DATA SHEET

Interflow™ – Readable, Searchable and Actionable Records With Rich Context for Any Security Data

Why Interflow

Interflow was designed by Stellar Cyber engineers with the goal to address Goldilocks dilemma of cyber security by capturing network packets, files and logs in an effort to output a dataset 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 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.

Interflow Table | Interflow JSON


```
{
  "dstip": "54.36.137.146",
  "event_type": "delivery",
  "tenant_name": "All Tenants",
  "dstip_type": "public",
  "locid": "unassigned location",
  "tenantid": "",
  "vlanid": 0,
  "new_file": 0,
```


Contextual Data, Actionable Results

- Deep packet inspection and metadata extraction at ingestion
- Build context for the data through normalization, enrichment and correlation
- Correlate across seemingly unrelated events
- Deliver an actionable, searchable, exportable JSON record for each event

360° VISIBILITY

Stellar Cyber is designed cloud native, to be deployed anywhere from the beginning, and with multi-tier, multi-tenant and multi-region capability built-in

FAMILY OF SENSORS PROVIDES

Visibility across network, endpoint, user, cloud and applications

Network Sensors: collect metadata from physical or virtual switches and aggregate logs

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

Server 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

Log Forwarders: enables you to stream any logs to the sensor to be shipped to the data processor. It normalizes and fuses the logs into interflow

ACTIONABLE, SEARCHABLE AND EXPORTABLE

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

Interflow Process	Stellar Cyber Action
Deep-packet inspection (DPI)	Stellar Cyber's sensors 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 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.
Transformation	Data can come from various data sources in different formats such as logs of many different firewalls. Through normalization process, Interflow will have same format to allow the same search and the same detection to be applied to different source of data despite of the original format.
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 capabilities and third-party tools, 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	Stellar Cyber 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.