Information Lookup	5 min
URL Redirection and Destination Verification	5 min
Endpoint Detection (EDR/Sysmon) Log Analysis	20 min
Geolocation and ASN Verification	10 min
User Account Activity Review	10 min
Cross-Platform Log Correlation and Timeline	15 min
Stakeholder Notification and Escalation	10 min
Containment Actions Execution	15 min
Root Cause Analysis, Final Reporting	20 min



Morpheus AI

Alert Verification & Ticket Logging	5 s
Timestamp Correlation Across Platforms	5 s
Email Content and Header Analysis	5 s
Extraction of Malicious URL from Email	5 s
Firewall Log for Outbound Connections	5 s
Network Traffic Analysis	5 s
Authentication and AAD Sign-In Review	5 s
User Behavior Baseline Comparison	5 s
Threat Intelligence Lookup for URL/IP	5 s
Domain and WHOIS Information Lookup	5 s
URL Redirection and Destination Verification	5 s
Endpoint Detection (EDR/Sysmon) Log Analysis	5 s
Geolocation and ASN Verification	5 s
User Account Activity Review	5 s
Cross-Platform Log Correlation and Timeline	5 s
Stakeholder Notification and Escalation	5 s
Containment Actions Execution	15 s
Root Cause Analysis, Final Reporting	15 s



Security analyst



3.5 hr.

Per incident



In an entire shift...

**This analyst could handle 3
similar alert investigations**



Morpheus AI



< 2 min.

Per incident



With Morpheus...

- **100% alert coverage**
- **Expert investigations**
- **24-7-365**



MORPHEUS AI SOC

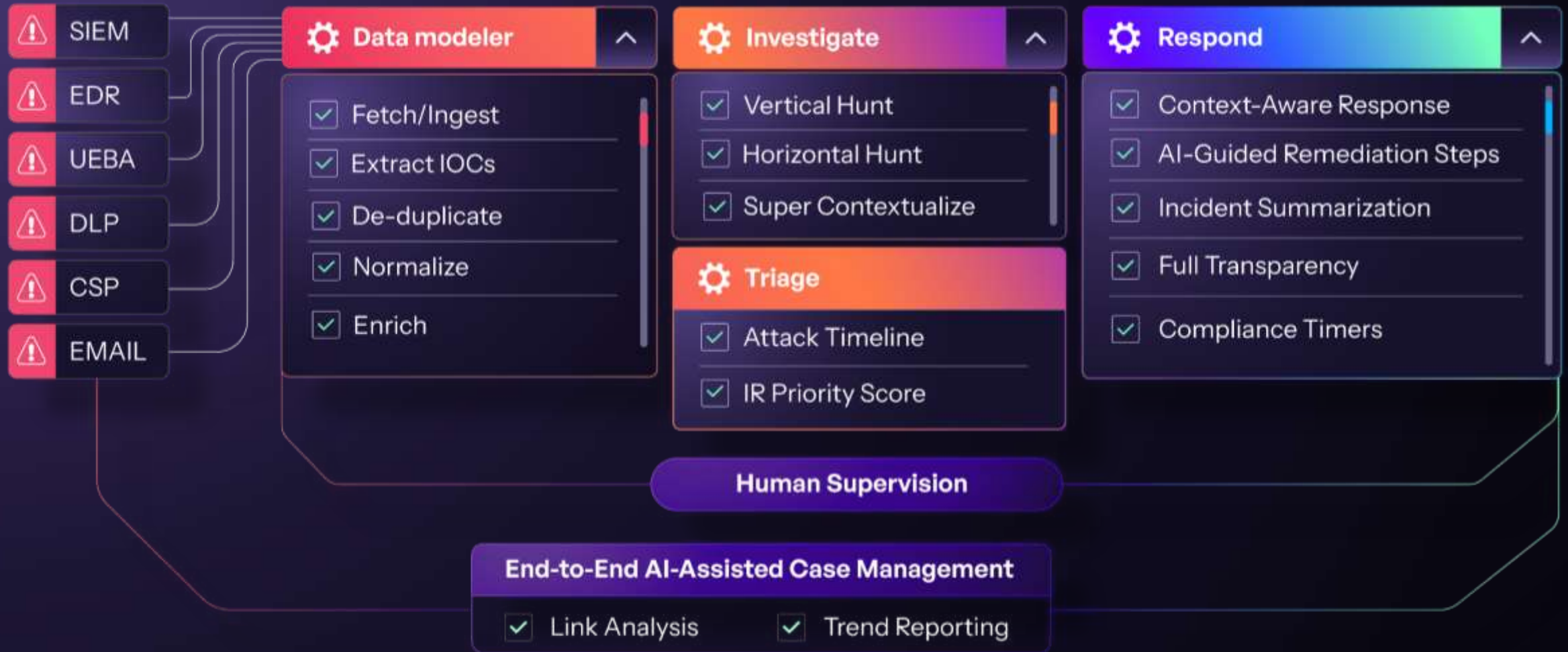




Image: *Horizontal & Vertical Proactive Threat Hunting*



Autonomic systems

are self-managing and can adapt to changing conditions, but they still operate within predefined boundaries and rules.

Autonomic systems focus on maintaining a stable and secure state by adjusting their behavior based on internal and external feedback.

Autonomic Security Operations combines philosophies, practices, and tools to improve an organization's ability to withstand security attacks through an adaptive, agile, and highly automated approach to threat management.

Autonomous systems

are self-governing and can make independent decisions without human intervention.

Autonomous systems have a greater degree of freedom and can learn and evolve based on their experiences.

Autonomous Security Operations would imply a higher level of self-governance, where security systems could independently identify, analyze, and neutralize threats without human input.



Privacy & Security

D3's fine-tuned models are for D3's use alone and never served to or shared with other LLM provider's customers or used to train other models

Zero data retention, request and response bodies are not persisted to any logging mechanism and exist only in memory in order to serve the request.

- ✓ Private
- ✓ Stateless
- ✓ No Logging
- ✓ No Training
- ✓ D3-hosted
- ✓ Tenant Scoped
- ✓ No Storage
- ✓ No Internet

