Global Cyber Security Challenges

THE PROBLEM
• Unable to continue Security Operations Center (SOC) operations at current pace of escalating cyber data threats
• Unable to process new cyber data with Traditional Data Management technologies

THE SOLUTION
• Establish platform to trigger data-driven, automated Cyber Defense at Machine Speed
• Deploy in Cloud with integrated Data Lake, Cognitive Analytics, and Workflow Automation for next generation Defensive Cyber Operations (DCO).
• Create Cognitive Analytic Fabric to operate with precision and low false positives

CURRENT STATUS
• Implement in Cloud with Microservices Architecture, Data Lake and Automation
• Design Active Cyber Defense Ecosystem for Continuous Delivery
• Cognitive Analytics with Artificial Intelligence and Machine Learning
• Design Analytics to detect known attacks, predict unknown attacks and remediate in real-time
Defensive Cyber Operations

• A Cyber Operations platform to disrupt and neutralize cyber attacks in real-time

• Automation for Next-Gen Defensive Cyber Operations (Humans on the Loop, Not in the Loop)

• Cognitive Analytics to trigger Defensive Cyber Operations actions

• Implementation based on Open Source, Open Architecture, and Open APIs

• Deployment at scale in Cloud or Hybrid-Cloud Environments

• Cost effective, Affordable, Resilient, Consistent, Dependable, Accurate, Speed
Defensive Cyber Operations Ecosystem

Data Lake & Mission Dashboards

- Data Feeds
  - AIS Indicators
  - CDM & NVD
  - Email Alerts
  - Net Events & Alerts
  - Host Events & Alerts
  - PCAP Data

Cyber Risk Map

- Cyber Ops & Mission Support
- Decision Making

Automation Playbook

- Actuators
  - Firewalls
  - IDSes & IPSes
  - Routers & Switches
  - Proxies
  - DLPs
  - Hosts
  - AIS & NVD

Cognitive Analytics

Active Cyber Defense Ecosystem
Data Lake Architecture

APPLICATION LAYER

- Configuration Dataflow
  - Ingest
  - Configuration Topics
  - Store
  - Configuration Indexes

- Vulnerability Dataflow
  - Ingest
  - Vulnerability Topics
  - Store
  - Vulnerability Indexes

- Network Dataflow
  - Ingest/Enrich
  - Network Topics
  - Store
  - Network Indexes

- Host Dataflow
  - Ingest/Enrich
  - Host Topics
  - Store
  - Host Indexes

SERVICE LAYER

- nifi
- kafka
- elastic
- splunk
- hadoop
- HDFS

INFR Structure LAYER

- NODE-1
- NODE-2
- NODE-3
- ... NODE-N
Cyber Data Lake

Fused Env on DATA LAKE

CDM NVD
Vulnerability/Configurations

Security Events
Customer Net/Host Data Capture

Malware Analysis
Advanced Malware Protection

Mgmt Control, Metrics & Production Control

AIS
Info-Sharing
Alert Data

Cyber Playbooks
Workflow Automation

Incident Reports
Detailed Analysis w/ Recommendations
Cognitive Analysis Framework

Cyber Attack Analysis | Cognitive Threat Engine 1
- Feature Engineering, Selection & Computation
- Trained Machine-Learning Model(s)
- Model predictions: probabilities

Cyber Attack Analysis | Cognitive Threat Engine 2
- Feature Engineering, Selection & Computation
- Trained Machine-Learning Model(s)
- Model predictions: probabilities
ACAP Features and Benefits

• Data Lake
  – Fast cyber data collection, transformation, and enrichment
  – Easily scalable with high throughput to support large mission operations
  – Quick view of operation status on mission dashboards

• Playbook Automation
  – Well defined processes in the form of digitized cyber operations workflows
  – Automated execution of cyber playbooks via analytic triggers
  – Built-in customized Case Management for customer mission

• Cognitive Analytics
  – Detect unknown threats
  – Deep learning to analyze cyber threats using anomaly, clustering, and classification
  – Artificial Intelligence / Machine Learning based knowledge management
THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN