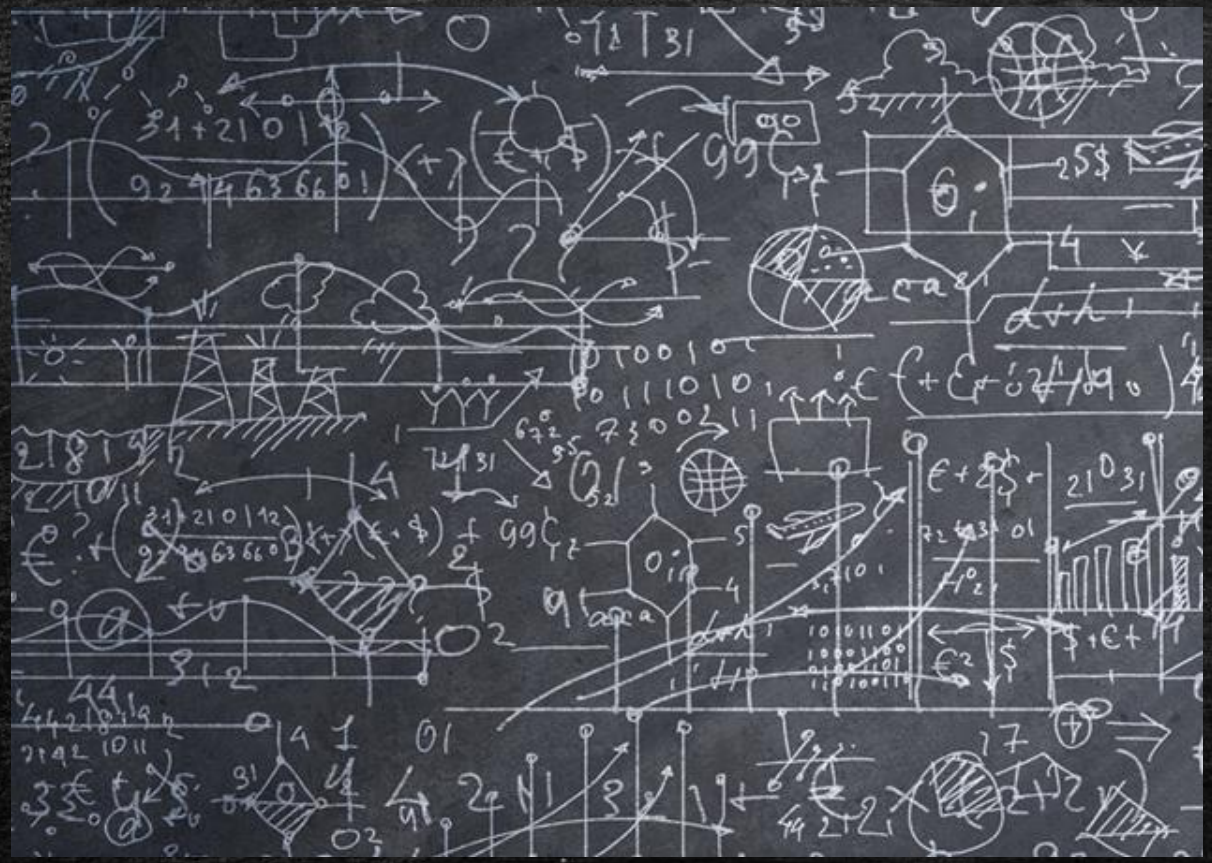
Complexity in Cybersecurity



Steven Schiavoni

C-ISR Team Lead

(SOC Manager)

Mission Defense Team

412th Communication Squadron

Edwards Air Force Base, CA

DISTRIBUTION STATEMENT A - Approved for public release; distribution is unlimited. 412TW-PA-22173

Current Mission and Background

The 412th Test Wing:

- Plans
- Conducts
- Analyzes
- Reports on

all flight and ground testing of aircraft, weapons systems, software and components as well as modeling and simulation for the USAF.

There are three core components for this mission: flying operations, maintenance, and engineering.

The 412CS Mission Defense Team (MDT)

- The Wing Commanders organic DCO-IDM element
- Focused on defending Test Mission
- NOT compliance focused

Supported by an Enterprise Scale Network:

- Thousands of endpoints/network devices
- Multiple classifications
- On Prem and Cloud Data Centers
- Hardware and software unique to test

Capabilities:

- Threat research
- Network Security Monitoring
- Incident Response
- Digital Forensics

Who Am I?

- SOC Manager
- Lead Planner
- Threat Research
- Project Manager

What is Complexity?

This?

Common Usage:

- Consisting of many components and interactions closely connected
- Cannot be easily separated without destroying essence of the whole
- Resistant to simplification

The whole is something else than the sum of its parts…
-Aristotle

Or This?

Kolmogorov Complexity:

The shortest program x that produces output y
The shortest specification k that produces results z

Maybe This?

$n = Number\ of\ Basic\ Elements\ of\ Structure$
$N = Number\ of\ Possible\ Substructures$
$D = Degree\ of\ Complexity$
$C = Complexity$

$$D = \frac{N}{n} \qquad C = DN$$

Context for Discussion

Test and Evaluation is a data driven endeavor

The combination of the two is ripe for opportunity and challenge
Not the least of which is driven by volume and interrelationship of data
Hence: Complexity is all the more relevant

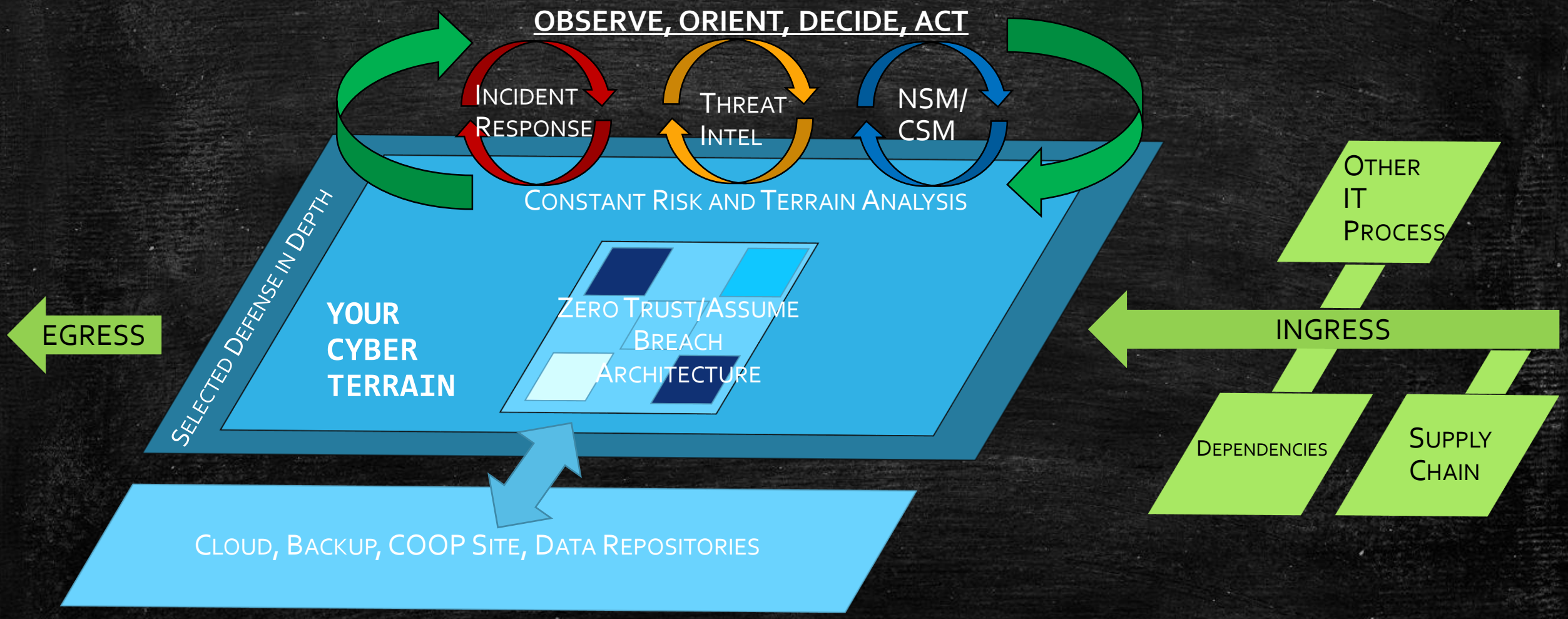
Information Security is a Data Drive Endeavor

Origins of Complexity in Cybersecurity

Cybersecurity: The Platonic Ideal…

How do you decrease the chances of a material impact to mission due to a cyber incident?

- Rick Howard
Cybersecurity 1st Principle



Gives Rise to Emergent Complexity…

Technical Complexity

Mission Systems

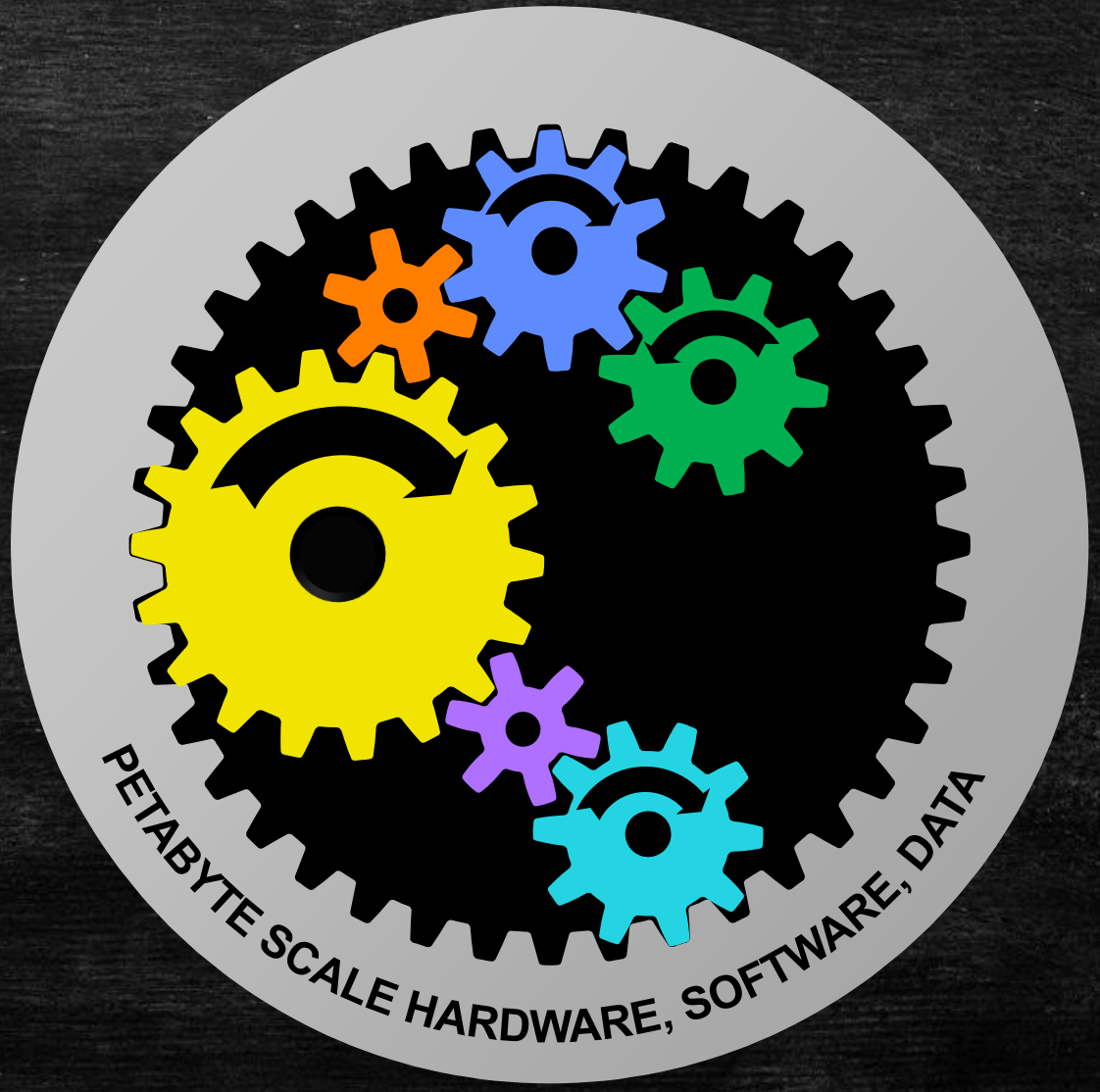
Security Data Collection

Threat Intelligence Platform

Security Data Analysis

Security Data Presentation

Monitoring and Incident Response



ADMINISTRATIVE COMPLEXITY

- HR
- Acquisition
- Budgeting
- Approvals

Authorities Race Condition

- Incident Coordination
- Reporting
- Access Requests
- Authorities

Review Board

Approve?

- C2
- COMREL

Reporting

Project Management

The Psychological Factor

Biases

Available Info

Cognitive Load

Confirmation

Absence of evidence is TOTALLY evidence of absence

Base Rate

How often does that REALLY happen?

Satisficing

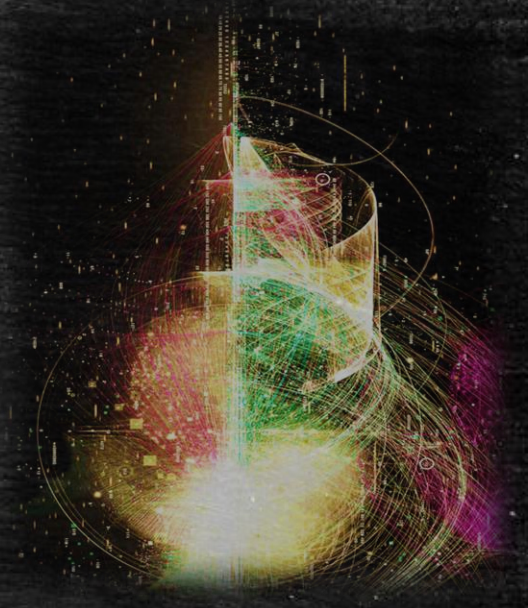
Meets RMF? Good enough.

Framing

Heuristics

Domain Knowledge

Other Factors



DECISION

Under Conditions of Uncertainty

Coping with Complexity

A lot less technical than some may have hoped…

But not nearly as managerial as others assumed…

Fundamentally an Issue of Problem Solving…

Mindset:
- Operational
- Defensive

Structured Problem Solving

Graphs Not Lists

Know Your Threats

Know Your Risks

Know Your Terrain

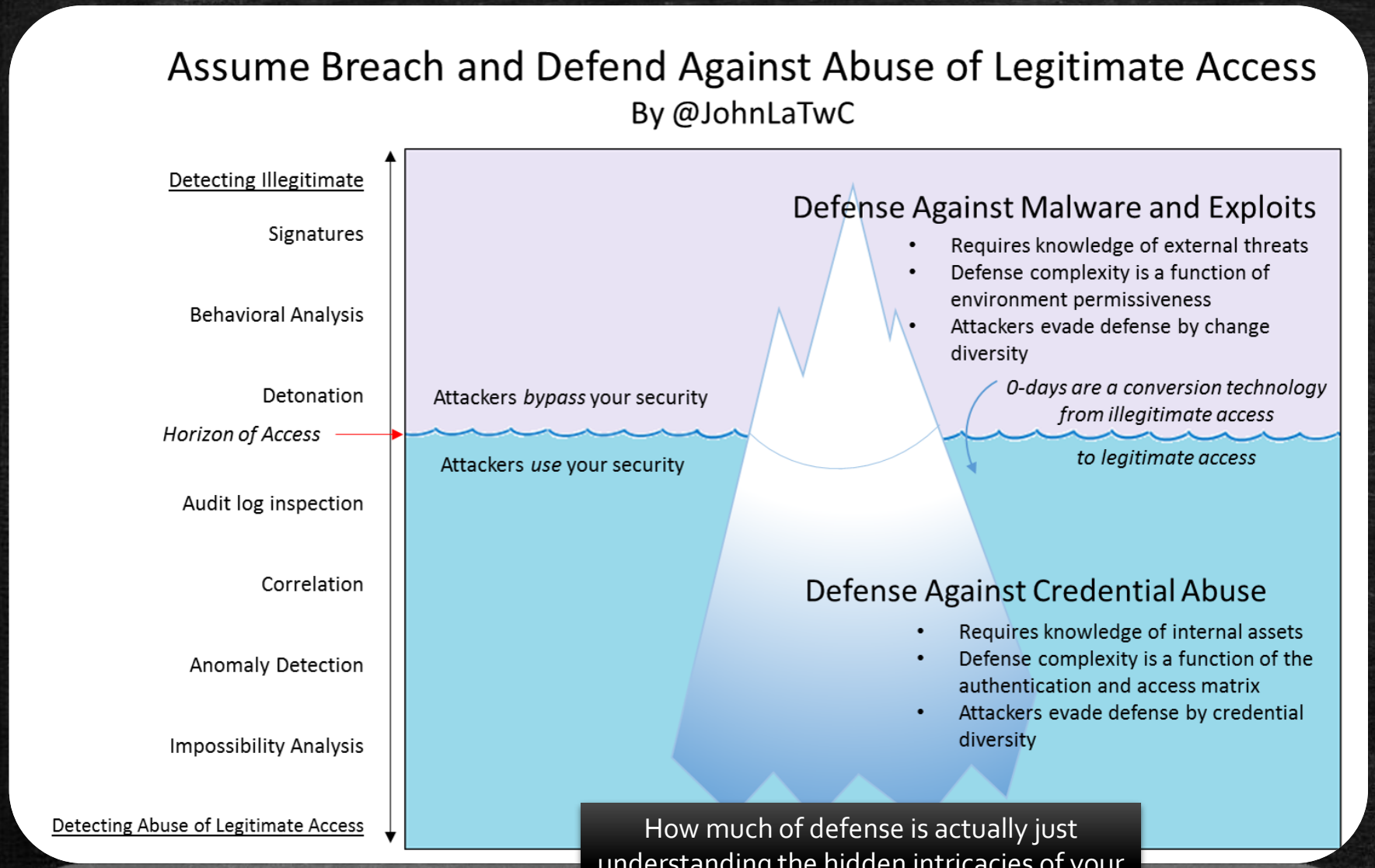
One Risk Prioritized Bite at a Time

How does all this translate to reduced data complexity?

Key Cyber Terrain and potential nexuses of complexity emerge as you work the overall problem

Understanding of the variables that shape, drive, and obscure complex relationships

Armed with the context to start to making technical and procedural changes to manage complexity



The iceberg analogy and the complexity that lurks beneath.

- Knowing yourself
- Knowing the enemy
- Knowing the attack paths

From John Lambert
Microsoft Threat Intelligence Center

From John Lambert
Microsoft Threat Intelligence Center

"Defense Complexity is a Function of the Authentication and Access Matrix"

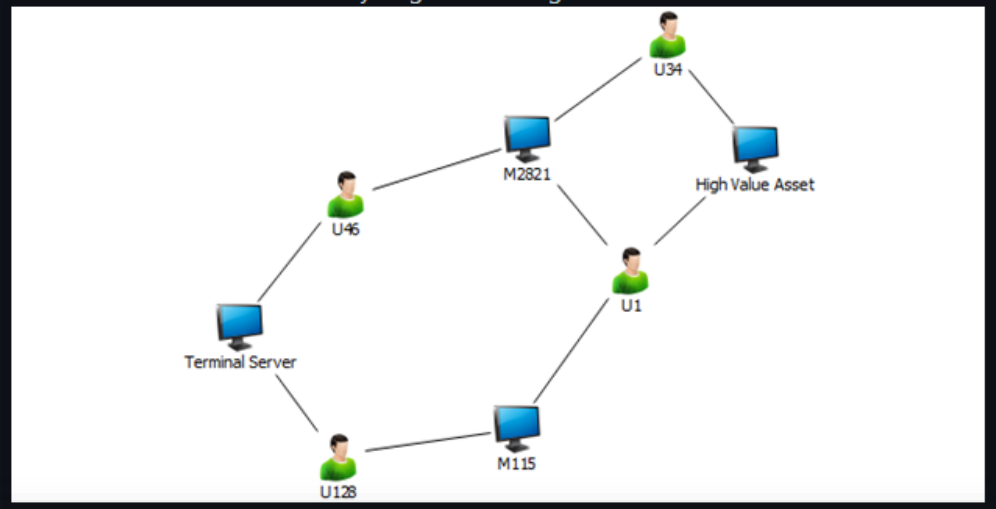
- Thinking in graphs versus lists as a defender
- You (should) already have the data as defender
- Exposes actual complexity, but gives you tools to mathematically reduce through SNA
- End Result: Clearly see adversary attack paths

Attackers can lay in wait on a compromised machine, using a password dumper such as mimikatz until a high value account logs on to the machine. Let's examine an example graph.

(Graph/Matrix Equivalence)

The cluster on the left is single Terminal Server used by hundreds of users. If attackers compromise this machine, they can dump the credentials of many users over time.

How can attackers move laterally to get to the High Value Asset?



By searching the graph, attackers discover multiple paths to the High Value Asset. Compromising the terminal server can allow attackers to also compromise User46 and User128. Those users are admins on Machine2821 and Machine115 respectively. Compromising those workstations allows attackers to compromise User1 and User34, both of which are admins on the High Value Asset. For the High Value Asset to be protected, all the dependent elements must be as protected as thoroughly as the HVA—forming an equivalence class.

Origin of Complexity

Mitigating Approaches

Conception of the problem and interaction of stakeholders

Set the Mental Framework

- Mission centric problem-solving mindset (Operational)
- Reduce odds of material impact of cyber event
- Defensive mindset, think like an attacker, think in graphs

The sum total of possible interactions between systems

Understand the Scope

- Tailored structured planning process, operationally and administratively
- Build relationships with stakeholders, like it or not, DCO is enmeshed
- Understand the threat – "Nation State MCA's. Done. Next." is a copout
- Understand your risks

Collection of security relevant data

Know Where to Focus

- Continuously learn your terrain
- Use risk and threat to prioritize efforts.
- ALL EFFECTIVE DCO EXTENDS FROM KNOWING YOUR TERRAIN.

Security backend infrastructure

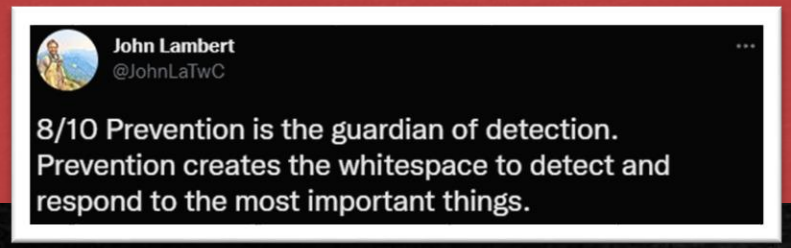
Minimize Distractions

- For every tool, from text editor to threat intelligence:
  - Supply chain
  - Dependencies (and attack surface!)
  - Other support requirements
- Make hard decisions based on the tail cost/benefit

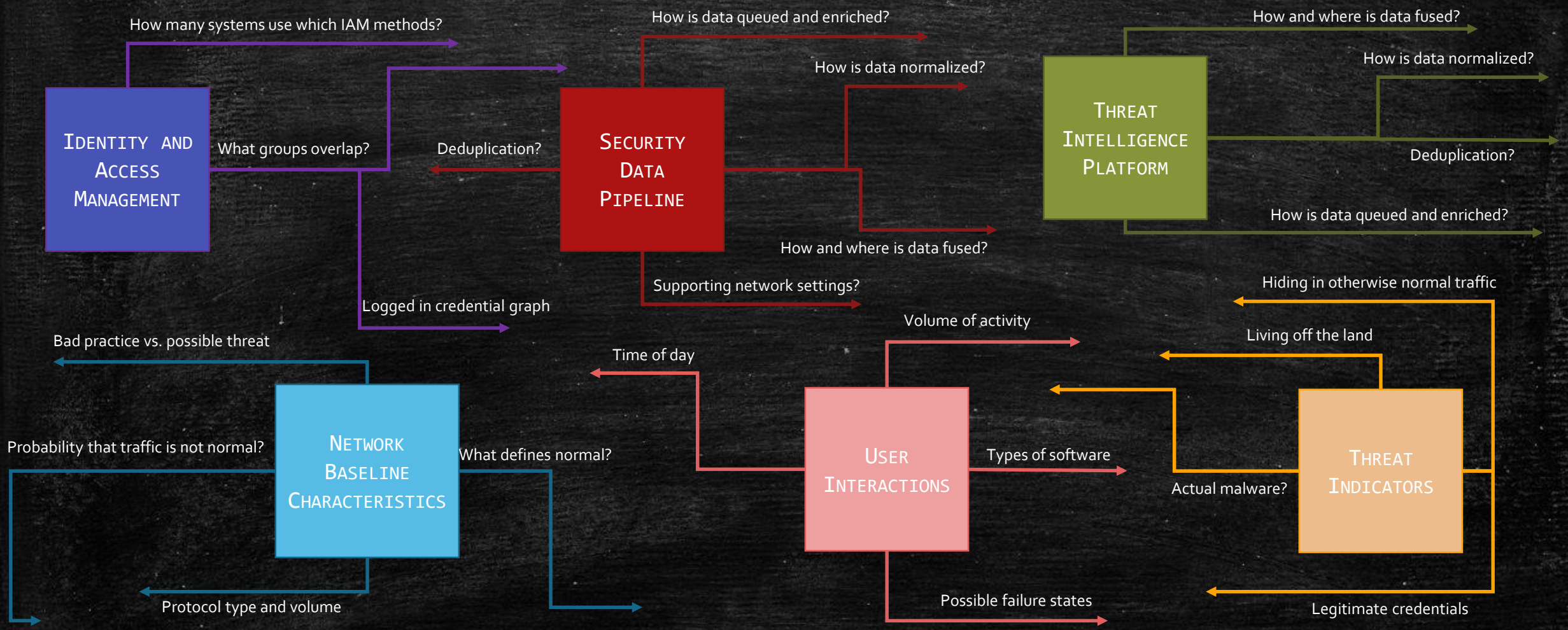
Analysis, presentation, and action driven by security data

See the Signal Through the Noise

- UPFRONT PREVENTION: Whitelisting, IAM, patching, asset management, etc.
- Reduce volume of data
- Tune your logging and alerts
- Properly architect your pipeline
- Prioritize complex and expensive transforms and enrichments



Some Specific Nexuses of Security Data Complexity



These become self-evident when you approach the problem correctly…

Pitfalls

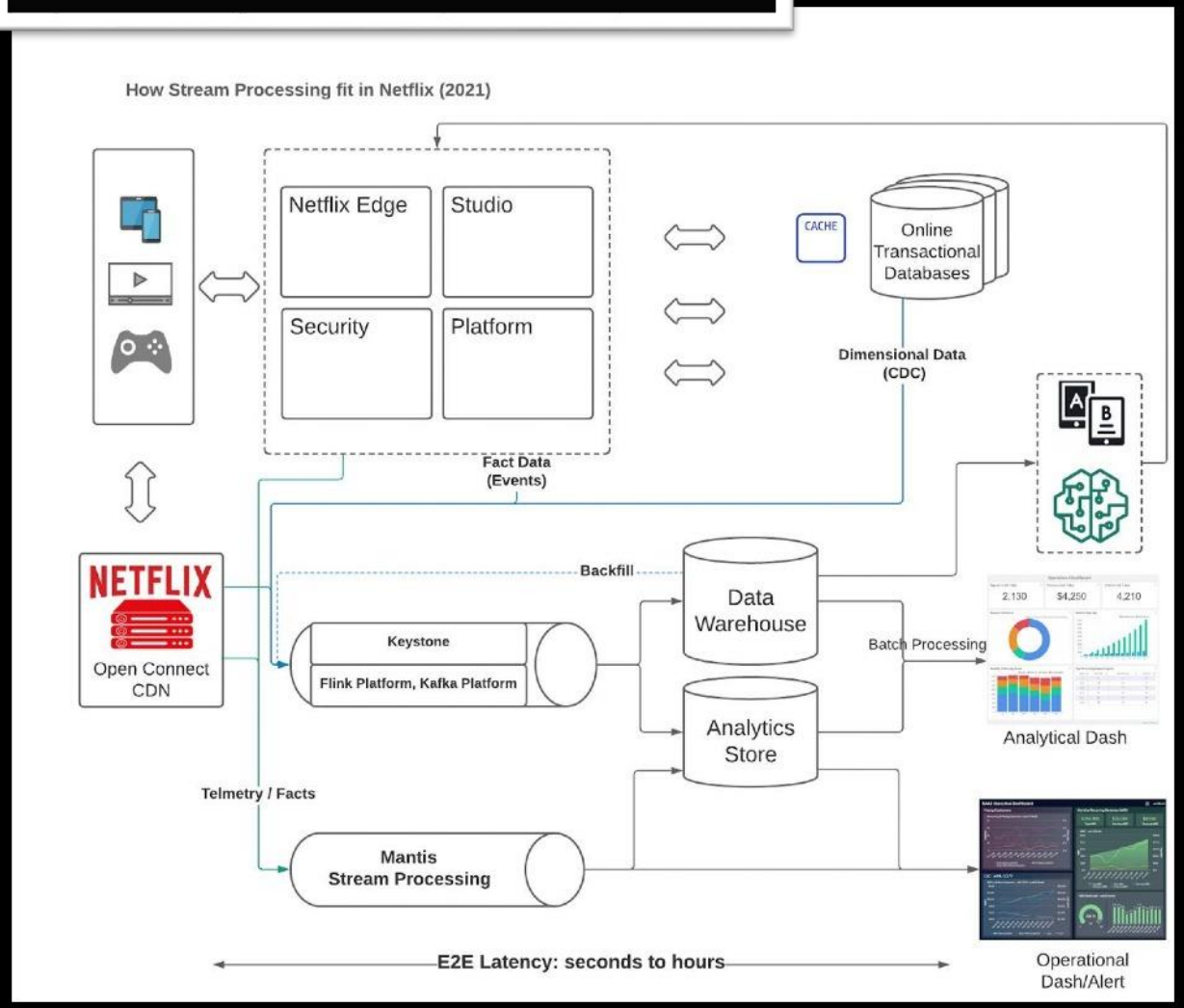
- The AI/ML bandwagon
- Beware of turnkey solutions – hides complexity to make things seems simple
- Too much, too soon – collection, analysis, and capabilities
- Not enough, too soon – especially threat intelligence
- Death by a 1000 support infrastructure papercuts – dependency hell
- Over proceduralized
  - Good process and procedures helps "automate" away the repetitive and simple
  - Leaving decision space and time for the crux of the problem and creative approaches
- Under proceduralized

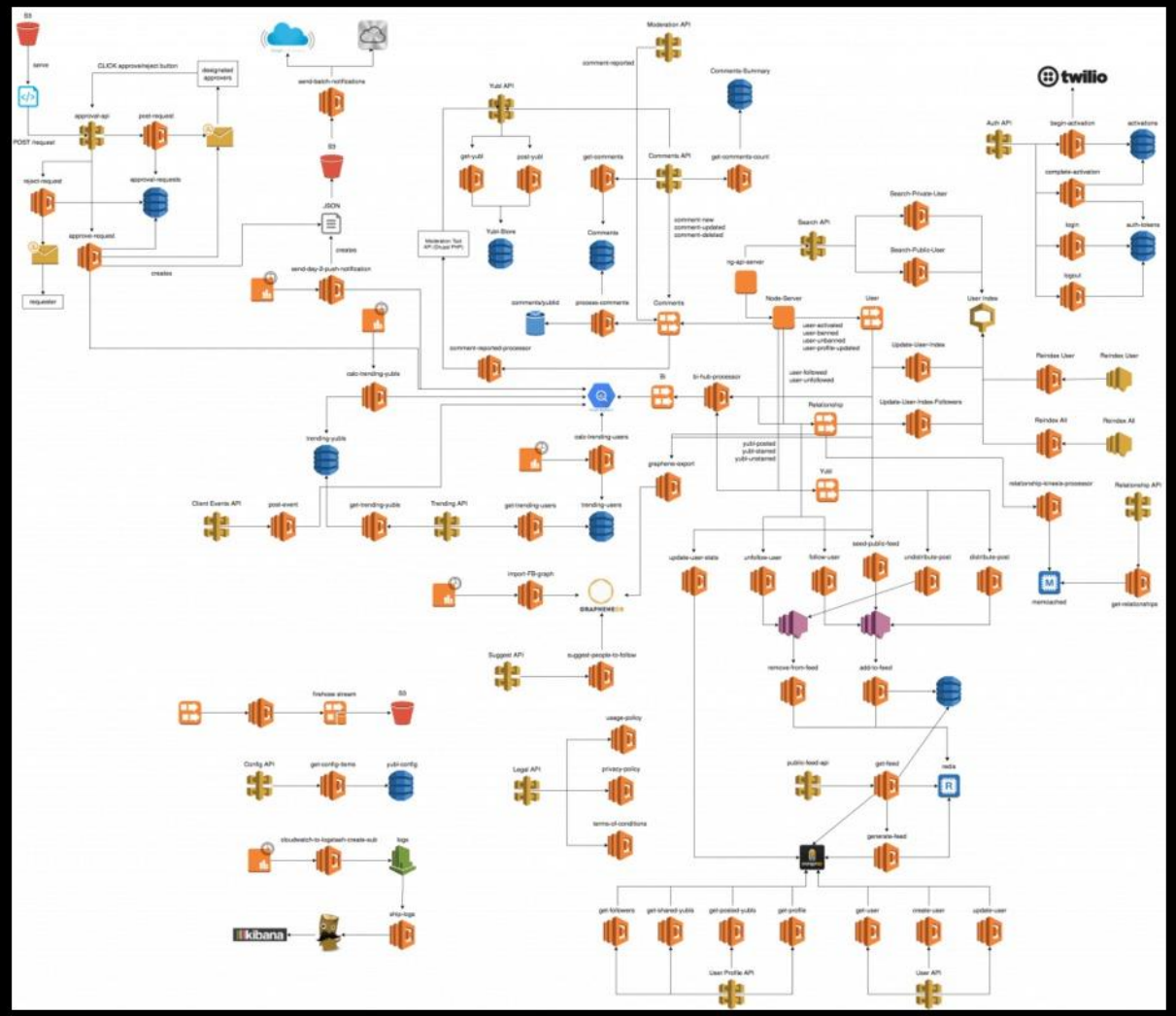
kvm @__kvm · Apr 29

Netflix infra to handle a trillion events every day

v/s

Series A startups with five customers





How **NOT** to Handle Complexity

Ignore It

Artificially Reduce It

Add More Process

Remove More Process

Buy Your Way Out

Lie Your Way Out

Conclusion

- Inherently complex endeavor, growing more so all the time
- The mindset matters more than a technical solution
- Well framed to determine what is unavoidable and what is self inflicted
- The technical solution will fall into place once you take the time to understand the **nature** of the complexity
- You may not know how to untie the Gordian Knot but you at least appreciate the fact it's made of rope which comes with its own well-defined set of properties