

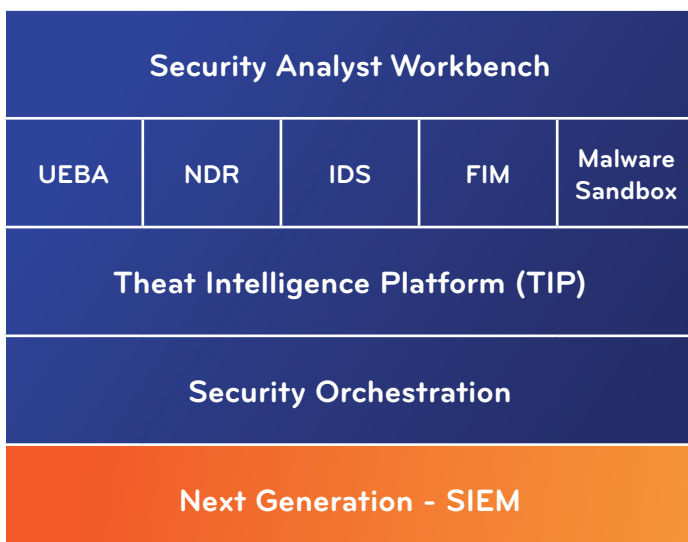
Stellar Cyber Next Generation SIEM

A Component of the AI-Driven Open XDR Platform

Lean security teams are looking for a Next-Generation SIEM (NG-SIEM) to increase their ability to identify advanced multi-vector attacks against their environments. Unfortunately, most do not meet their needs. Most NG-SIEMs require dedicated resources to deploy and maintain them and ongoing expertise to write correlation rules to identify threats. These requirements put undue stress on the typical lean security team whose resources are already stretched thin.

Stellar Cyber Next-Generation SIEM, as a critical component within the Stellar Cyber Open XDR Platform, is the only NG SIEM on the market specifically designed to meet the needs of the lean security team.

Packed with automation, purpose-built machine learning, and turnkey 3rd party integrations, Stellar Cyber Next Generation SIEM enables lean security teams to focus on delivering the security the business needs.



With Stellar Cyber Next-Generation SIEM, you can:

- Ingest and retain security alerts, log data, and network telemetry into a single centralized repository to meet their compliance requirements.
- Normalize, analyze, and enrich collected data automatically to gain context.
- Automatically triage security alerts to eliminate false positives, duplicate, and irrelevant alerts.
- Identify multi-vector attacks using the built-in advanced threat detection based on machine learning and custom correlation rules.
- Automatically correlate individual alerts into a single case, showing the entire attack making investigations faster.
- Rapidly and easily search contextualized data, speeding threat-hunting actions.

Stellar Cyber Next-Generation SIEM Benefits



Meet your security and compliance requirements without additional resources, making the platform accessible to everyone.



Identify high-fidelity threats without manually creating correlation rules, improving MTTD, MTTR, and efficiency.



By deploying NexGen SIEM, you get the benefits of the entire Open XDR platform, increasing the ROI of your investment.

Unlimited Data Sources	Incorporate and retain data from any security control, IT, and productivity tool into Stellar Cyber using pre-built integrations with no limitations.
Sensor-driven Data Collection	Use the proprietary Stellar Cyber sensors to collect raw network telemetry and log data to identify additional threats your existing security stack does not see.
Data Normalization and Enrichment	Data from any source is automatically normalized and enriched with context such as threat intelligence, user information, asset information, and GEO location by Stellar Cyber to enable comprehensive, scalable data analysis.
Automated Threat Hunting	Security analysts can use easy-to-understand querying formats to create customized threat hunts that can be run ad-hoc or on a set schedule.
Advanced Threat Detection Engine	Identifies complex threats using a combination of supervised and unsupervised machine learning and automated threat hunting to deliver the most comprehensive view of threats possible.
Machine Learning Correlation	Graph machine learning techniques combine seemingly disparate alerts into cases, providing security analysts with contextualized and prioritized threats to investigate.
Guided Investigations	Correlated incidents include the underlying data and context a security analyst needs to complete investigations fast, increasing efficiency and effectiveness.
Fast Incident Response	Security analysts can take decisive response actions manually or fully automate responses on the same platform using predefined response actions or customizable response playbooks.

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 Next-Generation SIEM, you get the capabilities to keep your business secure with your existing team. Visit www.stellarcyber.ai today to start your journey.



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 an 8X improvement in MTTD and a 20X improvement in MTTR. The company is based in Silicon Valley. For more information, visit <https://stellarcyber.ai>.