it's about time

# Kx for Cyber

Mike Thomas
SVP Cyber, Kx

Kx25
May 18, 2018

# Overview

- Introduction
- Cyber Landscape
- Kx For Cyber
- Applying kdb+ to Cyber
  - Customer
  - Ourselves

# Cyber Landscape

- Increasing # of attacks/data volumes
- Attacks increasingly visible
- 3-5M $ per compromise
- 230B market by 2021
- 100 days to detect a compromise
- 60 days to remediate
- Huge growth in Cyber startups
- 3.5M unfilled Cyber jobs by 2021
- SecOps/DevOps, Analysts, Developers

# Cyber Data – All the things

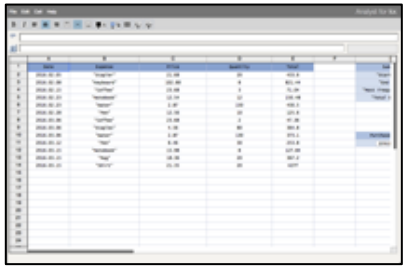
- Structured
- Unstructured
- Varied
- Time Series
- Fusion
- Visualization
- Real Time
- Historical
- Relationship/Graph
- Edge to Cloud

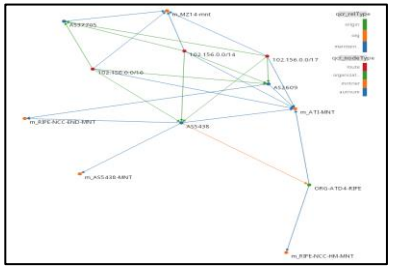
# Kx for Cyber

- Rich environment combines traditional SIEM with data exploration at scale

**Traditional SIEM**
- Ingest
- Monitor
- Alert

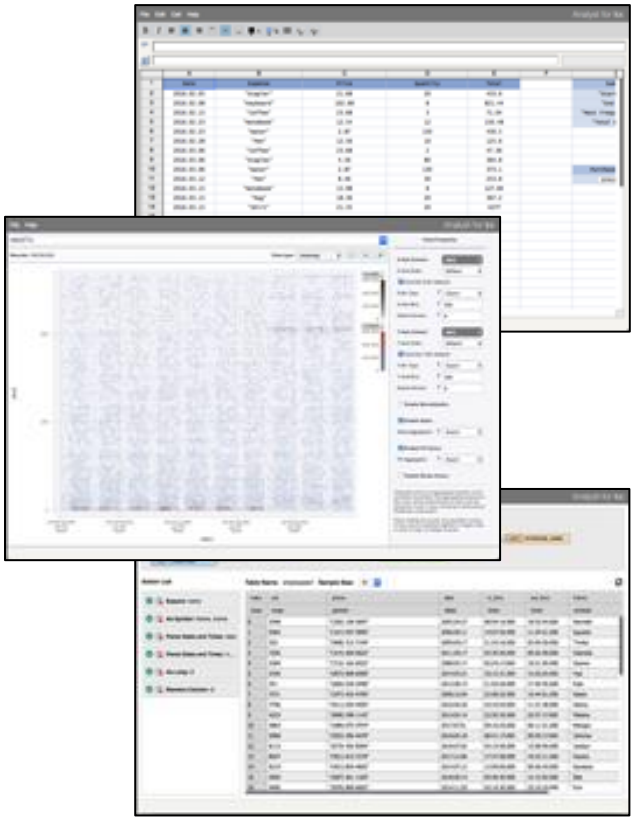
**Adhoc Data Exploration**
- Enrich
- Transform
- Analyze
- Query
- Visualize



# Think, Compute, See

- **Rich interactive environment for developers**
  - Editor, Differ, Debugger, Visual Explorer
  - Built-in TDD, Linting, QuickCheq
  - Collaborative
- **Self-serve tools for analysts**
  - Import and export wizards
  - Transform, filter and query UI's
    - Compile workflows to functions
  - Real-time adhoc data visualization tools
  - Custom visualizations using grammar of graphics
  - Analytic Spreadsheet (cells can be huge data sets)
  - Text Analytics (NLP)



# Speed and performance

- Raw execution speed
- Think, Compute, See!
- Time to failure
  - Fail fast
  - Expand art of the possible
- Rapid ad-hoc analysis
  - Expressiveness of language
  - Rapid prototyping
  - Time to visual
- Force multiplier in a skills shortage world

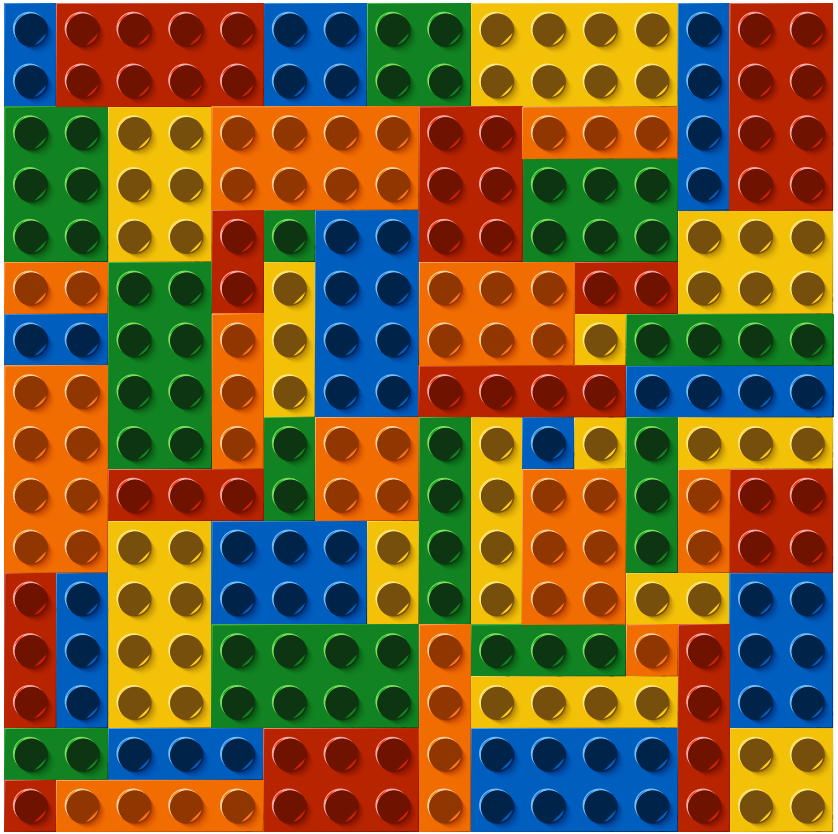
***"Helps me develop analytics at the speed of thought - as opposed to the cycle of: write program, run program, inspect outputs and then go through the whole cycle again"***

***"The quick responsiveness enables the analytic aspect to remain Cached in my mind to more quickly adjust it as I work things through"***

***Kx for Cyber customer***

# Integration

- Use the best, build the rest
- Play well with others
- Cyber requires a polyglot approach
- Leverage existing investment
- Must integrate with existing systems
- Fusion
  - C/C++
  - Python
  - ML

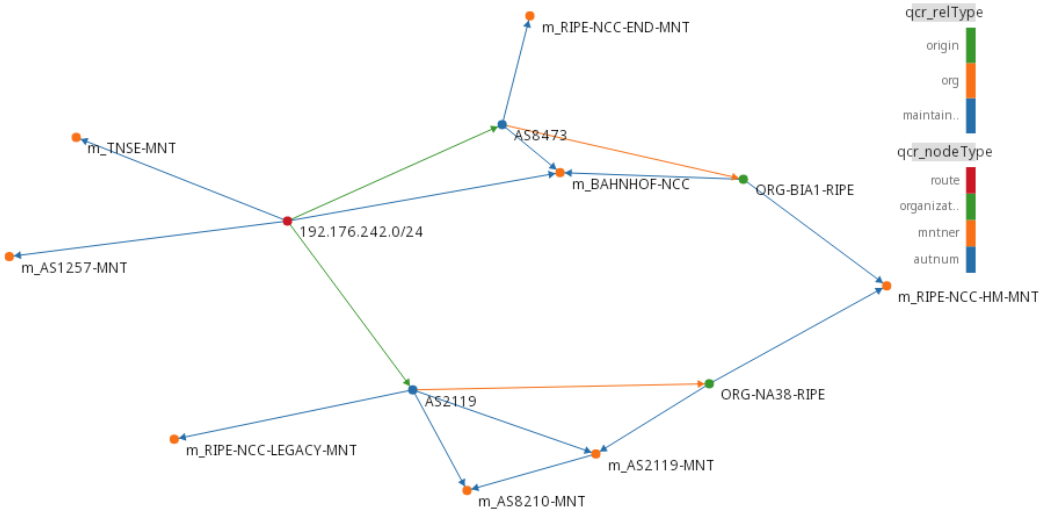


# Deploy from edge to cloud

- Analytics at the Edge
  - Hardware constraints
  - Bandwidth constraints
  - Locality of action
- kdb+ provides
  - Unified runtime
  - Small footprint
  - Push/pull real-time updates
  - On the fly reconfiguration

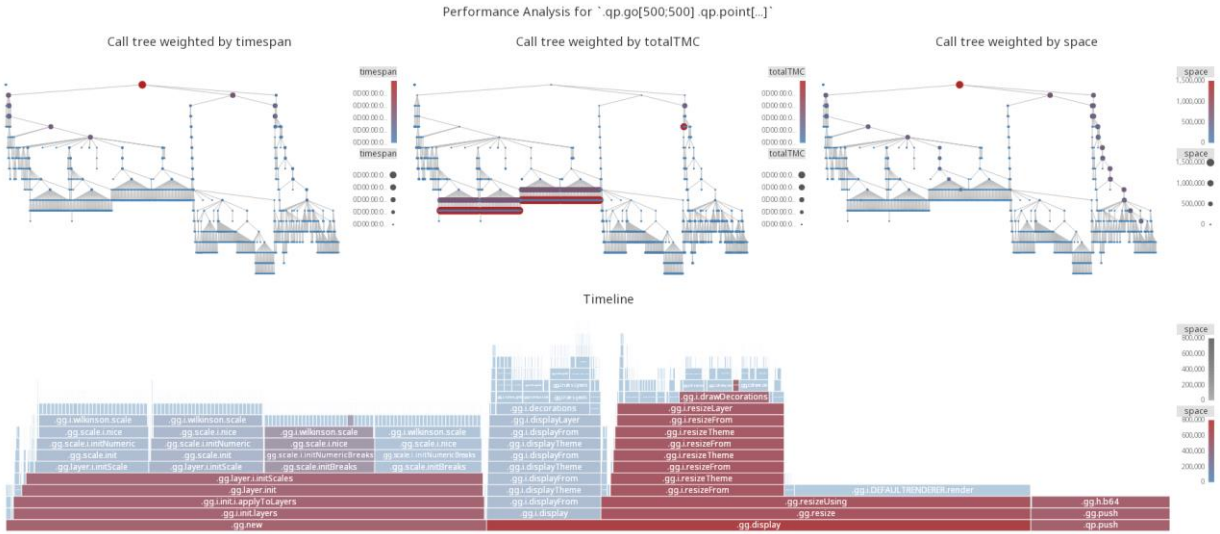
# Leveraging kdb+ to build Kx for Cyber

- kdb+ is a general purpose programming language
- Kx for Cyber ~90K lines of q/k
- DSLs
  - small, custom languages
  - in-process data locality
  - STIX -> kdb+ parser
- Graph DB
  - 2200 lines of q to implement DB
  - 300 to implement Cypher



# kdb+ for dev tooling

- Profiler
- qoverage
  - Test coverage tool
- qcumber
  - BDD
- quickcheck
  - Property-based testing
- qlint linter



# Thank You!