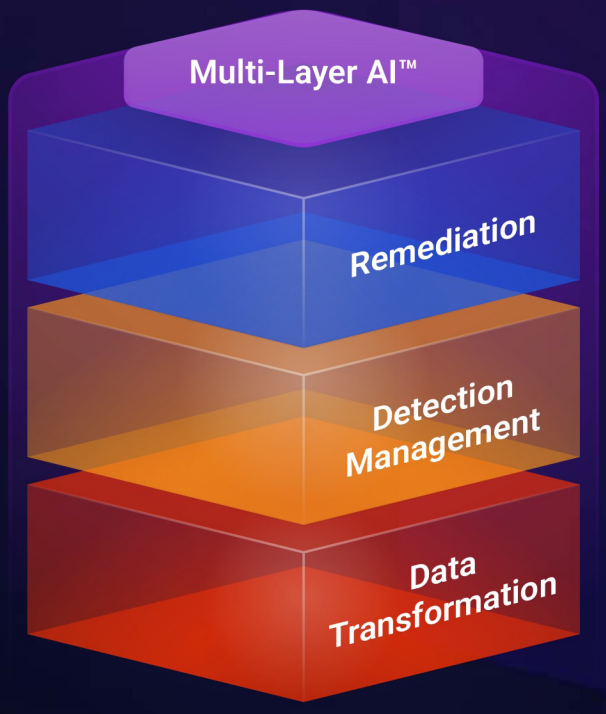
STELLAR CYBER®

DATA SHEET

Multi-Layer AI™
From Signals to Autonomous Security Outcomes

Stop chasing alerts. Start containing attacks.

Security teams today are overwhelmed. Too many tools. Too many alerts. Too little time to respond before attackers move deeper into the environment. The traditional SOC model, fragmented detection tools, manual correlation, and slow investigation, cannot keep page with modern threats.



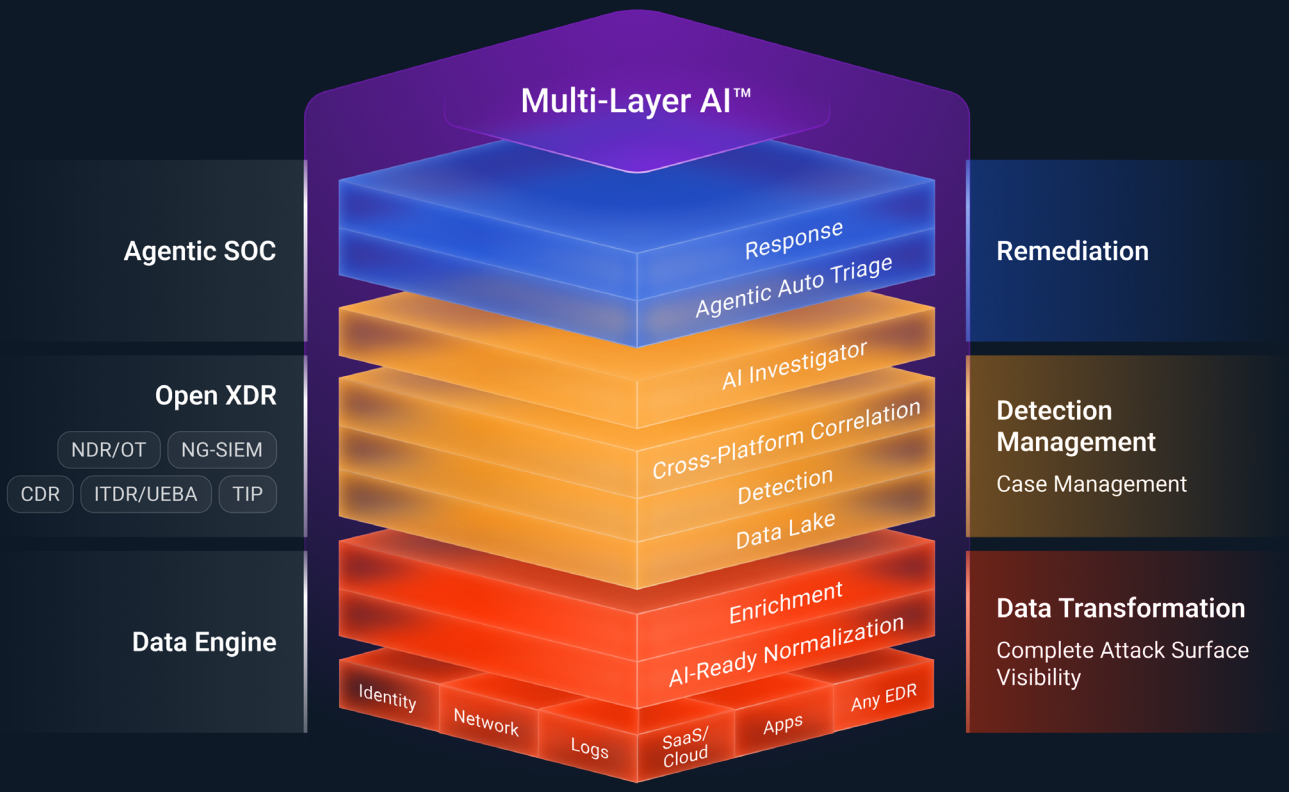
Stellar Cyber Multi-Layer AI™ changes the equation.

By embedding artificial intelligence across the entire security operations lifecycle, from telemetry ingestion to automated remediation, Multi-Layer AI™ transforms raw data into **prioritized decisions and automated response actions**. Instead of managing alerts, your SOC manages outcomes.

The architecture applies supervised and unsupervised machine learning, deep learning, graph ML< generative AI, and Agentic AI across every layer of the security stack. The result is a security platform that detects threats earlier, correlates signals across tools, investigates incidents automatically, and executes remediation workflows at machine speed.

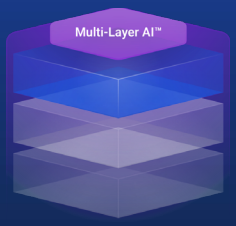
The Architecture: Intelligence at Every Layer

Multi-Layer AI operates across three integrated layers that convert telemetry into automated security outcomes.



Layer	Mission	Core Capabilities	AI Enablement
Autonomous SOC	Decision and Response	AI investigation, automated triage of alerts and phishing email, automated remediation.	• Agentic AI • GenAI LLM • MCP
Open XDR Platform	Detection and Correlation	NG-SIEM, NDR, UEBA, CDR using any EDR Threat Intel enrichment Detections & Case Correlation.	• Machine Learning • Graph ML
AI-Native Data Engine	Data Pipeline	Telemetry ingestion, normalization, enrichment.	• Machine Learning

Together these layers move security teams from **data collection to autonomous security operations.**



AUTONOMOUS SOC

Security That Responds at Machine Speed

At the top of the architecture sits the Autonomous SOC, where AI transforms security intelligence into immediate action.

WHAT THE PLATFORM DOES AUTOMATICALLY

Instead of forcing analysts to manually investigate thousands of alerts, the platform automatically:

- Prioritizes alerts and suppresses false positives
- Reconstructs attack timelines across telemetry sources
- Builds contextual investigation cases linking users, devices, and attack paths
- Hunts for behavioral anomalies across the environment
- Performs continuous feedback with analysts to get better accuracy of Alert Verdicts.

This dramatically reduces analyst workload while accelerating response.

THE OPERATIONAL IMPACT IS CLEAR

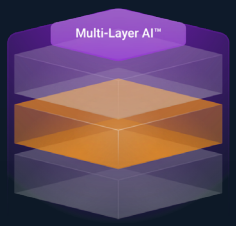
MTTD
Faster detection through AI-driven correlation

MTTR
Faster response via automated remediation

Productivity
Higher analyst productivity through automated investigations

Dwell time
Reduced attacker dwell time

> **In short, security operations teams move from reactive monitoring to proactive cyber defense.**



OPEN XDR

Full-Cycle Detection and Correlation

At the core of the platform is an Open XDR architecture that unifies detection across the entire attack surface while integrating existing security tools—including any EDR.

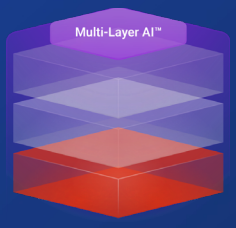
The platform correlates signals across identity, endpoint, network, and cloud environments using technologies such as:

Technology	What it detects
NDR + OT monitoring	Lateral movement and command-and-control traffic
NG-SIEM analytics	Insider threats and malware activity
ITDR + UEBA	Credential abuse and privilege escalation, via behavioral analysis
Cloud Detection & Response (CDR)	Cloud and SaaS attack detection
Threat Intelligence Platform (TIP)	Enriches detections with global threat context

GRAPH MACHINE LEARNING

Thousands of alerts become a handful of high-confidence incidents.

Using Graph Machine Learning, the system links alerts across these data sources to reconstruct full attack chains and automatically generate investigation cases.



AI-NATIVE DATA ENGINE

Complete Attack Surface Visibility

Everything begins with the AI-Native Data Engine, the telemetry pipeline powering the platform. The engine ingests security telemetry across the entire attack surface, network, endpoint, cloud, identity, email, and OT environments, then normalizes and enriches it into an AI-ready schema.

CAPABILITIES INCLUDE

Ingest
High-scale data ingestion across security infrastructure

Normalize
AI-ready normalization of heterogeneous logs

Enrich
Context enrichment with identity, asset, and threat intelligence

Stream
Real-time telemetry streaming for AI analysis

Store
Centralized security data lake for correlation

This unified data layer gives detection engines complete context across the organization's attack surface.

HOW IT WORKS

Multi-Layer AI in Action

When an attack occurs, the platform orchestrates detection and response across the stack.

> **Fewer alerts, faster investigations, and dramatically faster response.**

- Data Engine automatically ingests and normalizes telemetry
- Open XDR detects anomalies and correlates attack signals in real time to core cases that should be investigated
- Graph ML reconstructs attack paths across all your tools and telemetry
- Autonomous Agentic AI triages alerts automatically
- Automated playbooks contain and remediate the threat

THE RESULT

Security Operations That Deliver Outcomes

Organizations deploying Stellar Cyber Multi-Layer AI achieve:

ALERT NOISE	INVESTIGATIONS	THREAT CONTAINMENT	OPERATING COSTS	VISIBILITY
Dramatically reduced	Faster	Automated	Lower	Across the attack surface

> **Replace reactive alert handling with autonomous, outcome-driven security operations.**

Stellar Cyber is a full-cycle AI-native SecOps platform purpose-built for enterprise security teams and MSSPs. Since 2015, Stellar Cyber delivers the whole threat picture, empowering organizations to see every threat, know what matters most, and act with speed and confidence, always with the human in the loop.
By applying the right AI to the right problem, Stellar Cyber combines machine learning to uncover hidden anomalies, GraphML to connect relationships across entities and activity, LLMs to accelerate investigation and understanding, and agentic AI to guide triage and response — with human-augmented decision-making where expertise is essential. Stellar Cyber's results are empirically proven: analyst productivity improved by more than 80%, false positives reduced by over 90%, and security teams free to focus on what matters.

Learn more at stellarcyber.ai.

STELLAR CYBER®

www.stellarcyber.ai | sales@stellarcyber.ai