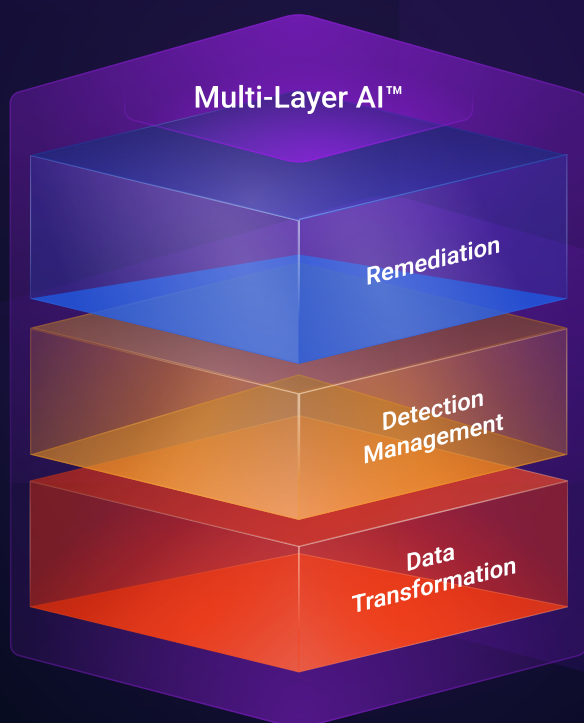


Multi-Layer AI™ From Signals to Autonomous Security Outcomes

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 pace with modern threats.



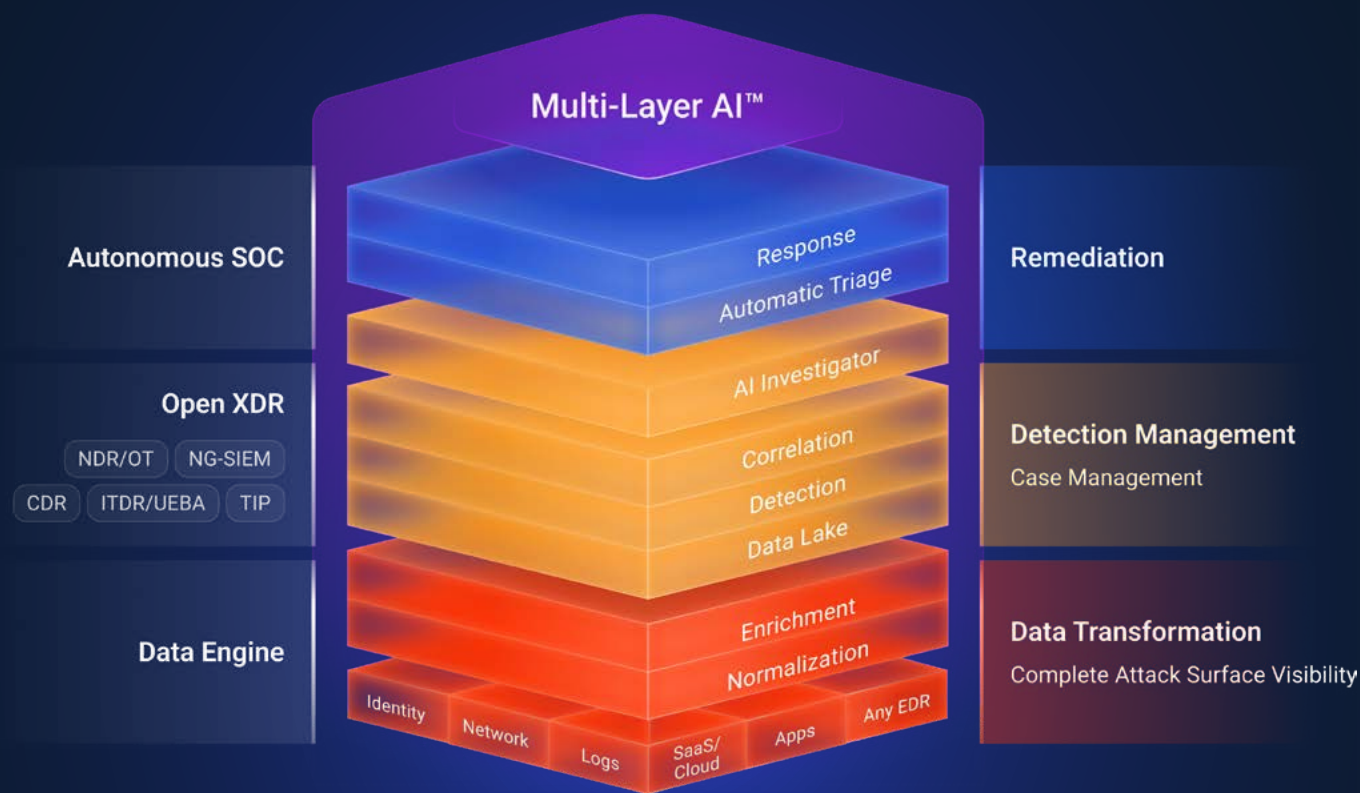
Stellar Cyber Multi-Layer AI changes the equation.

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.

This 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.

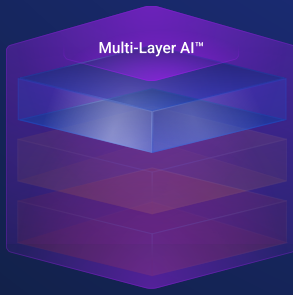
The Architecture: Intelligence at Every Layer

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.

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

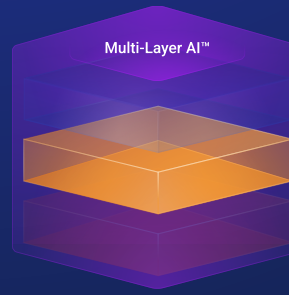
- Prioritizes alerts and suppresses false positives
- Reconstructs attack timelines across telemetry sources
- Builds contextual investigation cases linking users, devices, and attack paths
- Hunts for behavioral anomalies across the environment
- Performs continuous feedback with analysts to get better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

This dramatically reduces analyst workload while accelerating response.

The operational impact is clear:

- **Faster detection (MTTD)** through AI-driven correlation
- **Faster response (MTTR)** via automated remediation
- **Higher analyst productivity** through automated investigations
- **Reduced attacker dwell time**

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



Open XDR: Full-Cycle Detection and Correlation

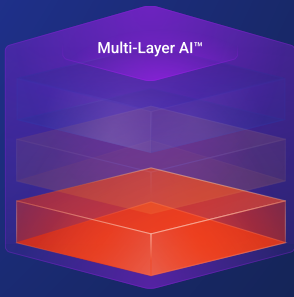
At the core of the platform is an Open XDR architecture that unifies detection across the entire attack surface while integrating existing security tools—including any EDR.

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

- NDR and OT monitoring to detect lateral movement and command-and-control traffic
- NG-SIEM analytics to uncover insider threats and malware activity
- ITDR and UEBA behavioral analysis to identify credential abuse and privilege escalation
- Cloud Detection and Response (CDR) for cloud and SaaS attack detection
- Threat Intelligence Platform (TIP) to enrich detections with global threat context

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

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



The 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:

- High-scale data ingestion across security infrastructure
- AI-ready normalization of heterogeneous logs
- Context enrichment with identity, asset, and threat intelligence
- Real-time telemetry streaming for AI analysis
- Centralized security data lake for correlation

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

Multi-Layer AI in Action

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

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

The outcome is simple: fewer alerts, faster investigations, and dramatically faster response.

The Result: Security Operations That Deliver Outcomes

Organizations deploying Stellar Cyber Multi-Layer AI achieve:

- Dramatically reduced alert noise
- Faster incident investigations
- Automated threat containment
- Lower security operating costs
- Unified visibility across the entire attack surface

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

By shining a bright light on the darkest corners of security operations, Stellar Cyber empowers organizations to see incoming attacks, know how to fight them, and act decisively – protecting what matters most. Stellar Cyber's award-winning open security operations platform includes NG SIEM, NDR, Open XDR, and Multi-Layer AI™ under one single platform. With almost 1/3 of the top 250 MSSPs and over 14,000 customers worldwide, Stellar Cyber is one of the most trusted leaders in security operations. Learn more at <https://stellarcyber.ai/>