







Supercharge Your Splunk: Augment with Stellar Cyber for Unmatched Coverage and Flexibility

Prepared By: Product & Technical Product Marketing

This paper evaluates the benefits of using Stellar Cyber to augment Splunk, enhancing its capabilities to meet the demands of modern cybersecurity. It explores why to augment & questions to ask, key use cases, possible joint architecture, and addresses common challenges with practical strategies for resolution.

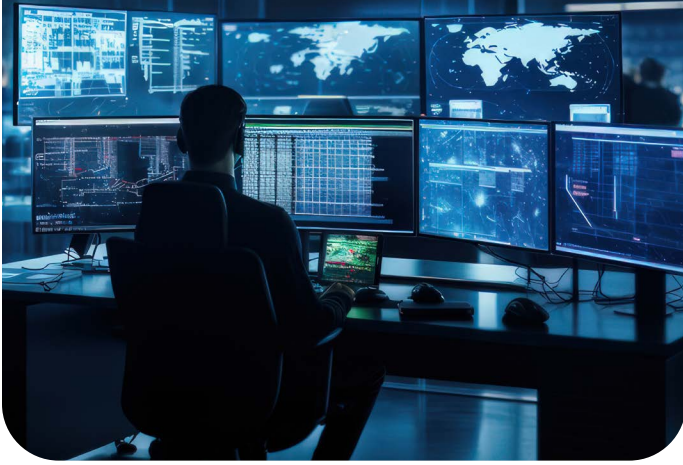
The insights provided are valuable for organizations currently using Splunk who want to address its limitations, as well as those seeking to **optimize their overall SOC operations & efficiency**. For existing Stellar Cyber users, this guide offers actionable recommendations for designing an optimal joint architecture to maximize security outcomes.

Why Augment?

-  **Enhanced Threat Visibility:** Augmenting your SIEM allows for deeper insights into network traffic (especially with Stellar Cyber!), applications, servers, and user behavior. By integrating additional sources like raw packets, metadata extraction, and advanced network analytics, organizations can uncover threats that traditional log-based systems may overlook.
-  **Improved Detection Accuracy:** Advanced technologies like deep packet inspection (DPI) and behavioral analytics enable broader detection of sophisticated threats, such as lateral movement, data exfiltration, and anomalous behavior. This reduces the risk of missed threats and ensures a more robust defense.
-  **Cost-Effective Data Management:** Parsing and filtering data at ingestion significantly reduces the volume of irrelevant information stored and processed, cutting storage costs and optimizing licensing expenses. This approach ensures that only actionable, security-relevant data is sent to the SIEM.
-  **Faster Incident Response:** Enriching alerts with contextual information—such as user identity, geolocation, and threat intelligence—enhances root-cause analysis, enabling faster detection and response. This approach significantly reduces the mean time to detect (MTTD) and mean time to respond (MTTR), ultimately boosting the overall efficiency of the SOC.
-  **Seamless Integration and Scalability:** Augmenting your SIEM with open and scalable solutions allows for easy integration with hybrid, multi-cloud, and on-premises environments. This flexibility supports growing data demands and evolving infrastructure without disruption.
-  **Comprehensive Security Coverage:** Adding capabilities such as malware sandboxing, FIM, application-aware analytics, and advanced behavioral models provides end-to-end security across the network, endpoints, and users. This bridges visibility gaps and ensures a unified approach to threat detection and mitigation.

Questions to Ask if You Need to Augment

- Are you confident that your current SIEM provides full visibility into all network traffic, applications, and user behavior, or do you suspect blind spots might exist?
- How do you currently detect threats that operate at the application layer or involve lateral movement across your network?
- Do you rely solely on logs for threat detection, and how do you ensure you're not missing critical insights from network traffic or metadata?
- How effective is your SIEM at identifying advanced threats, such as anomalous user behavior, data exfiltration, or malware hidden in encrypted traffic?
- How do you ensure that only security-relevant data is ingested and stored, rather than overloading your SIEM with irrelevant information with extra cost?
- When a security alert is triggered, how quickly can your team perform root-cause analysis and respond to the threat?
- Do you have mechanisms to enrich alerts with contextual information like user identity, device history, or Geolocation to speed up investigation and response?
- Are you able to detect threats across the entire network, endpoints, and users, or do you rely on additional tools to fill these gaps?
- How do you handle unknown or suspicious files? Do you have a built-in sandboxing solution to analyze and identify potential threats safely?



5 Reasons Why Augmenting with Stellar Cyber is the Game-Changer Your SOC Needs

Network Detection & Response (NDR)

Initially built for IT error detection, Splunk's outdated architecture fails to scale effectively or meet the real-time demands of modern cybersecurity, leaving critical visibility gaps and driving up costs.

Stellar Cyber's NDR provides unparalleled network visibility by combining raw packet capture with NGFW logs, NetFlow, and IPFix from diverse sources, including physical and virtual switches, containers, servers, and public cloud environments. Its advanced modular sensors leverage a powerful DPI engine for detailed analysis of over 4,700 applications, extracting L2 - L7 metadata and inspecting files to uncover advanced threats often missed by traditional log-based detection methods. With full coverage of IT and OT traffic, these distributed sensors offer flexible capacities and enable local actions, such as blocking IPs or disabling users on local systems. The platform enriches alerts with contextual insights like user identity and device status, while its integrated sandbox detonates suspicious files safely, enhancing detection accuracy. By correlating these insights with UEBA and NDR models, Stellar Cyber delivers granular, application-layer visibility and advanced threat detection, far surpassing the capabilities of traditional solutions.

Unified SecOps with AI-powered UEBA, Network/Sensor/Endpoint Behavior Analytics (NBA, SBA, EBA)

Splunk's UBA product is a bolt-on solution, lacking integration with its core SIEM platform, resulting in disjointed workflows and limited scalability. Its scope is narrow, providing minimal entity coverage and basic behavioral insights, leaving significant blind spots in threat detection. Unlike modern solutions, it struggles to detect lateral movement or advanced threats and lacks visualization strengths, making it cumbersome for SOC teams to gain actionable insights.

Stellar Cyber delivers a 360-degree view of activity across users, devices, applications, and networks, ensuring comprehensive

visibility into your environment. Sensor Behavior Analytics (SBA) and Network Behavior Analytics (NBA) detect unusual behaviors like lateral movement and data exfiltration, while User and Entity Behavior Analytics (UEBA) and Endpoint Behavior Analytics (EBA) identify compromised users and endpoints. Together, these capabilities provide unparalleled coverage and insights, enabling rapid detection and response to advanced threats.

Enhanced Visibility

Splunk's approach to visibility is heavily dependent on log data, often leaving critical gaps in network, endpoint, and user activity, especially in hybrid or multi-cloud environments. Its reliance on disparate modules for different data sources creates siloed insights, hindering comprehensive threat detection.

Stellar Cyber enhances visibility by providing rich context for anomalies, such as user actions, endpoint changes, and network traffic patterns, enabling deeper investigations and more accurate threat detection. It uncovers subtle, hard-to-spot anomalies across users, endpoints, sensors, and networks that traditional signature-based methods often miss. With tailored correlation rules and detections customizable to your SOC's unique needs, Stellar Cyber expands use case coverage, empowering SOCs to address a broader range of threats with precision and efficiency. This comprehensive approach ensures nothing is overlooked in your security environment.

Cost Effective Management

Splunk's "index everything" model inflates storage requirements and costs, while its delayed data parsing slows searches and retrieval, making long-term compliance expensive. Designed for IT troubleshooting, its resource-intensive architecture struggles in modern cloud environments.

Stellar Cyber reduces costs by filtering and parsing data at ingestion, retaining only relevant security information through a security-centric model. This approach minimizes data volume, significantly lowering storage costs while optimizing performance. By supporting cost-efficient data archiving with fast access to logs—whether days or years old—organizations can achieve seamless operations without expensive overhead. Additionally, Stellar Cyber delivers dramatically higher search performance without driving up costs, making it an ideal augmentation solution for cost-conscious security environments.

Hyper-Enriched Threat Context During Data Ingestion

Splunk's context enrichment is limited and often requires additional costly integrations or manual configuration to incorporate threat intelligence feeds. Its lack of native threat intelligence aggregation and prioritization can delay threat detection and response. The recent acquisition of Cisco enabled them to integrate with Talos.

Stellar Cyber's Threat Intelligence Platform (TIP) seamlessly aggregates commercial, open-source, government, and proprietary threat intelligence feeds, including Proofpoint, DHS, OTX, OpenPhish, and PhishTank, to enhance detection and response capabilities. By prioritizing feeds based on security research, the platform ensures data is enriched only once after aggregation, delivering actionable insights with minimal noise. Organizations can also integrate additional feeds using STIX/TAXII standards, tailoring threat intelligence to their specific needs. Constant, automated updates ensure all Stellar Cyber deployments benefit from the latest intelligence without administrative overhead. With no added cost, the TIP works in the background to continuously collect, aggregate, and distribute threat intelligence, making it a powerful augmentation tool for any security environment.

Augmenting Your SIEM with Stellar Cyber: Real-World Scenarios

Let's explore scenarios where Stellar Cyber is used to augment existing SIEM solutions, addressing gaps and enhancing security operations. In many cases, Stellar Cyber is deployed as an **NDR, NG-SIEM, OT Security** – or all of the above. Meanwhile, the existing SIEM may continue to handle specific tasks, such as compliance reporting or basic log management.

This coexistence enables organizations to optimize their security operations by integrating Stellar Cyber's advanced

features with their current SIEM. For instance, Stellar Cyber can handle tasks like **deep packet inspection (DPI), behavioral analytics, and malware sandboxing**, while the primary SIEM focuses on traditional log-based use cases.

Integration for Success

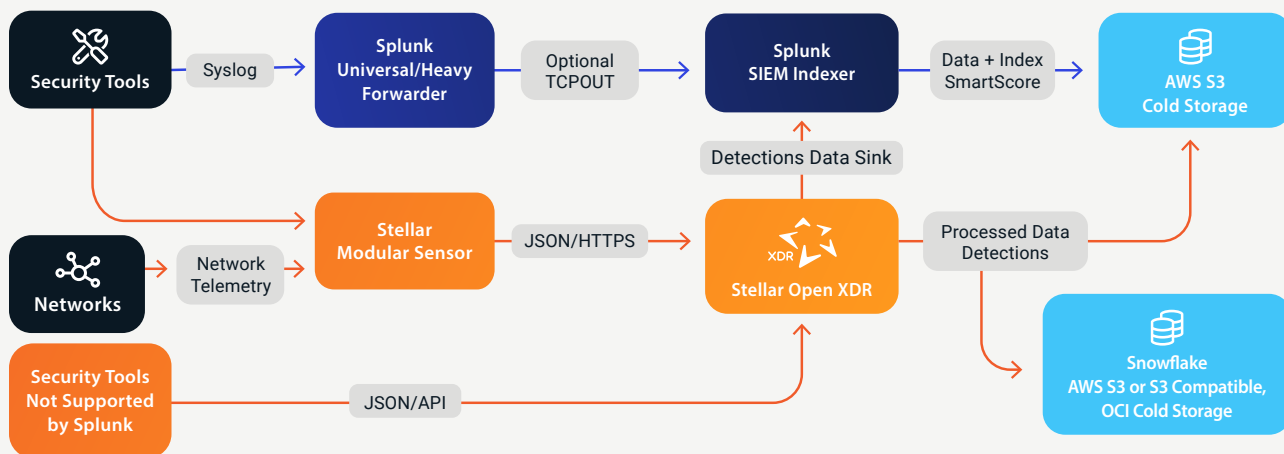
In augmentation scenarios, integrating Stellar Cyber with an existing SIEM ensures seamless workflows for detection, reporting, and hunting missions. Organizations striving for excellence in these areas, without significantly increasing costs, often choose Stellar Cyber to bridge the gaps in their legacy SIEM platforms.

From Augmentation to Transition

In many cases, as Stellar Cyber integrates into an organization's environment, it gradually takes on more responsibilities due to its comprehensive capabilities. Initially deployed for **NDR or incident investigation**, Stellar Cyber often evolves to handle **detection, response, and even compliance reporting**, reducing reliance on the legacy SIEM.

For example, an organization might start by using Stellar Cyber to augment detection capabilities for lateral movement and advanced persistent threats, while keeping the existing SIEM for log management. Over time, Stellar Cyber's efficiency, **cost-effectiveness**, AI-Based Detections, NG-SIEM, Open XDR, NDR, and **scalability** lead to a transition where the legacy SIEM is relegated to niche uses, or even phased out entirely.

Splunk Augmentation Deployment



Stellar Cyber offers a powerful solution to augment Splunk SIEM, providing seamless integration and advanced capabilities that enhance SOC efficiency. The Stellar Modular Sensor enables ingestion of syslog data from various security tools and delivers Network Detection and Response (NDR) functionality by tapping directly into network traffic. Through its Open-XDR platform, Stellar Cyber connects to a wide range of security tools via APIs, ensuring comprehensive data integration. Hot data is centralized in the Stellar Cyber data lake, where advanced detection engines analyze it to generate high-fidelity alerts and actionable cases. These insights can be seamlessly ingested into Splunk SIEM using the Data Sink feature creating a unified view for the SOC. While Splunk can function as external cold storage, leveraging solutions like AWS S3 or Snowflake, Stellar Cyber's detections also enhance Splunk's native analytics, making it a cost-effective and powerful combination for modern security teams.

Other Use Cases Stellar Cyber Can Solve for You!



Open XDR: Splunk, as a legacy SIEM, lacks the native capabilities of Open XDR solutions, requiring costly integrations and customizations to achieve comparable functionality. Its reliance on log-based detection limits visibility and coverage, making it inefficient for addressing modern, multi-vector threats. Unlike Splunk, Open XDR provides seamless integration, enhanced detections, and multi-functional modular sensors that deliver full-spectrum visibility across endpoints, networks, and applications. With automated detections and streamlined workflows, Open XDR reduces operational overhead and provides faster, more comprehensive threat detection and response, outperforming Splunk in scalability, efficiency, and cost-effectiveness.

Stellar Cyber offers seamless, non-disruptive augmentation, allowing customers to maintain existing processes, rules, and teams while enhancing their security stack with next-gen Open XDR, delivering immediate cost savings. By front-ending Splunk, Stellar Cyber provides enhanced detections with AI-driven capabilities, improved coverage through comprehensive Open XDR connectors and multi-functional modular sensors, including network and server sensors like FIM. Additionally, it reduces manual effort with hundreds of out-of-the-box automated detections, streamlining operations and boosting SOC efficiency.



NG-SIEM: Splunk, while a legacy SIEM, lacks the advanced capabilities needed for a true Next-Generation SIEM (NG-SIEM). Its reliance on static rule-based detection and log-centric architecture results in limited scalability, slow detection, and high costs, making it ineffective for modern threat landscapes.

Stellar Cyber, as an NG-SIEM, combines AI-driven analytics, deep packet inspection (DPI), and real-time enrichment to deliver unparalleled threat detection and response. With native integration of UEBA, NDR, and automated case management, Stellar Cyber provides comprehensive visibility, faster insights, and cost-effective scalability, far surpassing Splunk's outdated SIEM capabilities.



IT/OT Convergences: Splunk struggles with IT/OT convergence due to its limited support for OT-specific protocols, lack of visibility across operational environments, and reliance on siloed log data. It fails to provide comprehensive monitoring of OT assets, leaving critical gaps in detecting threats that move laterally between these domains.

Stellar Cyber SecOps Platform uniquely addresses IT/OT security challenges with advanced NDR capabilities, enabling organizations to handle the complex threat landscape across IT, DMZ, and OT environments. By collecting and analyzing data from IT to OT, Stellar Cyber detects incidents involving lateral movement, ensuring comprehensive breach coverage. With support for 4,700+ protocols, including 57 SCADA and 18 IoT protocols, real-time file reconstruction, and updates from paid signatures, the platform offers unparalleled threat detection capabilities. Stellar Cyber integrates logs from OT security products like Nozomi, OT devices like Honeywell, and sources within Level 3 and the DMZ, while leveraging AI to detect threats, discover assets, and support third-party tools like Tenable. These features position Stellar Cyber as a leading augmentation solution for IT/OT environments.

Stellar Cyber offers a powerful solution to augment Splunk SIEM, providing seamless integration and advanced capabilities that enhance SOC efficiency.



BYODL (Bring Your Own Data Lake): Integrating Splunk with external data lakes often involves complex setup processes, requiring custom configurations and potential development work, which can be both time-consuming and error-prone. Additionally, Splunk's platform lacks native support for seamless integration with external data lakes, leading to inefficiencies in data handling and synchronization. Its rigid data management architecture further limits flexibility, making it difficult to adapt to the diverse data sources and formats typically associated with external data lakes.

In contrast, Stellar Cyber's SecOps Platform delivers robust BYODL capabilities with seamless integration into existing data lakes, including Splunk, Snowflake, Elastic, AWS, or any S3-compatible storage. The platform efficiently collects raw security event data, normalizes and enriches it at ingestion, and filters out unnecessary data to reduce storage costs and optimize processing. Real-time and on-demand synchronization ensures external data lakes remain up-to-date, even during connectivity disruptions.



FIM (File Integrity Monitoring): Splunk lacks native File Integrity Monitoring (FIM) capabilities, often requiring third-party tools or complex integrations, which increases costs and operational overhead. It does not offer advanced features like real-time file monitoring, over-the-wire file reconstruction, or classification, leaving gaps in detecting malicious file activity. This makes file-based threat investigation more time-consuming and less efficient compared to solutions like Stellar Cyber, which provide these capabilities natively and seamlessly.

Stellar Cyber integrates FIM directly into its platform, enabling real-time monitoring of file changes and leveraging advanced features like over-the-wire file reconstruction and classification. This provides seamless detection of malicious file activity, reduces response times, and ensures comprehensive file-based threat investigation without the need for costly add-ons.

"Stellar Cyber revolutionized our operations by providing more comprehensive data than Splunk, enabling us to process critical information in minutes instead of hours. Stellar not only included key data sources that Splunk missed, such as sensors across three city departments, but it also presented the information in an intuitive, easy-to-visualize format. The platform's ease of use significantly reduced the learning curve for our team, empowering us to act quickly and effectively on insights. Over time, Stellar Cyber allowed us to completely replace Splunk, cutting our costs by 50%. Stellar's exceptional support ensured a seamless transition and continues to be a reliable partner in our SecOps journey."

– SecOps Professional from a Large American City

Stellar Cyber's Automation-driven Security Operations Platform, including NG-SIEM and NDR and powered by Open XDR, delivers comprehensive, unified cybersecurity without complexity. It empowers lean security teams of any skill level to successfully secure their environments. As part of this unified platform, Stellar Cyber's Multi-Layer AI™ enables enterprises, MSSPs, and MSPs to reduce risk with early and precise threat identification and remediation while slashing costs, retaining investments in existing tools, and improving analyst productivity. This delivers a 20X improvement in MTTD and an 8X improvement in MTTR. The company is based in Silicon Valley. For more information, please visit our [website](#).