CYBER WARNING RECEIVER (CyWRv)

AI/ML Driven, Low-SWaP Cyber Warning System

Bringing advanced, securely trained AI/ML anomalous behavior detection to the on-board, low-SWaP, tactical edge environment

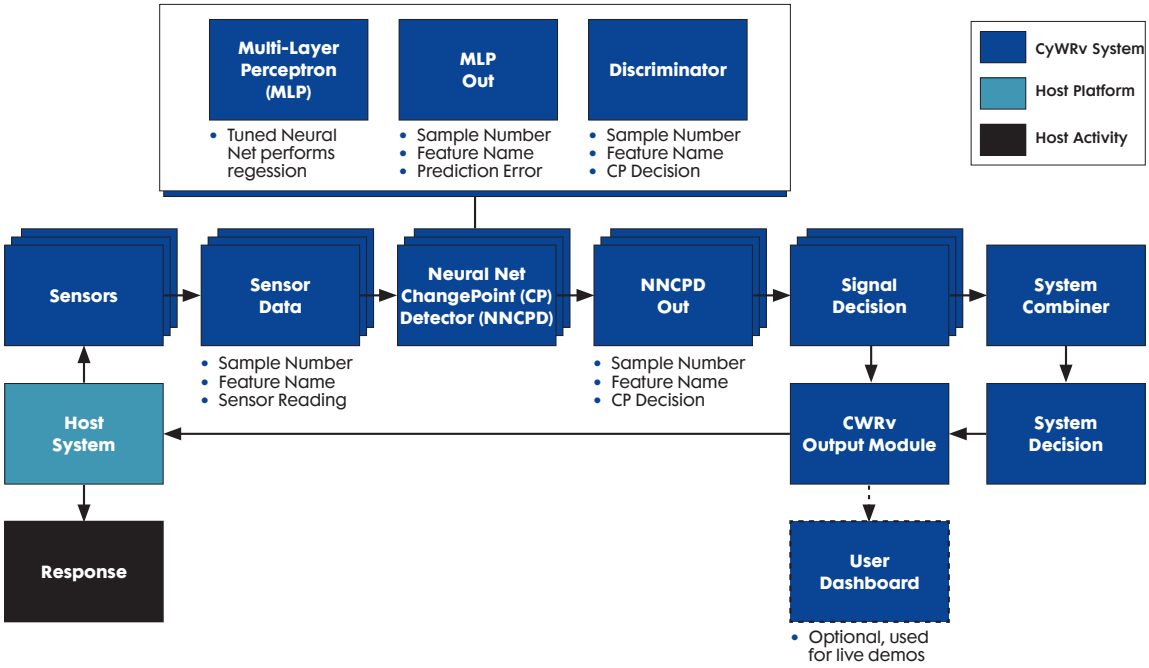
There are currently very few product offerings that prevent, mitigate, and recover from cyber-attacks for embedded weapon systems. Legacy and current weapons systems are unable to survive and operate in a cyber-contested environment or after exposure to cyber threats which prevent the completion of critical operational missions. Technologies need to be developed or enhanced in order to meet cyber survivability requirements authorized by the JROC's Cyber Survivability Endorsement Implementation Guide.

The Northrop Grumman Cyber Warning Receiver (CyWRv) is an anomaly detection system that detects cyber intrusions in real-time (streaming) within embedded systems (weapon systems, subsystems, test equipment, etc.) CyWRv applies a novel blend of signal processing and machine learning (ML) techniques to monitor data streams and process incoming data through a Single Stream Detector (SSD). Each SSD uses multiple algorithms to identify anomalies on a per-feature basis (for example, identify an anomaly in your latitude data or CPU usage metric). System-level (multiple SSD) analysis is also done to identify system-level anomalies and trigger an alerting mechanism, similar to a "check engine" light.

Unlike intrusion detection systems that attempt to detect signatures of historical adversarial exploits or enterprise solutions that are not tailored to the needs of weapon systems, our solution is a real-time, adaptive system that detects mission-impacting anomalies that is modular and is both platform and protocol agnostic. CyWRv uses neural networks to build regression (predictor) models, one for each signal under watch, and uses these models to detect all manner of anomalies. This adaptive approach enables our solution to detect even zero-day attacks.

Models are built offline for security and to allow for dedicated training and tuning. Open-source and internally-developed tools are used to assist in neural network tuning. Models are assessed using "loss functions," typically mean squared error, interpreted with respect to the signal's power. Prediction error is then fed through a Buffered Discriminator that analyzes error to identify the existence of a "change-point," or anomaly. Buffered Discriminators seek to find balance between robust detection and low false alarm and this balance is also tailorable to the host platform's needs.

CyWRv System Architecture

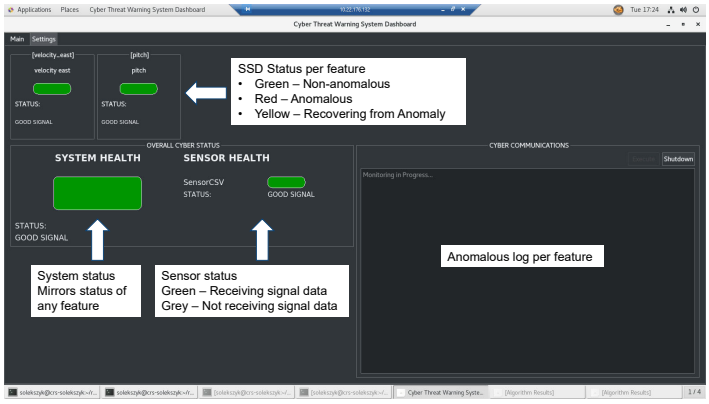


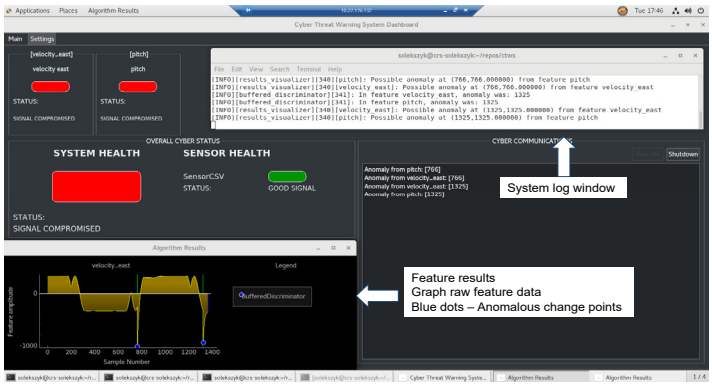
Key Features:

- Target Detection Rate (birth): 100%
- Target False Alarm Rate: <3%
- Target Data Ingest Rate: 50 Hz

Key Capabilities:

- CyWRv is a low size, weight, and power (SWaP) solution designed to accommodate embedded systems on resource-limited platforms
- Detection is ML-based and is adaptive (capable of detecting even a zero-day attack)
- ML models are tuned specifically for each signal under watch, which enables tailored execution and high performance to meet each customer's needs
- CyWRv has the ability to collect metrics from a host operating system (OS), processor, or Docker container. This allows CyWRv to monitor a host system's hardware to identify anomalies
- CyWRv has been implemented on a variety of host signals, including hardware parameters, raw sensor data feeds, as well as traffic metadata





For more information, please contact:
Northrop Grumman Mission Systems
Rusty Toth
Phone: 703-949-2335
roger.toth@ngc.com