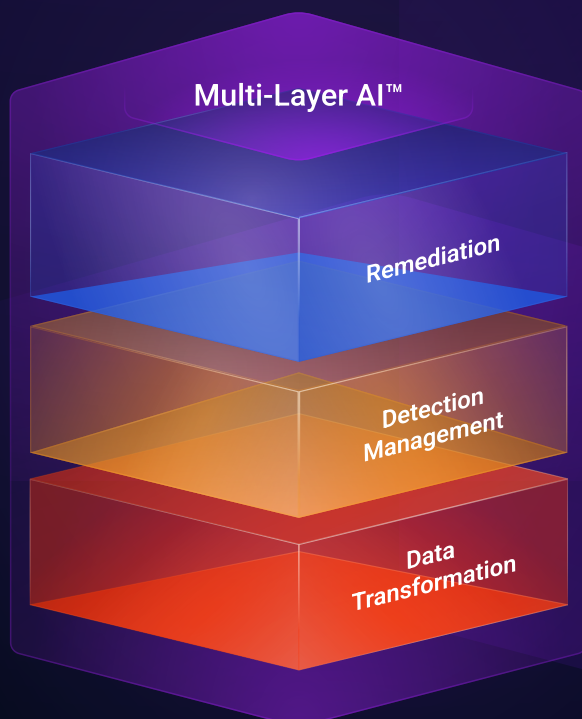


Multi-Layer AI™

Von Signalen zu autonomen Sicherheitsergebnissen

Schluss mit der Alert-Jagd. Angriffe gezielt eindämmen.

Security-Teams sind heute überlastet. Zu viele Tools. Zu viele Alerts. Zu wenig Zeit, um zu reagieren, bevor Angreifer tiefer in die Umgebung vordringen. Das traditionelle SOC-Modell mit fragmentierten Erkennungstools, manueller Korrelation und langsamer Untersuchung kann mit modernen Bedrohungen nicht Schritt halten.



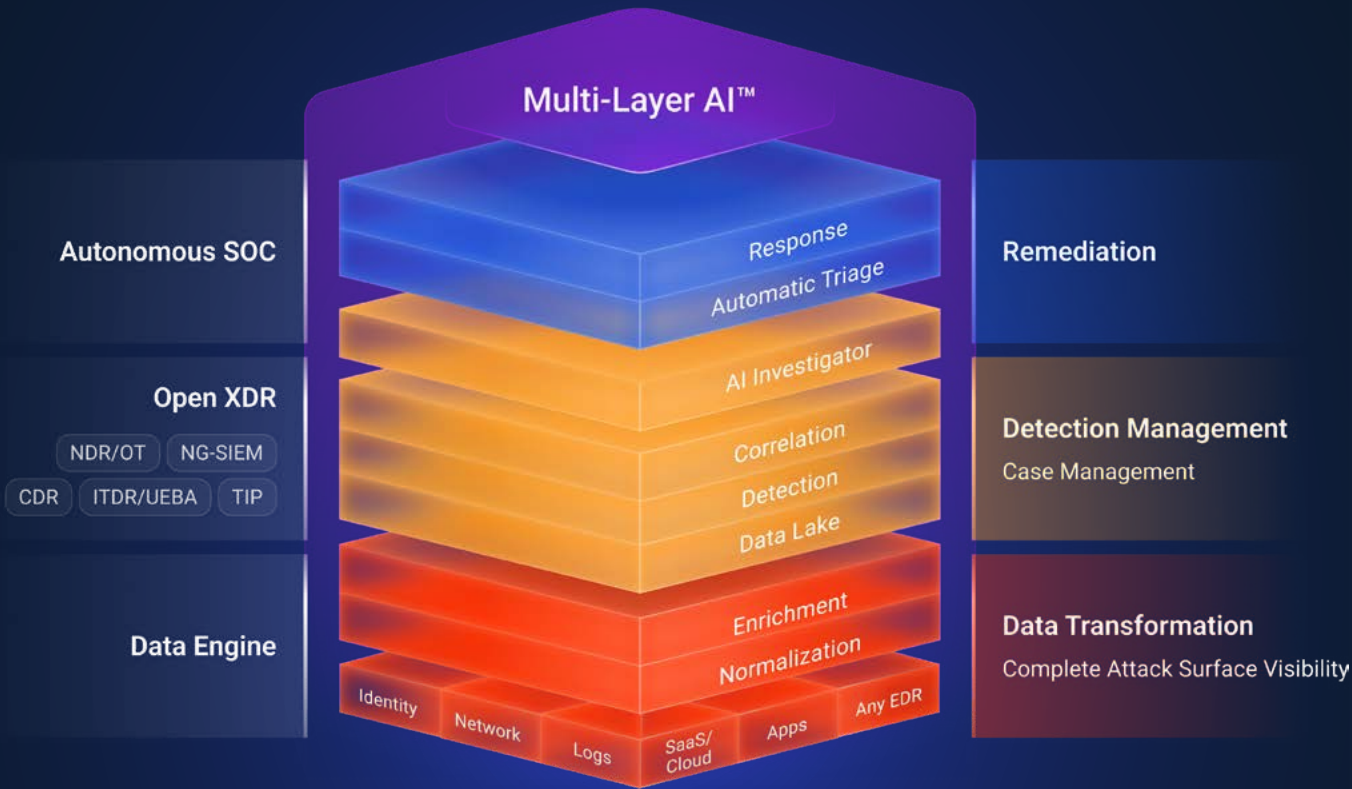
Stellar Cyber Multi-Layer AI verändert die Spielregeln.

Durch den Einsatz künstlicher Intelligenz über den gesamten Security-Operations-Lebenszyklus – von der Erfassung der Telemetrie bis zur automatisierten Behebung – verwandelt Multi-Layer AI™ Rohdaten in **priorisierte Entscheidungen und automatisierte Reaktionsmaßnahmen**. Statt Alerts zu verwalten, steuert Ihr SOC Ergebnisse.

Diese Architektur nutzt überwachtes und unüberwachtes **Machine Learning, Deep Learning, Graph ML, generative KI und Agentic AI auf jeder Ebene des Security-Stacks**. Das Ergebnis ist eine Sicherheitsplattform, die Bedrohungen früher erkennt, Signale toolübergreifend korreliert, Vorfälle automatisch untersucht und Behebungs-Workflows in Maschinengeschwindigkeit ausführt.

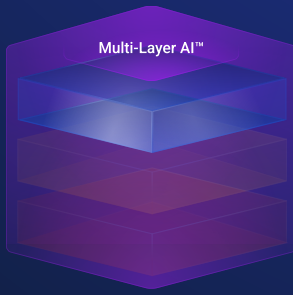
Die Architektur: Intelligenz auf jeder Ebene

Multi-Layer AI arbeitet über drei integrierte Ebenen, die Telemetrie in automatisierte Sicherheitsergebnisse umwandeln.



Ebene	Aufgabe	Kernfunktionen	KI-Unterstützung
Autonomous SOC	Entscheidung und Reaktion	KI-gestützte Untersuchung, automatisierte Triage von Alerts und Phishing-E-Mails, automatisierte Behebung	• Agentic AI • GenAI LLM • MCP
Open XDR-Plattform	Erkennung und Korrelation	NG-SIEM, NDR, UEBA, CDR mit jedem beliebigen EDR Anreicherung mit Threat Intelligence Erkennungen & Fallkorrelation	• Machine Learning • Graph ML
KI-native Data Engine	Datenpipeline	Erfassung, Normalisierung und Anreicherung von Telemetrie	• Machine Learning

Gemeinsam führen diese Ebenen Security-Teams von der **Datenerfassung zu autonomen Security Operations**.



Autonomous SOC: Sicherheit, die in Maschinen- geschwindigkeit reagiert

An der Spitze der Architektur steht das **Autonomous SOC**, in dem KI Sicherheitsinformationen in sofortiges Handeln umsetzt.

Statt Analysten zu zwingen, Tausende von Alerts manuell zu untersuchen, übernimmt die Plattform automatisch:

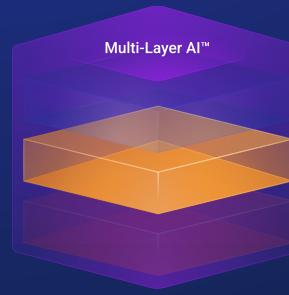
- Priorisierung von Alerts und Unterdrückung von False Positives
- Rekonstruktion von Angriffszeitlinien über alle Telemetriequellen
- Aufbau kontextbezogener Untersuchungsfälle, die Benutzer, Geräte und Angriffspfade verknüpfen
- Suche nach Verhaltensanomalien in der gesamten Umgebung
- Kontinuierliches Feedback mit Analysten für immer genauere Alert-Urteile

Das reduziert die Arbeitslast der Analysten drastisch und beschleunigt die Reaktion.

Die operativen Auswirkungen sind eindeutig:

- **Schnellere Erkennung (MTTD)** durch KI-gestützte Korrelation
- **Schnellere Reaktion (MTTR)** durch automatisierte Behebung
- **Höhere Analysten-Produktivität** durch automatisierte Untersuchungen
- **Kürzere Verweildauer von Angreifern**

Kurz gesagt: Security-Operations-Teams wechseln vom reaktiven Monitoring zur **proaktiven Cyberabwehr**.



Open XDR: Durchgängige Erkennung und Korrelation

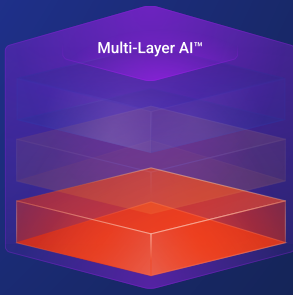
Im Kern der Plattform steht eine Open XDR-Architektur, die die Erkennung über die gesamte Angriffsfläche vereint und vorhandene Sicherheitstools – einschließlich jedes beliebigen EDR – integriert.

Die Plattform korreliert Signale aus Identitäts-, Endpoint-, Netzwerk- und Cloud-Umgebungen mithilfe von Technologien wie:

- NDR- und OT-Monitoring zur Erkennung von Lateral Movement und Command-and-Control-Verkehr
- NG-SIEM-Analysen zur Aufdeckung von Insider-Bedrohungen und Malware-Aktivitäten
- ITDR- und UEBA-Verhaltensanalysen zur Erkennung von Missbrauch von Anmeldedaten und Rechteausweitung
- Cloud Detection and Response (CDR) zur Erkennung von Angriffen auf Cloud und SaaS
- Threat Intelligence Platform (TIP) zur Anreicherung von Erkennungen mit globalem Bedrohungskontext

Mit Graph Machine Learning verknüpft das System Alerts über diese Datenquellen hinweg, rekonstruiert vollständige Angriffsketten und erstellt automatisch Untersuchungsfälle.

Aus Tausenden von Alerts wird eine Handvoll hochzuverlässiger Vorfälle.



Die Data Engine: Vollständige Transparenz über die Angriffsfläche

Alles beginnt mit der KI-nativen Data Engine, der Telemetrie-Pipeline, die die Plattform antreibt.

Die Engine erfasst Sicherheitstelemetrie über die gesamte Angriffsfläche – Netzwerk-, Endpoint-, Cloud-, Identitäts-, E-Mail- und OT-Umgebungen – und normalisiert und reichert sie zu einem KI-fähigen Schema an.

Zu den Funktionen gehören:

- Hochskalierbare Datenerfassung über die gesamte Sicherheitsinfrastruktur
- KI-fähige Normalisierung heterogener Logs
- Kontextanreicherung mit Identitäts-, Asset- und Threat-Intelligence-Daten
- Echtzeit-Streaming von Telemetrie für die KI-Analyse
- Zentraler Security Data Lake für die Korrelation

Diese einheitliche Datenebene gibt den Erkennungs-Engines den vollständigen Kontext über die gesamte Angriffsfläche des Unternehmens.

Multi-Layer AI in Aktion

Bei einem Angriff orchestriert die Plattform Erkennung und Reaktion über den gesamten Stack:

1. Die Data Engine erfasst und normalisiert Telemetrie automatisch
2. Open XDR erkennt Anomalien und korreliert Angriffssignale in Echtzeit zu den wichtigsten Fällen, die untersucht werden sollten
3. Graph ML rekonstruiert Angriffspfade über alle Ihre Tools und Telemetriedaten
4. Autonome Agentic AI triagt Alerts automatisch
5. Automatisierte Playbooks dämpfen die Bedrohung ein und beheben sie

Das Ergebnis ist einfach: weniger Alerts, schnellere Untersuchungen und eine drastisch schnellere Reaktion.

Das Ergebnis: Security Operations, die Ergebnisse liefern

Unternehmen, die Stellar Cyber Multi-Layer AI einsetzen, erreichen:

- Drastisch reduziertes Alert-Rauschen
- Schnellere Untersuchung von Vorfällen
- Automatisierte Eindämmung von Bedrohungen
- Geringere Kosten für den Sicherheitsbetrieb
- Einheitliche Transparenz über die gesamte Angriffsfläche

Ersetzen Sie reaktive Alert-Bearbeitung durch autonome, ergebnisorientierte Security Operations.

Stellar Cyber bringt Licht in die dunkelsten Ecken der Security Operations und versetzt Unternehmen in die Lage, eingehende Angriffe zu erkennen, zu wissen, wie sie abzuwehren sind, und entschlossen zu handeln – um zu schützen, was am wichtigsten ist. Die preisgekrönte offene Security-Operations-Plattform von Stellar Cyber vereint NG-SIEM, NDR, Open XDR und Multi-Layer AI™ in einer einzigen Plattform. Mit fast einem Drittel der Top-250-MSSPs und über 14.000 Kunden weltweit gehört Stellar Cyber zu den vertrauenswürdigsten Anbietern im Bereich Security Operations. Mehr erfahren unter <https://stellarcyber.ai/>