DATA SHEET

Stellar Cyber Open XDR Platform

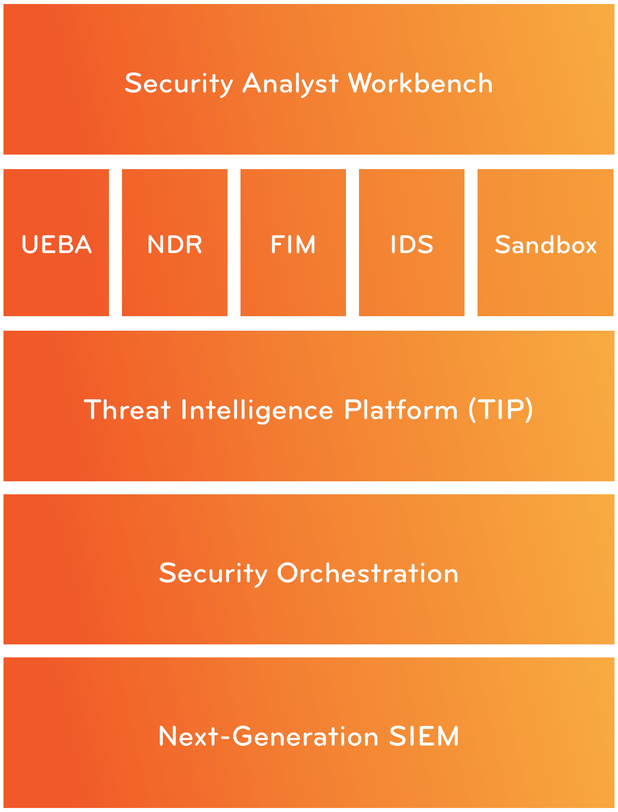
Security Applications and Data Management-at-a-Glance

The Stellar Cyber Open XDR platform delivers many core security technologies that security operations teams need to secure their environments. With our Open XDR platform, you can automatically collect and analyze data from any security, IT, OT, and productivity tool to identify potential threats in real-time.

Unlike "closed" XDR solutions that are extensions of a vendor's endpoint detection and response (EDR) product and only work with the vendor's specific EDR product, Stellar Cyber's "Bring your Own EDR" approach means you can use any EDR product you want with Stellar Cyber. Currently, Stellar Cyber supports all major EDR vendors.

The platform includes all the technology described below under an all-in single license. This licensing approach eliminates the surprise fees and upcharges typical with other security platforms.

Stellar Cyber Security Applications



Security Analyst Workbench

UEBA

NDR

FIM

IDS

Sandbox

Threat Intelligence Platform (TIP)

Security Orchestration

Next-Generation SIEM

Security Analyst Workbench: The analyst workbench is an intuitive user interface where all activities occur. Analysts can dive into the details of any case from the workbench, perform fast threat-hunting, initiate response actions, and more.

User and Entity Behavior Analytics (UEBA): Baselines users and entity behaviors, automatically identifying behaviors outside the norms as potential security risks.

Network Detection and Response (NDR): Combines raw packet collection with NGFW, logs, Netflow, and IPFix from physical or virtual switches, containers, servers, and public clouds to identify IT and OT network threats.

File Integrity Monitoring (FIM): Monitors critical files you tag across Microsoft Windows and Linux environments and generates alerts when unauthorized changes are detected.

Intrusion Detection System (IDS): Monitors network traffic for suspicious activity based on known attack signatures.

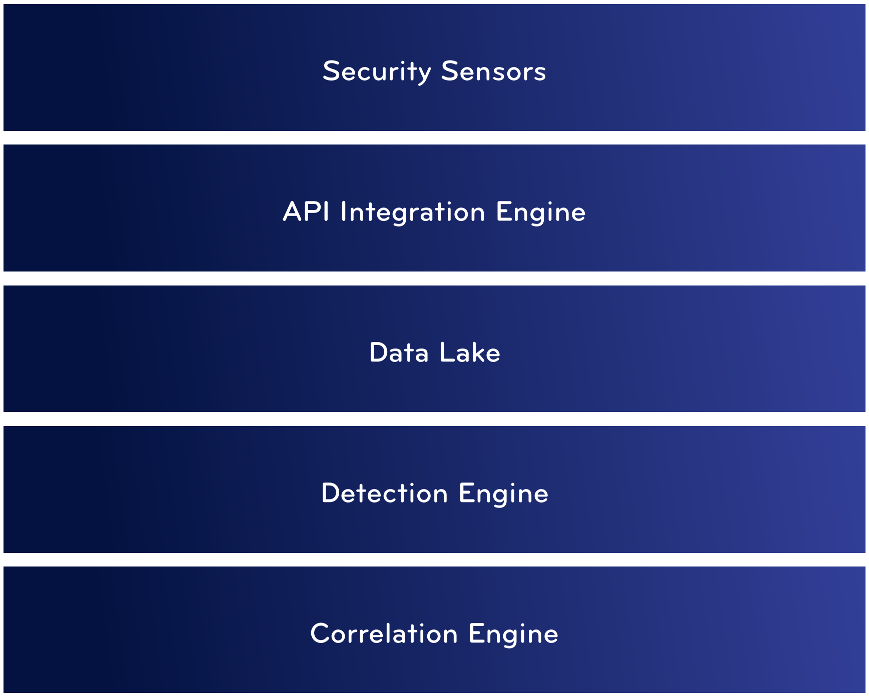
Sandbox: Suspicious files detonate automatically and safely to determine if they have malicious intent.

Threat Intelligence Platform (TIP): Data from third-party threat intelligence sources are automatically ingested and associated with related alerts and suspicious activities to give security analysts the context they need to understand the impact of threats.

Security Orchestration: Respond to cyber threats using pre-defined playbooks, ensuring consistent security outcomes.

Next-Generation SIEM (NG-SIEM): Collects and automatically normalizes data from any source to optimize search and threat-hunting functions, with the added benefit of making data audit-ready for compliance purposes.

Stellar Cyber Data Management


Security Sensors

API Integration Engine

Data Lake

Detection Engine

Correlation Engine

Security Sensors: Physical or virtual devices with embedded capabilities to collect and analyze security-relevant data "at the edge," generating alerts and initiating automated response actions if required.

API Integration Engine: With over 400 turnkey integrations included, you can bring in relevant data from any security, IT, and business application automatically. Additionally, if you use a product not currently integrated, Stellar Cyber commits to deliver the integration free of charge.

Data Lake: All collected data is normalized, enabling faster analysis, threat-hunting, and overall performance.

Detection Engine: Detects anomalies and potential threats using custom machine learning models and curated threat intelligence.

Correlation Engine: Using AI and ML to analyze natively generated and collected alerts to correlate seemingly unrelated security events into a single case ready for analyst investigation.

Enablement Included

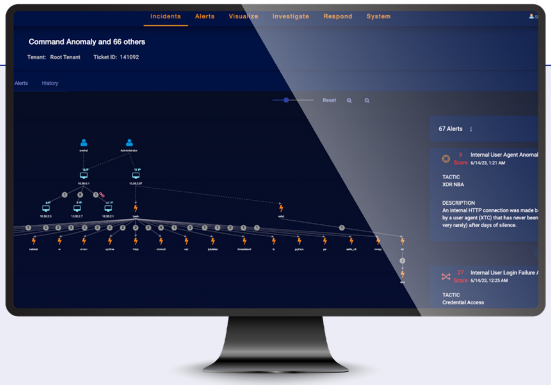
- ✓ **For MSSPs:** We train your SOC team to use the platform and your sales team to sell the platform effectively.
- ✓ **For Enterprises:** We train your administrators and analysts to use the platform as effectively as possible.

Learn more about how the Stellar Cyber Open XDR Platform can help you reach your security goals at stellarcyber.ai.

TAKE THE FIRST STEP TODAY

Every security team should be able to deliver continuous, consistent security regardless of their skills or experience. With Stellar Cyber, you get the capabilities you need to keep your business secure without the hassle.

Visit stellarcyber.ai today to start your journey.



Command Anomaly and 66 others

Tenant: Root Tenant Ticket ID: 141092

8 Score Internal User Agent Anomal
6/14/23, 1:21 AM

TACTIC
XDR NBA

DESCRIPTION
An internal HTTP connection was made b
by a user agent (XTC) that has never been
very rarely) after days of silence.

27 Score Internal User Login Failure
6/14/23, 12:25 AM

TACTIC
Credential Access

Stellar Cyber delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering an 8X improvement in MTTD and a 20X improvement in MTTR. The company is based in Silicon Valley. For more information, contact stellarcyber.ai.