Cyberdefense Platform for Weapon Systems (CyPaWS)

Open Source Flexible
Cyber Defense Orchestrator

Leveraging AI/ML to Identify Currently Undetectable Threats in Mission/Weapon Systems

The challenge for developing cyber resilient and survivable weapon systems lies in the differences between Enterprise Information Technology (IT) systems (IT) and Operational Technology (OT)/Cyber Physical systems (CPS). Solutions developed for IT networks do not translate to/fit the needs of weapon system environments where unique data types and threat vectors exist. Northrop Grumman has focused its Cyber Survivability Portfolio on cyber solutions that can mitigate high tier cyber threats for weapons systems. The Cyber Survivability Portfolio consists of several cyber capabilities that address key attributes, techniques, and approaches for survivable and resilient weapon systems; integrating these capabilities into an end-to-end architecture is a comprehensive Cyber System Engineering (CySE) process based on NIST 800-160.

The Northrop Grumman Cyberdefense Platform for Weapon Systems (CyPaWS) is an open-source flexible cyber defense orchestrator (multiple configurations offered) with deep learning-enabled anomaly detection for weapon system data. The anomaly detection capability is protocol agnostic and can scale with the complexity and size of the weapon system.

CyPaWS' architecture is modular, portable, and scalable, uses standardized open source tools, and is deployable to physical, virtual, and cloud environments.

CyPaWS expands the capability of COTS/open source tools to include operational technology data (e.g., control devices, Internet of Things [IoT], physical security, and facility data) and weapon system specific data, and is based on an open architecture that includes a data lake to ingest structured or unstructured data.

CyPaWS' architecture enables cutting edge AI/ML techniques to identify threats in mission/weapon systems that are currently undetectable by traditional, enterprise network-based IDS solutions. CyPaWS detects any unusual network traffic, including but not limited to: unauthorized or unusual commands, data or system exposure, and denial of service. Using these techniques, CyPaWS can focus a spotlight on insider threats, malware, misconfigurations of systems, and even maintenance related issues.

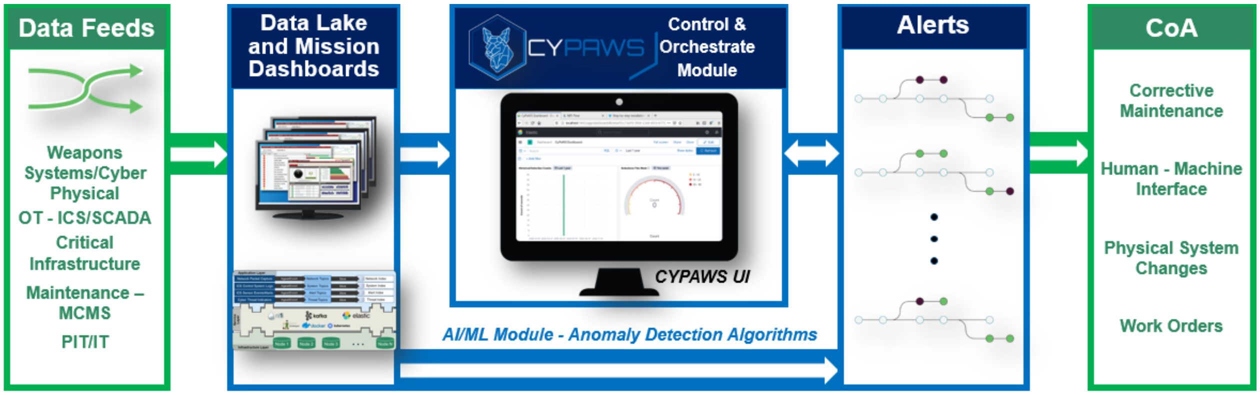
CyPaWS includes a user interface and dashboard based on the work of Northrop Grumman's digital transformation and user experience (UX) initiatives, which integrates well with an Elasticsearch backend.

Key Features:

- Protocol-agnostic anomaly detection trained on entirely normal network traffic enables detection of zero-day attacks
- Uses protocol-agnostic anomaly detection due to commonly found un-decodable protocols (e.g., proprietary, home-grown)
- CyPaWS' anomaly detection component, Cyber Bidirectional Encoder Representations from Transformers (CyBERT), leverages the state-of-the-art deep learning, modified for use on network traffic

Key Components:

- Elasticsearch – indexed storage
- FileBeat, Logstash – system logs
- Kibana – data exploration
- NiFi – complex data flows
- Wazuh, Tripwire – host monitoring demonstration (HIDS and FIM)



Data Feeds

Weapons Systems/Cyber Physical

OT - ICS/SCADA

Critical Infrastructure

Maintenance – MCMS

PIT/IT

Data Lake and Mission Dashboards

Control & Orchestrate Module

CYPAWS

CYPAWS UI

AI/ML Module - Anomaly Detection Algorithms

Alerts

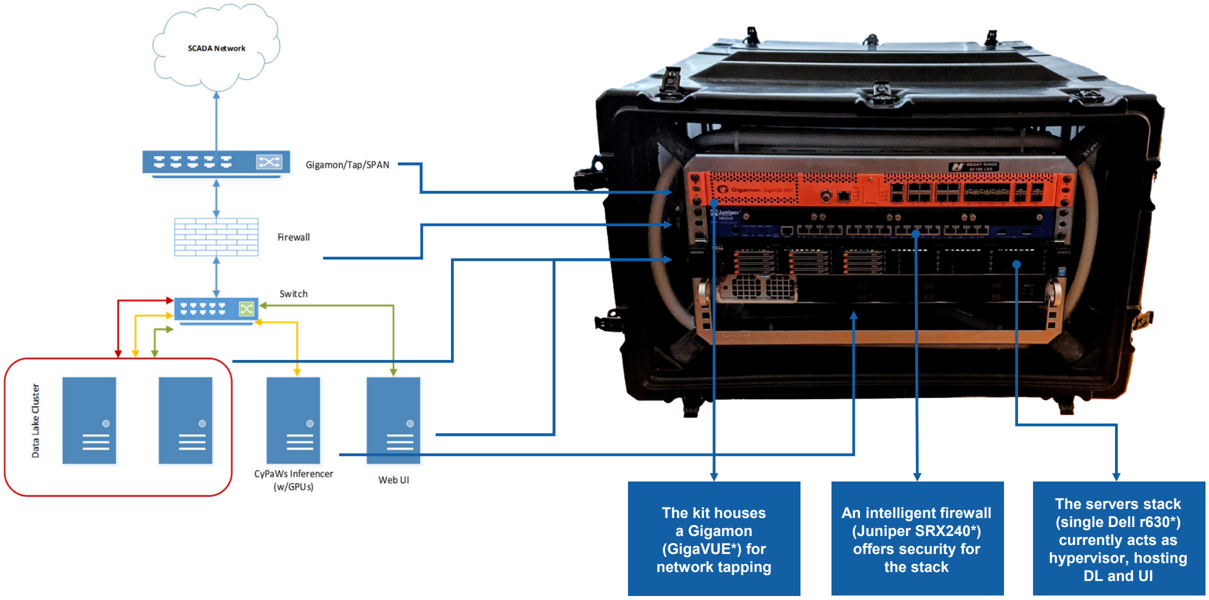
CoA

Corrective Maintenance

Human - Machine Interface

Physical System Changes

Work Orders



The kit houses a Gigamon (GigaVUE*) for network tapping

An intelligent firewall (Juniper SRX240*) offers security for the stack

The servers stack (single Dell r630*) currently acts as hypervisor, hosting DL and UI

For more information, please contact:

Northrop Grumman Mission Systems
Rusty Toth
Phone: 703-949-2335
roger.toth@ngc.com

Approved for Public Release: NG22-0957.

CS-17668c

northropgrumman.com