DATA SHEET

Stellar Cyber Next-Generation SIEM

The Intelligent, Efficient SIEM for Lean Security Teams

With Stellar Cyber Next-Generation SIEM you can:

- ✔ Ingest and retain security alerts, log data, and network telemetry into a single repository to meet your compliance needs
- ✔ Normalize, analyze, and enrich collected data automatically to gain full threat context
- ✔ Automatically triage security alerts to eliminate false positive, duplicate, and irrelevant alerts
- ✔ Identify multi-vector attacks using the built-in multi-modal threat detection based on machine learning and hueristics
- ✔ Automatically combine individual alerts into an incident showing the entire attack path through machine learning
- ✔ Rapidly and easily search contextualized data, speeding threat hunting actions

Stellar Cyber Next-Generation SIEM:

Lean security teams wanting to increase their ability to identify advanced multi-vector attacks against their environments have few, if any, Next-Generation (NG) SIEMs that meet their needs. Most NG SIEMs require dedicated resources to deploy and maintain them as well as ongoing expertise to write correlation rules for the NG SIEM to identify threats. These requirements put undue stress on the typical lean security team.

Stellar Cyber Next-Generation SIEM, a component of 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.

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 Next-Generation SIEM you get the benefits of the entire Stellar Cyber Open XDR platform, increasing the ROI of your investment

STELLAR CYBER®

STELLAR CYBER'S NEXT-GENERATION SIEM CORE CAPABILITIES:

Ultra-Flexible Data Sourcing

Incorporate data from any existing security control, IT, and productivity tool into the Stellar Cyber using pre-built integrations with no human intervention

Sensor-Driven Data Collection

Use the proprietary Stellar Cyber sensors to collect raw network telemetry and log data to identify additional threats not seen by your existing security stack

Purpose-Built Data Normalization and Enrichment

Data from any source is automatically normalized and enriched with context such as threat intelligence, user information, asset information, GEO location by Stellar Cyber to enable comprehensive, scalable data analysis

Automated Threat Hunting

Using easy-to-understand querying formats security analyst can create customized threat hunts that can be run ad-hoc or on a set schedule

Multi-Modal 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

Using graph machine learning techniques, seemingly disparate alerts are combined into incidents 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

Deterministic Incident Response

Using pre-defined response actions or customizable response playbooks, security analysts can take decisive response actions manually or fully automate responses on the same platform

TAKE THE FIRST STEP TODAY

Every security team can deliver continuous, consistent security regardless of their skills or experience. With Stellar Cyber Next-Generation SIEM, you get the capabilities you need to keep your business secure with your existing team. **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.