TAC MEETING

CanSSOC Architectural Overview

FEBRUARY 19, 2019

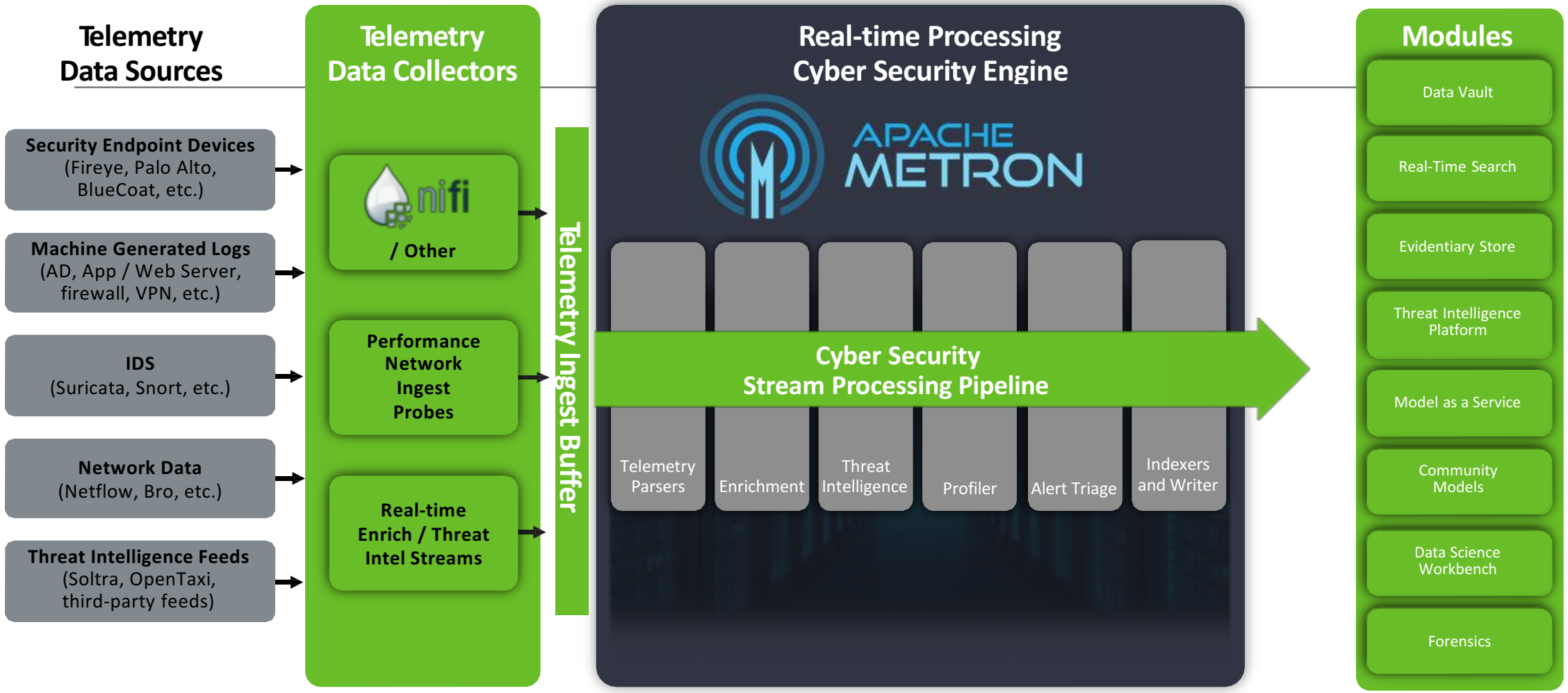
ADDRESSING PAIN POINTS

- Efficiency through collaboration
- Standardizing tool sets and telemetry
- Detection and integrated Action
- Common platform enabling quicker assessment and analysis

NEEDLE IN A HAYSTACK

PLATFORM – APACHE METRON

- Real-Time ingestion of application and system logs
- Real-Time cyber security dashboard and cyber workbench
- Real-Time ingestion, correlation and enrichment of NetFlow telemetries
- Real-Time integration of Cyber security feeds
- Advanced statistical and machine learning models to detect cyber security attacks
- Integration with existing SIEMs and enterprise assets


Telemetry Data Sources
Security Endpoint Devices (Fireye, Palo Alto, BlueCoat, etc.)
Machine Generated Logs (AD, App / Web Server, firewall, VPN, etc.)
IDS (Suricata, Snort, etc.)
Network Data (Netflow, Bro, etc.)
Threat Intelligence Feeds (Soltra, OpenTaxi, third-party feeds)
Telemetry Data Collectors
nifi
/ Other
Performance Network Ingest Probes
Real-time Enrich / Threat Intel Streams
Telemetry Ingest Buffer
Real-time Processing Cyber Security Engine
APACHE METRON
Cyber Security Stream Processing Pipeline
Telemetry Parsers
Enrichment
Threat Intelligence
Profiler
Alert Triage
Indexers and Writer
Modules
Data Vault
Real-Time Search
Evidentiary Store
Threat Intelligence Platform
Model as a Service
Community Models
Data Science Workbench
Forensics

- Ingest:
  - Apache NiFi: syslog, socket, file, web services, SQL, RDBMS, Windows Event Log, FTP, MQ, JMS
- Parsers:
  - Cisco ASA
  - Bluecoat
  - Fireeye
  - Palo Alto
  - SourceFire
  - WebSphere
  - Snort
  - Bro
  - YAF (Netflow, IPFIX)
  - Grok (Custom)
  - Java (Custom)
  - JSON
  - Applications: DHCPD, AD
- Enrichments and threat feeds:
  - Geo
  - Whois
  - HBase
  - JDBC
  - Stellar
  - CSV
  - Stix, Taxii threat intel feeds
- Analytics features:
  - Profiler
  - Model Services
  - Threat Triage
- Indexing and search:
  - Elasticsearch, Kibana
  - Solr
  - HDFS
  - Kafka
- Data science features:
  - Spark Machine Learning
  - Zeppelin notebooks and reporting
  - Wide partner eco-system

ASSET & LOG INTAKE

- Real-Time ingestion of application and system logs
- Real-Time cyber security dashboard and cyber workbench
- Real-Time ingestion, correlation and enrichment of NetFlow telemetries
- Real-Time integration of Cyber security feeds
- Advanced statistical and machine learning models to detect cyber security attacks
- Integration with existing SIEMs and enterprise assets

LOCAL DATA COLLECTOR - VM

- A VM can be built to installed at the member institutions to facilitate log collection and queueing in case of external network disruption.
- Bootstrap process to customize the server, RAM, vCPU, Storage location and size, IP Address etc.
- Multiple options for VM base;
  - Virtualbox and Packer
  - VMWare and Packer
  - Docker

A FEW “WINS”

- **SOC Analyst**: Won’t spend days looking at alerts created by rules when only a few warrant action – the goal is to deliver actionable alerts. Lower level tasks such as event log review that is currently manual can be automated and offloaded to CanSSOC.
- **SOC Manager**: Automatically create incidents/cases with integrated workflow systems
- **Forensic Investigation**: “Just-in-time evidence collection response” transforms data in real-time
- **Security Platform Engineer**: Single platform to manage and operate the ingestion, processing of data and feeds
- **Security Data Scientist**: Perform data science activities: train, evaluate and score analytical models

Service Request Integration

- Use Metron to automate service request creation with member institutions via API
- Integrate local service requests systems and build interfaces if the service request platforms require it to integrate with CanSSOC's service request system
- Develop Categories and Sub-Categories for request tracking and prioritization;
  - Attack in Progress
  - Attack Blocked
  - Attack already detected at member institution and blocked

Service Request Cont’d.

- Prioritize requests according to each member institutions assets
- Alert based on each institutions escalation process (TBD).
- Document and integrate CanSSOC Service Desk processes with local Incident Response procedures and Contact processes.
- Develop response plan and Use Cases for incident response processes and integrate into the Service Desk.