

Stellar Cyber: The Open and Unifying SecOps Platform

Delivering what SIEMs never did, but always promised

Stellar Cyber delivers the platform security teams have been waiting for. Unlike legacy SIEMs that only collected logs and buried analysts in noise, Stellar Cyber combines SIEM with built-in NDR+, ITDR, TIP, UEBA, and **Multi-Layer AI**. The result: a SecOps platform that unifies detection, investigation, triage, and response from day one.

Because it's open and unifying, Stellar Cyber works with everything you already run — including **any EDR** — maximizing investments while cutting complexity.

Security Applications



Security Analyst Workbench

All analyst activities in one UI. Dive into cases, hunt threats, or trigger responses without switching tools.



XDR with Any EDR

Unify telemetry from any EDR with NDR+, ITDR, TIP, and SIEM to build complete cases across endpoints, networks, cloud, and OT.



ITDR + UEBA

Detect insider threats, account compromise, and identity abuse by baselining normal behavior and highlighting anomalies.



NDR+

Unify IT and OT visibility with sensors analyzing packets, flows, firewall logs, and cloud traffic. Detect lateral movement and hidden threats SIEMs miss.



File Integrity Monitoring (FIM)

Track unauthorized changes across Windows and Linux systems for compliance and early warnings.



Intrusion Detection System (IDS)

Identify suspicious activity with curated and customizable signatures.



Sandbox

Detonate suspicious files in a safe environment to reveal hidden malware.



Threat Intelligence Platform (TIP)

Built into the core. Ingests third-party and premium threat feeds (including CrowdStrike in 6.1) and applies them at ingestion for stronger detection.



Security Orchestration

Automate response with pre-built or custom playbooks for consistent, fast actions.



AI-Driven SIEM with Multi-Layer AI

Collect and normalize any data — logs, cloud APIs, OT telemetry — and enrich with context. Multi-Layer AI drives detection (ML), correlation (GraphML), triage (LLMs), and response automation, turning alerts into actionable cases with timelines, entity mapping, and recommendations.

Data Management Components



Security Sensors

Deploy physical or virtual sensors across IT, OT, and cloud to collect and enrich network and log data at the edge.



API Integration Engine

Choose from 400+ turnkey integrations, including any EDR, to unify your telemetry.



Data Lake

Store and normalize all ingested data for hunting, forensics, and compliance.



Detection Engine

Apply ML, behavioral analytics, curated rules, and premium TI at ingestion for earlier detections.



Correlation Engine

Use AI and ML to fuse signals into high-fidelity cases, eliminating legacy SIEM noise.

Why It Matters

Modern attacks move across endpoints, identities, SaaS, OT, and cloud APIs in minutes. Siloed tools miss these transitions. SIEMs tried, but failed. Bolt-on ML and SOAR only reacted after alerts fired. **XDR-style unification and Multi-Layer AI** changed the game — and only Stellar Cyber built the platform that ties it all together.

With Stellar Cyber, you gain:

- Earlier detections at ingestion, not hours later.
- Stronger cases through cross-domain correlation.
- Faster investigations powered by Multi-Layer AI.
- Automated responses that reduce risk instantly.
- Real ROI from the tools you already own.



Take the First Step

Every team deserves enterprise-grade protection without added complexity. With Stellar Cyber, you finally get the SIEM that delivers on its promises — as part of a unifying SecOps platform.

Visit www.stellarcyber.ai to start your journey.

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 license. 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/>.