DATA SHEET

Interflow™ – Designed to build actionable records with rich context for any set of related security events

Why Interflow

Interflow was designed by Stellar Cyber engineers with the goal to capture network packets, files and server logs in an effort to output a dataset to other tools that is richer than Netflow (too little), significantly lighter weight than PCAP (too big) and fused with context (just right) such as host name, user information, Threat Intelligence and geolocation.

Interflow starts at ingestion through the broadest suite of sensors and agents to literally collect all data from anything, or anywhere data and applications reside–on the network, servers, containers, physical and virtual hosts, on premises, in public clouds and with service providers.

Stellar Cyber's Starlight is the only comprehensive open detection and response (Open-XDR) security platform providing maximum protection of applications and data because of Interflow.

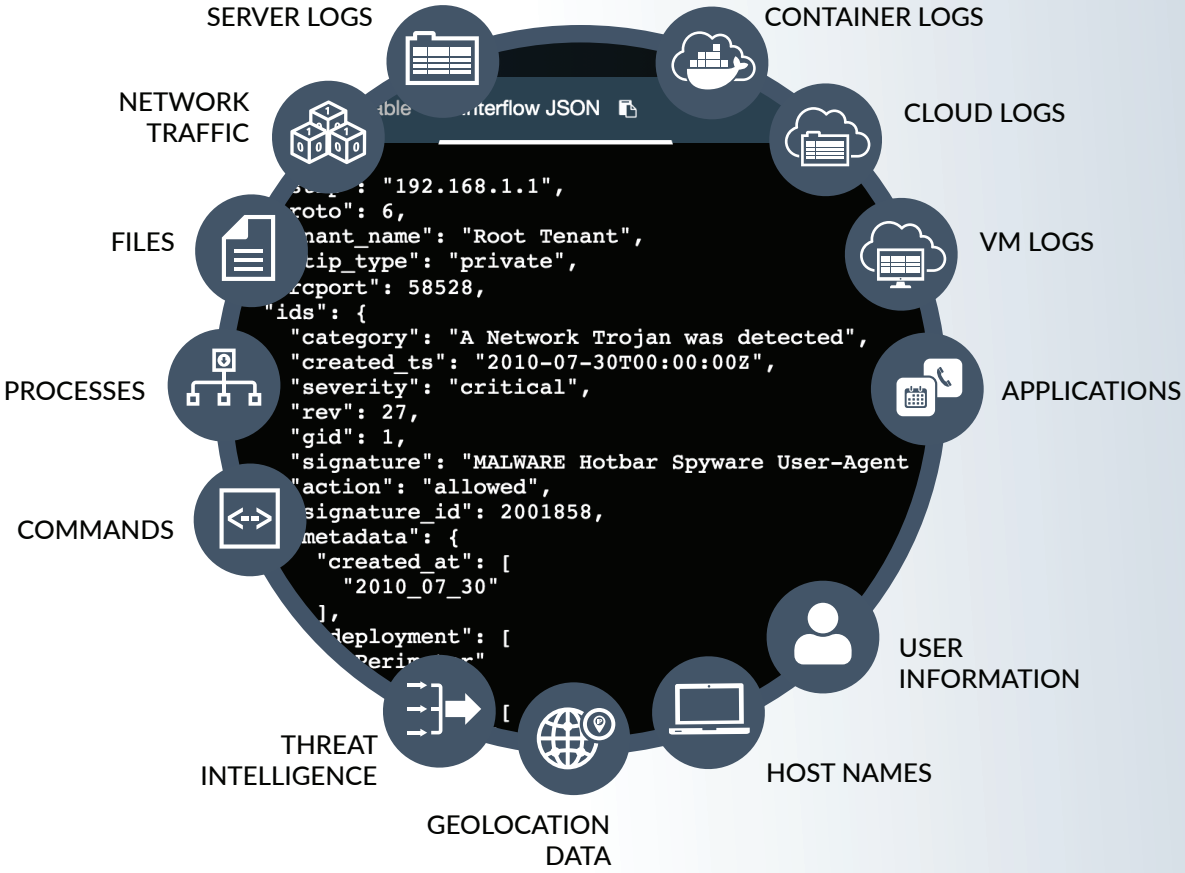
Contextual Data, Actionable Results

- **Deep packet inspection and metadata extraction at ingestion**
- **Build and process contextual metadata through enrichment of any data source**
- **Correlate across seemingly unrelated events**
- **Deliver an actionable, searchable, exportable JSON record for each event**

FAMILY OF SENSORS AND AGENTS PROVIDES

Pervasive data collection in any environment

PERVASIVE DATA INGESTION



Starlight operates wherever applications and data reside including on-premises, public cloud or with service providers.

Network Sensors: collect data from physical or virtual switches

Security Sensors: collect metadata from physical and virtual switches as well as detect intrusions and malware

Agent Sensors: collect data running on Linux and Windows servers including traffic, commands, processes, file and application information. These sensors operate on Windows 98 and up, Ubuntu, CoreOS, Debian and Red Hat

Container Sensors: collect data from, and operate inside Docker environments

Deception Sensors: act as honeypots within your environment and operate on VMware, KVM, Hyper-V and VirtualBox

Connectors ensure visibility into Software-as-a-Service applications or service provider environments including: AWS Cloudtrail, Office365, G-Suite, OKTA, vulnerability scanners, Active Directory and SNMP

ACTIONABLE, SEARCHABLE AND EXPORTABLE

Interflow documents ingestion, reduction, enrichment and correlation of each event.

Interflow Process	Starlight Action
Deep-packet inspection (DPI)	Stellar Cyber's sensors and agents transform raw data into Interflow records at ingestion and immediately start processing information. The integrated and advanced DPI engine can identify 4,000+ network applications, extract metadata from these applications, and reassemble files. The right amount of metadata, including DNS domain names, URLs, SQL queries, etc. are extracted. This capability leverages the distributed nature of the Starlight platform, ensuring that any pre-processing is done to ensure performance at scale.
Reduction	Interflow reduces data overhead by removing parts of the packet / payload that are not needed to study your security attack surface, such as video content. Data reduction from PCAP to Interflow can be up to two orders of magnitude. The data volume is reduced while providing ample evidence for advanced detection and forensics analysis.
Enrichment	Data in isolation is useless – Interflow adds rich context to the data such as geolocation and Threat Intelligence, ensuring analysis is more meaningful. Thorough enrichment delivers real-time detection and threat hunting /investigation through a data lake with searchable indexed big data.
Correlation	Once this data is reduced and enriched, it then runs complex analytics on the dataset to identify high-fidelity breach events. Interflow normalizes security data shared between integrated applications and third-party applications, driving single-pane-of-glass visibility and control across security toolsets. Interflow's two-staged machine learning ensures that seemingly unrelated or 'normal' events are in fact related to a complex multi-pronged attack.
Readable / Searchable	Starlight provides a workbench for security analysts – this allows them to perform simple Google-like or Boolean-logic searches of Interflow JSON records for anything including specific users, application types and specific locations.
Exportable	Interflow records are in JSON format and are easily exported to compatible systems.
Actionable	Interflow is a human-readable JSON record that is evidence of an event without the size of full packet capture. Interflow records can be used to trigger automatic responses directly or through SOAR integration.