

# Fragilence\*

The quantum state of survivable resilience in a world of fragile indifference

Twitter: @beaker

\**Fragile Resilience*



# What I want you to take away:

1. I haven't delivered a public talk in 7 years.
2. We are more art and compliance than science
3. Where we do make use of science, it's siloed
4. We aren't organized properly
5. We don't define, model or manage risk well
6. We are not agile
7. Our definition of "Resilience" varies and it is insufficient
8. Instead of resilient, we need to be:

**ANTIFRAGILE**





**Oh for the love of Odin, not  
another grumpy “InfoSec is  
broken rant!?”**

What's missing is the context...









# Cyber “Resilience” - Context Matters

Definitions run the gamut across a spectrum of stressors and impacts

## NIST SP 800-172

*The ability to **anticipate**, **withstand**, **recover from**, and **adapt** to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.*


Context	Term	Definition
National Security	Resilience	“The ability to <b>adapt</b> to changing conditions and <b>prepare</b> for, <b>withstand</b> , and rapidly <b>recover</b> from disruption.” [WH 2010]
Critical Infrastructure	Infrastructure resilience	“Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to <b>anticipate</b> , <b>absorb</b> , <b>adapt</b> to, and/or rapidly <b>recover</b> from a potentially disruptive event.” [NIAC 2010]
Critical Infrastructure Security and Resilience	Resilience	“...the ability to <b>prepare</b> for and <b>adapt</b> to changing conditions and <b>withstand</b> and <b>recover</b> rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.” [WH 2013]
DoD Cybersecurity	Operational resilience	“The ability of systems to <b>resist</b> , <b>absorb</b> , and <b>recover</b> from or <b>adapt</b> to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.” [DoD 2014]
Network Engineering	Resilience	“The ability of the network to provide and <b>maintain</b> an acceptable level of service in the face of various faults and challenges to normal operation.” [Sterbenz 2006]
Resilience Engineering	Resilience engineering	“The ability to build systems that are able to <b>anticipate</b> and circumvent accidents, survive disruptions through appropriate learning and <b>adaptation</b> , and <b>recover</b> from disruptions by restoring the pre-disruption state as closely as possible.” [Madni 2009]
Homeland Security	Resilience	The ability to <b>adapt</b> to changing conditions and <b>prepare</b> for, <b>withstand</b> , and <b>rapidly</b> recover from disruption.” [Risk 2010]

Cybersecurity performance characteristics			
CHARACTERISTICS	LEADERS	NON-LEADERS	FEDERAL AGENCIES
Stop more attacks 	1 in 27 attacks breach security	1 in 8 attacks breach security	1 in 18 attacks breach security
Find breaches faster 	88% detect breaches in less than one day	22% detect breaches in less than one day	45% detect breaches in less than one day
Fix breaches faster 	96% fix breaches in 15 days or less	36% fix breaches in 15 days or less	58% fix breaches in 15 days or less
Reduce breach impact 	58% of breaches have no impact	24% of breaches have no impact	35% of breaches have no impact




# Story Time

A purely fictional tale of "resilience"



*The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.*

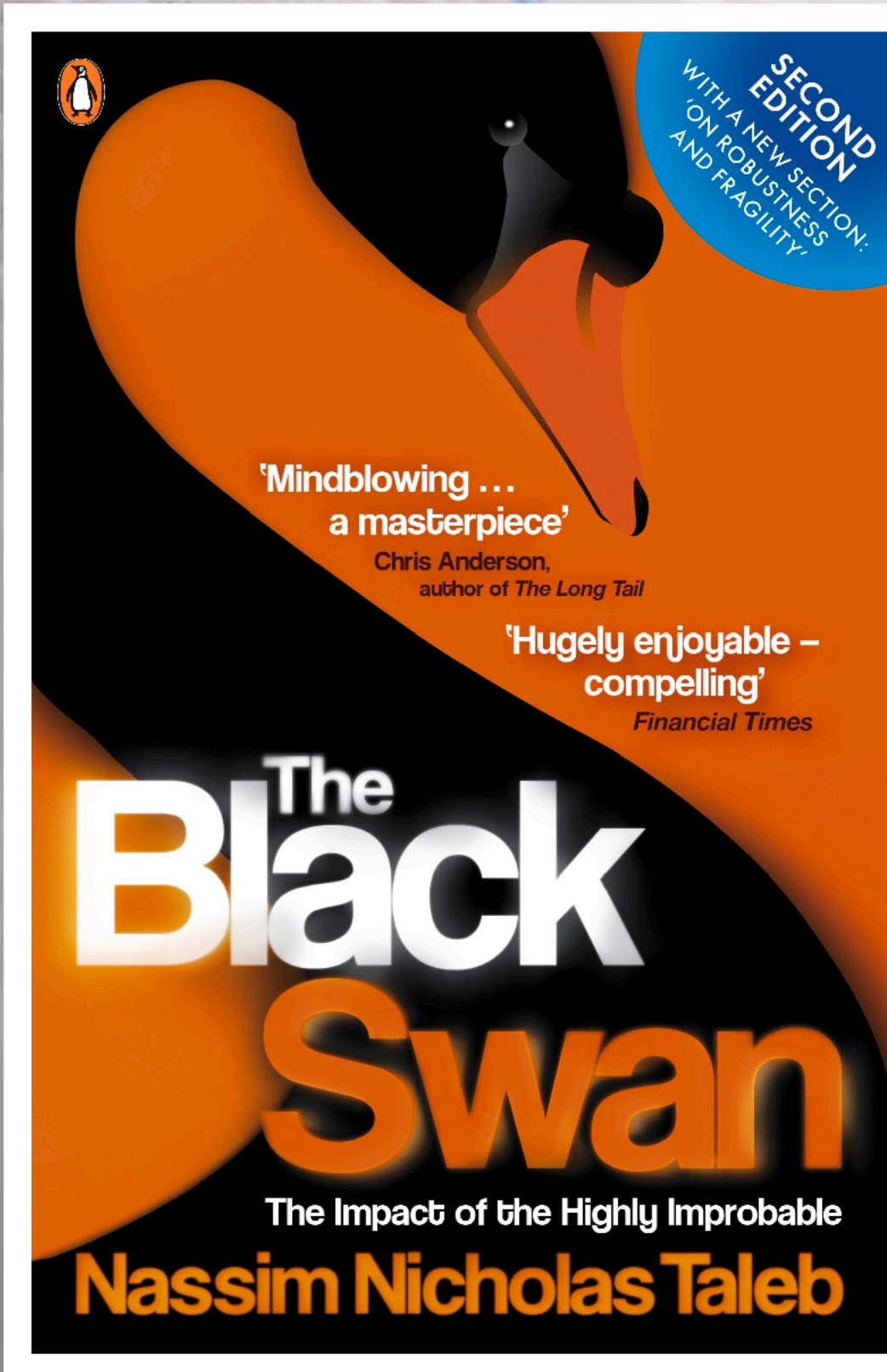




***Resilience...You keep  
using that word...I  
do not think it  
means what you  
think it means...***

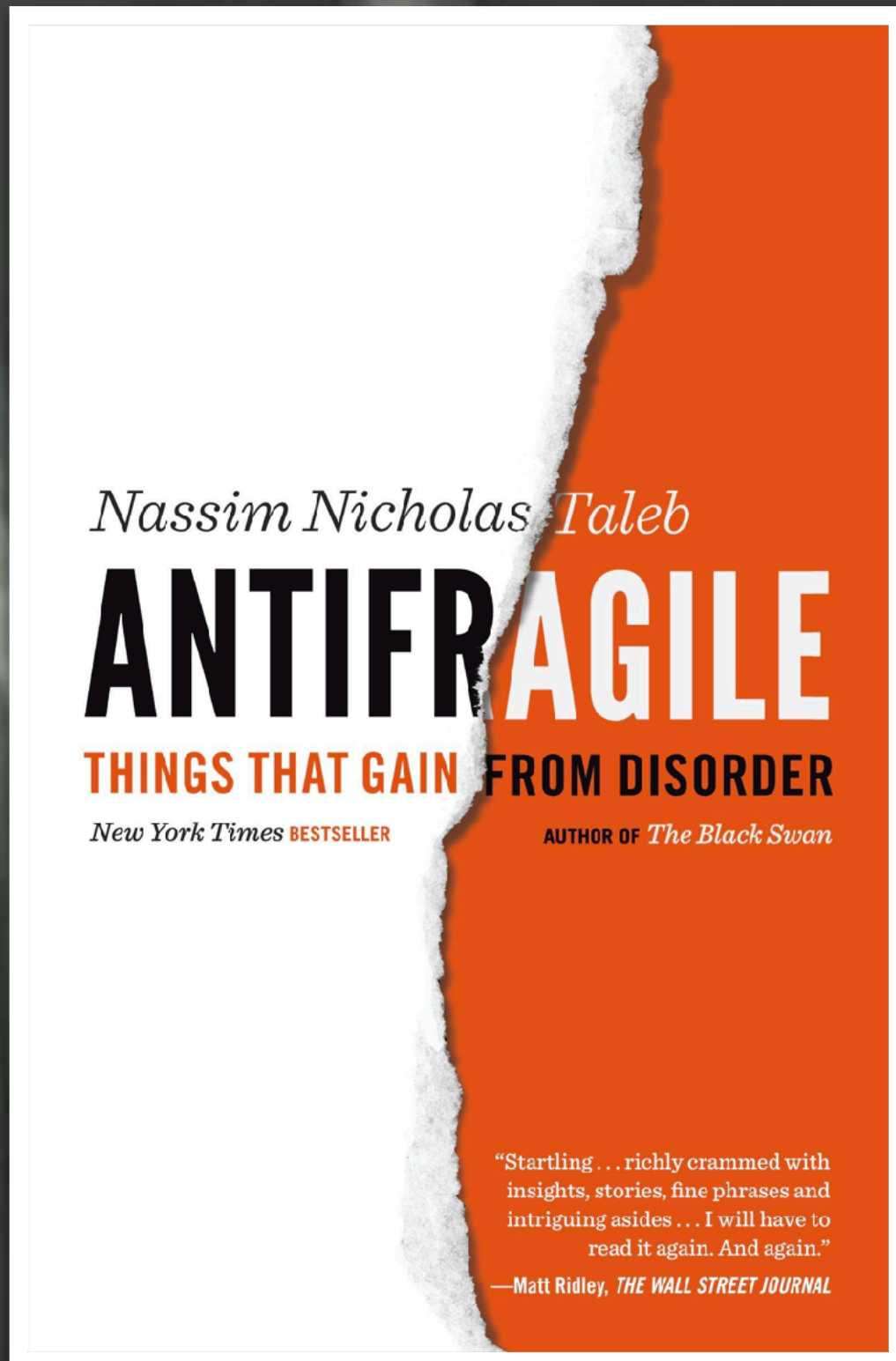
***...and if it does mean  
what you think it  
means, it's probably  
not enough and you  
probably can't  
achieve it.***





“ The black swan theory or theory of black swan events is a metaphor that describes an event that comes as a surprise, has a major effect, and is often inappropriately rationalized after the fact with the benefit of hindsight. ”

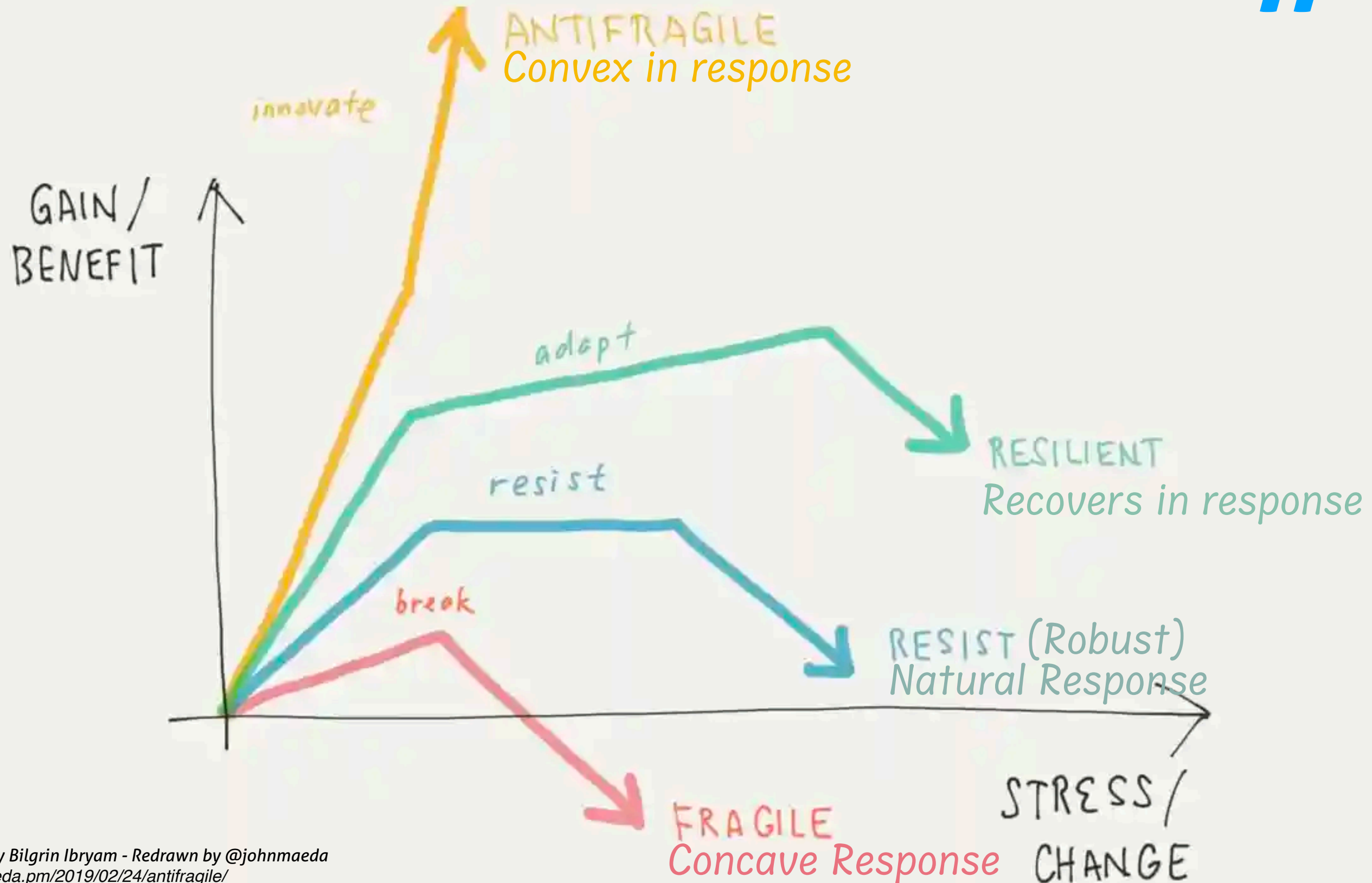




Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder, and stressors and love adventure, risk, and uncertainty. Yet, in spite of the ubiquity of the phenomenon, there is no word for the exact opposite of fragile. Let us call it antifragile.



The resilient resists shocks and stays the same; the antifragile gets better.





# THIS is where Antifragile lives

(Hates Disorder)			Volatility		(Loves Disorder)	
Harm or Penalize ("Nothing to gain")		Not Change	Randomness		Change	Gain or Benefit ("Nothing to lose")
<b>Fragile</b>	<b>Antiagile</b>	<b>Robust</b>			<b>Agile</b>	<b>Antifragile</b>
(Suffers and Wants Tranquility "at best unharmed")	(Not Adapts)	(Sustains and Doesn't care too much "at best and at worst unharmed")			(Adapts)	(Evolves and Grows from Disorder "at worst unharmed")
Resist Disorder	Resist Change	Manage Change			Embrace Change Inspect & Adapt	Embrace Disorder Adapt & Evolve
Resists shocks and stays the same (Resilient during normal change)		<b>Stressors</b> <small>Copyright © 2015 Sinan SI Alhir</small>		Absorbs shocks and Gets better (Resilient during unusual change)		

# TW: Security is — at best — (generally) here

Focus on stability, resist change, resist shock.

(Hates Disorder)		Volatility	(Loves Disorder)	
Harm or Penalize ("Nothing to gain")	Not Change	Randomness	Change	Gain or Benefit ("Nothing to lose")
<b>Fragile</b>	<b>Antiagile</b>	<b>Robust</b>	<b>Agile</b>	<b>Antifragile</b>
(Suffers and Wants Tranquility "at best unharmed")	(Not Adapts)	(Sustains and Doesn't care too much "at best and at worst unharmed")	(Adapts)	(Evolves and Grows from Disorder "at worst unharmed")
Resist Disorder	Resist Change	Manage Change	Embrace Change Inspect & Adapt	Embrace Disorder Adapt & Evolve
Resists shocks and stays the same (Resilient during normal change)		<b>Stressors</b>	Absorbs shocks and Gets better (Resilient during unusual change)	

Copyright © 2015 Sinan SI Alhir



InfoSec is:

~~FR~~AGILE

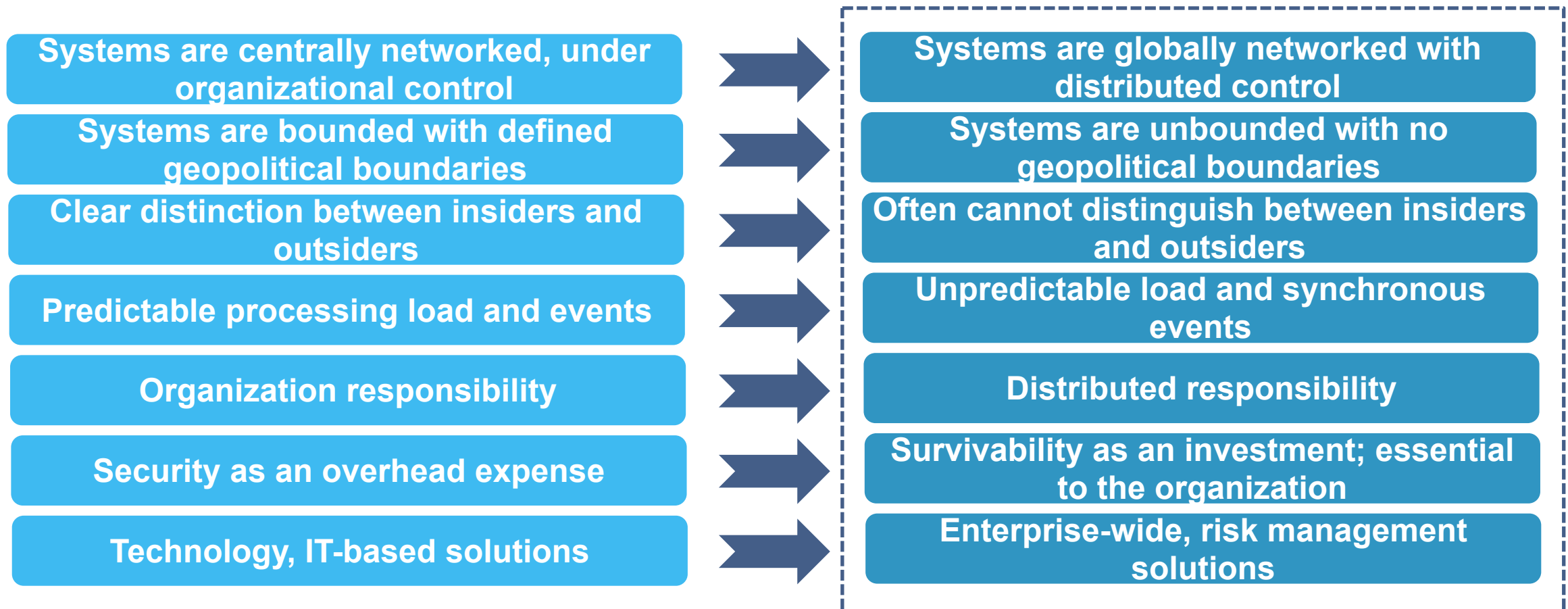




**Opportunity**



# This is NOT a new concept...



In recent years, there have been dramatic changes in the character of security problems, in their technical and business contexts, and in the goals and purposes of their stakeholders. As a consequence, **many of the assumptions underlying traditional security technologies are no longer valid**. Failure to recognize the depth and breadth of these changes in combination prevents effective solutions to modern security problems. Survivability provides a new technical and business perspective on security, which is essential to our search for solutions. Moreover, our **survivability approach expands the view of security from a narrow technical specialty, accessible only to security experts, towards a risk-management perspective** that requires the participation of an organization as a whole (executive management, security experts, application domain experts, and other stakeholders) to protect mission critical systems from cyber-attacks, failures, and accidents.

**We conflate tactical informational and taxonomic frameworks (what) and directional linear action — “chains” (how) — with decision systems for complex system problems (why, when & who)**

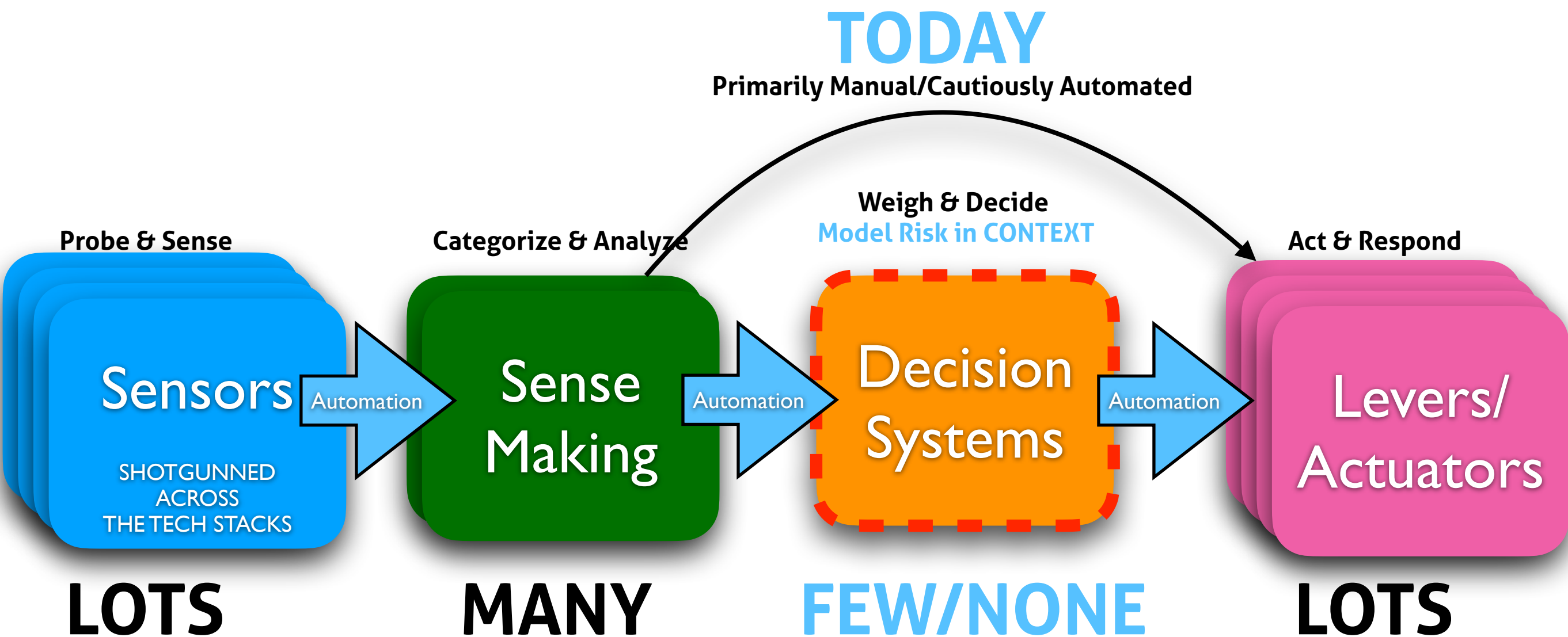
**They are related but not the same.**

**Why is this important?**



# Security: Data/Tech Rich & Information Poor

We have almost everything we need to make good decisions, we often don't know how  
AND we don't have the processes or context to integrate them into how we do things



\*Depending upon organizational/tech stack maturity, task automation is:

0. Absent, 1. Instrumented, 2. Manually analyzed, 3. Augmented, 4. Automated, 5. Automatic, 6. Autonomic

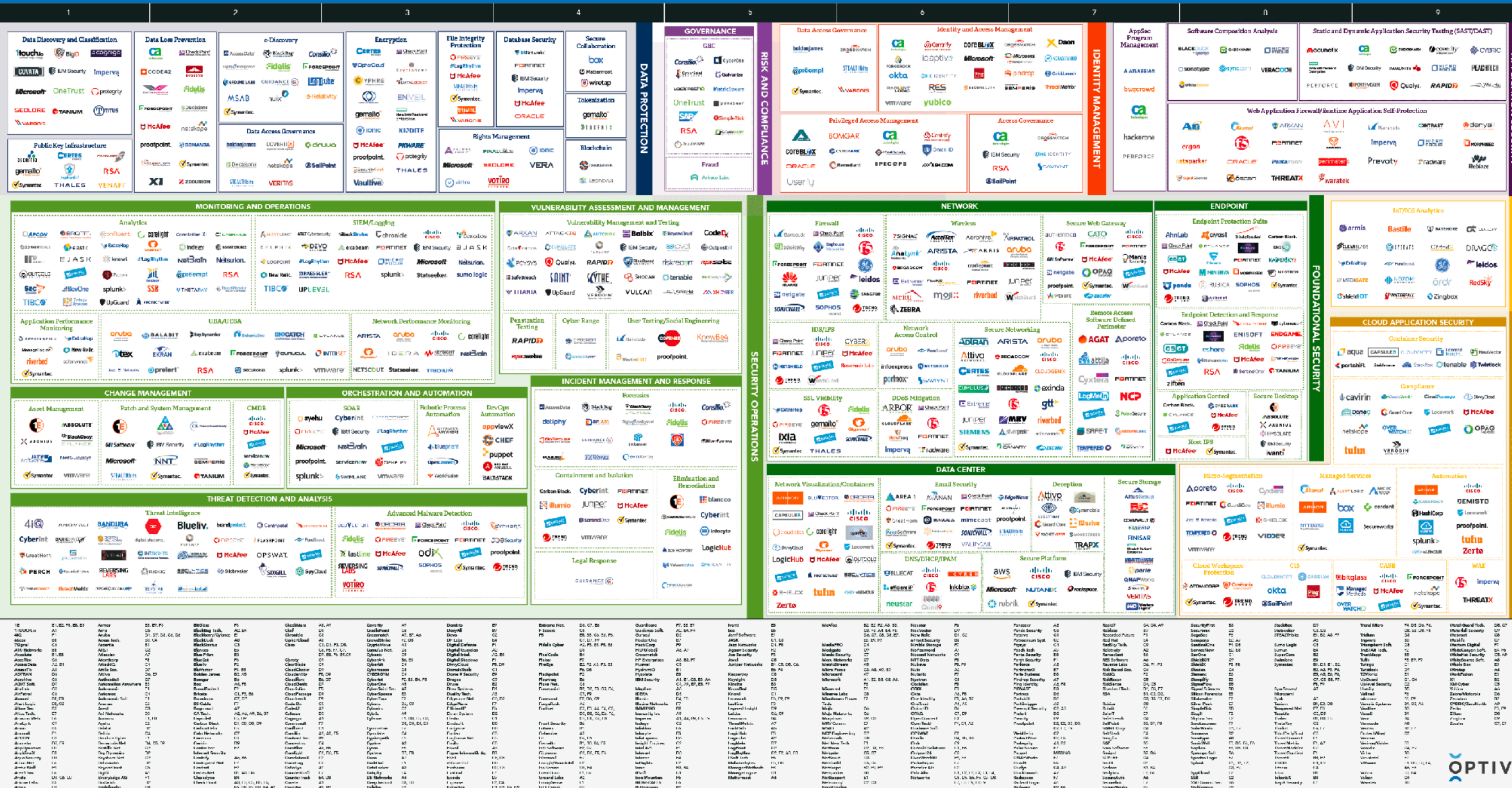


# Fragilence

## The quantum state of survivable resilience in a world of fragile indifference

## Optiv Cybersecurity Technology Map

Navigate Cybersecurity at [Optiv.com](http://Optiv.com)



This graphic doesn't cover the startups or up-starts that this particular reseller/integrator doesn't represent. There are literally multiple thousands of vendors in the cyber security market space...

<https://www.optiv.com/navigating-security-landscape-guide-technologies-and-providers>



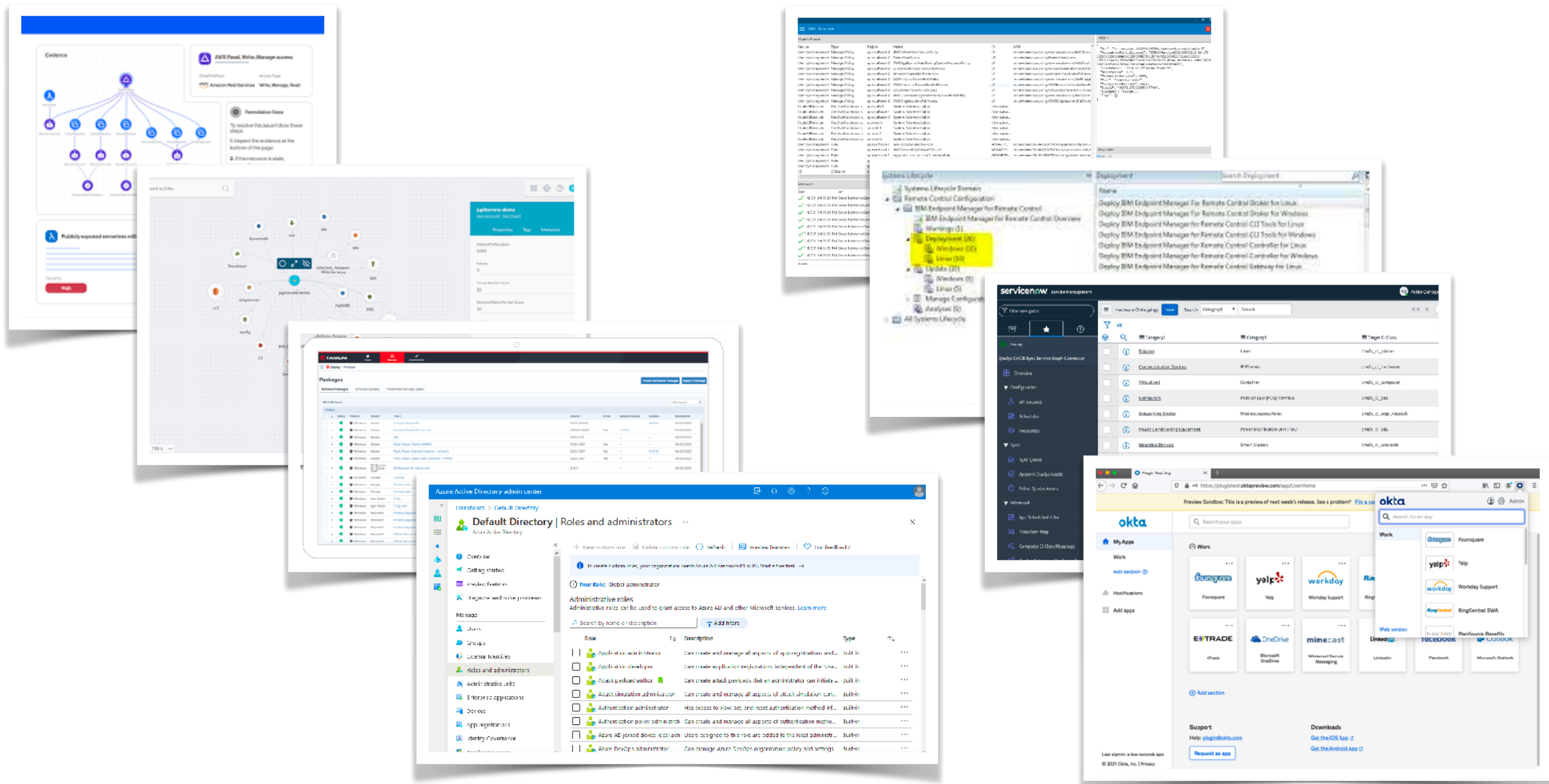


## Requisite Cat Picture



# Inventory (of stuff) Systems - Multiple “Pains” of Glass

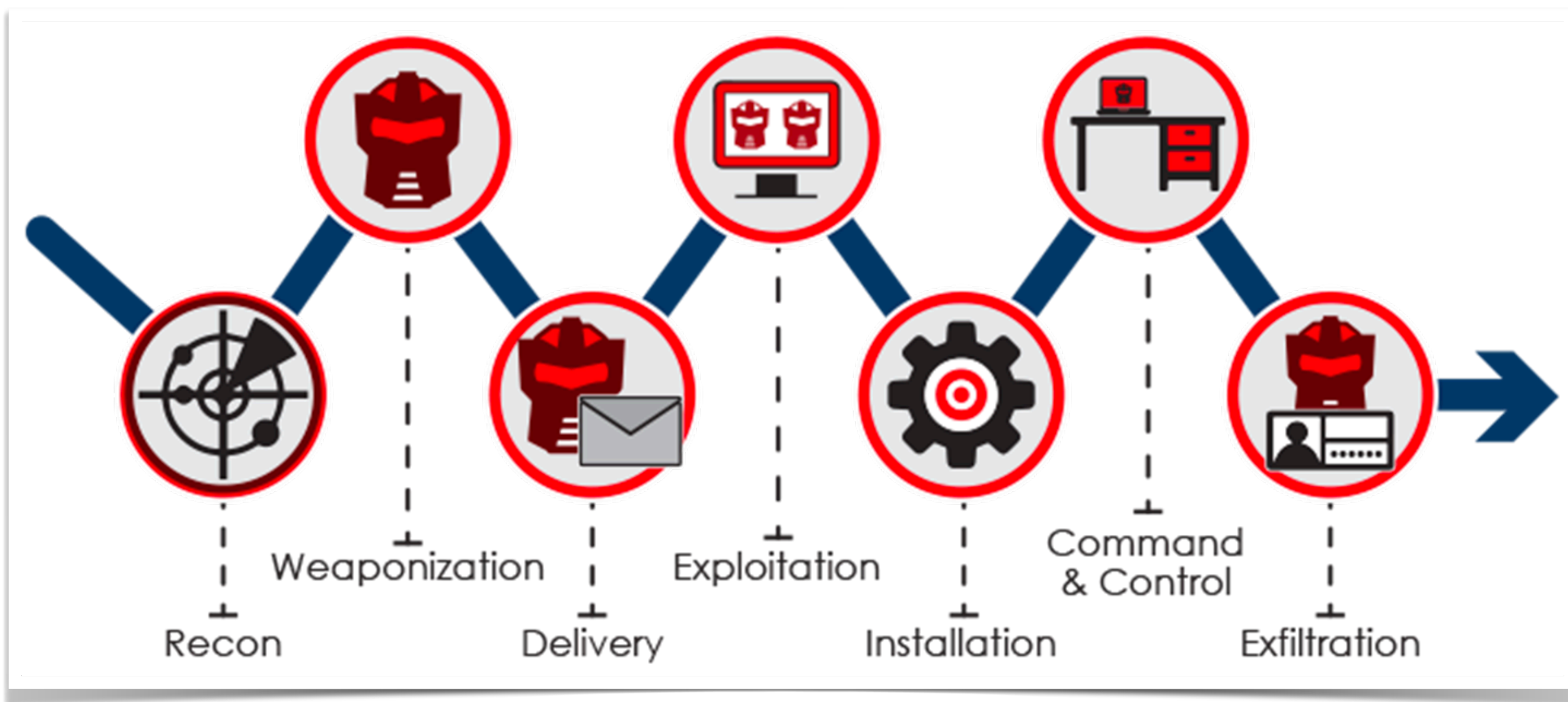
LOTS of them; disconnected and unaligned to the DIE (Distributed, Immutable, Ephemeral)\* model





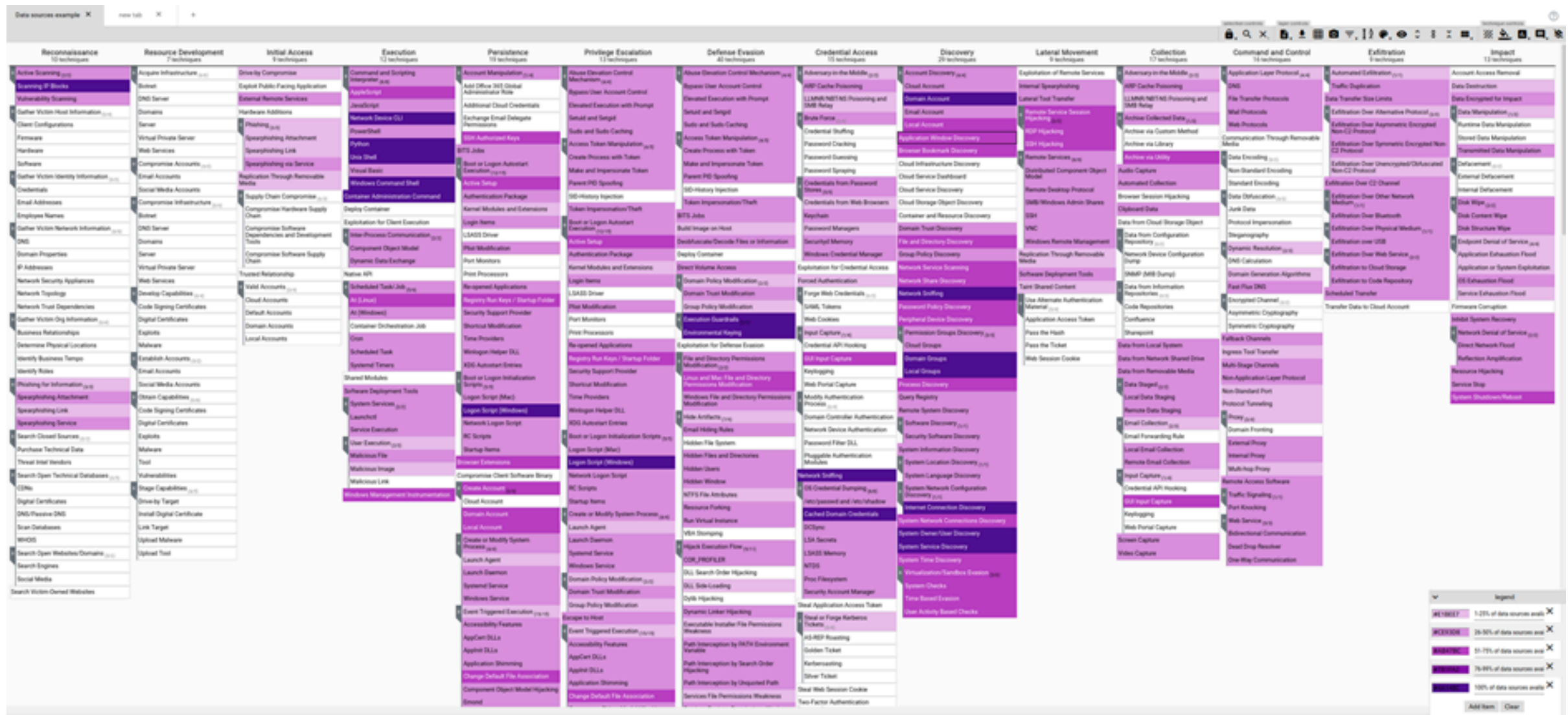
# The Lockheed Martin Cyber Kill Chain™

Describes how attackers use the cycle of compromise, persistence and exfiltration against an organization.



# MITRE ATT&CK

Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.



Reconnaissance (12 techniques)	Resource Development (7 techniques)	Initial Access (9 techniques)	Execution (13 techniques)	Persistence (10 techniques)	Privilege Escalation (11 techniques)	Defense Evasion (10 techniques)	Credential Access (10 techniques)	Discovery (20 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (14 techniques)	Exfiltration (13 techniques)	Impact (12 techniques)
Active Scanning (T1046)	Acquire Infrastructure (T1025)	Drive-by Compromise (T1211)	Command and Scripting Interpreter (T1059)	Account Manipulation (T1036)	Abuse Elevation Control Mechanism (T1054)	Abuse Elevation Control Mechanism (T1054)	Adversary in the Middle (T1028)	Account Discovery (T1005)	Exploitation of Remote Services (T1021)	Adversary in the Middle (T1028)	Application Layer Protocol (T1048)	Automated Exfiltration (T1041)	Account Access Removal (T1029)
Scanning IP Blocks (T1046)	Bitnet (T1025)	Exploit Public Facing Application (T1211)	Command and Scripting Interpreter (T1059)	Add Office 365 Global Administrator Role (T1036)	Reopen User Account Control (T1054)	Reopen User Account Control (T1054)	ARP Cache Poisoning (T1028)	Cloud Account (T1005)	Internal Spearphishing (T1021)	ARP Cache Poisoning (T1028)	DNS (T1048)	Traffic Degradation (T1041)	Data Destruction (T1029)
Vulnerability Scanning (T1046)	DMZ Server (T1025)	External Remote Services (T1211)	Network Service (T1059)	Additional Cloud Credentials (T1036)	Elevated Execution with Prompt (T1054)	Elevated Execution with Prompt (T1054)	LLMNR/NBNS Processing and SMB Relay (T1028)	Domain Account (T1005)	Lateral Tool Transfer (T1021)	LLMNR/NBNS Processing and SMB Relay (T1028)	File Transfer Protocols (T1048)	Data Transfer Size Limits (T1041)	Data Engineered for Impact (T1029)
Search Victim Host Information (T1046)	Domains (T1025)	Hardware Additions (T1211)	Network Service (T1059)	Exchange Email Delegate Permissions (T1036)	Setuid and Setgid (T1054)	Setuid and Setgid (T1054)	Brute Force (T1028)	Local Account (T1005)	Remote Service Session Hijacking (T1021)	Archive Collected Data (T1041)	Web Protocols (T1048)	Exfiltration Over Alternative Protocol (T1041)	Data Manipulation (T1029)
Client Configurations (T1046)	Server (T1025)	Phishing (T1211)	PowerShell (T1059)	SSIN Authorize Keys (T1036)	Subs and Subs-Caching (T1054)	Subs and Subs-Caching (T1054)	Credential Stuffing (T1028)	Application Window Discovery (T1005)	SSH Hijacking (T1021)	Archive via Custom Method (T1041)	Web Protocols (T1048)	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1041)	Persistent Data Manipulation (T1029)
Firmware (T1046)	Virtual Private Server (T1025)	Spearphishing Attachment (T1211)	Python (T1059)	Access Token Manipulation (T1036)	Access Token Manipulation (T1036)	Access Token Manipulation (T1036)	Password Cracking (T1028)	Browser Bookmark Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Stored Data Manipulation (T1029)
Hardware (T1046)	Web Services (T1025)	Spearphishing Link (T1211)	One-Shell (T1059)	Boot or Logon Automation (T1036)	Create Process with Token (T1054)	Create Process with Token (T1054)	Password Dumping (T1028)	Cloud Infrastructure Discovery (T1005)	Distributed Component Object Model (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Software (T1046)	Compromise Accounts (T1025)	Spearphishing via Service (T1211)	Visual Basic (T1059)	Make and Impersonate Token (T1036)	Make and Impersonate Token (T1036)	Make and Impersonate Token (T1036)	Password Spraying (T1028)	Cloud Service Dashboard (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Search Victim Identity Information (T1046)	Email Accounts (T1025)	Application Through Removable Media (T1211)	Windows Command Shell (T1059)	Powercat (T1036)	Powercat (T1036)	Powercat (T1036)	Credentials from Password Storm (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Credentials (T1046)	Social Media Accounts (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Email Addresses (T1046)	Compromise Infrastructure (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Employee Names (T1046)	Bitnet (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Search Victim Network Information (T1046)	DMZ Server (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Domain Properties (T1046)	Domains (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
IP Addresses (T1046)	Server (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Network Security Appliances (T1046)	Virtual Private Server (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Network Topology (T1046)	Web Services (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Network Trust Dependencies (T1046)	Develop Capabilities (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Search Victim Org Information (T1046)	Code Signing Certificates (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Business Relationships (T1046)	Digital Certificates (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Determine Physical Locations (T1046)	Exploits (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Identify System Temps (T1046)	Malware (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Identify Roles (T1046)	Establish Accounts (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Phishing for Information (T1046)	Social Media Accounts (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Spearphishing Attachment (T1046)	Develop Capabilities (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Spearphishing Link (T1046)	Code Signing Certificates (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Spearphishing Service (T1046)	Digital Certificates (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Search Cloud Sources (T1046)	Exploits (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Purchase Technical Data (T1046)	Malware (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Threat Intel Vendors (T1046)	Tool (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Search Open Technical Databases (T1046)	Vulnerabilities (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
COINs (T1046)	Stage Capabilities (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Digital Certificates (T1046)	Identify Target (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
DNS-Reverse DNS (T1046)	Install Digital Certificate (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Scan Databases (T1046)	Link Target (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
WHOIS (T1046)	Upload Malware (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Search Open Websites/Domains (T1046)	Upload Tool (T1025)	Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Search Engines (T1046)		Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Social Media (T1046)		Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)
Search Victim Owned Websites (T1046)		Supply Chain Compromise (T1211)	Windows Administrative Command (T1059)	Authentication Package (T1036)	Authentication Package (T1036)	Authentication Package (T1036)	Credentials from Web Browsers (T1028)	Cloud Storage Object Discovery (T1005)	Remote Desktop Protocol (T1021)	Archive via Library (T1041)	Communication Through Removable Media (T1048)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1041)	Transmitted Data Manipulation (T1029)

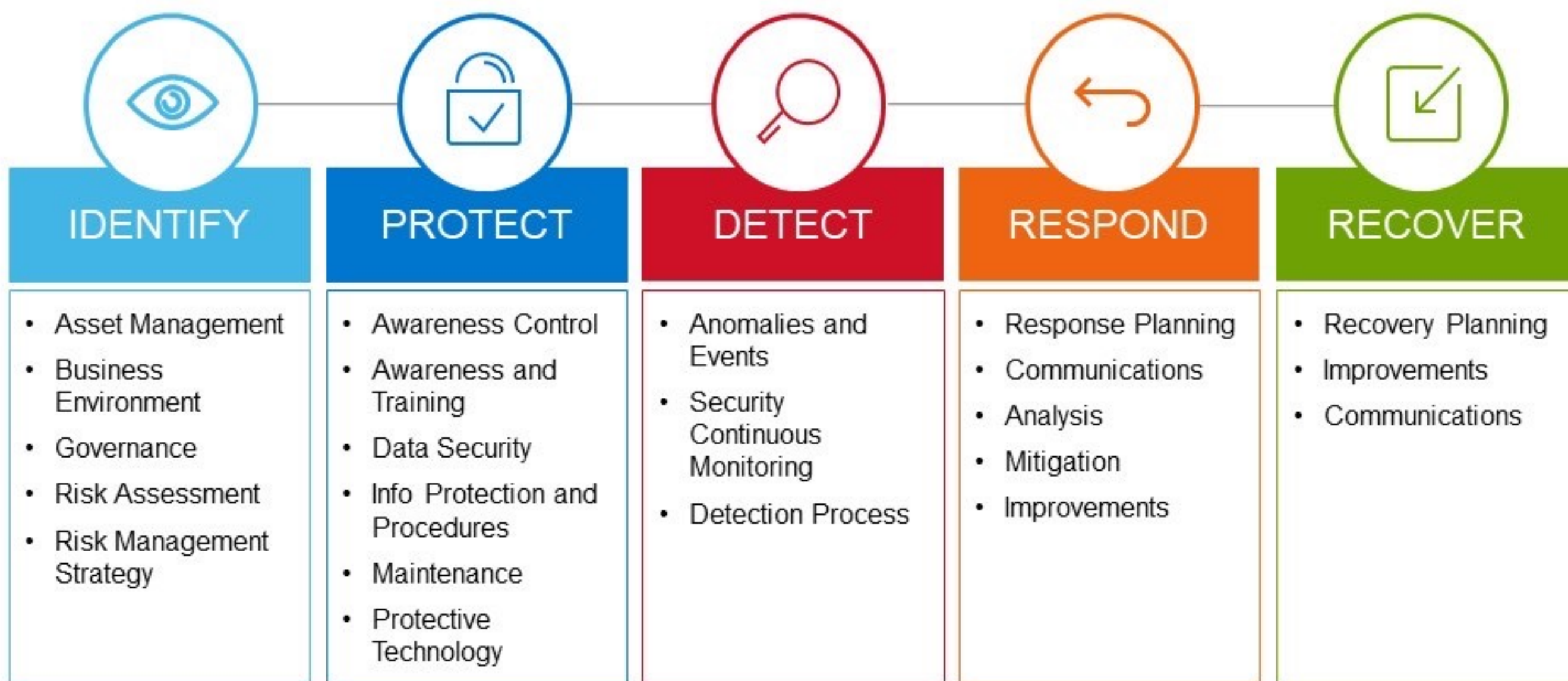
Detect Tactics, Techniques & Combat Threats to assist blue teams using MITRE ATT&CK to score and compare data log source quality, visibility coverage and detection coverage and Attack Flow represents the linkage of adversary behavior for a given attack flow.





# The NIST Cyber Security Framework (CSF)

Provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.



# Cyber Defense Matrix

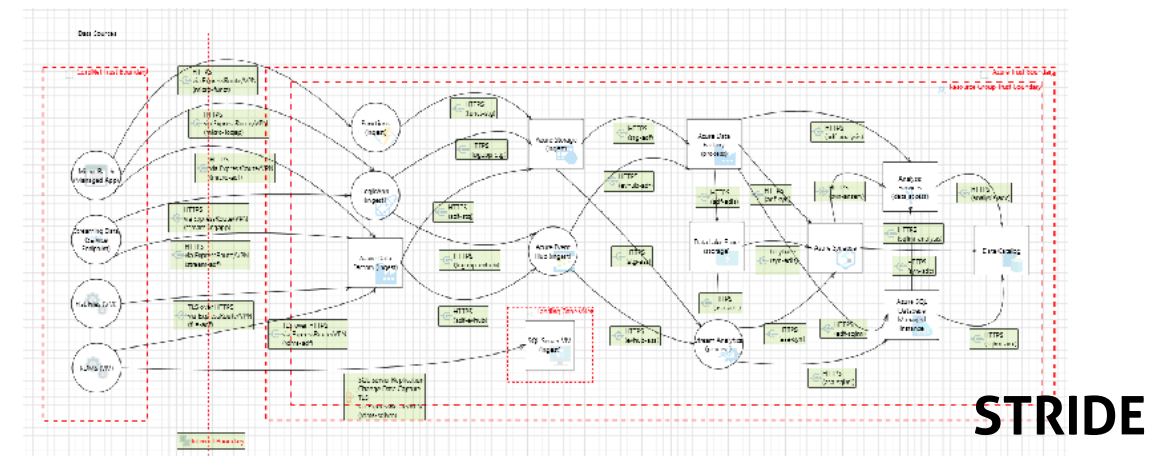
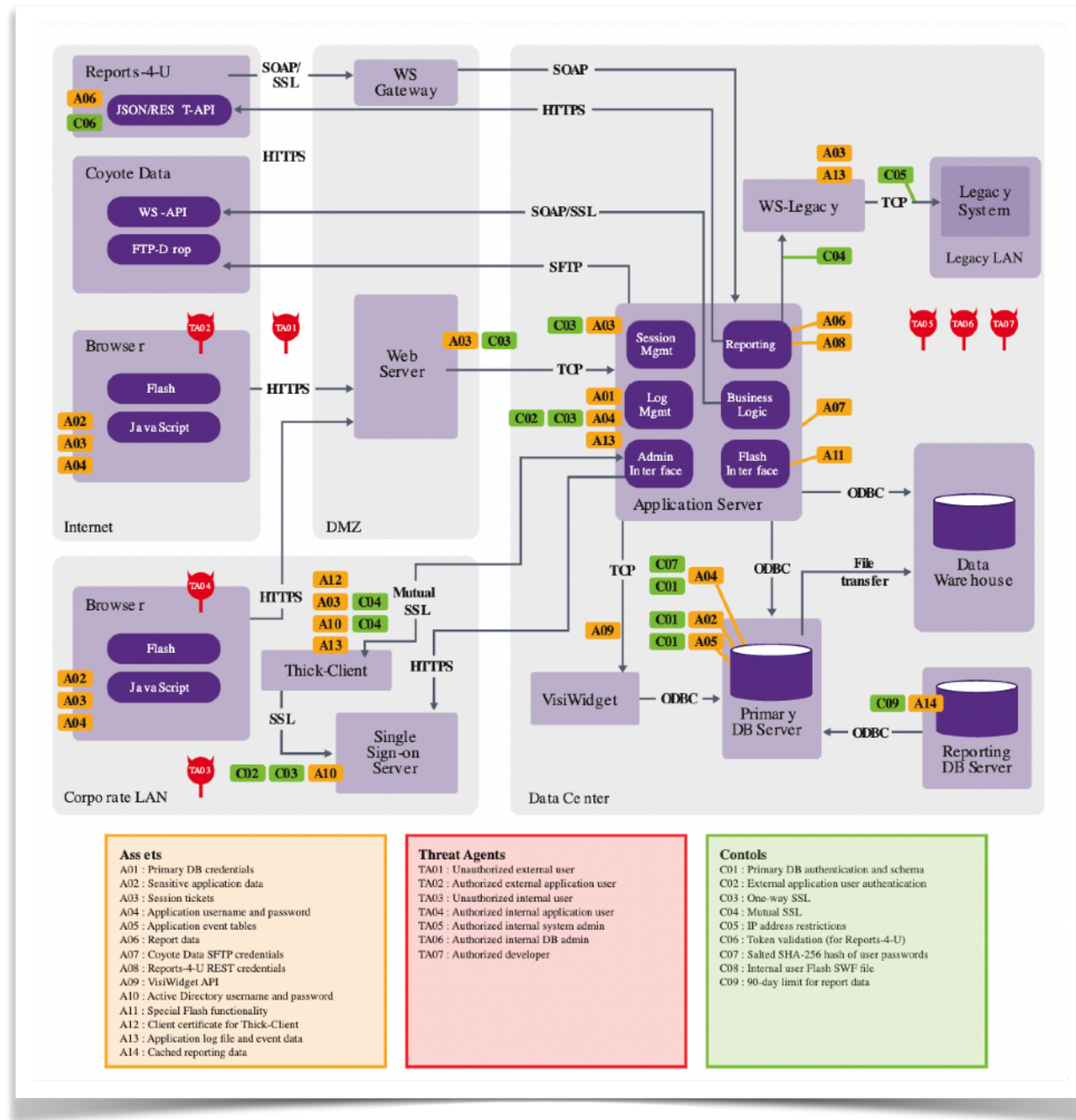
Provides a mechanism to ensure that we have capabilities across the entire spectrum of options to help secure our environments

	Identify	Protect	Detect	Respond	Recover
Devices	Config Mgt, Vuln Scanner	IAM AV, HIPS	Endpoint Detection & Response	EP Forensics	
Applications	SAST, DAST, SW Asset Mgt, Fuzzers	RASP, WAF			
Networks	Netflow, Network Vuln Scanner	Network Security (FW, IPS/IDS)	DDoS Mitigation	NW Forensics	
Data	Data Audit, Discovery, Classification	Encryption, Tokenization, DLP, DRM	Deep Web, Brian Krebs, FBI	DRM	Backup
Users	Phishing Simulations	Phishing & Security Awareness	Insider Threat / Behavioral Analytics		
Degree of Dependency	Technology				People
	Process				



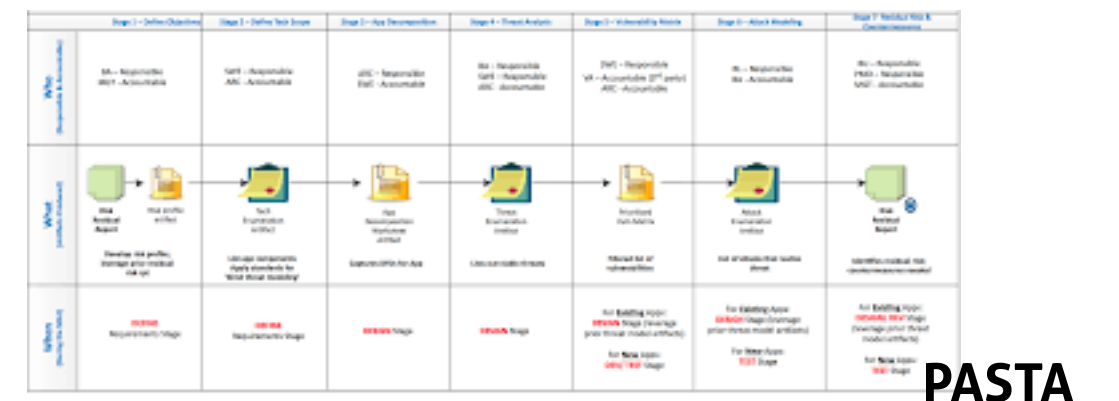
# Threat Modeling and STRIDE/DREAD/PASTA...

A structured process to identify security requirements, pinpoint security threats and potential vulnerabilities, quantify threat and vulnerability criticality, and prioritize remediation methods.



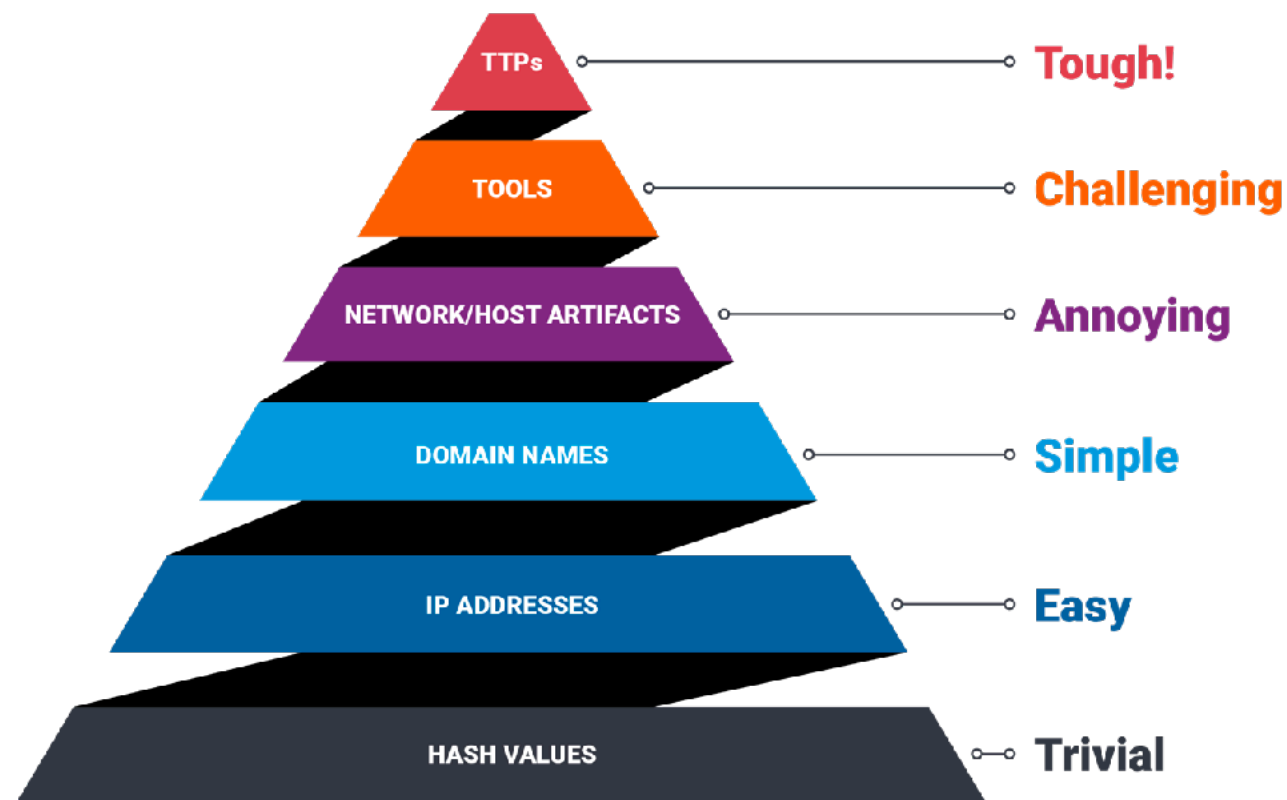
S. No.	Linguistic Variables	Linguistic Value & Range	Linguistic Value & Range	Linguistic Value & Range	Linguistic Value & Range	Linguistic Value & Range		
1	Damage Potential (DP)	Negligible 0-2	Slight 1-4	Moderate 3-6	Almost 5-8	Catastrophic 7-10		
2	Reproducibility (R)	Probably 0-2.5	Likelihood 1.5-4	Satisfiable 3.5-6	Critical 5.5-8	Vital 7.5-10		
3	Exploitability (E)	Least 0-3	Slight 2-5	Moderate 4-7	Almost 6-9	Extreme 8-10		
4	Affected users (AU)	Noticable 0-2	Satisfactory 1-4	Average 3-6	Disturbing 5-8	Unbearable 7-10		
5	Discoverability (D)	Least 0-2	Slight 1.5-5	Moderate 3.5-7	Almost 5.5-9	Extreme 7.5-10		
6	Fuzzy Risk Level (Output Variable)	Very Low 0-9	Low 1-17	Somewhat Low (S-W-Low) 14-24	Medium 21-31	Somewhat High (S-W-High) 28-37	High 35-43	Very High 40-50

DREAD



# Bianco's Pyramid of Pain & Effects/Outcomes

Explains that not all Indicators of Compromise (IOCs) are created equal. The pyramid defines the pain it will cause adversaries when Defenders are able to deny those indicators to them.



	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web Analytics	Policy to Prevent Forum Use			Create fake postings	
Weaponization						
Delivery	NIDS, User Education	Email AV Scanning		Email Queuing	Filter but respond with out-of-office message	
Exploitation	HIDS	Patch	DEP			
Installation						
C2	NIDS	HTTP Whitelist	NIPS	HTTP Throttling		
Action on Objectives	Proxy Detection	Firewall ACL	NIPS	HTTP Throttling	Honeypot	

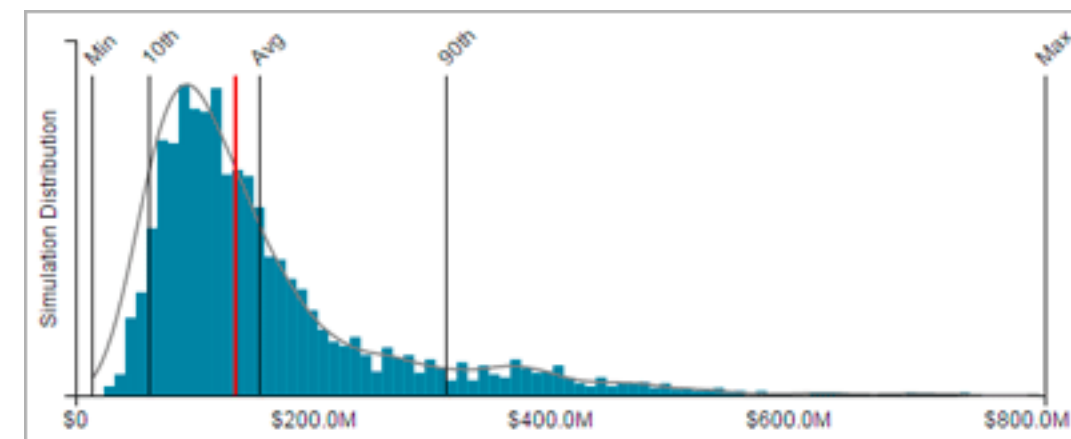
# FAIR Quantitative Risk Analysis

## Factor Analysis of Information Risk: approach to Operational and Cyber Risk Quantification

FAIR is a quantitative risk analysis model, whereas most information security risk methodologies in use today are Capability Maturity Models (CMM) or checklists.

Analytic models attempt to describe how a problem-space works by identifying the key elements that make up the environment and the relationships between those elements — e.g., Newton's laws of the physical world described how things like gravity work. If the models are relatively accurate (no models are perfect), then analyses performed using the models should consistently align with our experience and observations.

With those elements identified, measurements can be made that enable risk quantification and performance of what-if analyses, neither of which can be performed with checklist or CMM analyses.



***Risk = the probable frequency and probable magnitude of future loss***

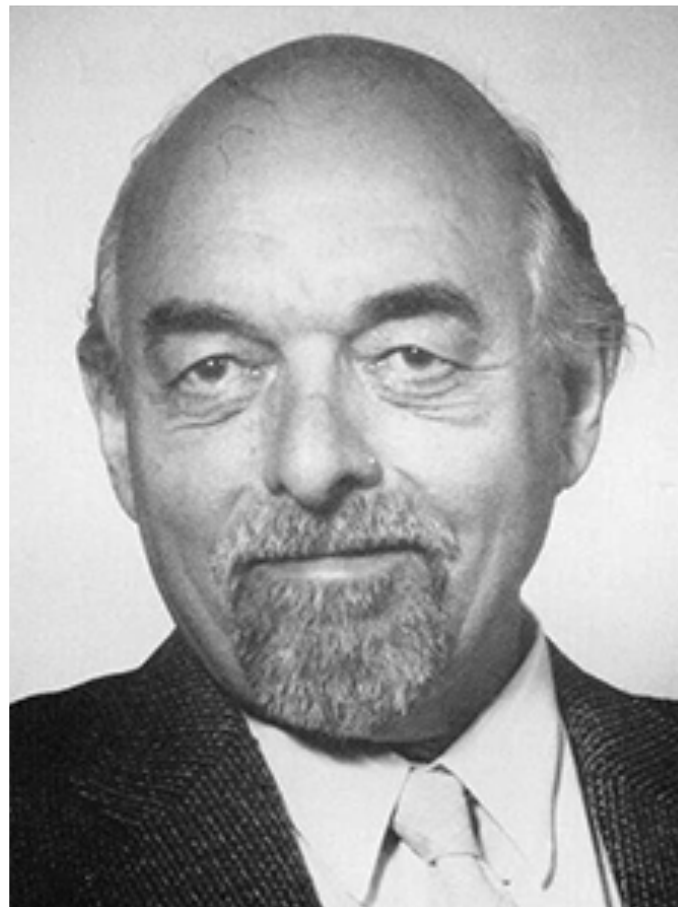
# If that's the case...

That seems like a sufficient amount of stuff to be able to assess our "resilience"

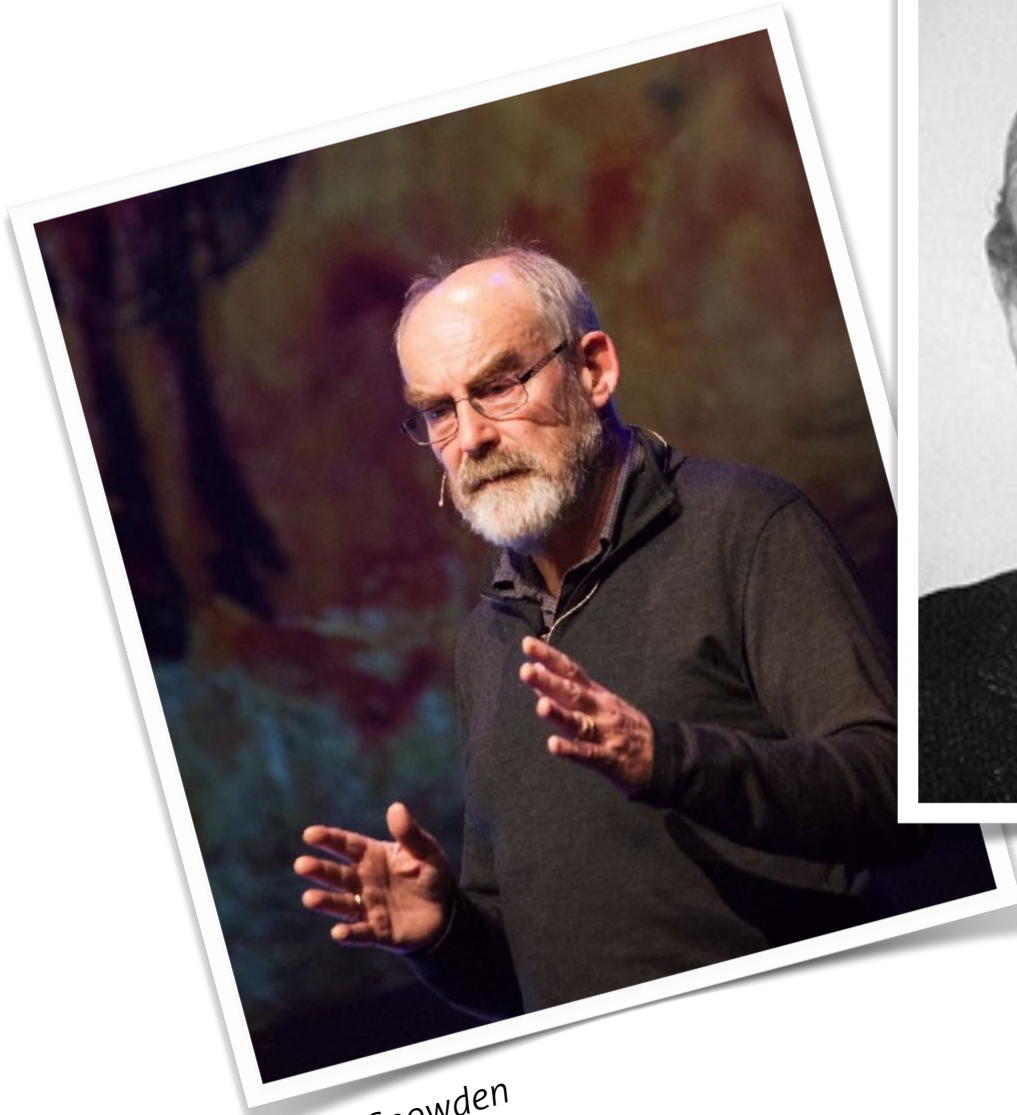


# These fellas disagree...

*Jens Rasmussen*



*Nicholas Taleb*



*Dave Snowden*



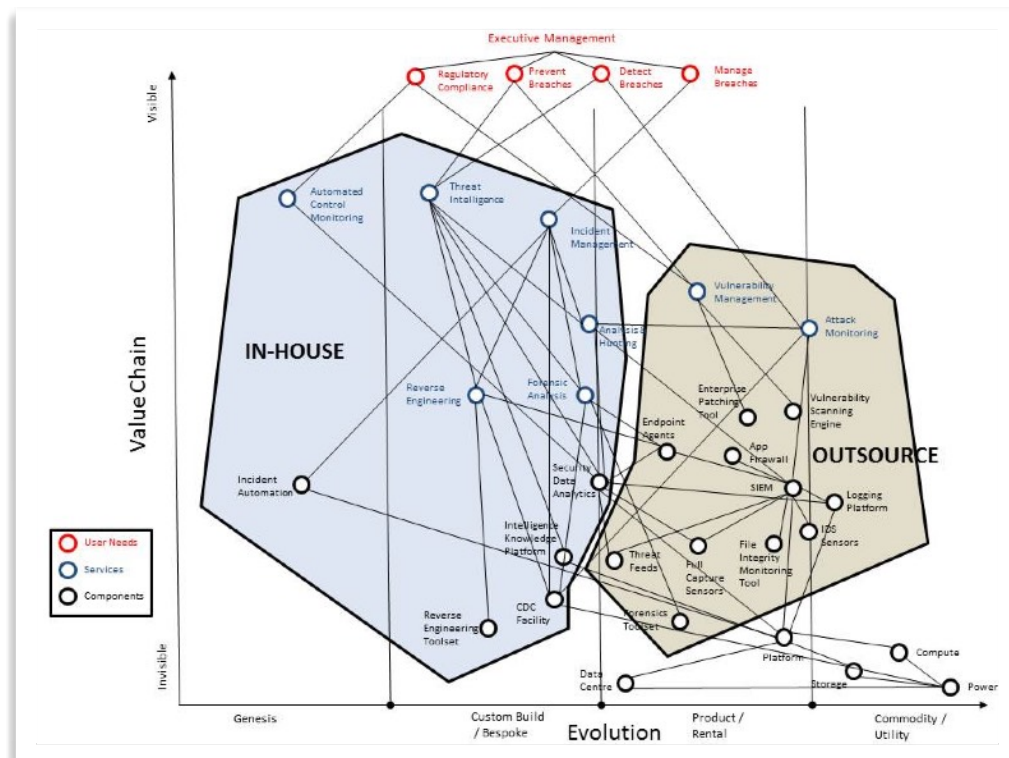
*Simon Wardley*





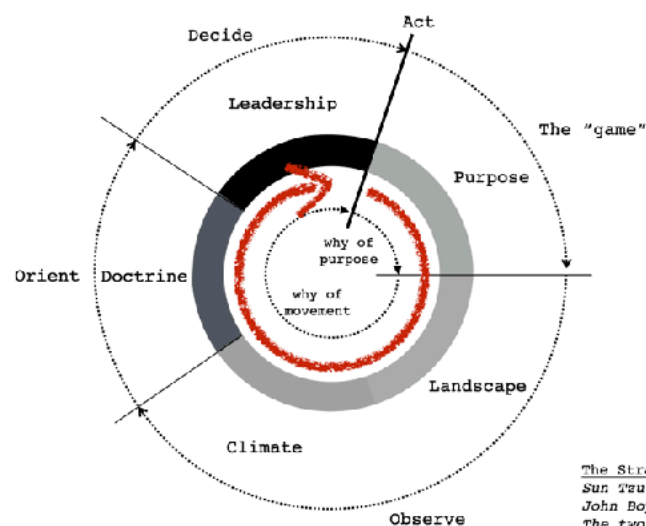
# Wardley Maps

A Wardley map is a map for strategy. Components are positioned within a value chain and anchored by the user need, with movement described by an evolution axis driven by doctrine.



"All maps are wrong. Some are useful."

Stage of Evolution	I	II	III	IV
x-axis labels (types of capital)	Activity (used)	Genesis	Custom	Product (+rental)
	Data (implied)	Unmodelled	Divergent	Convergent
	Practice (implied)	Novel	Emerging	Good
	Knowledge (implied)	Concept	Hypothesis	Theory
Characteristics				
Ubiquity	Rare	Slowly increasing	Rapidly increasing	Widespread in the applicable market / ecosystem
Certainty	Poorly understood / exploring the unknown	Rapid increases in learning / discovery becomes refining	Rapid increases in use / increasing fit for purpose	Commonly understood (in terms of use)
Publication Types	Describe the wonder of the thing / the discovery of some marvel / a new land / an unknown frontier	Focused on build / construct / awareness and learning / many models of explanation / no accepted forms / a wild west.	Maintenance / operations / installation / comparison between competing forms / feature analysis e.g. merits of one model over another	Focused on use / increasingly an accepted, almost invisible component
General Properties				
Market	Undefined market	Forming market / an array of competing forms and different models of understanding	Growing market / consolidation to a few competing but more accepted forms.	Mature market / stabilised to an accepted form
Knowledge management	Uncertain	Learning on use / focused on testing prediction	Learning on operation / using prediction / verification	known / accepted
Market (Ecosystem) Perception	Chaotic (non linear) / Domain of the "crazy"	Domain of "experts"	Increasing expectation of use / Domain of "professionals"	Ordered (appearance of being linear) / trivial / formula to be applied
User perception	Different / confusing / exciting / surprising / dangerous	Leading edge / emerging / uncertainty over results	Increasingly common / disappointed if not used or available / feeling left behind	Standard / expected / feeling of shock if not used
Perception in Industry	Future source of competitive advantage / unpredictable / unknown	Seen as a competitive advantage / a differential / looking for ROI and case examples	Advantage through implementation / features / this model is better than that	Cost of doing business / accepted / specific defined models
Focus of value	High future worth but immediate investment	Seeking ways to profit and a ROI / seeking confirmation of value	High profitability per unit / a valuable model / a feeling of understanding / focus on exploitation	High volume / reducing margin / important but invisible / an essential component of something more complex
Understanding	Poorly understood / unpredictable	Increasing understanding / development of measures	Increasing education / constant refinement of needs / measures	Believed to be well defined / stable / measurable
Comparison	Constantly changing / a differential / unstable	Learning from others / testing the water / some evidential support	Competing models / feature difference / evidential support	Essential / any advantage is operational / accepted norm
Failure	High / tolerated / assumed to be wrong	Moderate / unsurprising if wrong but disappointed	Not tolerated / focus on constant improvement / assumed to be in the right direction / resistance to changing the model	Surprised by failure / focus on operational efficiency
Market action	Gambling / driven by gut	Exploring a "found" value	Market analysis / listening to customers	Metric driven / build what is
Efficiency	Reducing the cost of change (experimentation)	Reducing cost of waste (Learning)	Reducing cost of waste (Learning)	Reducing cost of deviation (Volume)
Decision Drivers	Heritage / culture	Analysis & synthesis	Analysis & synthesis	Previous experience



The Strategy Cycle  
Sun Tzu's five factors  
John Boyd's OODA loop  
The two types of why

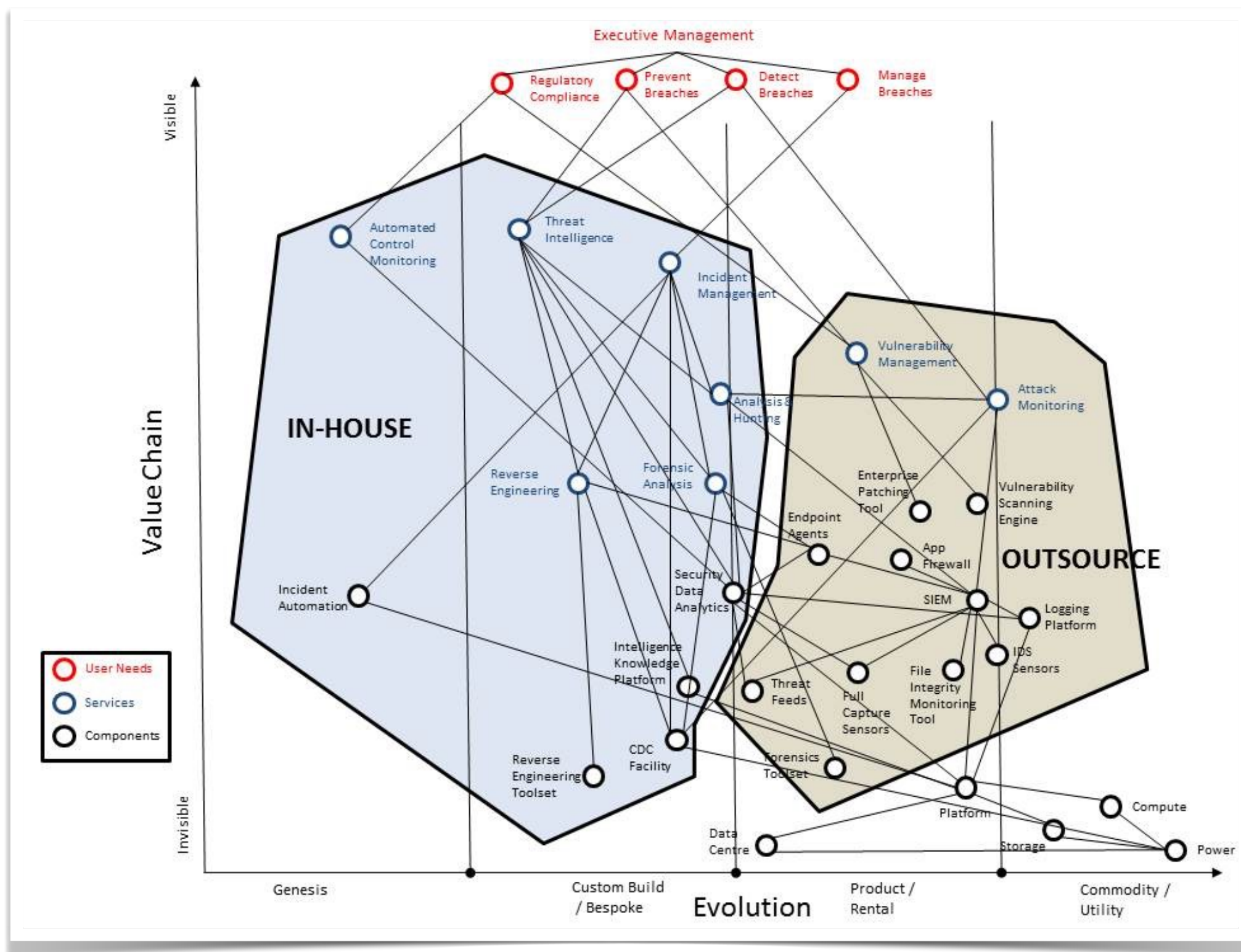
<https://learnwardleymapping.com/>

<https://twitter.com/swardley/status/1041658298427211778>

<https://www.securitydifferently.com/the-future-of-infosec-is-interdisciplinary-and-integrated/>



# Wardley Maps

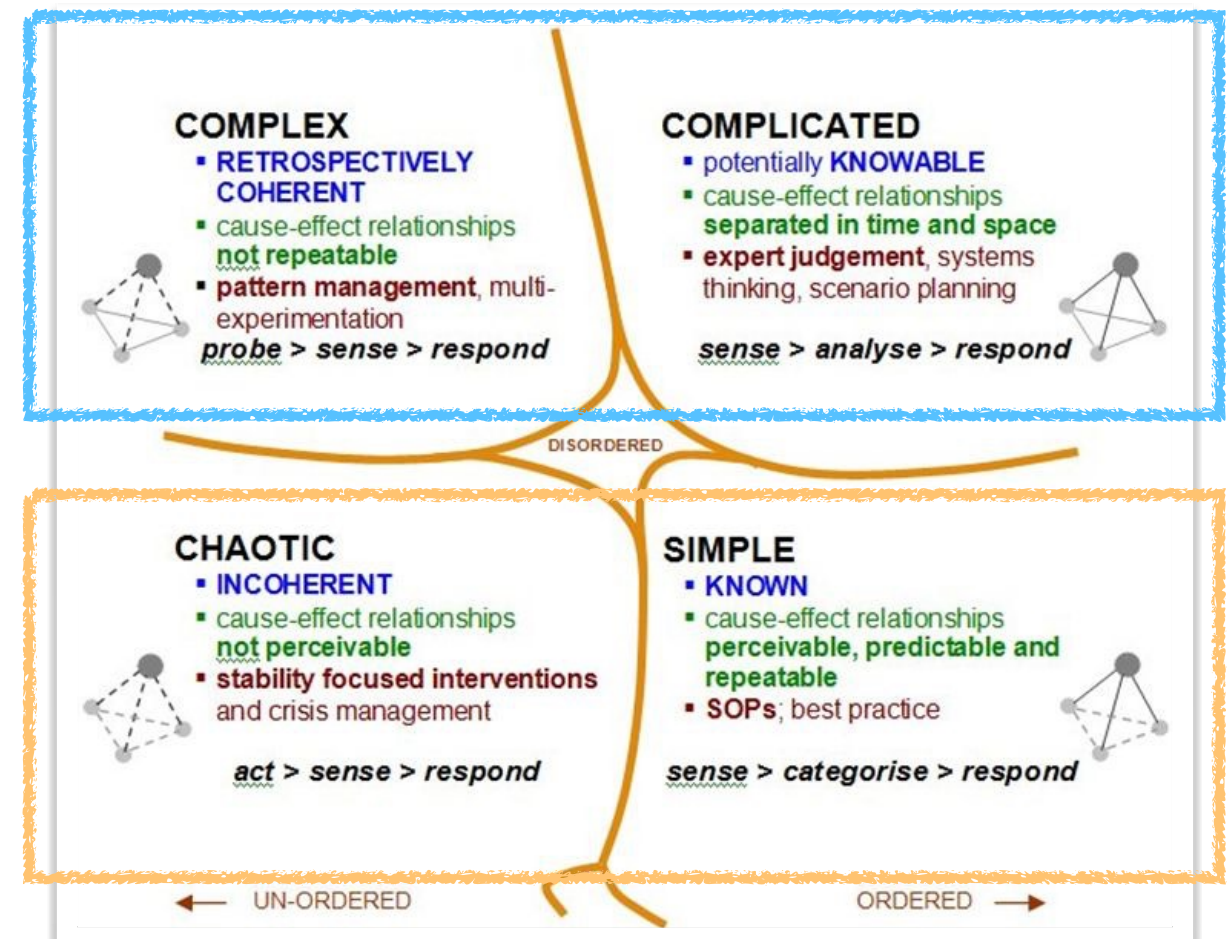
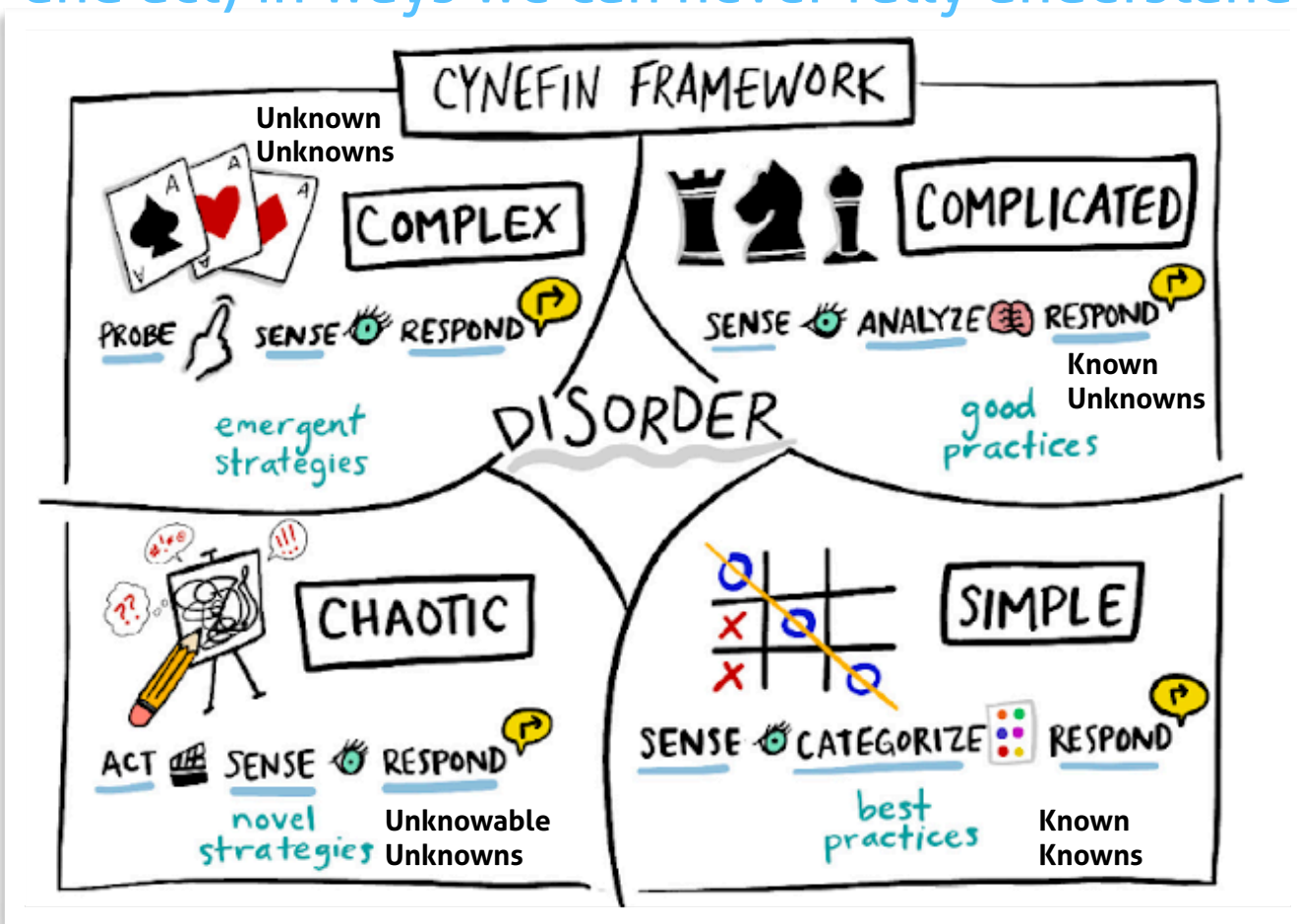






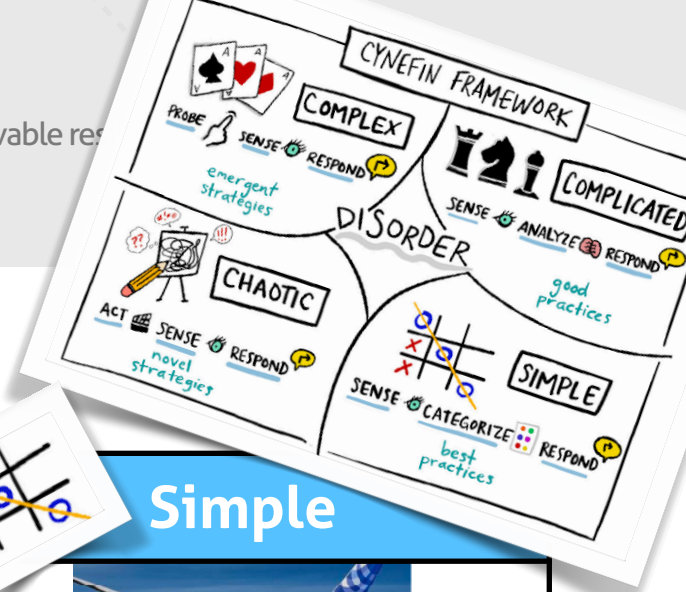
# The Cynefin Framework

Cynefin (kuh-nev-in) is a Welsh word for Habitat that signifies the multiple, intertwined factors in our environment and our experience that influence us (how we think, interpret and act) in ways we can never fully understand

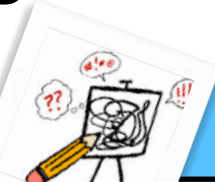









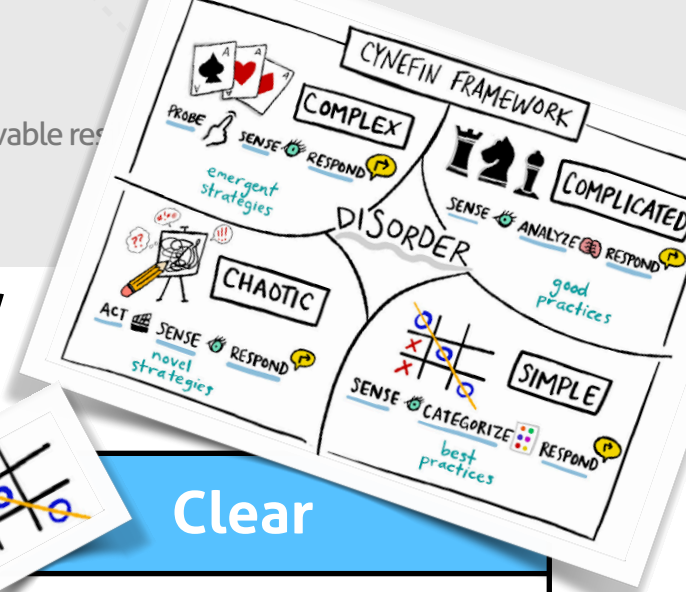
The system is dynamic, the whole is greater than the sum of its parts, and solutions can't be imposed; rather, they arise from the circumstances...and involves large numbers of interacting elements. The interactions are nonlinear, and minor changes can produce disproportionately major consequences. The system has a history, and the past is integrated with the present; the elements evolve with one another and with the environment; and evolution is irreversible.





# Cynefin in Practice - Aeronautics

 <b>Chaotic</b>	 <b>Complex</b>	 <b>Complicated</b>	 <b>Simple</b>
			
<p>At first, nobody knew “what to do to fly”.</p> <p>Everyone suspected that it could be possible by imitating birds, but really, no one had a clue.</p>	<p>As soon as the Wright brothers developed the first successful prototype airplane, everyone started to know where things were heading.</p> <p>Two wings, a front Propeller, etc.</p>	<p>Years passed and aircraft design began to improve.</p> <p>However, there was a problem:</p> <p>Long and transoceanic flights were a real challenge.</p>	<p>Today, there are no mysteries for aircraft designers.</p> <p>They know exactly how to design a safe, durable and fast airplane that can fly anywhere in the world.</p>
<p>Many people <b>tried</b> to develop a “flying machine” by building different designs.</p> <p>Sometimes, these designs looked weird but... Who knew...</p>	<p>A good stable and safe plane was still a long way off, but people had clues to follow.</p>	<p>Engineers knew what they needed, but not exactly how to get it:</p> <ul style="list-style-type: none"> <li>• Isolated cabins.</li> <li>• Resistant materials.</li> <li>• Light fuselages.</li> <li>• Good Turbines</li> <li>• Cost-efficient.</li> </ul>	<p>There are still challenges in the aircraft industry? Of course.</p> <p>But the development of a normal airplane that covers the basic needs of “flight” is well known in the aeronautical industries</p>
<p>How could people make good decisions?</p> <p>Just trying things out and learning what worked and what didn’t.</p>	<p>How could engineers make the best decisions?</p> <p>By Testing what was already known and making small improvements.</p>	<p>How could engineers make the best decisions?</p> <p>By analyzing hundreds of materials, designs and Test them to get what they knew they needed.</p>	<p>If a group of engineers want to develop a new plane in this Clear situation:</p> <p>They would apply all existing knowledge and follow the Steps necessary to build it.</p>



# Cynefin in Practice - Perimeter Security



Chaotic



Complex

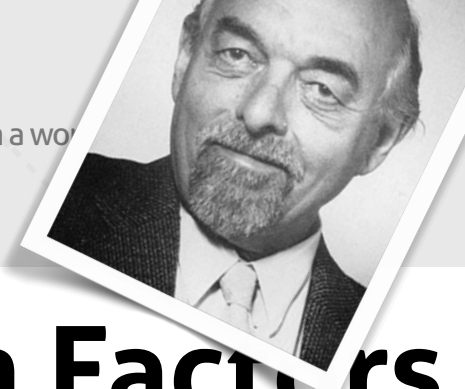


Complicated



Clear

Left as an  
exercise for  
the reader



# Jens Rasmussen: Safety Science & Human Factors

Cognitive Resilience, Dynamic Safety Models, Socio-Technical systems, Skills/Rules/Knowledge (SRK)

4 Major Themes emerge from Rasmussen's work:

1. Human operator performance results from behavior, shaping constraints that we can identify and model
2. The human operator is a flexible and adaptive element who "completes the design of the technical system (and compensates for its shortcomings)"
3. Human operators cope with complexity by applying mental models and modes of performance (See: SRK Model)
4. Risk management requires an understanding of the socio-technical context of work

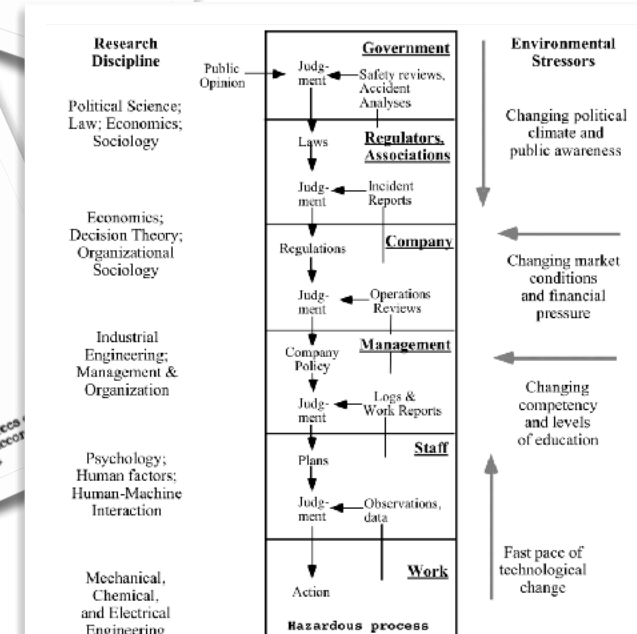
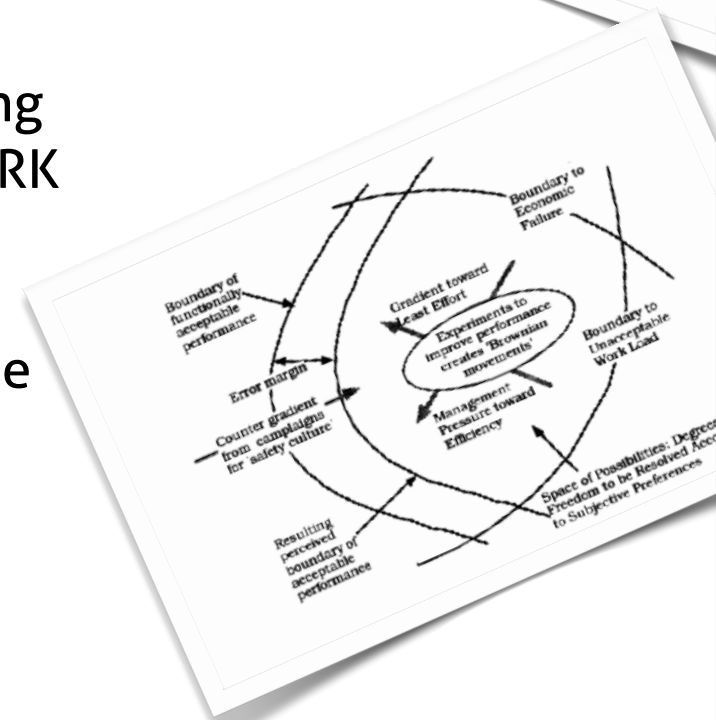
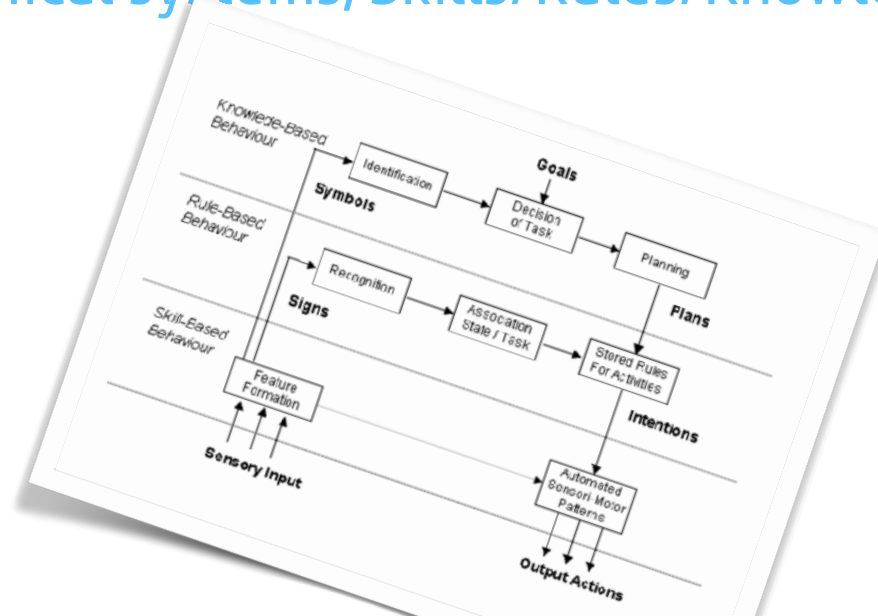


Figure 1. The socio-technical system involved in risk management.

**Cognitive Resilience: System resilience implies practitioners' capacity to cope with unexpected events**



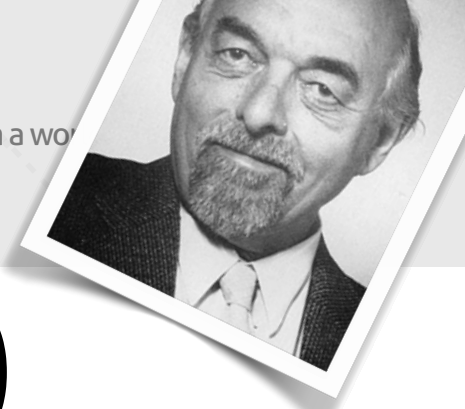


**It's made of  
PEOPLE!**

# So?

How do we apply all this stuff to what we do in InfoSec





# Jens Rasmussen: On Risk (& Antifragility)

Risk Management is complex...requires different strategies based on context

## Real-World Risk Management requires multiple strategies

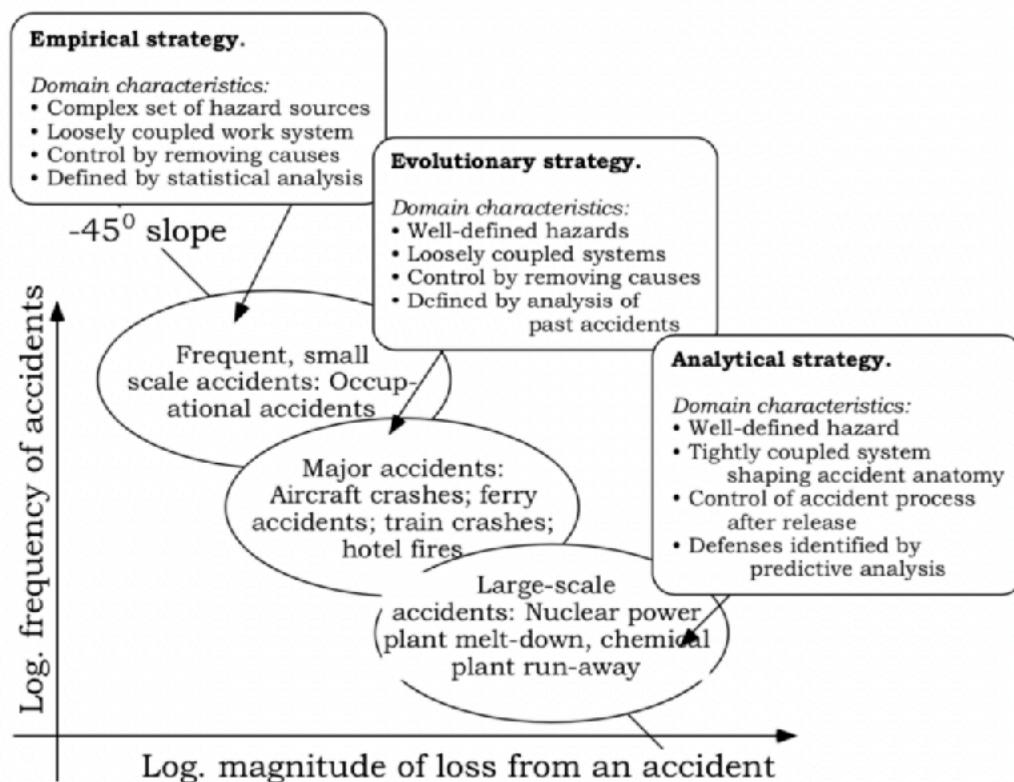


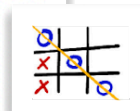
Figure 7. Hazard source characteristics and risk management strategies.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27(2-3), 183-213. [https://doi.org/10.1016/S0925-7535\(97\)00052-0](https://doi.org/10.1016/S0925-7535(97)00052-0)

**Empirical strategy** - where we can apply simple controls (automated governance), things happen often so it's simple to study and discuss with operators best approaches and heuristics to control them

**Evolutionary strategy** - we can analyse past events and understand how different parts of sociotechnical system interacted to produce conditions which led to incidents

**Analytical Strategy** - well-defined hazards but entanglements of systems are numerous, requires appreciation and understanding of entanglements and how failures in one part of the system can affect other parts



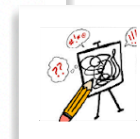
Simple



Complicated

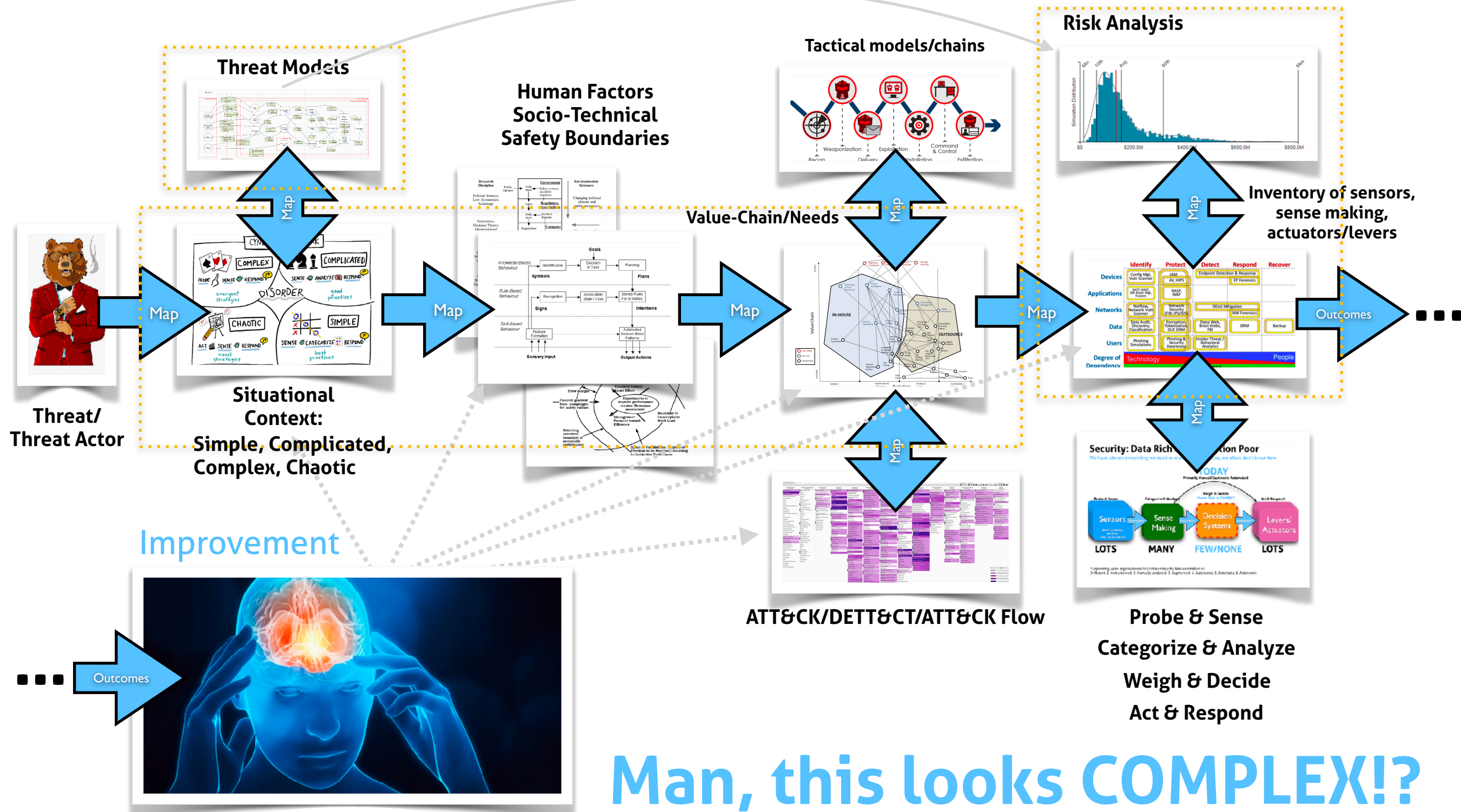


Complex



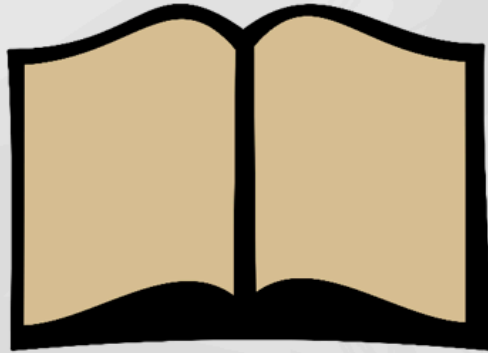
Chaotic

Here's where we might consider industrializing decision making systems into our workflow





# Conventional Wisdom in Defense



## Traditional Defenders

Defend a list of assets

Manage incidents

Minimize risks by keeping incidents secret

View pentest results as a report card

Think about stopping attacks

## Modern Defenders

Defend a graph of assets

Manage adversaries

Maximize learning by sharing incidents with trusted outside peers

View pentest results as an input

They think about increasing attacker requirements

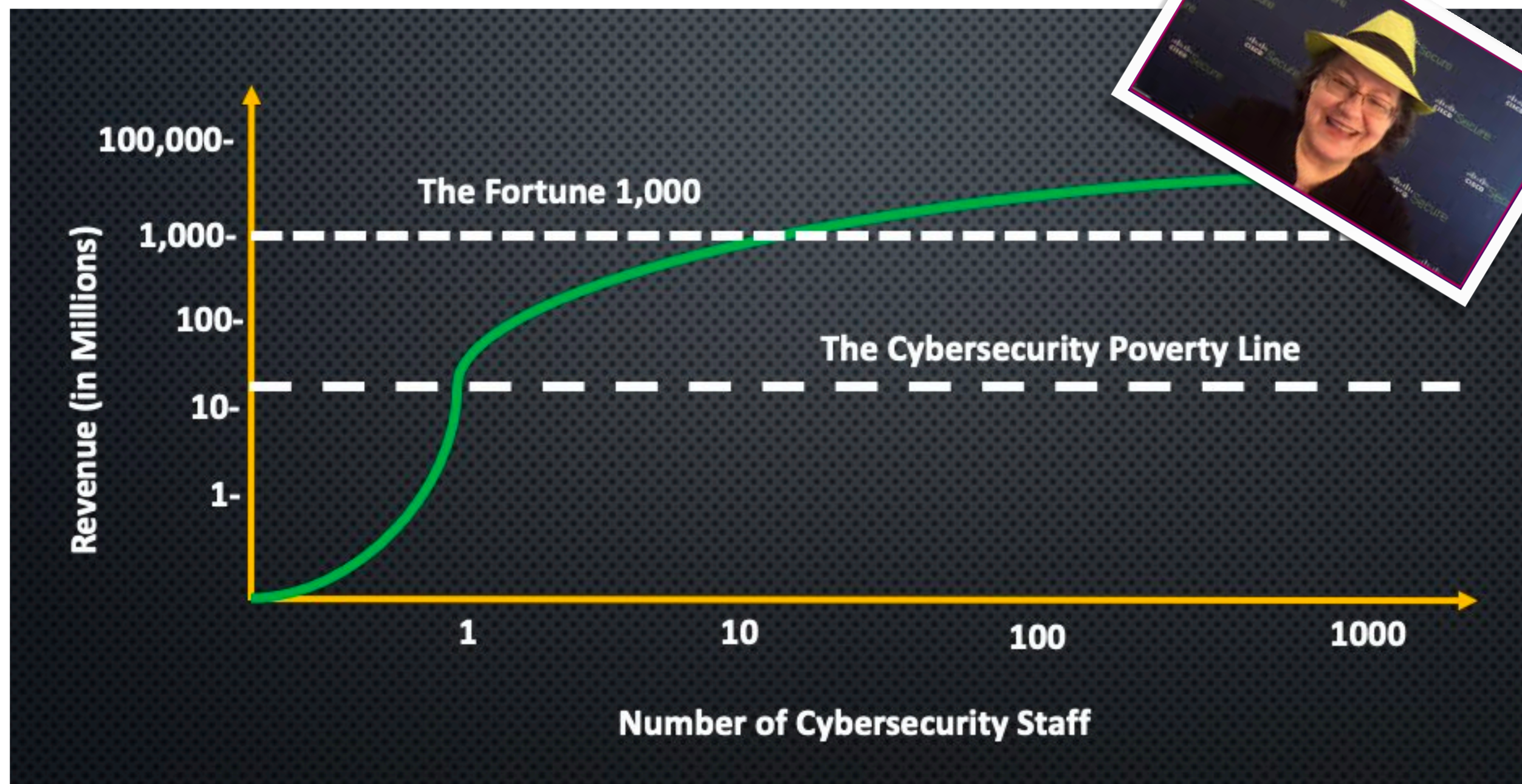


# Modern Defense In Action -Glimmers of Antifragility

- ▶ *Diffused & Embedded Security*
- ▶ *CI+CD & Security-as-a-service (CS)*
- ▶ *Cloud & Site Reliability Engineering*
- ▶ *Observability & Detection Engineering*
- ▶ *Robust Threat & Risk Modeling*
  - ▶ *Chaos Engineering*
  - ▶ *Team Topologies*

OBJECTS IN MIRROR ARE  
CLOSER THAN THEY APPEAR





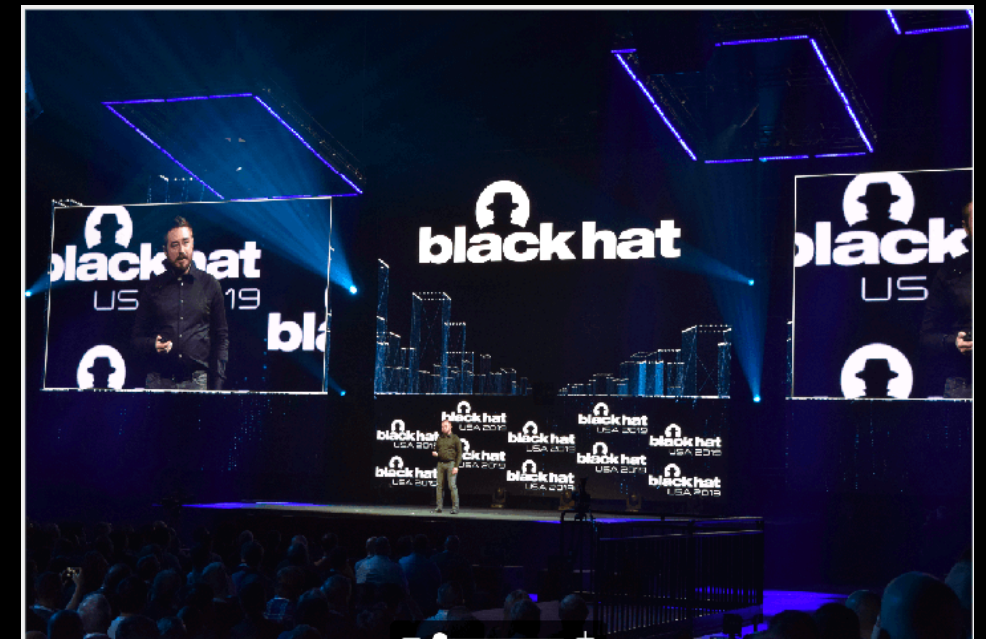
The majority of these Modern Defender's capabilities  
are NOT Technology investments...



There are two big shifts involved as teams begin to own their end-to-end impact: **software teams need to own their own security now and security teams need to become full-stack\* software teams.** Just as separate product management and quality assurance organizations diffused into cross-functional software teams, security must now do the same. At his re:Invent 2018 Keynote, Amazon's CTO Werner Vogels proclaimed that **"security is everyone's job now, not just the security team's."**

But if security is every teams' job, what is the security team's job? Just like how classic ops teams became internal infrastructure software teams, **security teams will become internal security software teams that deliver value to internal teams through self-service platforms and tools.** Security teams that adopt this approach will reduce the risk to the organization the most while also minimizing impact to overall productivity."

## (r)Evolution



**\*/me = the inclusion of this word is, IMHO, debatable depending on the definition of "stack"**



# So we should just rename ourselves, right?

Something, something Emperor & lack of clothing...

## Do we even want DevSecOps ?

### DevSecOps

**Abhay Bhargav** @abhaybhargav · Feb 24, 2019  
Replying to @dinodalzovi  
For one, **devsecops** fosters (or at least aims to) more collaboration with cross functional teams than traditional enterprise security constructs. Working with cross functional teams leads to a codified knowledge base (automation) and the cycle continues. 1/

**Avi Douglan** @sec\_bigger · Dec 5, 2019  
Replying to @secfigo @EndlessMason and 2 others  
Absolutely agree with this! For now, we still need to treat it like something on its own - because that's what it is, right now. But it shouldn't be, and that is what we need to be working towards, when **DevSecOps** is not a thing.

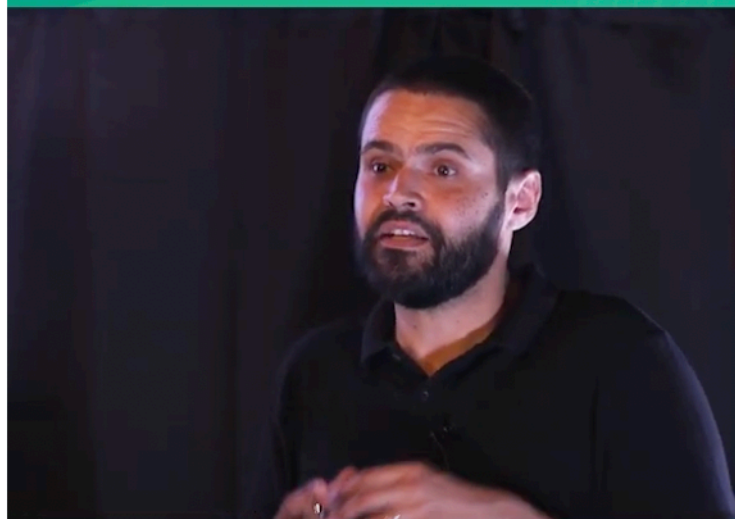
### Not DevSecOps

**Dino A. Dal Zovi** @dinodalzovi · Jul 21, 2019  
Replying to @basoule and @thephreck  
Yeah, I feel like a lot of "**DevSecOps**" still doesn't quite get the most important aspect of having security "be" engineering teams to increase empathy. Working to secure the org using the same tools and same environment prevents "do as I say, not as I do."

**Kelly Shortridge** @RSAC @swagitda · Jun 5, 2019  
Replying to @swagitda @anton\_chuvakin and @nicolelv  
My definition of **DevSecOps** is "a marketing term invented for security professionals who don't understand how to work with DevOps but who want to preserve their relevancy without real effort, ideally by buying a solution they understand with a new shiny label"



**Evolving Security in context - Mario Platt**  
people | process | technology



MORE VIDEOS

If your strategy mentions the word 'DevSecOps' or Security in DevOps and you're not

- Helping your Governance teams benefit from short feedback loops and training them to understand DevOps
- Not increasing the agency and ownership of security across your Product or Project teams in THEIR language, not YOURS
- Not enabling the best possible Developer and Engineering Experience of Security you can afford
- Not actively trying to breakdown silo-ed barriers and connect governance systems

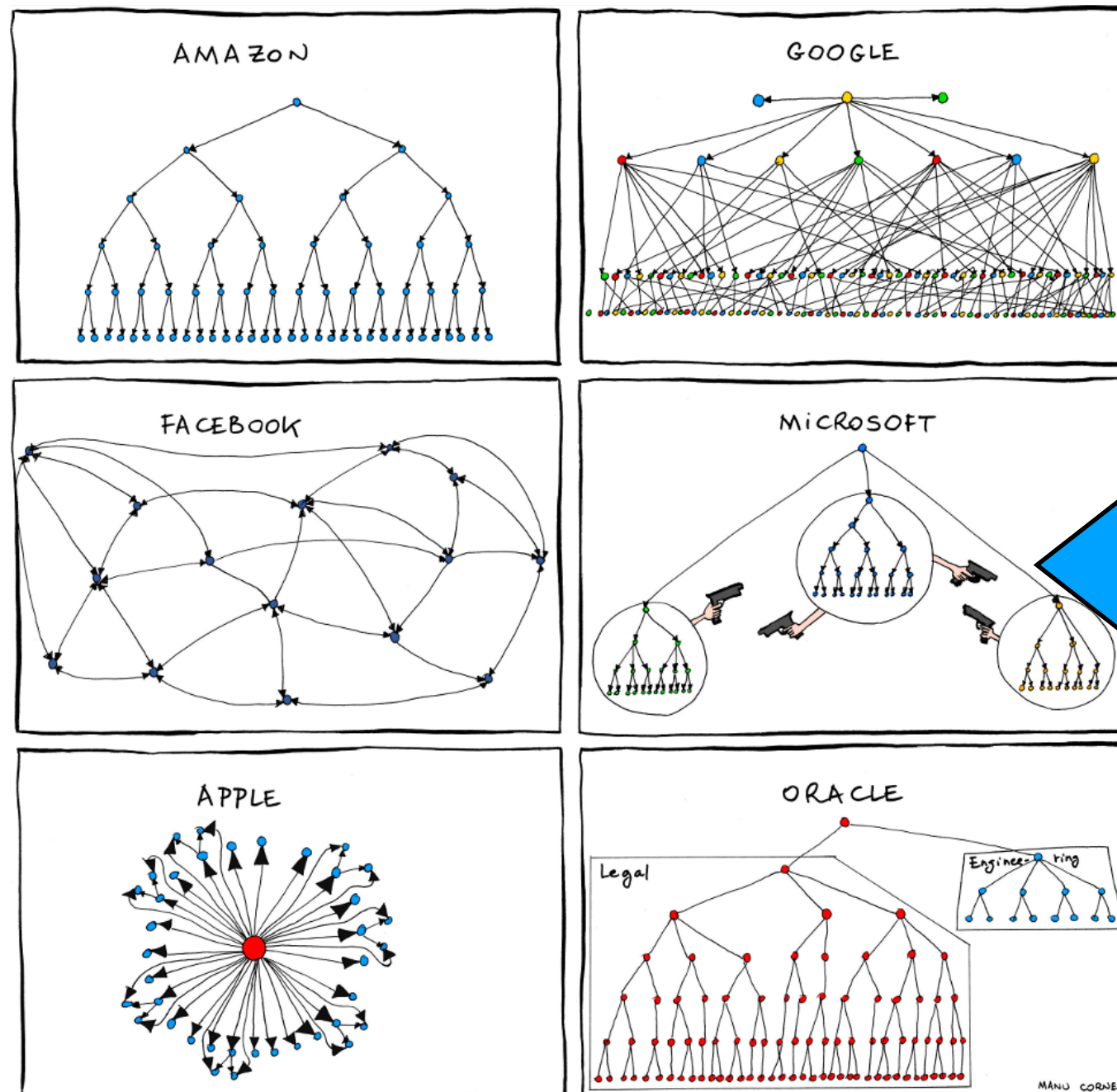
You're probably doing it wrong!

broadlight.io

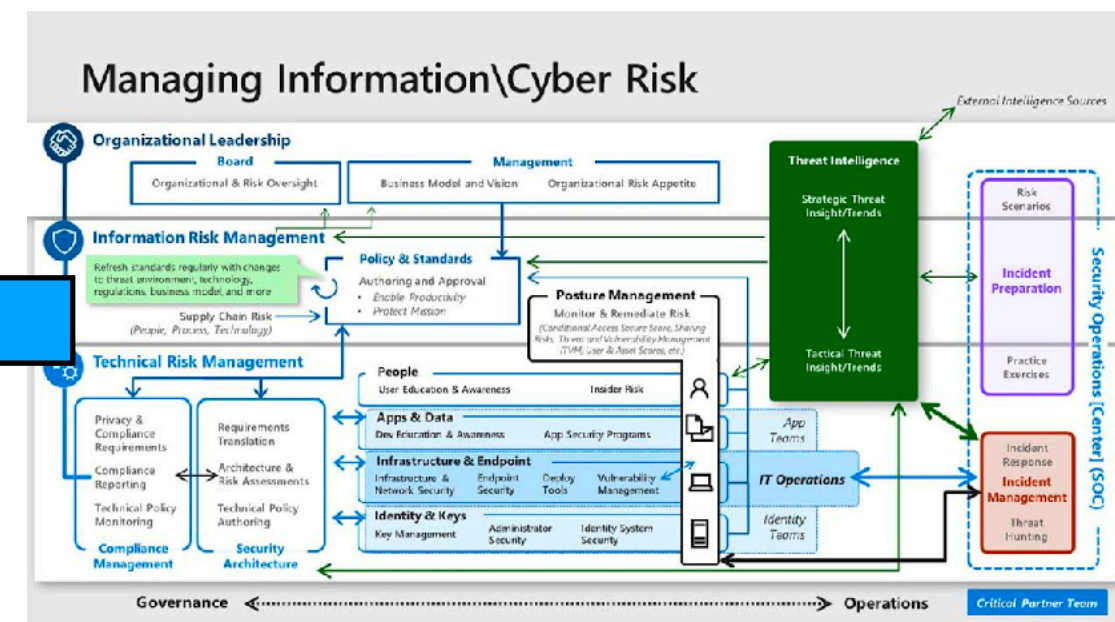


# Conway's Law

Organizations, who design systems, are constrained to produce designs which are copies of the communication structures of these organizations.

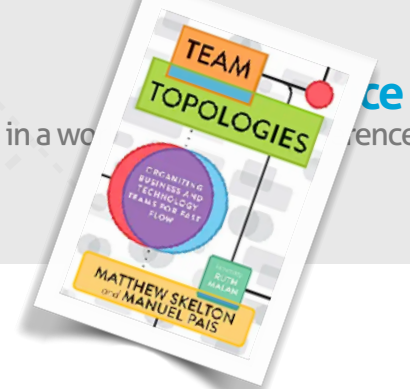


## THE SAME GOES FOR SECURITY ORGS!



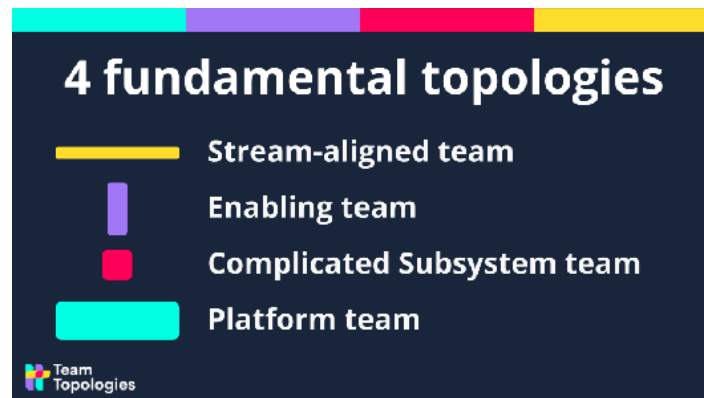
The **Reverse Conway Maneuver** should align teams and architectures in a manner that lowers cognitive load, minimizes dependencies, and matches product direction.





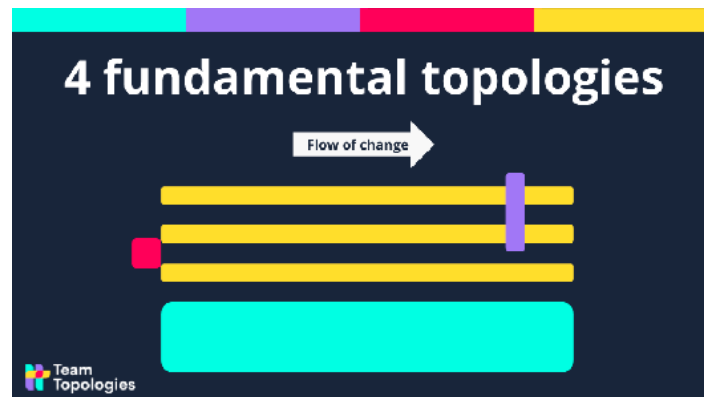
# Team Topologies In a Nutshell

Focuses on creation of dynamic team structures and interaction modes that can help teams adapt quickly to new conditions, and achieve fast and safe software delivery.



## FOUR FUNDAMENTAL TOPOLOGIES

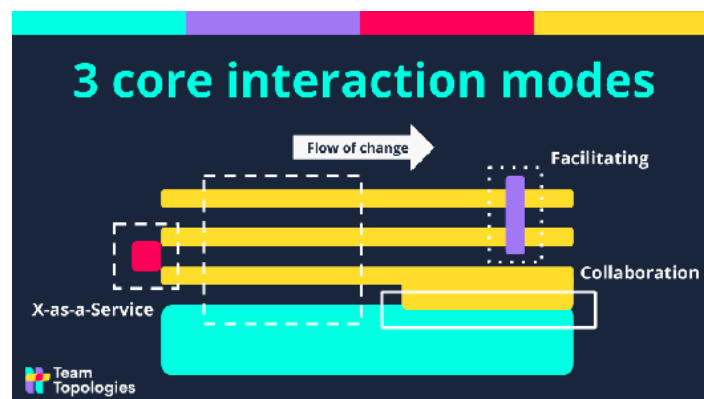
- Stream-aligned team: aligned to a flow of work from (usually) a segment of the business domain
- Enabling team: helps a Stream-aligned team to overcome obstacles. Also detects missing capabilities.
- Complicated Subsystem team: where significant mathematics/calculation/technical expertise is needed.
- Platform team: a grouping of other team types that provide a compelling internal product to accelerate delivery by Stream-aligned teams



## FOUR FUNDAMENTAL TOPOLOGIES - WITH THE FLOW OF CHANGE

The flow of change is shown left-to-right. Stream-aligned teams own an entire slice of the business domain (or other flow) end-to-end. The Stream-aligned teams are “You Built It, You Run It” teams.

There are no hand-offs to other teams for any purpose. This diagram is a snapshot in time. The team relationships WILL change as new goals are set and the teams discover new things.



## THREE TEAM INTERACTION MODES

There are only three ways in which team should interact:

- Collaboration: working together for a defined period of time to discover new things (APIs, practices, technologies, etc.)
- X-as-a-Service: one team provides and one team consumes something “as a Service”
- Facilitation: one team helps and mentors another team

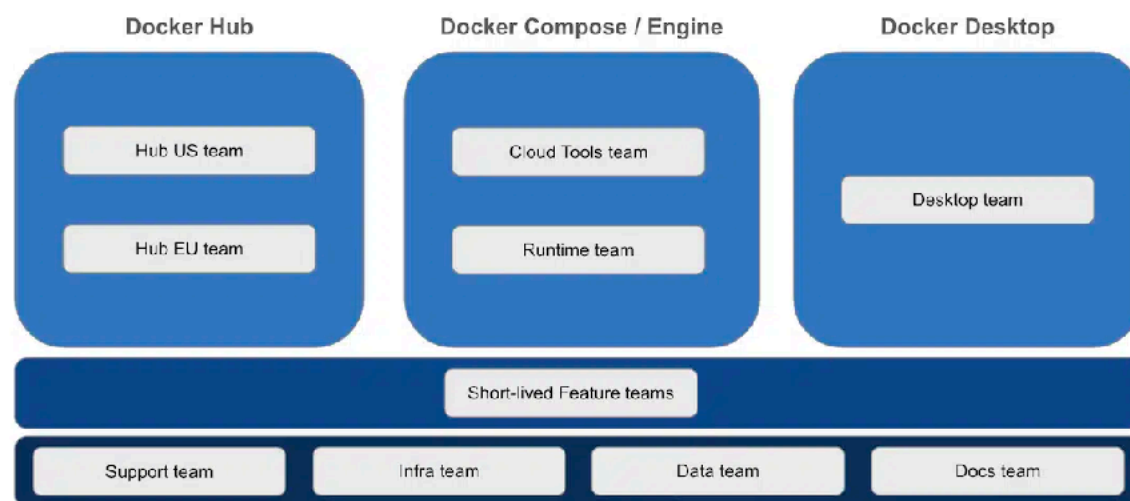
# Team Topologies — Enabling flow in SWE

What does this look like in reality?

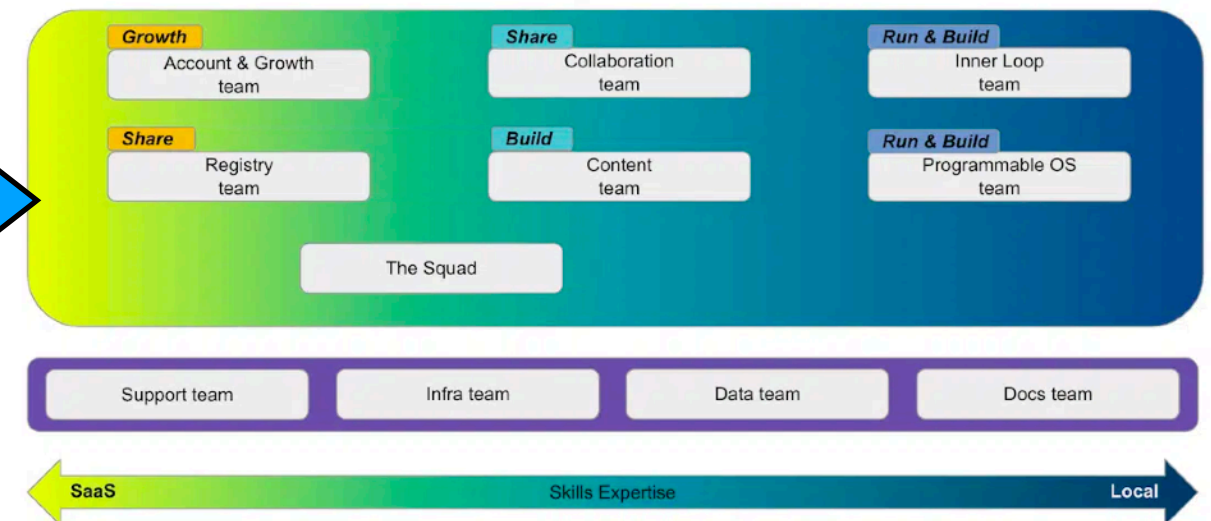


## Building Stronger, Happier Engineering Teams with Team Topologies

Docker Product Development - **Previous** Structure

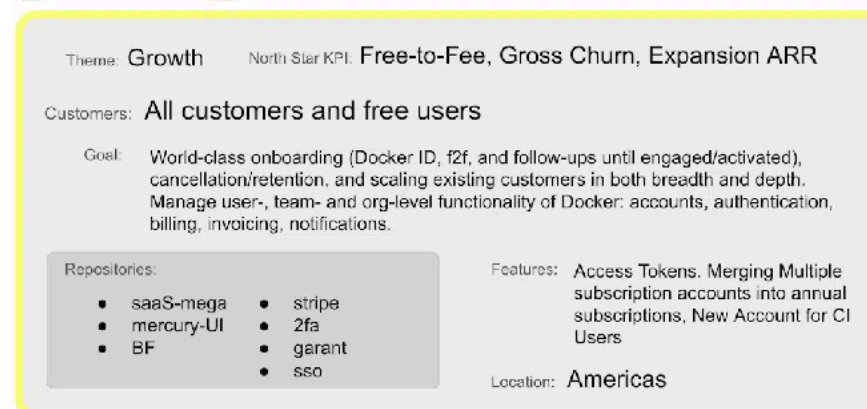


Docker Product Development - **New** Structure



### Accounts & Growth Team

Stream-Aligned SaaS expertise

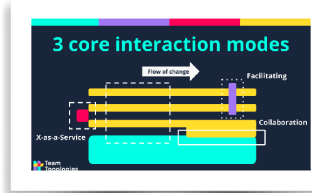
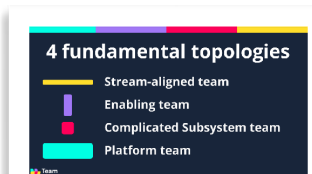
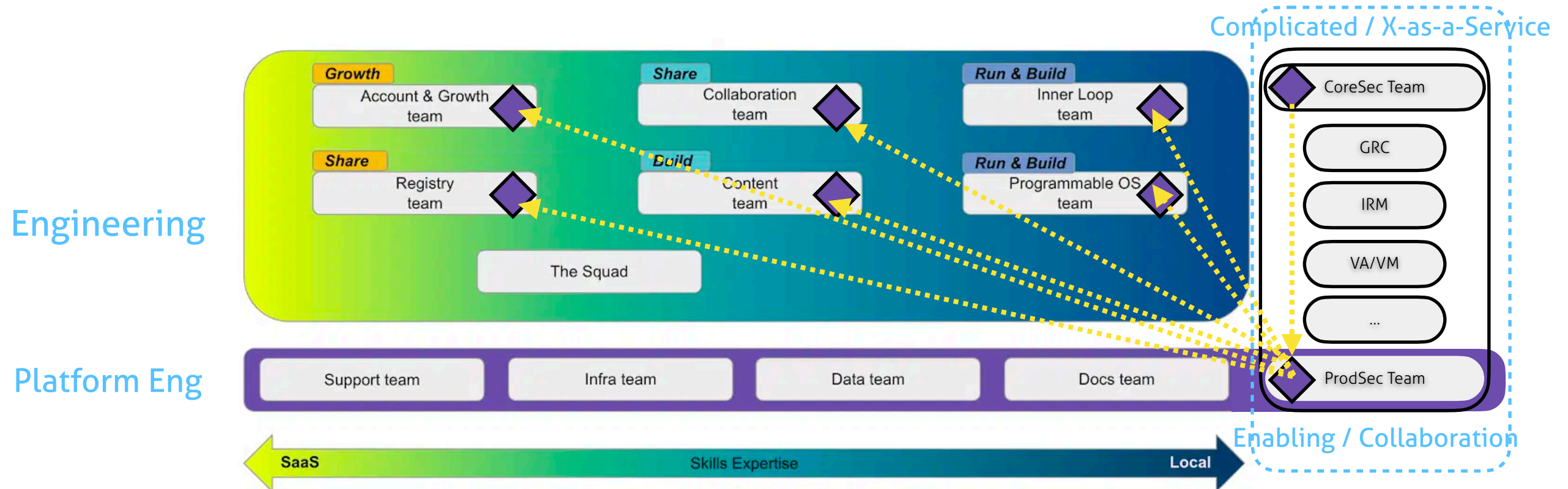




# Team Topologies — Bursting the InfoSec Org Bubble

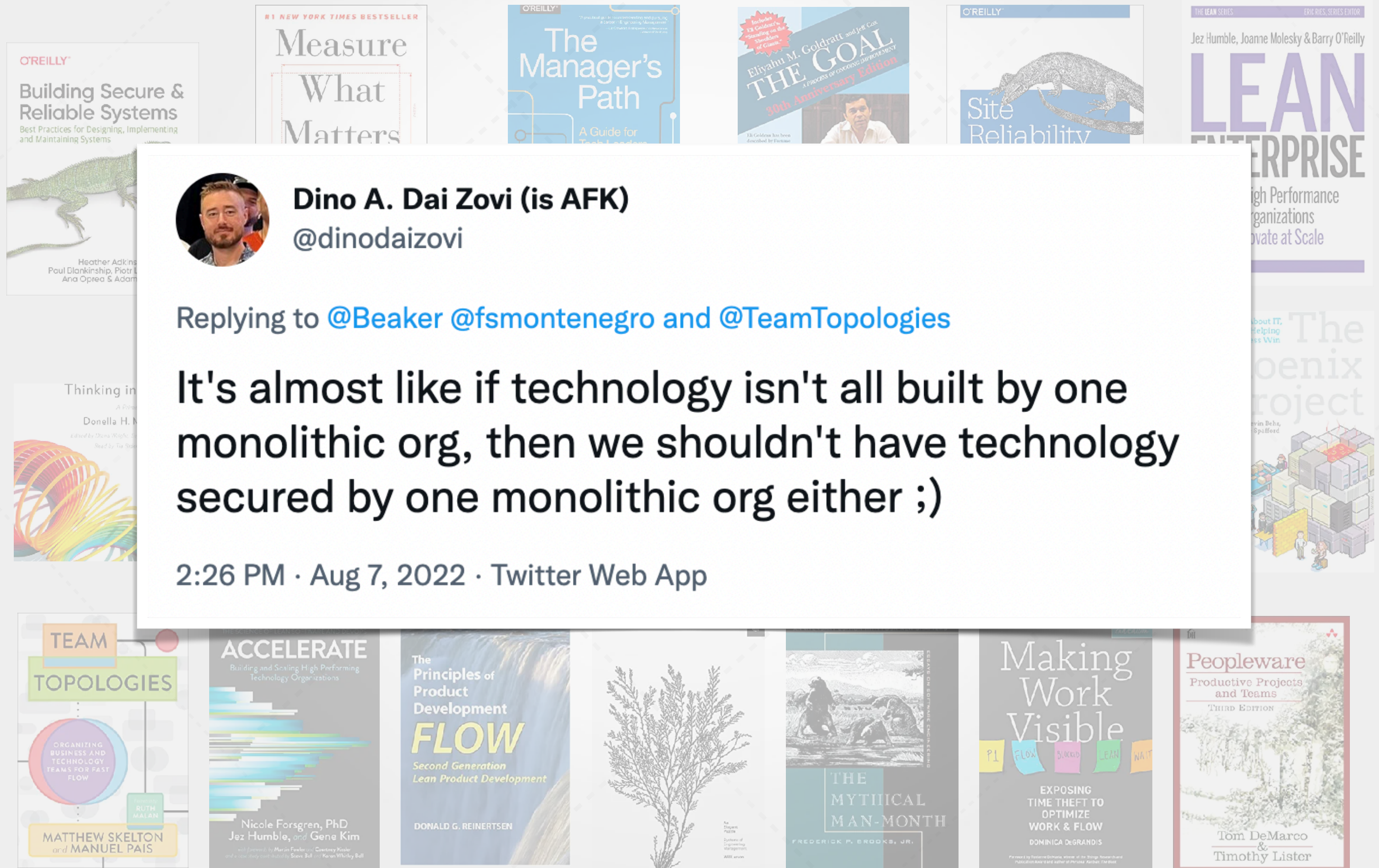
Modern organizations are at odds with compliance-designed security monoliths

## Docker Product Development - New Structure



- Stream-aligned team: aligned to a flow of work from (usually) a segment of the business domain
- Enabling team: helps a Stream-aligned team to overcome obstacles. Also detects missing capabilities.
- Complicated Subsystem team: where significant mathematics/calculation/technical expertise is needed.
- Platform team: a grouping of other team types that provide a compelling internal product to accelerate delivery by Stream-aligned teams
- Collaboration: working together for a defined period of time to discover new things (APIs, practices, technologies, etc.)
- X-as-a-Service: one team provides and one team consumes something "as a Service"
- Facilitation: one team helps and mentors another team

Please note: this is MY extrapolation of how one might envision extending a Team Topologies approach to include security in this org redesign





# Lest we forget: The Rugged Manifesto

Aimed at developers, but given the prior slides, should be applicable to evolved security teams...especially if security organizations become software engineering organizations...

## What is Rugged?

*“Rugged” describes software development organizations that have a culture of rapidly evolving their ability to create available, survivable, defensible, secure, and resilient software. Rugged organizations use competition, cooperation, and experimentation to learn and improve rather than making the same mistakes over and over.*

...

*Rugged is NOT a technology, process model, SDLC, or organizational structure. It's not even a noun. Rugged is NOT the same as secure. Secure is a possible state of affairs at a certain point in time. But rugged describes staying ahead of the threat over time.*

### The Rugged Manifesto

I am rugged and, more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

I recognize these things - and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

I am rugged, not because it is easy, but because it is necessary and I am up for the challenge.

# But my company doesn't develop software?

That may be true, but you consume it, and as such, you're subject to the same challenges...



**Mark Andreessen**  
founder of Netscape,  
renowned Venture Capitalist  
Andreessen-Horowitz

Software is eating the  
world, in all sectors

In the future every  
company will become a  
**software** company

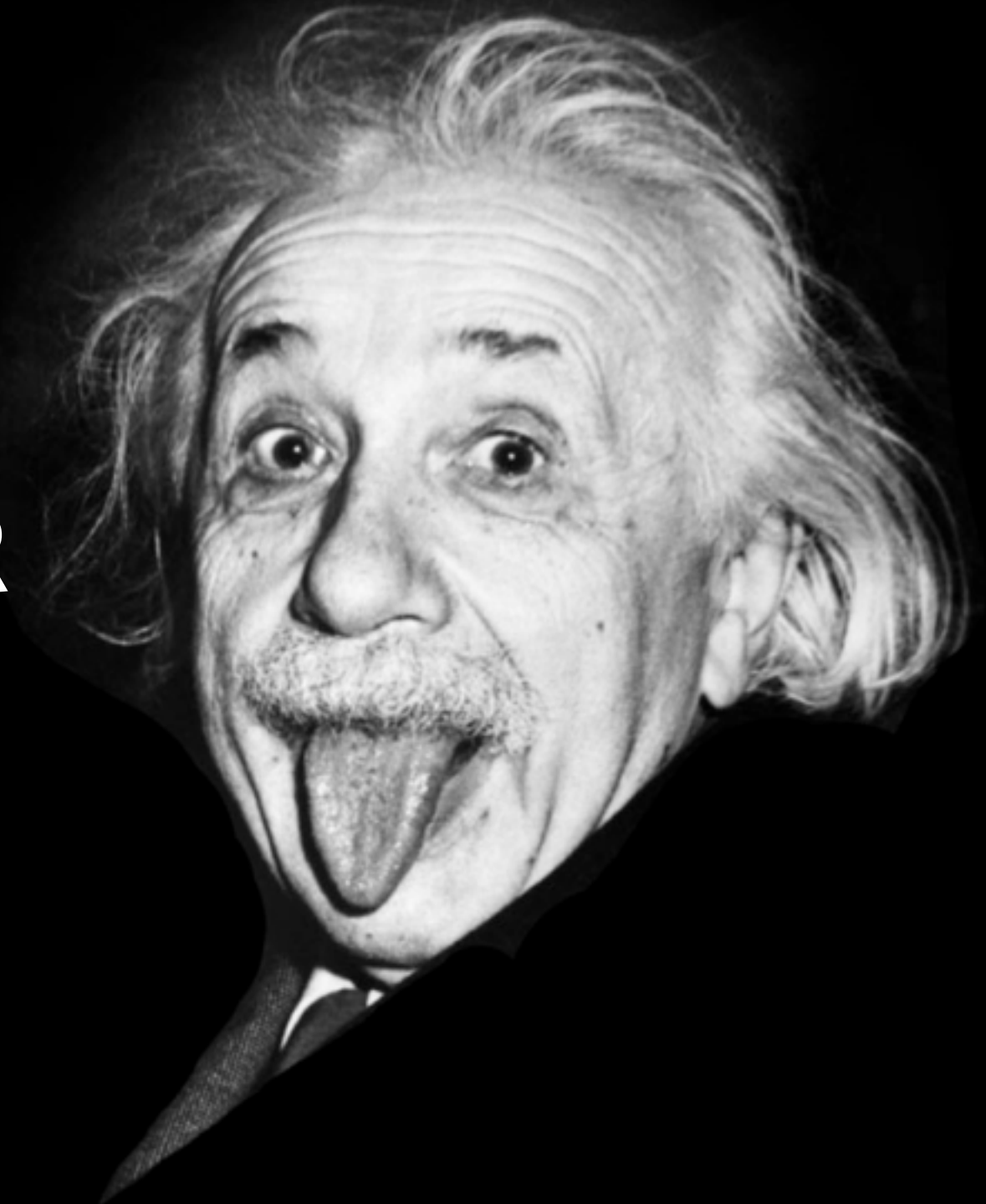
The Uber logo, consisting of the word "Uber" in white sans-serif font on a black rectangular background.The Amazon logo, consisting of the word "amazon" in black lowercase sans-serif font with a curved orange arrow underneath it.The Netflix logo, consisting of the word "NETFLIX" in bold red uppercase sans-serif font.

*Whether you develop or own the software you're using or not, the same principles apply. You must consider how everything we just discussed affects your "resilience," — and antifragility.*

*In many cases, putting your most critical business processes and data in the hands of SaaS vendors with little to no recourse should something bad happen to them is potentially an even worse case scenario...*



**INSANITY:**  
**DOING THE SAME**  
**THING OVER & OVER**  
**AND EXPECTING**  
**DIFFERENT RESULTS**





# Leadership



Waiting for an extinction event



# Organization & Culture



**Not My Monkey...**



# Signal vs Noise

**Cognitive Load**



# Outcomes



**Surviving vs Thriving**



# Incentives



**Punitive**



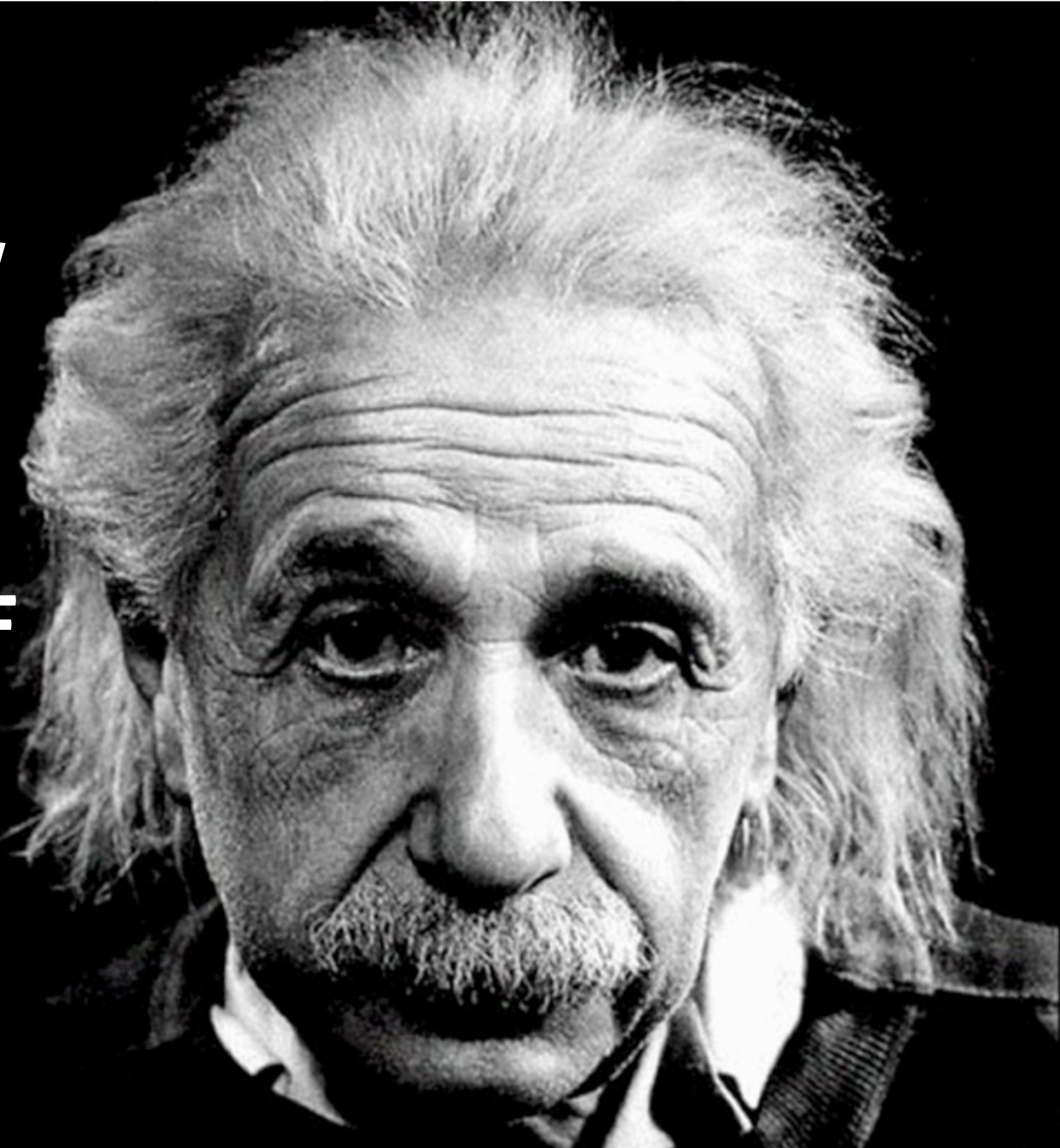
# Language



High Speed Operators of Meal Team 6



**OUT OF CLUTTER,  
FIND **SIMPLICITY.**  
FROM DISCORD,  
FIND **HARMONY.**  
IN THE MIDDLE OF  
DIFFICULTY LIES  
**OPPORTUNITY.****





# What I wanted you to take away:

1. I haven't delivered a public talk in 7 years!
2. We are more art and compliance than science
3. Where we do make use of science, it's siloed
4. We aren't organized properly
5. We don't define, model or manage risk well
6. We are not agile
7. Our definition of "Resilience" varies and it is insufficient
8. Instead of resilient, we need to be:
9. We can be!

**ANTIFRAGILE**

**How'd I do?**



Work like Hell. Share all you know.  
Abide by your handshake. Have fun.

— Dan Geer —

**Email:** [choff@packetfilter.com](mailto:choff@packetfilter.com) (not work)  
[christofer.hoff@goto.com](mailto:christofer.hoff@goto.com) (work)

**Blog:** <http://www.rationalsurvivability.com>

**Twitter:** @beaker

I Really Value Your Input. Please Send Me Some...Positive Or Otherwise