ESSENCE → GRIDSTATE

CEDS Program Review

Robert Larmouth, PM, Craig Miller, PI

December 2016

PROJECT SUMMARY - ESSENCE

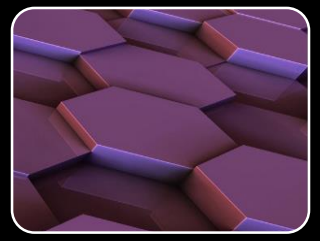
- Cost: $2,813,548 Federal Share + $1,125,239 cost share
- Partners: PNNL, CMU, Cigital, five (5) utility cooperatives
- Project Purpose: Anomaly detection and remediation for utility networks
- Five layer approach and objectives:
  - Real-time capture of utility network traffic without increasing attack surface (Layer 1)
  - High speed data processing – dynamically reconfigurable (Layer 2)
  - Boolean composer to explicitly specify rules; network mapper to identify unfamiliar addresses; machine learning classifier (Layer 3)
  - Support for decision makers in analyzing anomalies for remediative action (Layer 4)
  - Making changes in the network in response to anomalous behavior (Layer 5)
- Results: all objectives met in layers 1-4; layer 5 needs additional work

FIVE APPROACHES TO CYBER SECURITY

Eliminate the Bad Guys

Protect the Perimeter

Reduce Vulnerabilities



Segment the Architecture

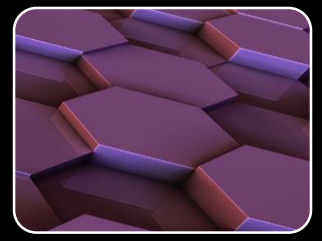
React to Breach

FIVE APPROACHES TO CYBER SECURITY

Eliminate the Bad Guys

Protect the Perimeter

Reduce Vulnerabilities

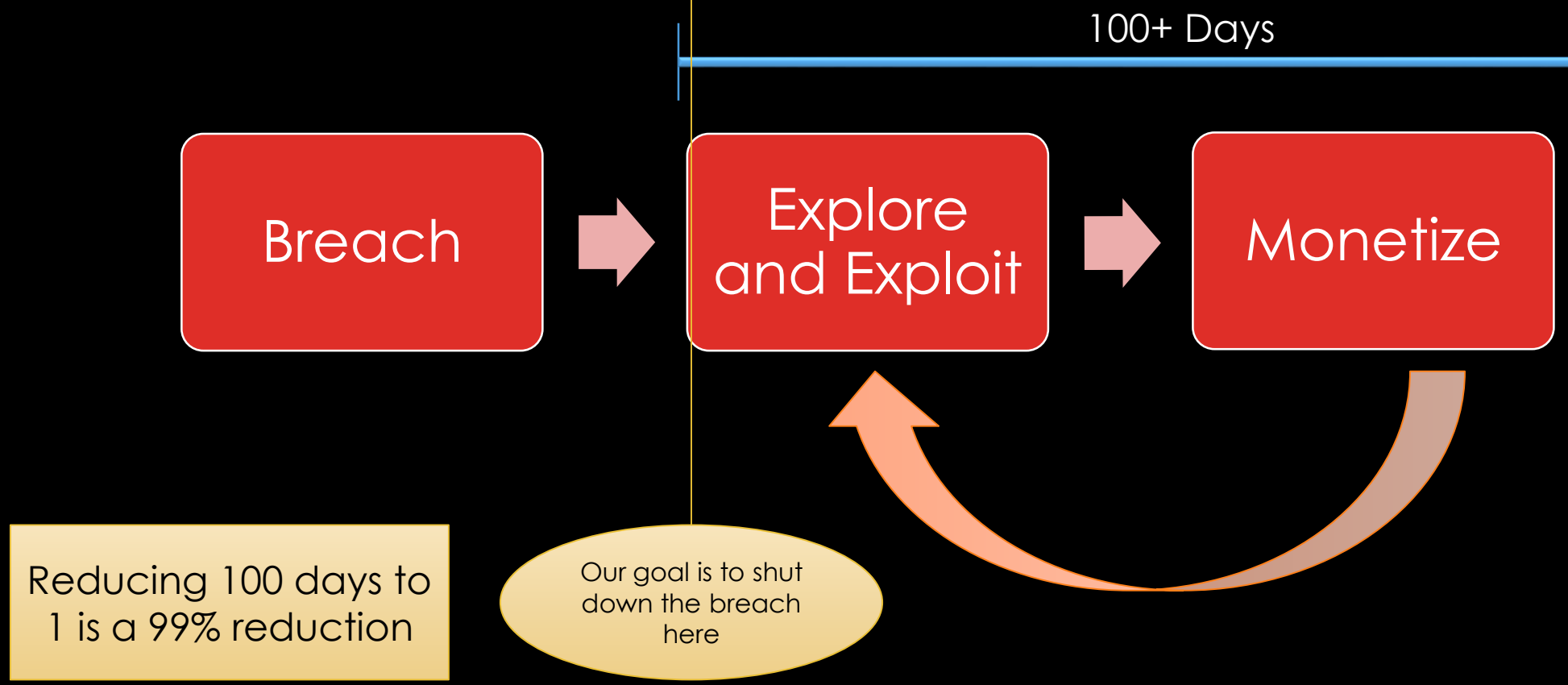


Segment the Architecture

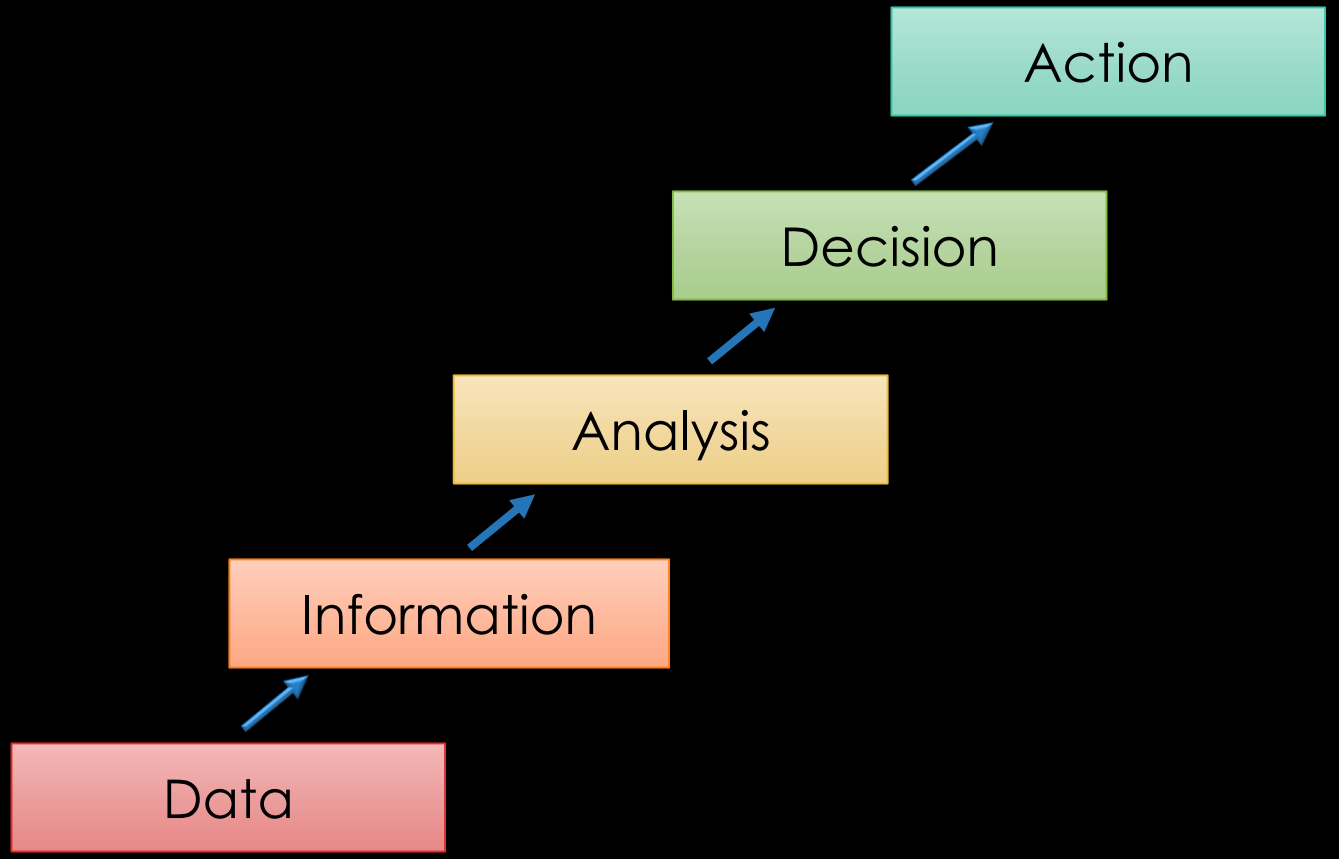
React to Breach

100+ Days – Breach to Detection, Start of Remediation

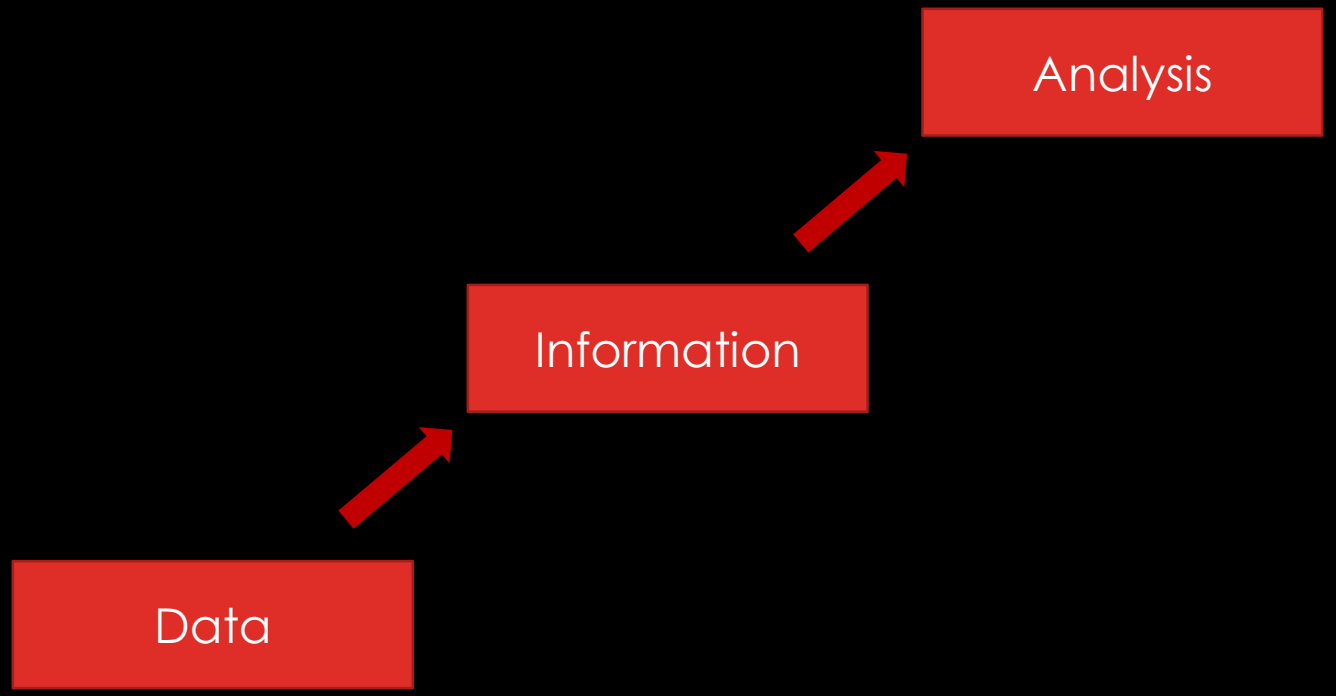
OPPORTUNITY FOR IMPROVEMENT



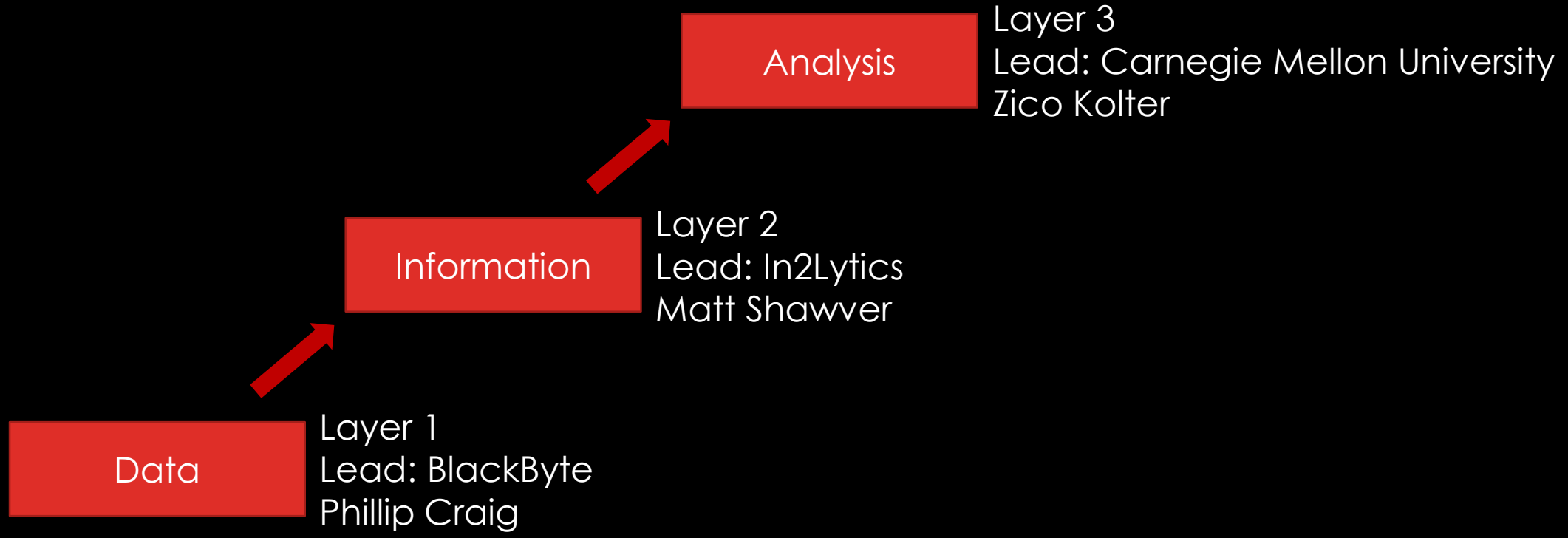
HOW APPLICATIONS ARE BUILT



ESSENCE TECHNICAL DEVELOPMENT



ESSENCE TECHNICAL DEVELOPMENT



Data

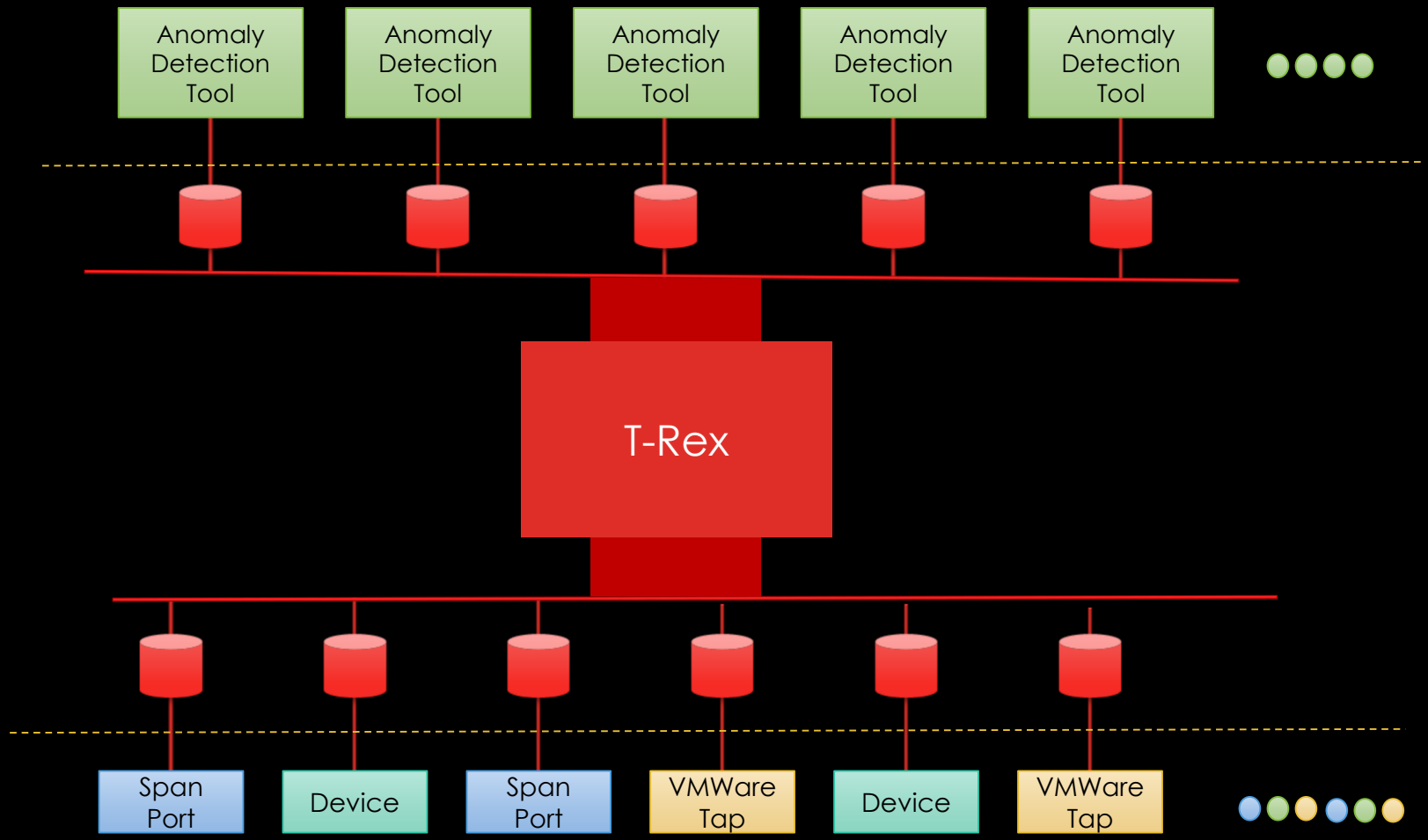
LAYER 1
LEAD: BLACKBYTE
PHILLIP CRAIG

Work to Date

- New Device
- Deployments: See Next Slide
- Protocols
  - Sensus Meters
  - MultiSpeak
  - CMEP
  - *DNP3 ← in process*
  - *ModBus ← in process*

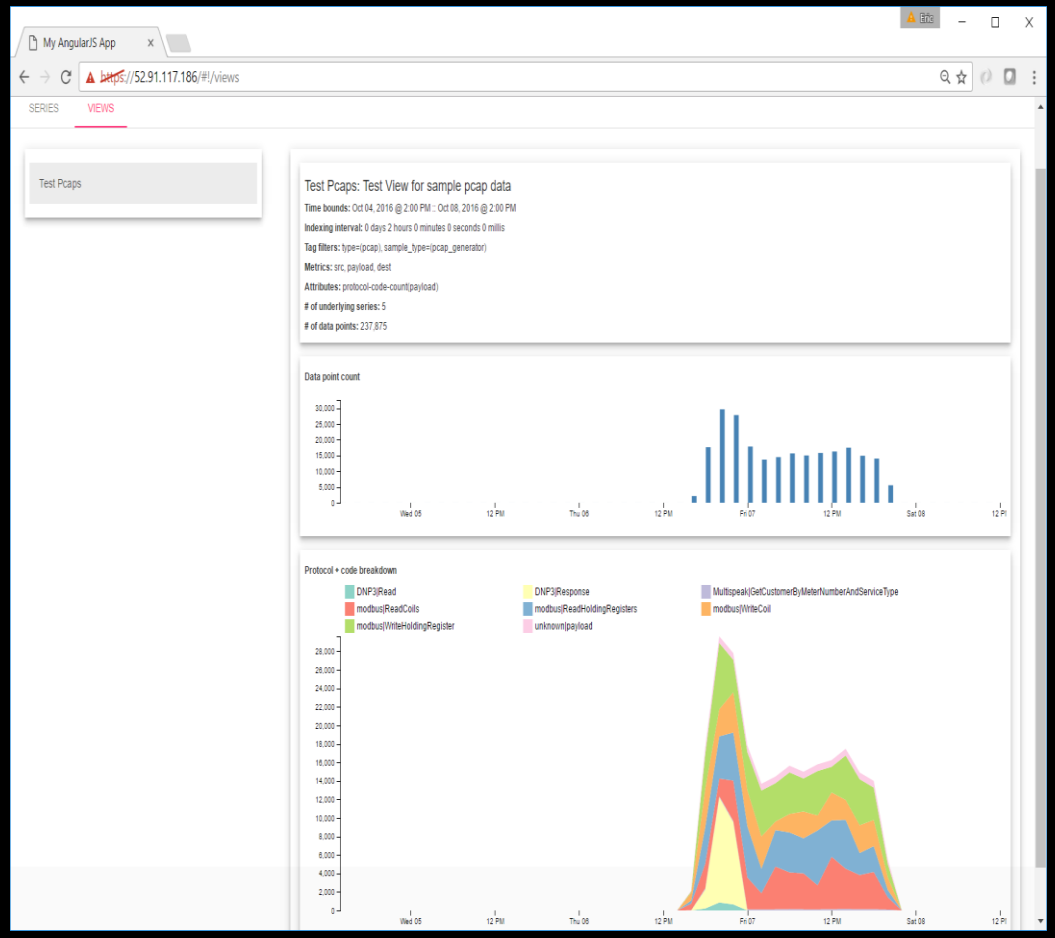
INFORMATION

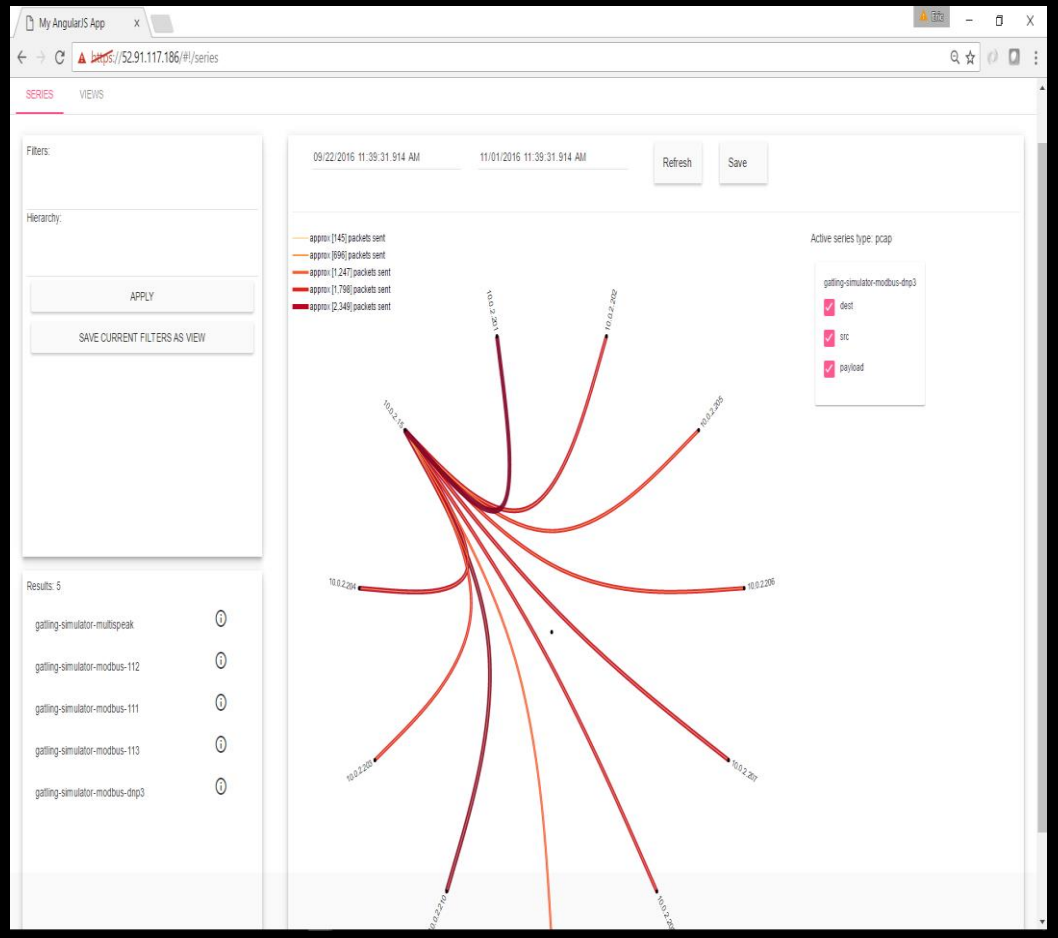
LAYER 2
LEAD: IN2LYTICS
MATT SHAWVER



INFORMATION

LAYER 2
LEAD: IN2LYTICS
MATT SHAWVER





LAYER 2 PERFORMANCE / GOALS

- SCADA
  - 5000 sensors, 2 second rate
- AMI
  - 500,000 sensors, 15 minute rate
- PMU
  - 500 sensors, 60x per second rate

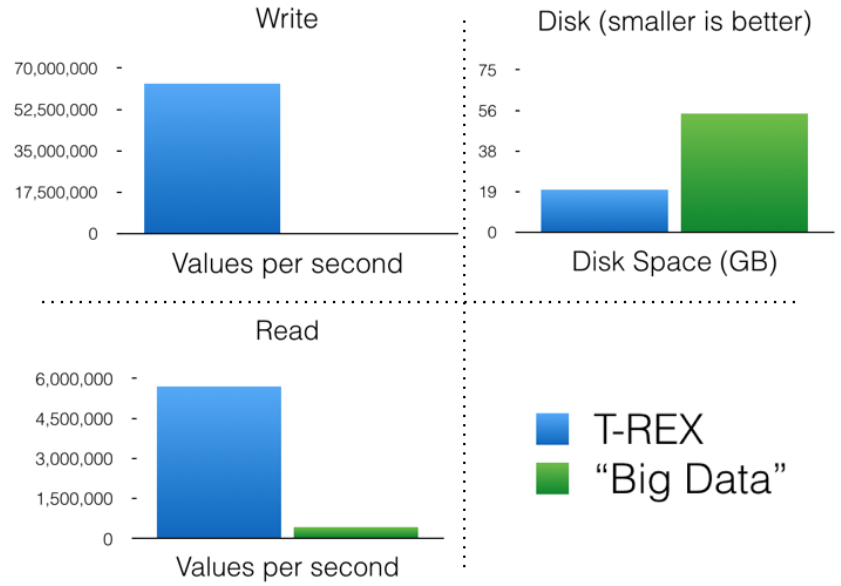
- Goals
  - Support real-time and bulk load
  - Support immediate read
  - All data into the same DB
  - Don't lose any information
  - Fast <sensor, time range> queries
  - Be as disk space efficient as possible
  - Provide reasonable persistence guarantees
  - Idempotent writes
  - Rollback partially failed writes

T-REX VS CASSANDRA

- Most grid analytics problems are I/O performance bound…
- Benchmark
  - 1000 sensors
  - Recorded synchronously in groups of 5
  - 4 million values recorded per sensor
  - 4 billion total measured values
  - Values are random (not compressible)
  - Write all data, then read all data for one measurement

	T-REX	"Big Data"	Improvement
Write (s)	63 (1 min)	70555 (19.5 hrs)	1120x
Write (values/s)	63,500,000	56,700	
Read (s)	0.7	9.7	14x
Read (values/s)	5,700,000	412,000	
Disk (GB)	19.61	54.83	3x
Disk (bytes/value)	4.9	14.7	

30x with real data (estimated)

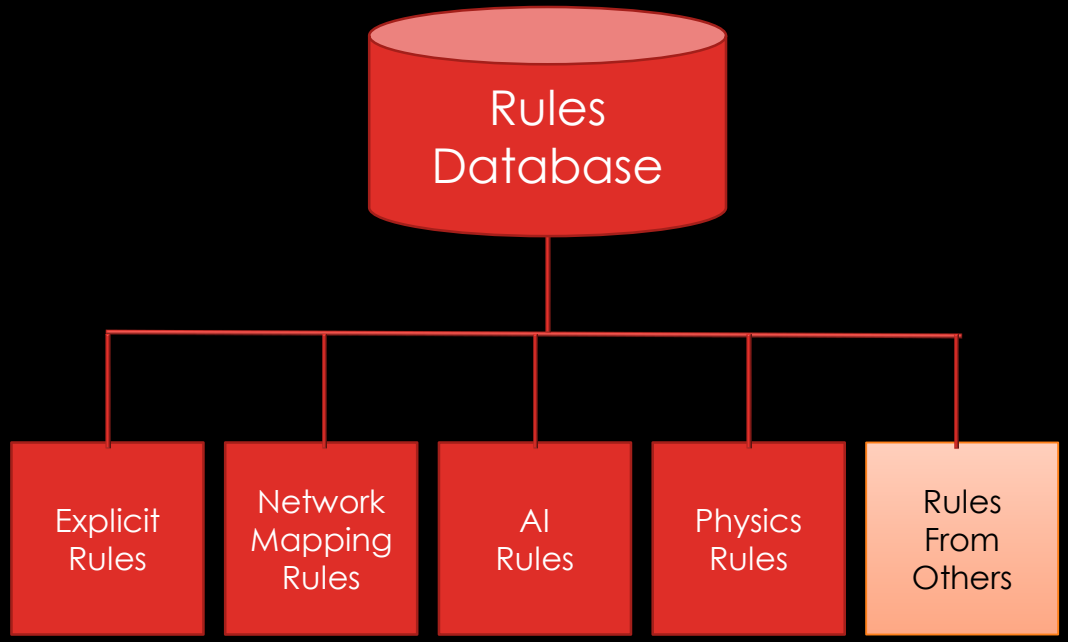


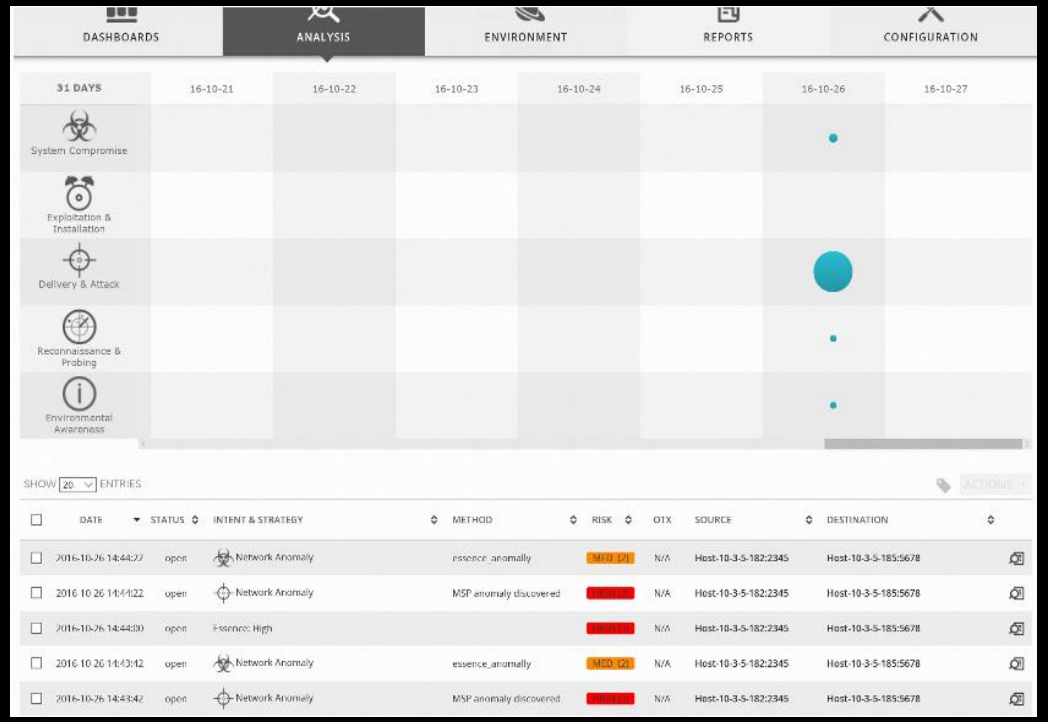
- T-REX can provide single server performance that requires 100's of "big data" servers
- Full access to data from engineering tools and third party apps
  - Avoid collecting data from 100's of machines in the cloud
  - Enables forensics, real-time, and multi-vendor applications that are difficult/impossible in the cloud
- Small footprint on-premise deployment
  - Reduces cloud and system admin costs
  - Lower initial and recurring costs
  - Reliability: Less reliance on service providers (ISP, cloud)
  - Reliability: Smaller hardware footprint

ANALYSIS

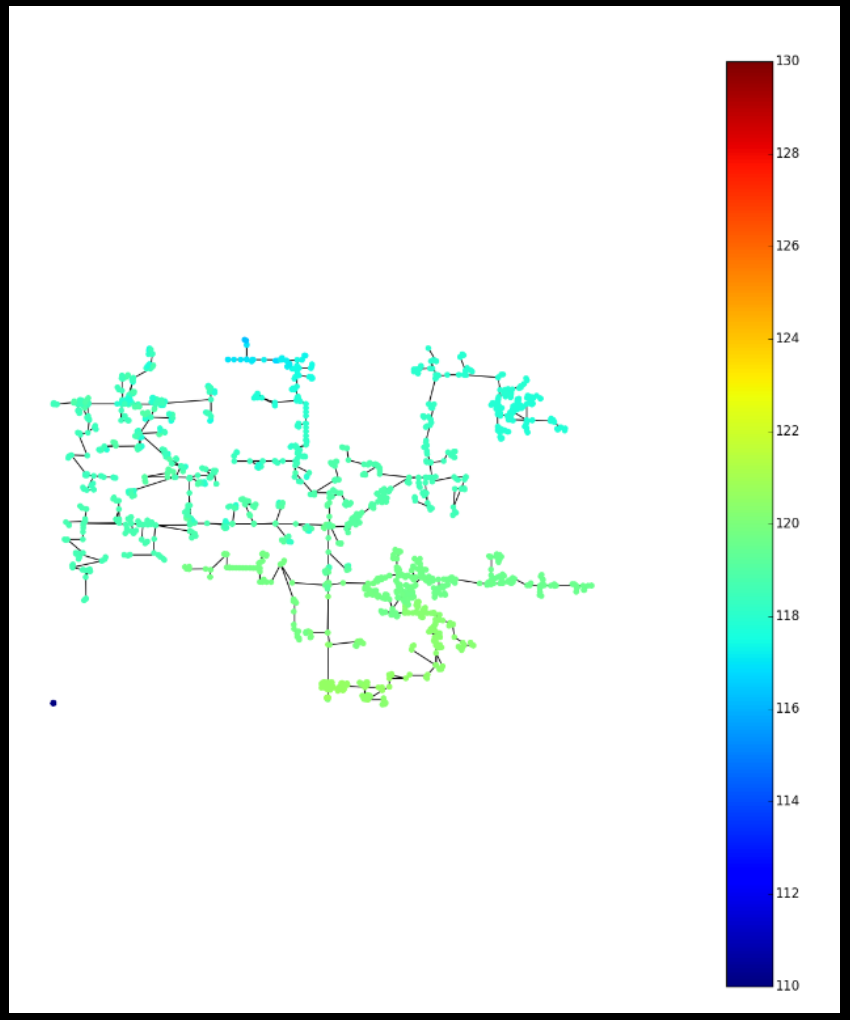
LAYER 3
LEAD: CARNEGIE MELLON
ZICO KOLTER

Goal: Unified Rules Syntax





TESTING: ABEC FEEDER



TEST FILE

Quads: time, node number, voltage, current, frequency, angle
Control signal: time, node, control signal

June 2016
30 days x 24 hours x 12 mesurements per hour x 200 nodes = 1,728,000 records
+ 1000 control records

1. IMPORT FEEDER MODEL
2. MODIFY GRIDLAB-D TO EXPORT QUAD AT EACH TIME CLICK
3. MODIFY GRIDLAB-D TO EXPORT CONTROL SIGNALS

GOING TO MARKET

SEDC

+

MILSOFT
Utility Solutions

NRTC

GOING TO MARKET

n-dimension solutions

260 SEDC

ALIEN VAULT™ + 1000 MDFT Utility Solutions

500 NRTC