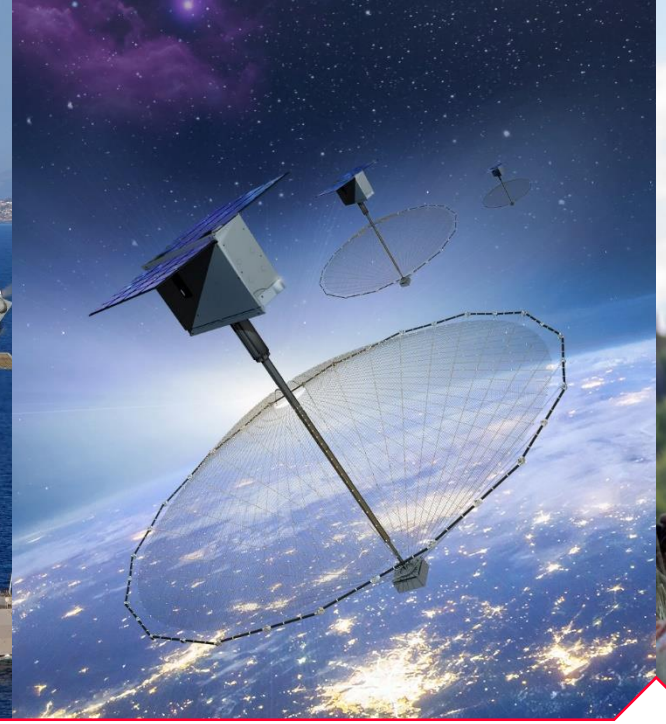
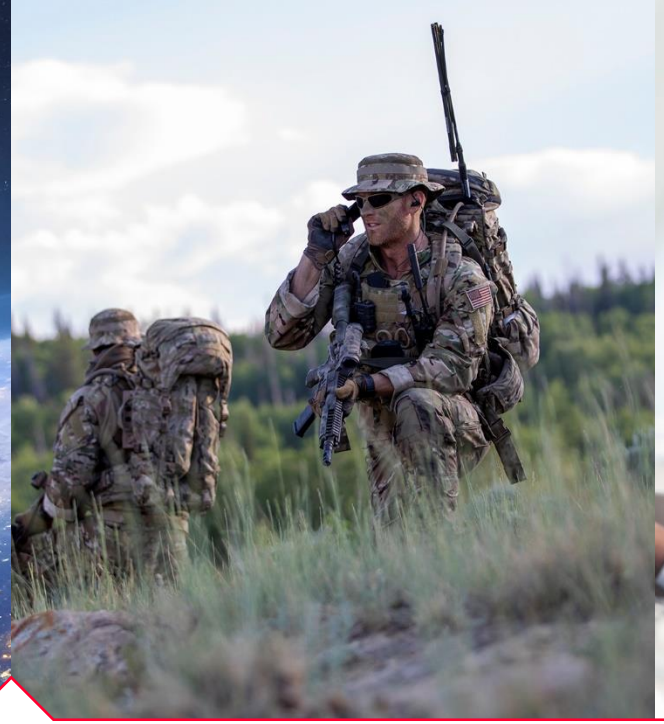





Use of U.S. DoD visual information does not imply or constitute DoD endorsement.

L3HARRIS™

SECURE DATA INGEST

GSAW 2020

March 4th 2020

Gilles Kbidy, Manager, Software Development, L3Harris Technologies, Gilles.Kbidy@L3Harris.com, 858-694-7641

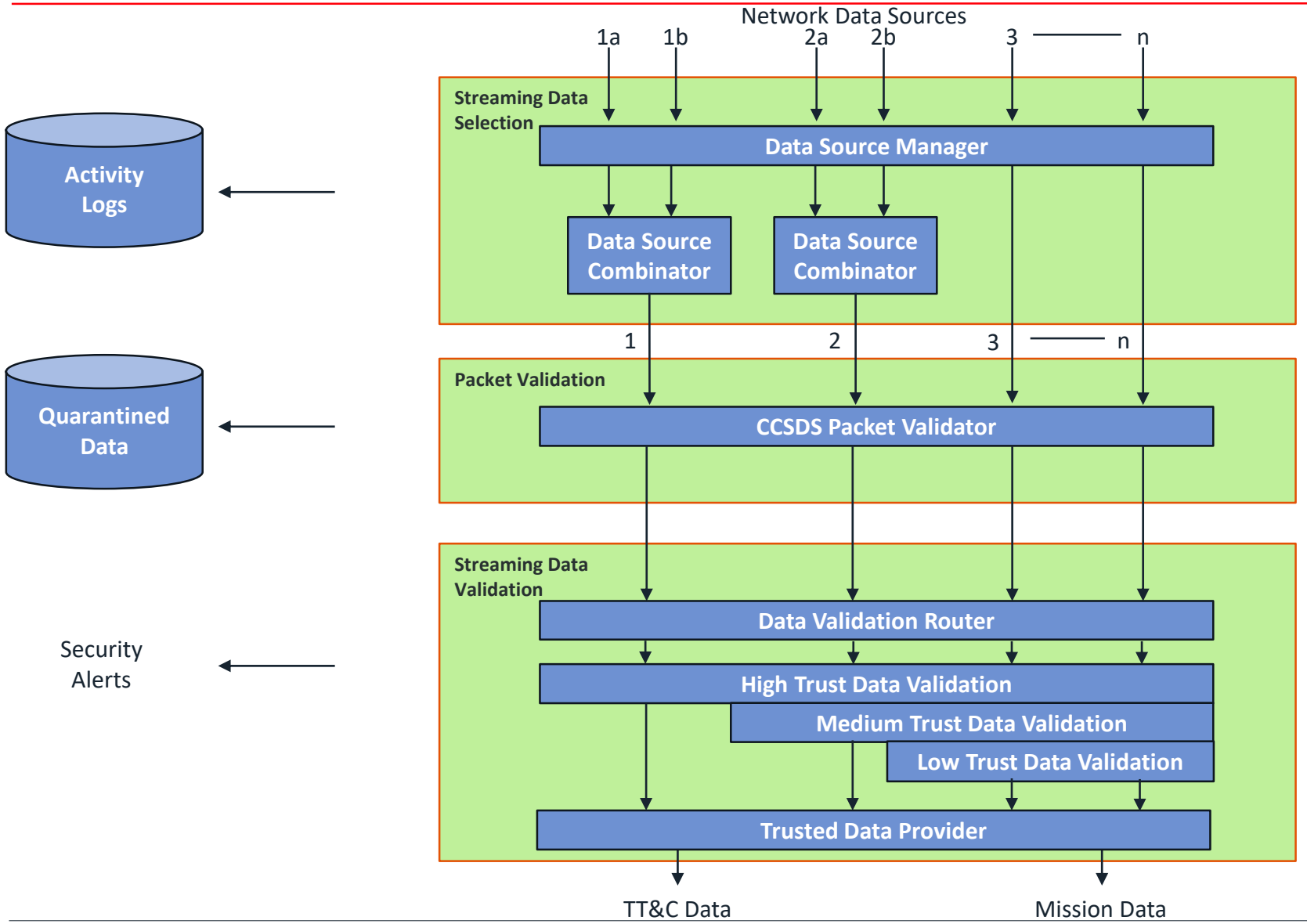
Secure Data Ingest Introduction

- Today's Ground Systems are typically engineered to provide high availability and integrity to insure mission success.
  - These missions often carry a NIST High level system categorization,
- As new missions become operational, the mission ground systems may leverage existing ground systems and ground stations
  - Existing ground systems are extended to handle the new missions
  - Existing partner or commercial ground stations provide satellite data uplink/downlink
- These extensions must be implemented without compromising existing system security
- This presentation describes a Common Service approach for implementing secure edge data ingest solutions to allow these enhancements

Secure Data Ingest Approach

- Communications between Partner and Commercial sites and the existing ground system occurs over IPsec Tunnels, which secures the data stream from the remote site.
- Existing Partner and Commercial sites will have their own cybersecurity controls in place, however, the data must be considered untrusted.
- This paper assumes that the overall information system includes layers of protection against common threats, such as existing firewalls and an integrated Intrusion Detection System (IDS)/Intrusion Protection System (IPS).
- The protections proposed in this paper for a Secure Ingest Common Service are meant to add additional layers of security to an enterprise infrastructure, with a focus on identifying security threats within the streaming data input sources.
- Common threats to streaming sources include:
  - Content Spoofing/Buffer Overflow/Man-in-the-middle:
    - The structure of the packets may be valid, but the payload could be corrupted.
    - Could simply be bad data, or it might contain malware. Buffers could be sent through a virus scan tool to check for malware.
- Denial of Service:
  - While many DoS attacks will be mitigated at the network security level, the system can be designed to support DoS mitigations that preclude the system from being bogged down to the point that other streams cannot be processed.

Secure Data Ingest Architecture



Data sources range from fully trusted U.S. entities to non-trusted, non-U.S. partners

The same data stream may be collected from multiple sources. A Data Combinator is provided to select or reconstruct the best source by fusing the inputs (subject to correlation delays)

Works for TT&C and Mission Data. Performs CRC, Reed Solomon decoding, etc

The level of data validation performed is configurable based on the data source. Validation is performed on streaming data (vs. files) and may include anti-virus checks, malware scanning, etc.

Data Source Manager

- Supervises incoming data sources.
- Provides the connection to the data source and collects metrics that support data source validation.
  – These metrics can include connection attempts, disconnects, reconnects and authentication errors.
- Includes a ‘Data Combinator’ feature which allows selecting and optionally fusing data from multiple sources.
  – Useful when a single data stream is acquired and received by multiple ground stations and further distributed to the secure ingest service for processing.
  – Selecting a data source for further processing based on data quality criteria is done in near real time
  – Fusing data requires time and data correlation between the different sources so it is subject to additional latency delays.

Packet Validation

- Validates various CCSDS protocol data units for proper sequencing and data content.
  - Level of validation is configurable: byte-by-byte, headers only, or none.
- When validating data units for headers only, the Packet Validator will check sequence counters and protocol fields for proper values, it will not examine the payload data zone.
  - This mode can be used to verify the correctness of the protocol.
- The Packet Validator can validate the following data types: CADUs, CVCDUs, VCDUs - AOS VCDUs or Packet Telemetry Transfer Frames, M_PDUs, B_PDUs, CCSDS Space Packets, Raw data.
- The Packet Validator has the following capabilities:
  - Statistics output at user specified intervals. Reports on errors and data throughput.
  - Reed-Solomon (10,6) VCDU header decoding and correcting (AOS format only).
  - Reed-Solomon (255,223) frame decoding and correcting.
  - Cyclic Redundancy Code (CRC) processing (check / ignore).
  - Detects and reports VCDU & Packet sequence errors, missing data units, data corruption, out of order reception, incorrect sizes.
  - Dump entire buffer on error, dump memory near the error, or no action.

Data Validation / Malware Detection

- Once past the CCSDS validation, there are several options available to scan mission data for malware.
- We are proposing a configurable data validation router to apply various data validation strategies based on the data source.
- For example, a data stream originating from a trusted U.S. entity would only go through the high-trust validation layer or none at all. Other data sources might go through the medium trust validation layer or the low-trust validation layer.
- Sending data through multiple validation layers will also increase processing time and overall latency but the system is configurable to allow the basic checks to work in near real-time.
- Additional scanning of the mission data relies on knowledge of the data itself.
- The proposed design assumes different protocols and data formats will be used for mission data, and would allow multiple types of Data Validator modules for input source validation.
- Additional checks for the TT&C data may also be possible
- Validation can occur for all data, using snap-shots or in parallel with source data streams.
  - Snap-shots validate every "nth" buffer thus handling high input data rates while providing strong data and protocol confidence.
  - Streams that have very high throughput, but deemed acceptable risk, may be forked; one stream sent to the data processing system to ensure low latency processing and the other through the scanning system to identify potential issues.

Logs, Alerting and Quarantine

- Identified risks generate an alert message that can be consumed by a connected system
  - Allow the data consumer to make decisions about what data to process.
  - The alerts would also be stored into the activity log.
- Data with errors could be quarantined or deleted, and not passed through to the consumer.
- If the approach taken were to quarantine data identified as containing a risk, then that data would be available for later analysis / forensic purposes.

Summary

- As new missions become operational, the most efficient ground system implementation leverages existing ground systems and ground stations
  - Existing ground systems are extended to handle the new missions
  - Existing partner or commercial ground stations provide satellite data uplink/downlink
- Secure Data Ingest adds additional security layers that enable this reuse of existing ground infrastructure by identifying security threats within the streaming data input sources.