Stellar Cyber

Product Portfolio-at-a-Glance

Single Platform, Single License

The Stellar Cyber Open XDR platform delivers the capabilities commonly found in NG-SIEM, NDR, and SOAR products in a single platform with a single license that empowers lean security teams of any skill to combat advanced cyberattacks consistently.

Threat intelligence (TIP) and advanced machine learning capabilities are shared across all capabilities delivering a comprehensive threat detection and automated response platform that eliminates the blindspots left behind by many other security products.

All the capabilities outlined in this document are included in the platform for all customers under a simple single license approach. This philosophy means customers can be confident that they will not be hit with surprise upcharges for a feature; everything is included.

Below is a brief overview of the Stellar Cyber Open XDR Platform capabilities, broken out by the product category where they would typically be found.

NG-SIEM

Next-Generation SIEM (NG-SIEM)

Stellar Cyber NG SIEM enables security teams to collect and automatically normalize log data from any data source making data audit ready for compliance needs. Once collected, data is enriched with threat intelligence and other contextual information to optimize search and threat hunting functions. With user entity behavior analysis capabilities included (UEBA), anomalous and suspicious behaviors will be identified automatically to eliminate potential security threats missed by other security controls.

Network Detection and Response (NDR)

Stellar Cyber NDR combines raw packet collection with NGFW logs, NetFlow, and IPFix from physical or virtual switches, containers, servers, and public clouds, enabling deep packet analysis for over 4,000 applications and L2-L7 metadata and files from network traffic. With IDS and malware sandbox included, suspicious files will be automatically detonated safely to determine if they have malicious intent.

NDR

Security Orchestration and Automated Response (SOAR)

Stellar Cyber SOAR allows security teams to respond to cyber threats using pre-defined playbooks, ensuring consistent security outcomes. With hundreds of pre-built integrations to security, IT, and productivity products, users can create virtually any workflow required to ensure identified cyber threats are mitigated appropriately.

SOAR

Open Extended Detection and Response (Open XDR)

Stellar Cyber Open XDR enables organizations to collect log and alert data from any security control, from the endpoint to the cloud and anywhere between. Then using advanced machine learning techniques and threat detection rules to identify, correlate, and respond to advanced cyber-attacks in real-time. Unlike "closed" XDR solutions that are essentially extensions of a vendor's endpoint detection and response (EDR) product and only work with the vendor's specific EDR data, Stellar Cyber's "Bring your Own EDR" approach means organizations can use any EDR product they want with Stellar Cyber. Currently, Stellar Cyber supports all major EDR vendors.

Open XDR Platform

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 www.stellarcyber.ai today to start your journey today.

Stellar Cyber Open XDR platform 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 a 20X improvement in MTTD and an 8X improvement in MTTR. The company is based in Silicon Valley. For more information, contact https://stellarcyber.ai.

STELLAR CYBER®

www.stellarcyber.ai | sales@stellarcyber.ai