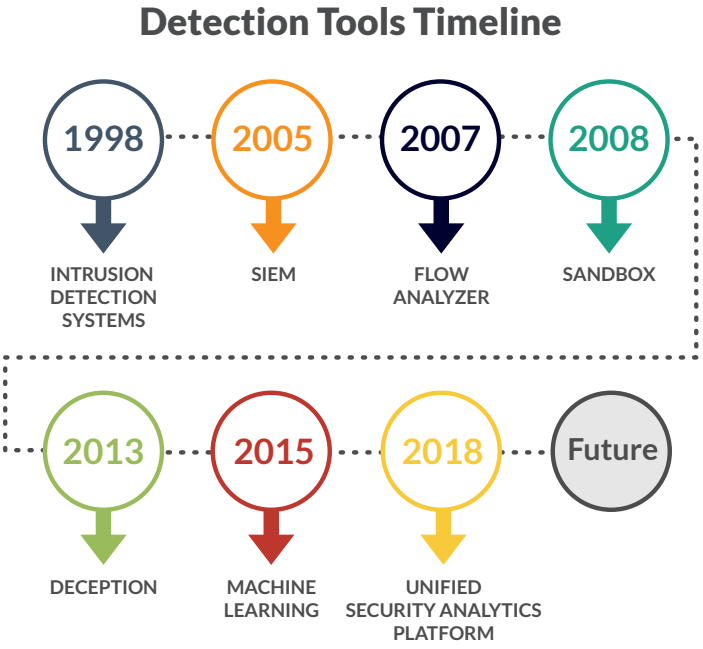
STELLAR CYBER

SOLUTION BRIEF

Starlight – Open XDR Security Platform

Reveal Hidden Attacks On Premises, Edge and Cloud



TODAY'S CYBER SECURITY CHALLENGE

Cyberattacks and breaches are soaring and security budgets are growing in response. Until now it has been necessary to juggle a multitude of expensive tools from multiple vendors. The industry doesn't need another point solution to cobble together. It needs a scalable, intelligent central platform that is fed with the right data and armed with the ability to automatically respond to threats.

WHY EXISTING APPROACHES FAIL

So why are organizations still getting breached? At Stellar Cyber, we believe it is because of complex environments with blind spots, disparate tools and alert noise. Today's environments consist of physical, virtualized, containerized workloads in public, private and hybrid clouds that create huge coverage challenges and an unmanageable amount of unactionable alerts. In this state, it is extremely difficult for security teams to efficiently respond to threats and identify the critical ones before data is stolen or damage is done. A better early warning detection system is needed.

THE SOLUTION

Stellar Cyber is solving these security challenges by delivering a the world's first open detection and response (Open-XDR) platform that combines the functions of pervasive data collection, big data processing and artificial intelligence through machine learning.

We believe the solution to today's security problem is to deploy a single technology that can be deployed across all environments to provide pervasive visibility. The technology should capture and correlate all types of data, such as network traffic, logs, server commands, processes, applications, user information, files, etc. The solution should be full stack, yet open, extensible, scalable, intelligent, and provide automation so the security staff can operate more efficiently. Lastly and most importantly, at Stellar Cyber, we believe that cyber security solutions should reduce the industry average of 200 days to detect a breach down to minutes to detect a breach while mitigating the risk of data ex-filtration or any other damage.

The Stellar solution, called Starlight, works by deploying sensors, agents and log forwarders on the network, servers, containers, physical and virtual hosts. The sensors and agents transform raw data into Interflow records and send it to a centralized data processor and data lake that deduplicates, correlates, enriches, indexes and stores the data that it receives. Once this data is received, it then runs complex analytics on the dataset to identify high fidelity breach events.

Starlight has tightly-integrated security applications that share data on one platform and features built-in analytics that leverage machine learning to eliminate alert noise and improve the accuracy of detecting critical security events. With this methodology, organizations can gain human work force efficiencies by augmenting security operations teams with big data analytics and artificial intelligence. The use cases of the solution are limitless in the areas of threat investigation, detection and response.

> "Starlight delivers the key benefits of the elimination of blind spots, reduced time to detect breaches and improved human capital efficiencies. With **comprehensive data collection and automated detection, investigation and response**, Starlight is a security operator's dream come true."
>
> *– John Peterson, Chief Product Officer, Stellar Cyber*

CAPTURE THE RIGHT DATA

Starlight has data collection and processing at the core of its capabilities and at Stellar Cyber, we believe that solving the data problem first is key. This is because security analysts struggle with having too much data, not enough data or no context for data. If the data collection problem isn't solved properly, tools will experience the age-old problem of garbage in / garbage out. Stellar Cyber's data collection technology is called Interflow.

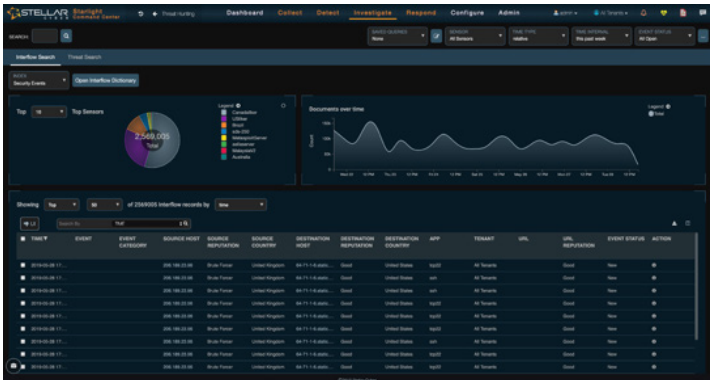
Interflow is a JSON formatted data record that is normalized, reduced and enriched with other telemetry to give context to what is actually occurring. Starlight's family of sensors and agents capture network application data, server process, command and file data as well as threat intelligence and geo location data. After collected, this data gets fused together to form one record.

DETECT THE REAL THREATS

Leveraging a built-in App Store, Starlight enables customized security workbenches to analysts get the tools they want. There are over 50,000 detections for known and unknown behaviors and these detections are mapped to the cybersecurity kill chain to act as an early warning detection system. Starlight, unlike other solutions in the market, has complete kill chain detection because of the its rich data collection.

For example, detections at the delivery stage of the kill chain require a malware sandbox, and detections at the exploitation stage require IDS technology. Starlight delivers the tools to detect and respond throughout the kill chain. The solution also combines legacy technologies such as IDS with machine learning in order to increase fidelity and lower false positives. Machine learning effectively creates a baseline of signatures that normally trigger often and eliminates them from being considered a high-fidelity alert. Machine learning also detects anomalous traffic patterns and server behavior.

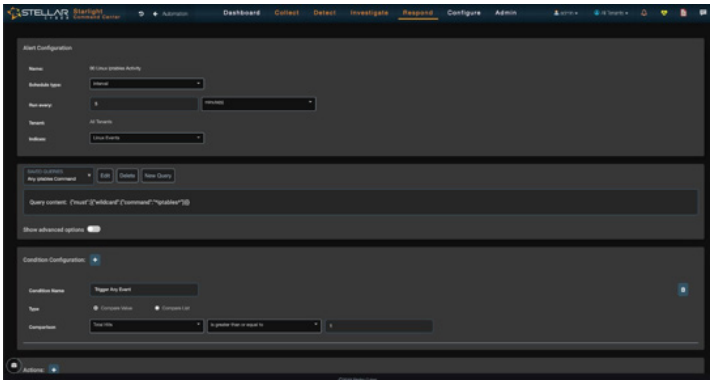
PINPOINT PROBLEMS



Threat Hunting has quickly become a popular strategy in cyber security operations, and the search for the unknown is as important as the detection of the unknown. With Starlight, organizations can search its rich dataset for malicious activity by creating simple or complex queries on the fly. It's like having a Google search engine on your data. For example, an operator can investigate for the execution of Windows Powershell commands on a server initiated from public IP addresses that has a pre-existing bad reputation. Another example is an operator wanting to search for a specific file (MD5 hash) uploaded to a server on the Internet by a specific user.

After these search queries are created, the operator can then save them and turn them into custom visualizations for future use and have them automatically executed to generate alerts and reports.

RESPOND AUTOMATICALLY



Detection and investigation for high-fidelity events are a must-have for any security platform, however the platform would not be complete if it didn't have the ability to also take action. Starlight has built-in event response capabilities. Operators can respond to an event by creating a trouble ticket with its built-in case management system, trigger email, Slack and restful API alerts, automatically send out PDF reports and signal firewalls to take appropriate action.

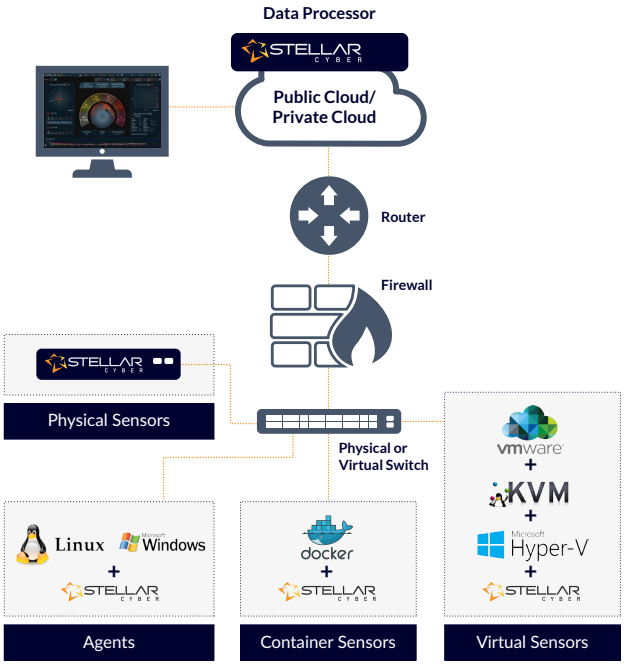
Along with these built-in response capabilities, Starlight also has orchestration plugins for SIEMs as well as SOAR tools such as Phantom Cyber and Demisto. The SIEM plugin streams events and the SOAR plugins allows Starlight's detections to automatically trigger playbooks that reside in orchestration products to perform a variety of instructions that could include executing scripts or integrating with other tools in the environment.

STARLIGHT DEPLOYMENT

The solution is delivered as software that can be installed on your own physical or virtual x86 servers in cloud providers such as AWS, Azure or Google, or purchased as pre-installed hardware appliances.

There are multiple components that create the total solution:

- Network sensors collect network traffic from ethernet switches.
- Agent sensors are installed on Linux and Windows on servers to collect traffic, command, process and file data.
- Container sensors collect traffic inside container environments.
- Deception sensors act as honeypots within your environment.
- Virtual appliance sensors can be deployed inside KVM, VMWare and HyperV environments.
- Data Processor nodes are deployed and can be clustered together to create an infinitely scalable big data platform for data storage and analytics.



FOUR SENSOR TYPES

GLOBAL PARTNER NETWORK

The Starlight solution is made available to customers through our global partner network. We have selected some of the best distributors and value added resellers around the globe that have a deep understanding of cybersecurity. Our partner first approach assures that we are able to deliver our products around the world as well as bring localized technical support and training.

ABOUT STELLAR CYBER

Stellar Cyber's Starlight is the world's first open detection/response (Open-XDR) platform, connecting the dots throughout the entire security infrastructure and automatically responding to attacks wherever they occur. Starlight integrates dozens of security applications from an App Store and presents results in an intuitive dashboard to supercharge analyst productivity.