New Paradigms for the Next Era of Security

Sounil Yu

@sounilyu

The measure of success is not whether you have a tough problem to deal with, but whether it is the same problem you had last year.

John Foster Dulles

We cannot solve our problems with the same thinking we used when we created them

Albert Einstein

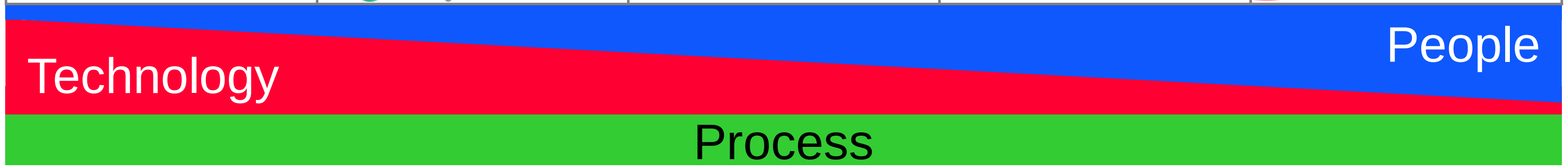
Cyber Defense Matrix

https://cyberdefensematrix.com

	Identify	Protect	Detect	Respond	Recover
Devices	CLAROTY, jamf, QUALYS, tenable, EverMore, TREND MICRO, SEVCO, infinipoint, armis, AXONIUS, sysdig, JupiterOne, eclypsium	proofpoint, CYBERARK The Identity Security Company, WATERFALL, AXIOMTEK, Bastion Zero, TREND MICRO, txOne networks, jamf, OPSWAT, VULCAN, BlackBerry, SentinelOne, senhasegura, MENLO SECURITY, CROWDSTRIKE, CLAROTY, ZIMPERIUM, proofpoint	CYCRAFT, Hunters., cybereason, CROWDSTRIKE, SentinelOne, sekoia, Uptycs, paloalto, HUNTRESS, SCYTHE	SentinelOne, Cellebrite, cybereason, CYCRAFT, CROWDSTRIKE, Malwarebytes, paloalto, NowSecure	
Applications	VERACODE, Checkmarx, CodeDx, insignary, snyk, enso, JupiterOne, SYNOPSYS, ENDOR LABS, valence, rezilion, CONTRAST SECURITY, bugcrowd, apiiro, BIONIC, hackerone	Reblaze, cycode, pangea, CYBERARK The Identity Security Company, f5, aqua, VERACODE, Akamai, Forcepoint, CONTRAST SECURITY, waratek, netskope, CLOUDFLARE, Araali Networks, A10, imperva, HENNGE, DAZZ., Astrix, SECURE CODE WARRIOR, TALA, cloudbric	Reveal security, TRUEFORT		Gremlin
Networks	REDSEAL, NIAGARA NETWORKS, infoblox, JupiterOne, DOMAINTOOLS, SKYBOX SECURITY	f5, allot, TREND MICRO, CDNetworks, OWL CYBER DEFENSE, PERCEPTION POINT, Forcepoint, Array, algosec, spirent, aruba, Akamai, FORESCOUT, perimeter 81, paloalto, FORTINET, FIREMON, A7 Networks, XENA NETWORKS	CUBRO NETWORK VISIBILITY, Gigamon, paloalto, DARKTRACE, corelight, ExtraHop, VECTRA, Fidelis Cybersecurity, Hunters., sekoia	paloalto, VECTRA, Fidelis Cybersecurity	
Data	SPHERE, wirewheel, RELYANCE AI, JupiterOne, eureka, VARONIS, CYERA, Dig, sentra, boldonjames A QinetiQ Company, Laminar, TITUS, Normalyze, BigID, POLAR	AKEYLESS, TrustView, DASERA, Ubiq, SPHERE, Armorblox, PIIANO, NAVCLOUDR, KeyXentic Inc., Nightfall, Symantec, INTRALINKS, NAKIVO, Openfind, ZAMA, netskope, satori, senhasegura, SendQuick	Symantec, CYBERHAVEN	BREACHRX	Acronis, Veeam, NAKIVO, VERITAS, COMMVAULT, CODE42, PA Power Admin, DELL, NeuShield
Users	AUTHENTREND, DUO, Authme, BehavioSec, COFENSE, BIOCATCH, JupiterOne, FUDO SECURITY, Delinea, okta, KnowBe4 Human error. Conquered., TOPPAN TOPPAN IDGATE, CYBERARK The Identity Security Company, ONE IDENTITY by Quest	livingsecurity, SILVERFORT, proofpoint, HABITU8, semperis, KnowBe4 Human error. Conquered., COFENSE, AUTHENTIFY, Elevate Security, inky	Trendzact, exabeam, ZEROFOX, SECURONIX, Forcepoint, Dtex systems, GURUCUL, observe it, CODE42		

Why are there so few things here? Is our industry actually solving the right problems?

Degree of Dependency

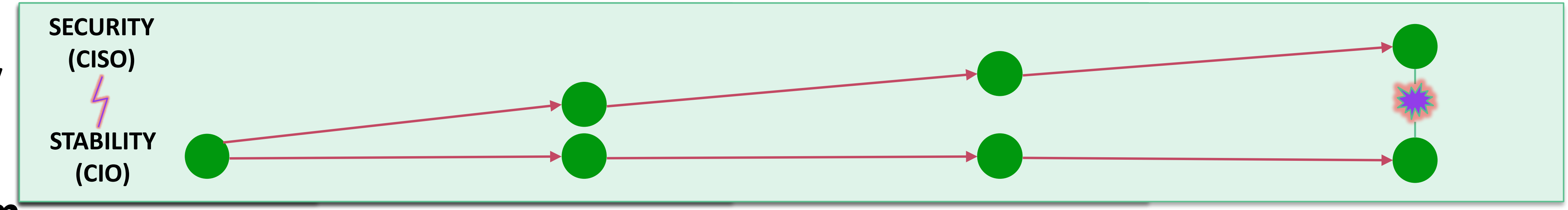


Disclaimer: Vendor logos shown are representative only. No endorsement should be construed because they are shown here.

A Quick History of IT and Security

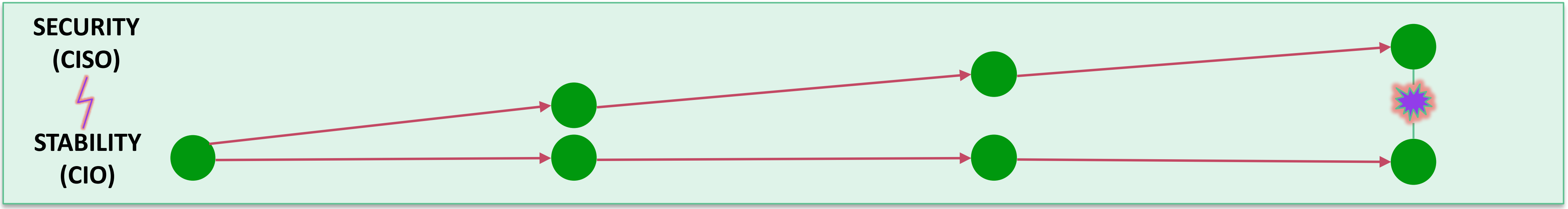
Era	1980s	1990s	2000s	2010s
Core Challenges	What did we buy and how does it support the biz?	Viruses, Server-side Attacks, Insecure Configs	Too many logs and alerts, Client-side attacks	Assume Breach, Raging Fires, Too Many Privileges
Solutions	Asset Mgt, Systems Mgt Tools	Anti-Virus, Firewalls, Secure Configs	IDS, SIEM	Incident Responders & IR Tools (EDR, SOAR)

IT / Security Tension



Security Team Composition & Focus	None	Hobby Shop / Vulnerability Mgt	Sec Ops Center / Threat Mgt	Dedicated Biz Unit / Risk Mgt

Mapping to the NIST Cybersecurity Framework

Era	1980s IDENTIFY	1990s PROTECT	2000s DETECT	2010s RESPOND
Core Challenges	What did we buy and how does it support the biz?	Viruses, Server-side Attacks, Insecure Configs	Too many logs and alerts, Client-side attacks	Assume Breach, Raging Fires, Too Many Privileges
Solutions	Asset Mgt, Systems Mgt Tools	Anti-Virus, Firewalls, Secure Configs	IDS, SIEM	Incident Responders & IR Tools (EDR, SOAR)
IT / Security Tension	 			
Security Team Composition & Focus	None	Hobby Shop / Vulnerability Mgt	Sec Ops Center / Threat Mgt	Dedicated Biz Unit / Risk Mgt

2020s: Age of Recovery (or Resiliency)

What kind of attacks should we see in the 2020s that would challenge to our ability to RECOVER or cause irreversible harm?

Confidentiality

Integrity

Availability

Ransomware

2020s: Age of Recovery (or Resiliency)

What kind of solutions directly support our ability to RECOVER or be RESILIENT?

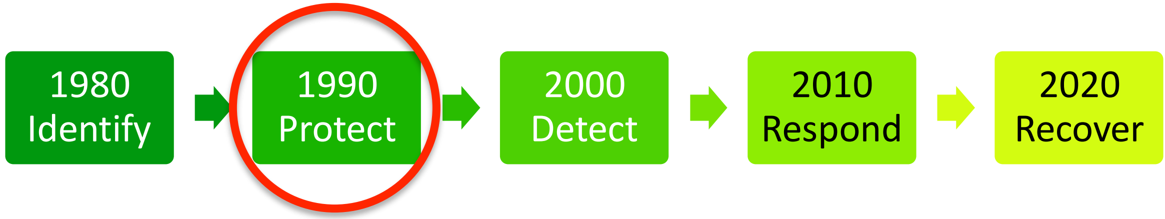
Forging ahead or regressing back?

Recent advertising campaign from major vendor

DINOSAURS REACT.
PROFESSIONALS PREVENT.
JOIN THE PREVENTION AGE
STOP CYBER BREACHES

JOIN THE **<u>PREVENTION</u>** AGE
STOP CYBER BREACHES

- A call to go back to the 1990s?



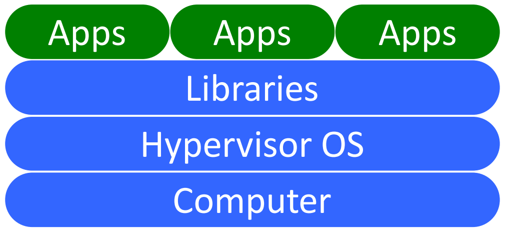
1980 Identify → 1990 Protect → 2000 Detect → 2010 Respond → 2020 Recover

- How will prevention mitigate the impact of ransomware?
  - Remember, we learned “assume breach” in the 2010s
  - Prevention minimizes the occurrences, **<u>but does not address the impact or ability to recover</u>**

2020s: Age of Recovery (or Resiliency)

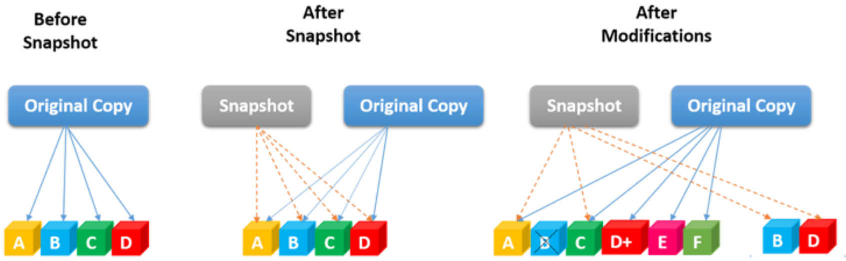
What kind of solutions directly support our ability to RECOVER or be RESILIENT?

SERVERLESS ARCHITECTURE



docker

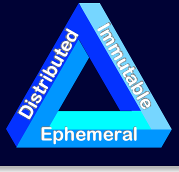
Content Delivery Network

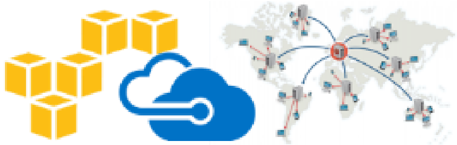


Copy on Write

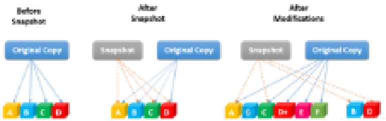
BLOCKCHAIN

The DIE Triad

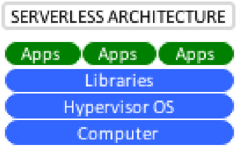




BLOCKCHAIN



docker



SERVERLESS ARCHITECTURE

Apps Apps Apps

Libraries

Hypervisor OS

Computer

Distributed

DDoS Resistant

The best solution against a distributed attack is a distributed service

Availability

Immutable

Changes Easier to Detect and Reverse

Unauthorized changes stand out and can be reverted to known good

Integrity

Ephemeral

Drives Value of Assets Closer to Zero

Makes attacker persistence hard and reduces concern for assets at risk

Confidentiality

The Alternative: An Endless Conveyor Belt of Vulnerabilities and Threats

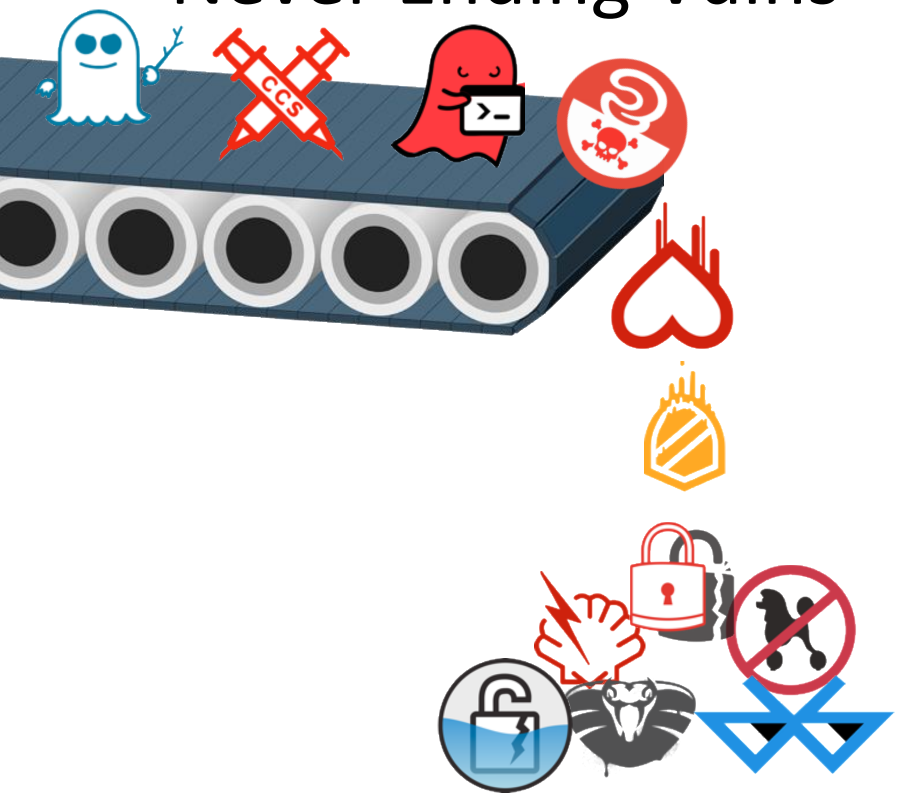
Distributed
Immutable
Ephemeral

Risk = Likelihood x Impact

Never Ending Vulns

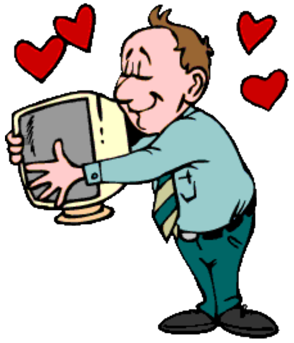
Confidentiality
Integrity
Availability

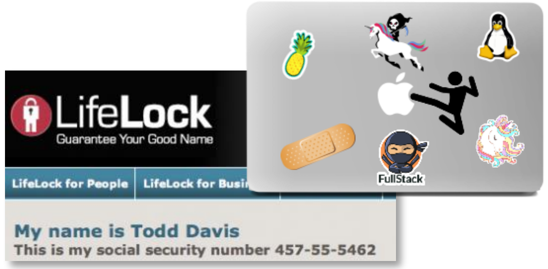
Never Ending Threats



Pets vs Cattle

- Given a familiar name
- Taken to the vet when sick
- Hugged



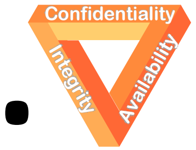


LifeLock
Guarantee Your Good Name

LifeLock for People | LifeLock for Busi

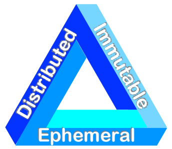
My name is Todd Davis
This is my social security number 457-55-5462

C.I.A.

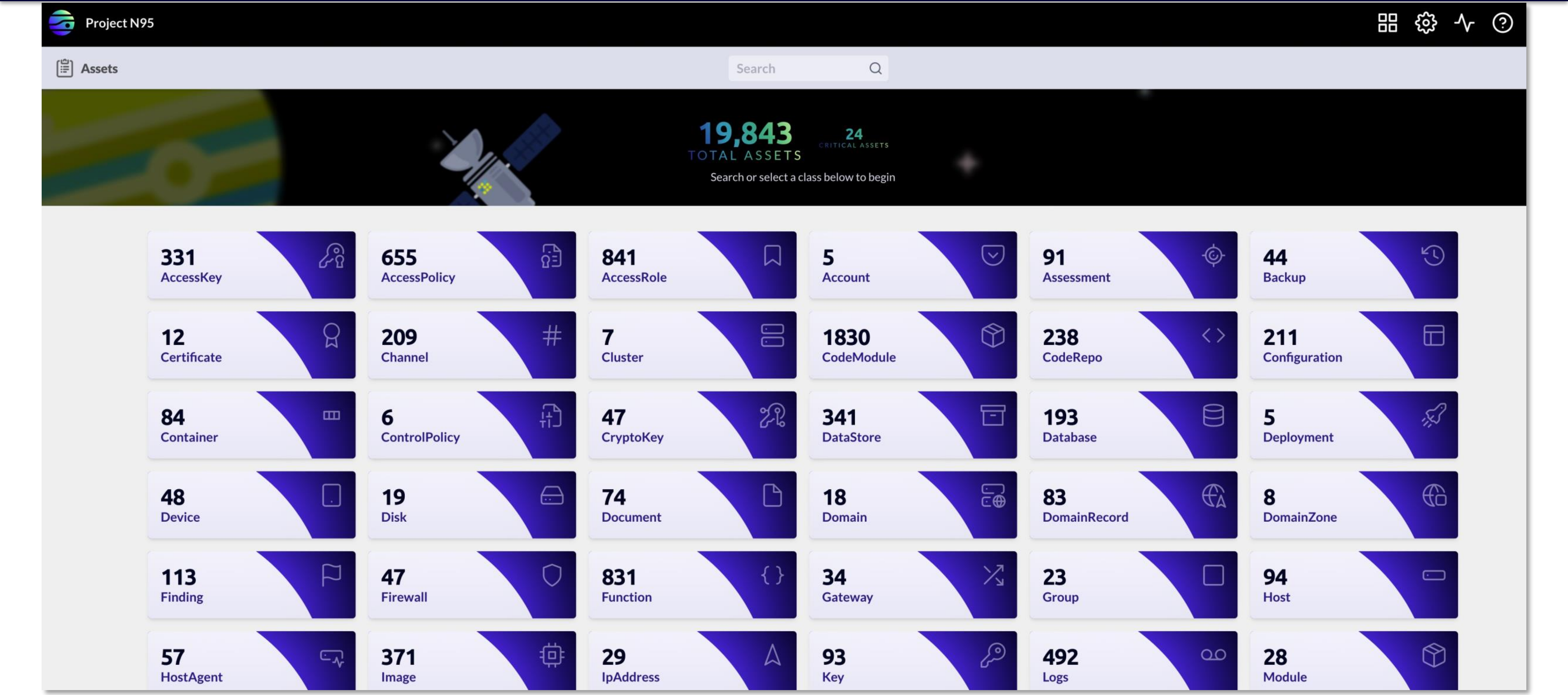


- Branded with an obscure, unpronounceable name
- Culled from herd

D.I.E.



Which of these are pets? Which are cattle?



19,843 TOTAL ASSETS

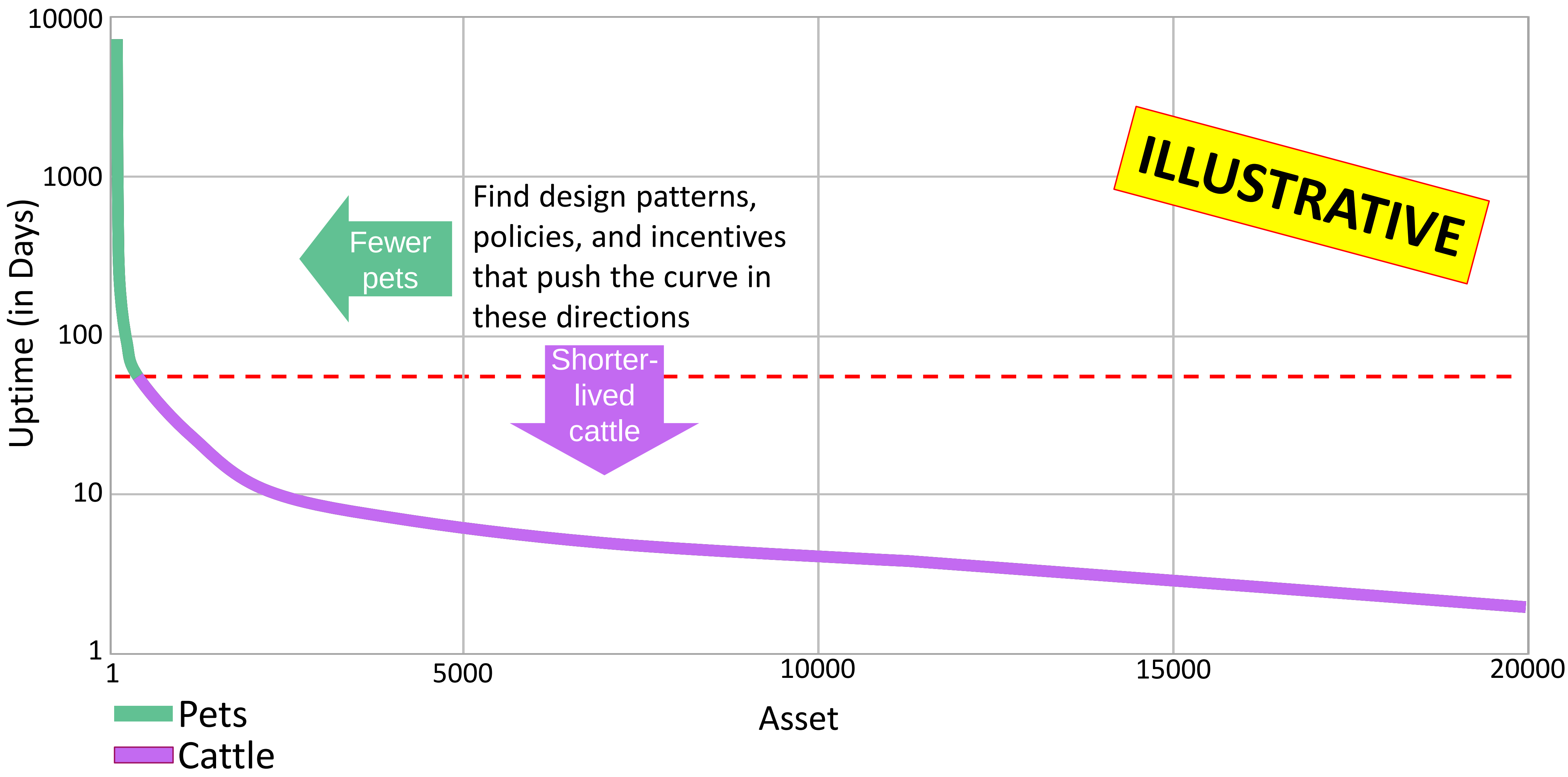
24 CRITICAL ASSETS

Search or select a class below to begin

331 AccessKey	655 AccessPolicy	841 AccessRole	5 Account	91 Assessment	44 Backup
12 Certificate	209 Channel	7 Cluster	1830 CodeModule	238 CodeRepo	211 Configuration
84 Container	6 ControlPolicy	47 CryptoKey	341 DataStore	193 Database	5 Deployment
48 Device	19 Disk	74 Document	18 Domain	83 DomainRecord	8 DomainZone
113 Finding	47 Firewall	831 Function	34 Gateway	23 Group	94 Host
57 HostAgent	371 Image	29 IpAddress	93 Key	492 Logs	28 Module

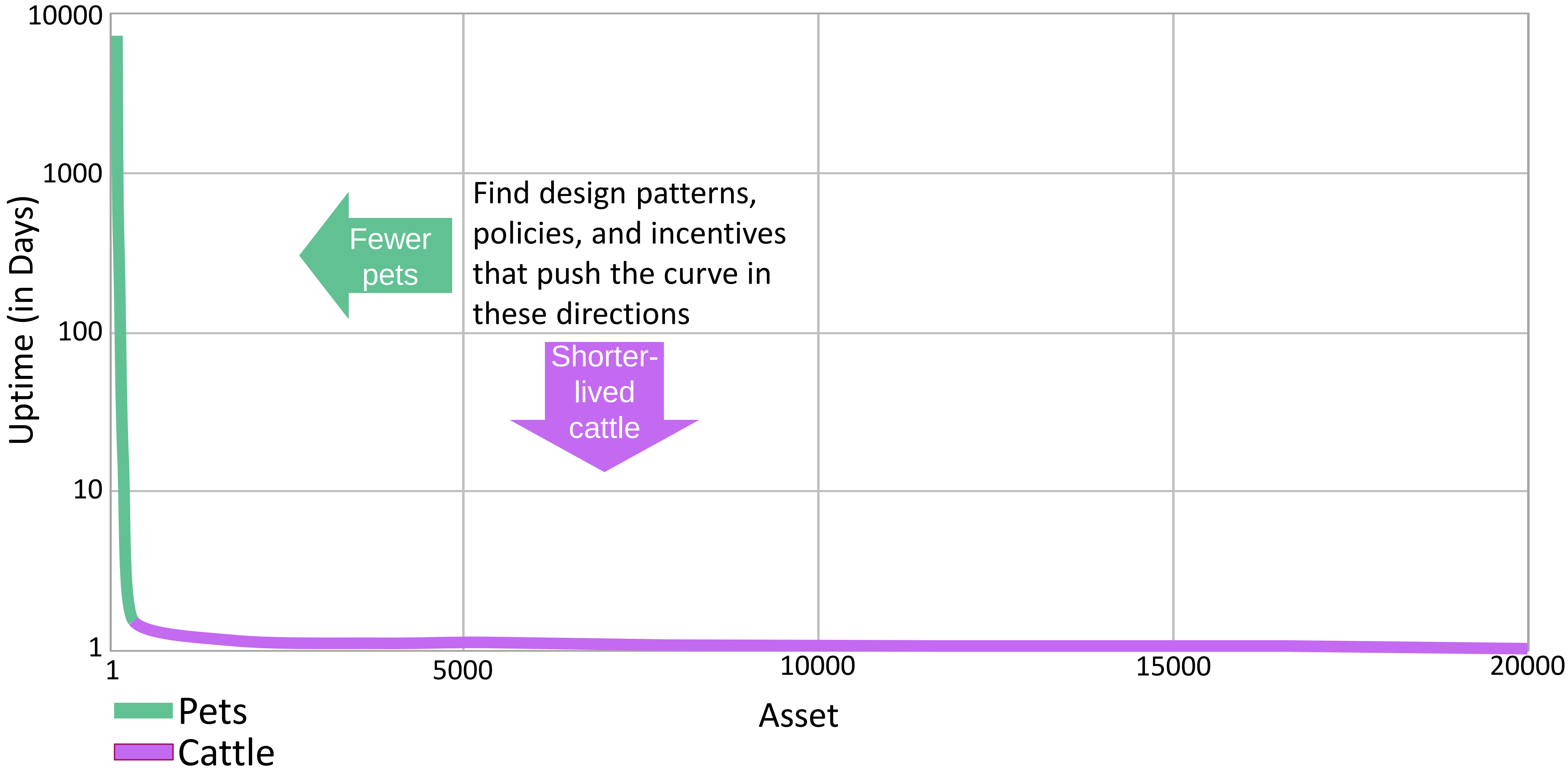
Source: Project N95 (https://projectn95.org) via JupiterOne (https://jupiterone.com)

Measuring Resiliency: Pets vs Cattle Curve



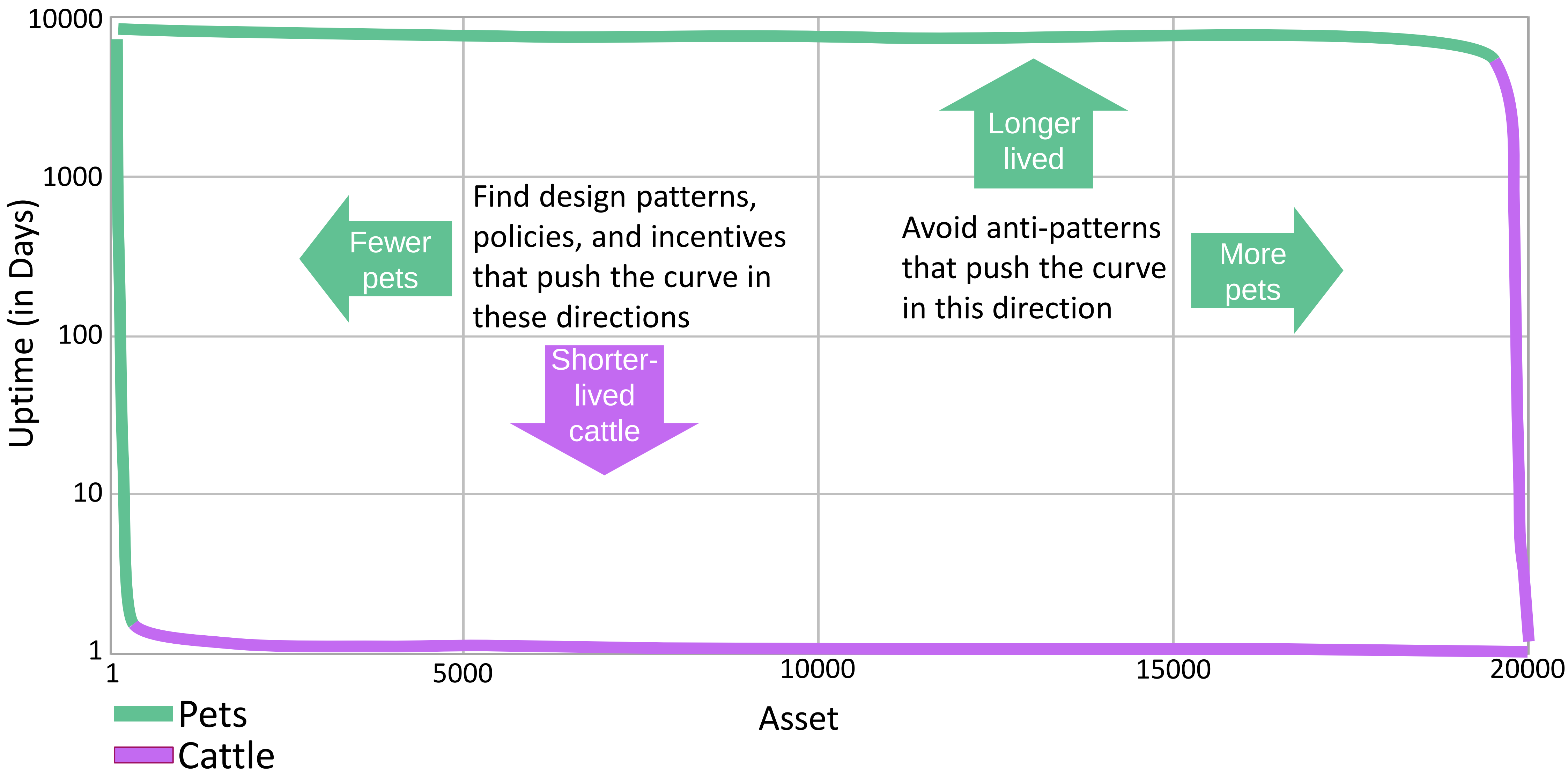
Find design patterns, policies, and incentives that push the curve in these directions

More Ephemeral = More Resilient?



Find design patterns, policies, and incentives that push the curve in these directions

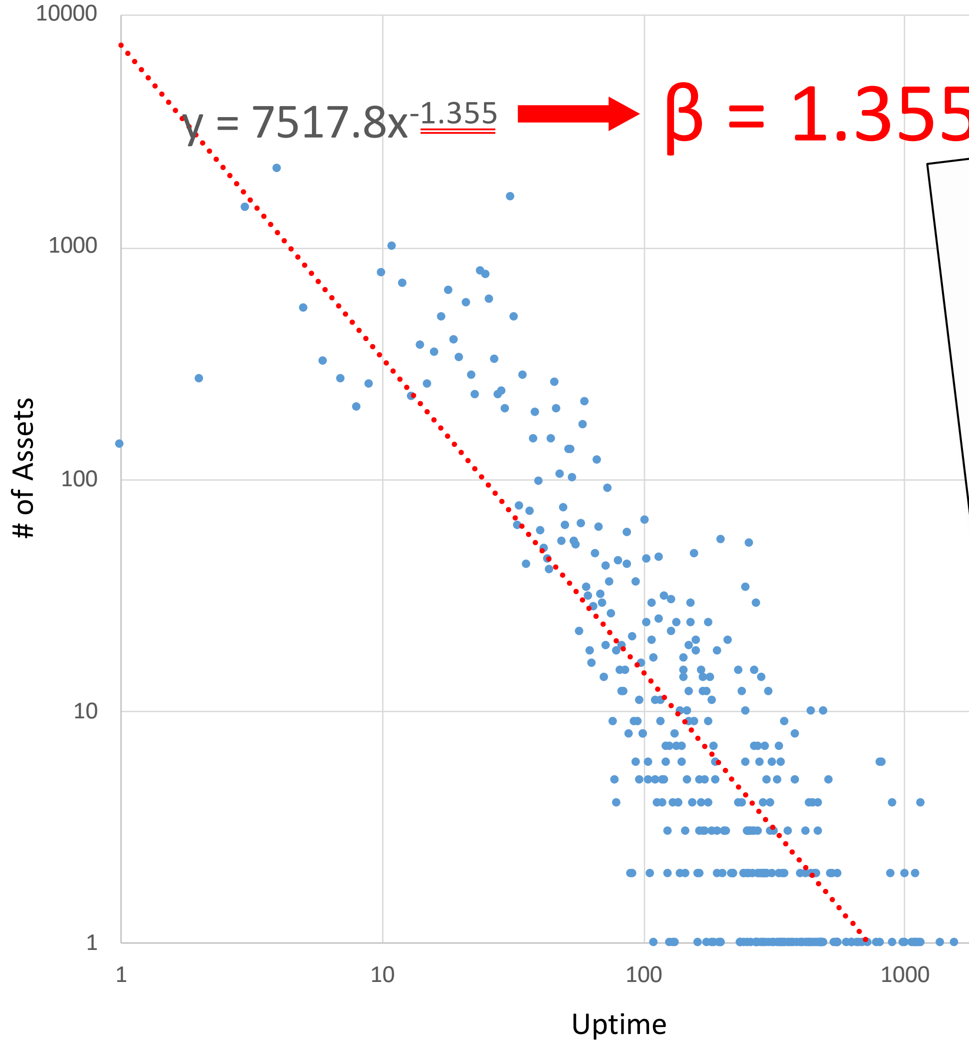
Less Ephemeral = Less Resilient?



Find design patterns, policies, and incentives that push the curve in these directions

Avoid anti-patterns that push the curve in this direction

Benchmarking Resiliency



$y = 7517.8x^{-1.355}$ → β = 1.355

J Comb Optim
DOI 10.1007/s10878-015-9893-7

Robustness of power-law networks: its assessment and optimization

Huiling Zhang[1] · Yilin Shen[1] · My T. Thai[1,2]

Abstract Many practical complex networks, such as the Internet, WWW and social networks, are discovered to follow power-law distribution in their degree sequences, i.e., the number of nodes with degree i in these networks is proportional to $i^{-\beta}$ for some exponential factor $\beta > 0$. However, these networks also expose their vulnerabilities to a great number of threats such as adversarial attacks on the Internet, cyber-crimes on the WWW or malware propagations on social networks. Although power-law networks have been found robust under random attacks and vulnerable to intentional attacks via experimental observations, how to better understand their vulnerabilities from a theoretical point of view still remains open. In this paper, we study the vulnerability of power-law networks under random attacks and adversarial attacks using the in-depth probabilistic analysis on the theory of random power-law graph models. Our results indicate that power-law networks are able to tolerate random failures if their exponential factor β is <2.9, and they are more robust against intentional attacks if β is smaller. Furthermore, we reveal the best range [1.8, 2.5] for the exponential factor β by optimizing the complex networks in terms of both their vulnerabilities and costs.

Huiling Zhang and Yilin Shen are co-first authors.

✉ My T. Thai
thaitramy@tdt.edu.vn; mythai@cise.ufl.edu

Huiling Zhang
huiling@cise.ufl.edu

Yilin Shen
yshen@cise.ufl.edu

[1] Department of Computer & Information Science and Engineering, University of Florida, Gainesville, FL 32611, USA

[2] Division of Algorithms and Technologies for Networks Analysis, Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Vietnam

Springer

Published online: 14 May 2015

- If β is < 2.9 ➔ tolerates random failures
- If β is <u>smaller</u> ➔ <u>more robust</u> against intentional attacks

(More short-lived cattle causes β to be smaller!!)

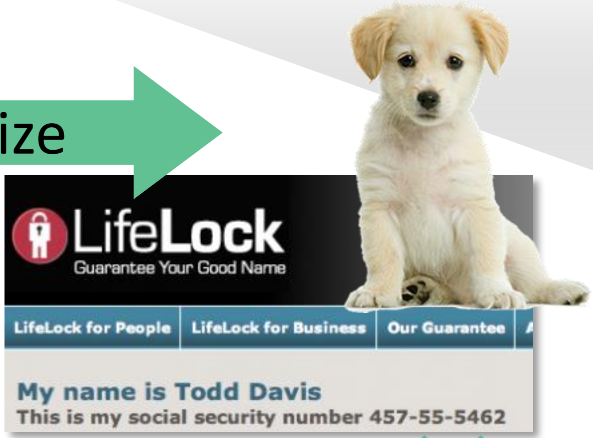
- Best range is 1.8 < β < 2.5 when optimizing for both vulnerabilities and costs
  - If β < 1.8 ➔ maintenance cost is very expensive
  - If β > 2.5 ➔ robustness is unpredictable because it depends on the specific attacking strategy

Source: Huiling Zhang, Yilin Shen, and My T. Thai; Robustness of power-law networks: its assessment and optimization, 2015; https://www.cise.ufl.edu/~mythai/files/15joco.pdf

Pets vs Cattle Controls

By signing this certificate I promise to give my puppy a lifetime of love, care, attention and fun! I promise to be their best friend forever.

Discourage / Disincentivize



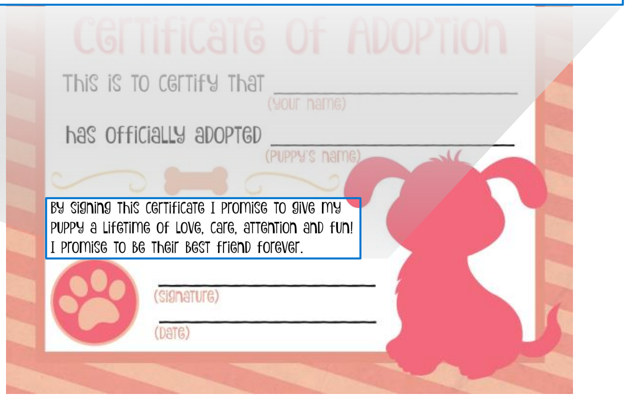
LifeLock

Guarantee Your Good Name

LifeLock for People | LifeLock for Business | Our Guarantee

My name is Todd Davis

This is my social security number 457-55-5462



Certificate of Adoption

This is to certify that ____________________

(your name)

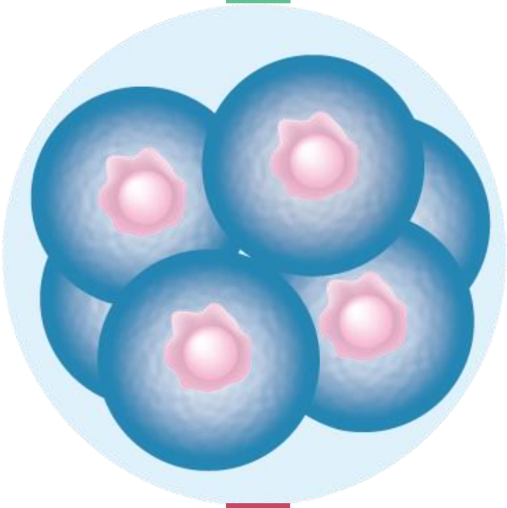
has officially adopted ____________________

(puppy's name)

By signing this certificate I promise to give my puppy a lifetime of love, care, attention and fun! I promise to be their best friend forever.

____________________ (signature)

____________________ (date)

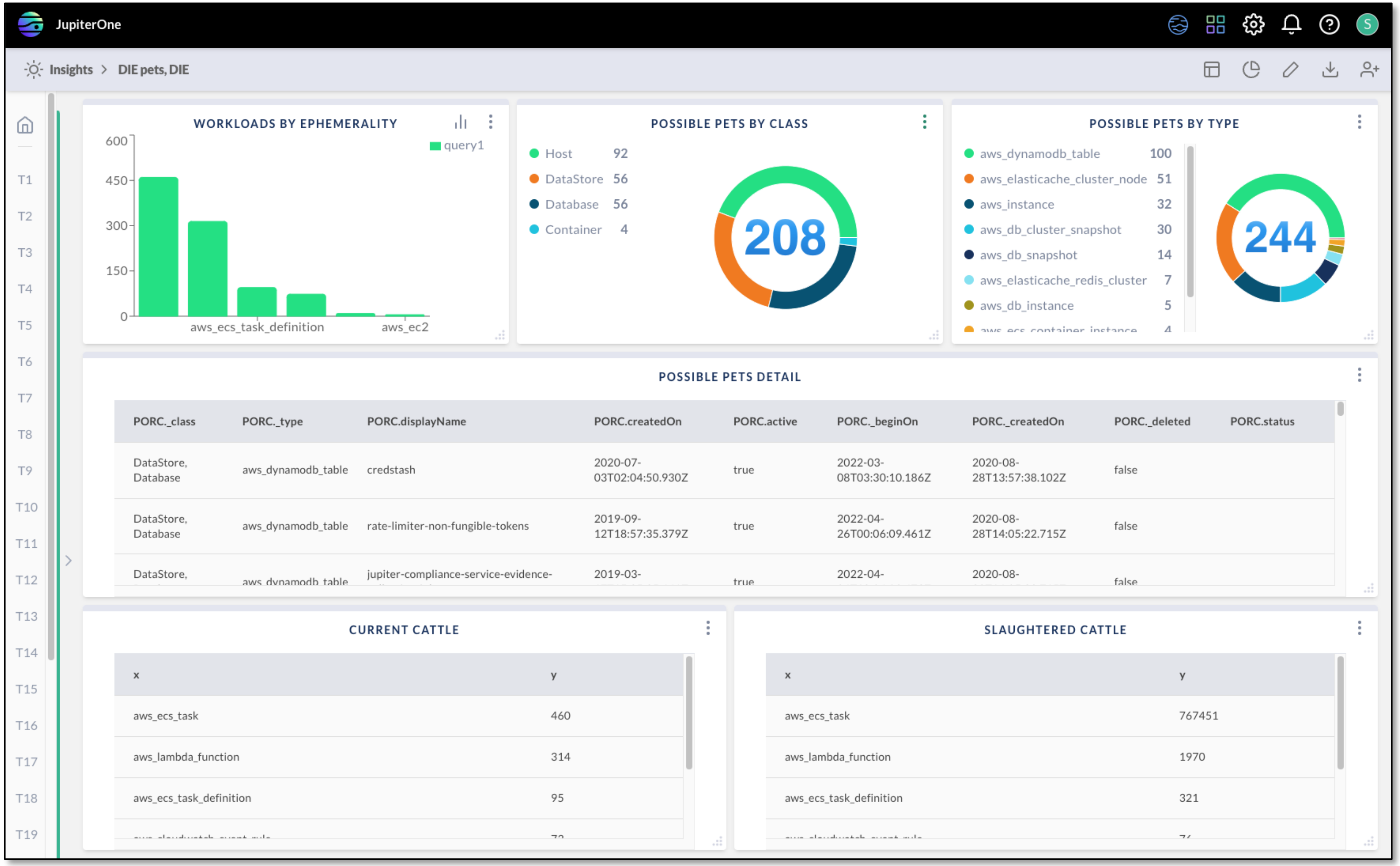


- decommissioning
- creative destruction
- rebooting/reimaging
- privacy enhancing tech

- modifying an immutable container
- letting an asset live longer than needed
- patching in place

Encourage / Incentivize

Pet Management at my $dayjob



POSSIBLE PETS BY CLASS

● Host	92
● DataStore	56
● Database	56
● Container	4

POSSIBLE PETS BY TYPE

● aws_dynamodb_table	100
● aws_elasticache_cluster_node	51
● aws_instance	32
● aws_db_cluster_snapshot	30
● aws_db_snapshot	14
● aws_elasticache_redis_cluster	7
● aws_db_instance	5
● aws_ecs_container_instance	4

POSSIBLE PETS DETAIL

PORC._class	PORC._type	PORC.displayName	PORC.createdOn	PORC.active	PORC._beginOn	PORC._createdOn	PORC._deleted	PORC.status
DataStore, Database	aws_dynamodb_table	credstash	2020-07-03T02:04:50.930Z	true	2022-03-08T03:30:10.186Z	2020-08-28T13:57:38.102Z	false	
DataStore, Database	aws_dynamodb_table	rate-limiter-non-fungible-tokens	2019-09-12T18:57:35.379Z	true	2022-04-26T00:06:09.461Z	2020-08-28T14:05:22.715Z	false	
DataStore,	aws_dynamodb_table	jupiter-compliance-service-evidence-	2019-03-	true	2022-04-	2020-08-	false	

CURRENT CATTLE

x	y
aws_ecs_task	460
aws_lambda_function	314
aws_ecs_task_definition	95
aws_cloudwatch_event_rule	72

SLAUGHTERED CATTLE

x	y
aws_ecs_task	767451
aws_lambda_function	1970
aws_ecs_task_definition	321
aws_cloudwatch_event_rule	74

The DIE Triad Changes Roles and Responsibilities

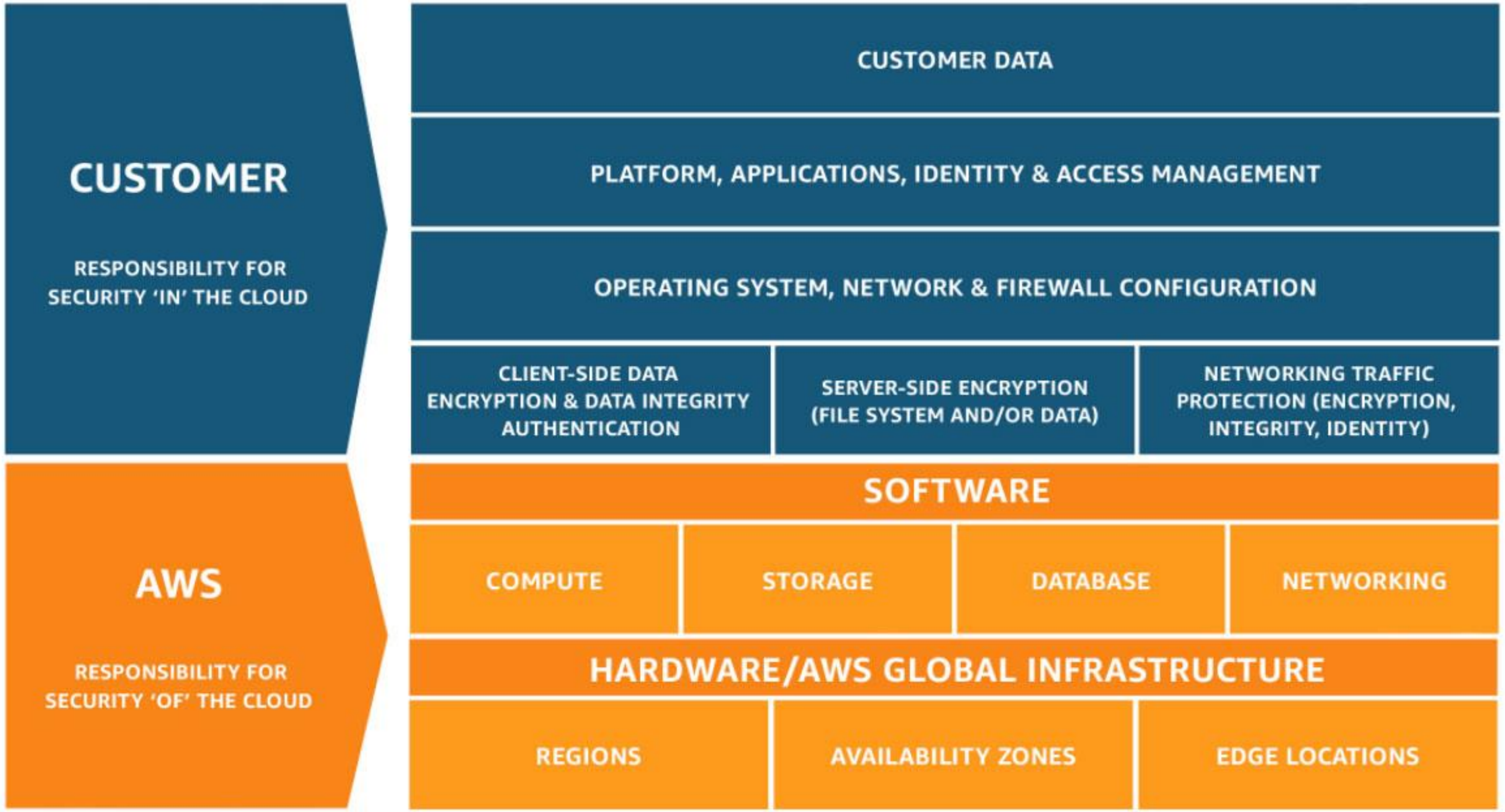
Cyber
Veterinarians

Confidentiality
Integrity
Availability

Cyber
Pet Control Officer

Distributed
Immutable
Ephemeral

The distribution of “Pets” and “Cattle” change across the Shared Responsibility Model and with cloud native maturity



CUSTOMER

RESPONSIBILITY FOR SECURITY ‘IN’ THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY ‘OF’ THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

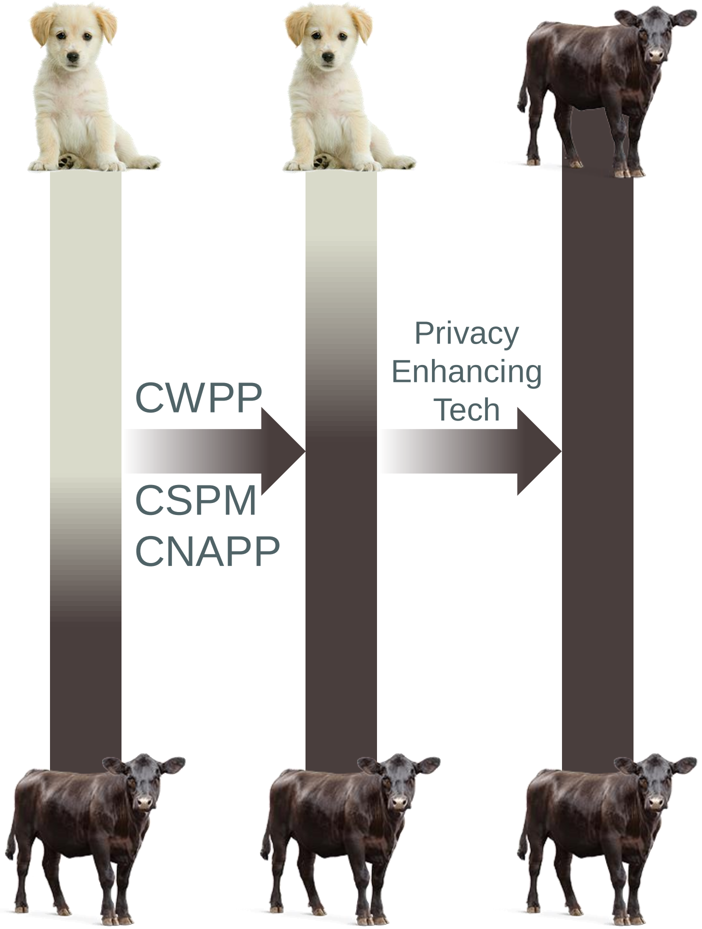
NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS



Applying DIE to Data: Privacy Enhancing Technologies

Data Minimization

Homomorphic Encryption

Secure Multiparty Computation

Blockchain

Synthetic Data / Differential Privacy

PII Vaults

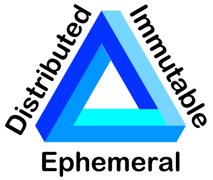
Tokenization

Trusted Execution Environments

Secret Sharing

Federated Learning

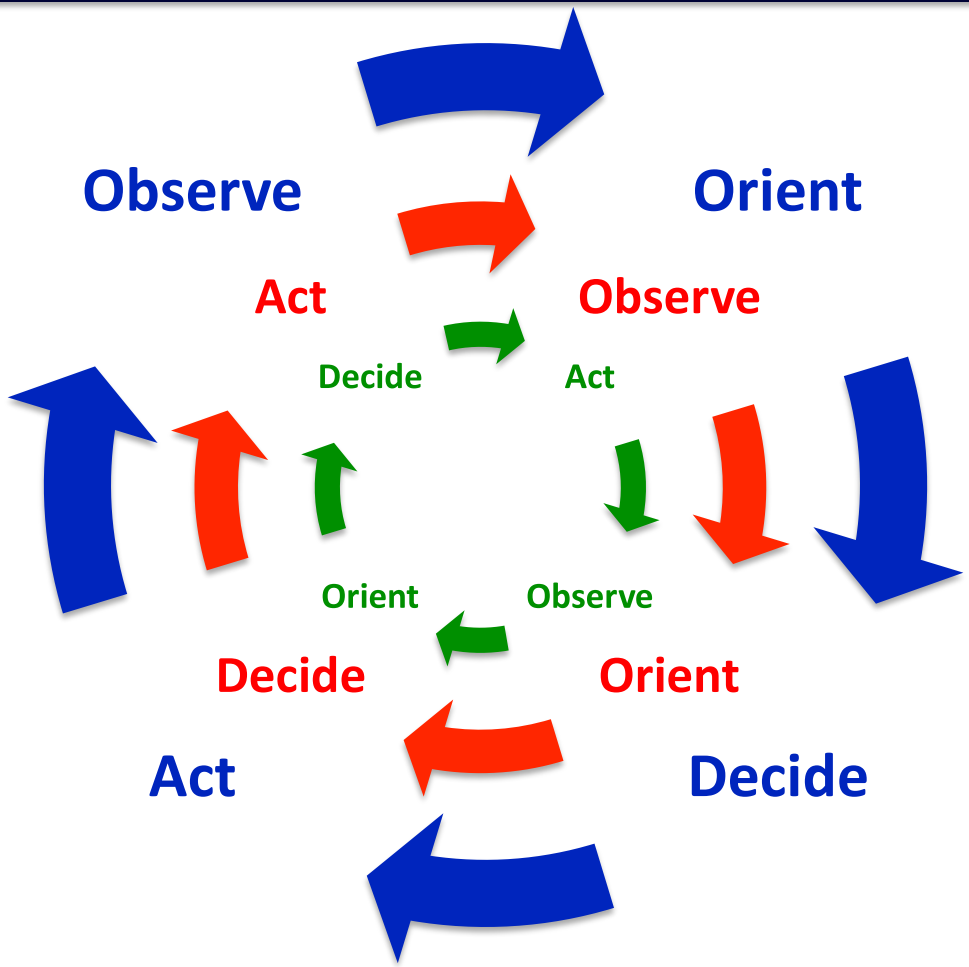
Applying DIE to Data: Privacy Enhancing Technologies



	DIE Triad Alignment
Data Minimization	Pet Control
PII Vaults	Pet Control
Secret Sharing	Distributed
Federated Learning	Distributed
Blockchain	Immutable
Homomorphic Encryption	Ephemeral
Tokenization	Ephemeral
Synthetic Data / Differential Privacy	Ephemeral
Trusted Execution Environments	Ephemeral
Secure Multiparty Computation	Ephemeral

Privacy By Design (DIE) is not the same as Security By Design (CIA)

DIE and the OODA Loop



⌛⌛⌛ Defender OODA Loop

⌛⌛ Attacker OODA Loop

⌛⌛⌛⌛ Business OODA Loop w/Traditional CIA Restrictions

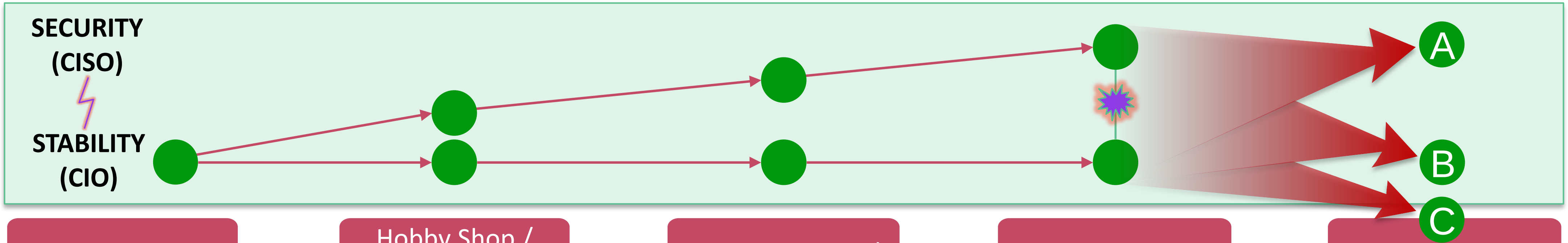
⌛ Natural Business OODA Loop with DIE

DIE design patterns that allow businesses to move faster **naturally shorten the OODA loop**

$$(\text{OODA}_{\text{Business}} – \text{OODA}_{\text{CIO+CISO}} = \text{Shadow IT})$$

> Larger swaths of risk are quickly being eliminated at newer companies, at earlier and earlier stages. And usually ***not because security*** was the goal.
>
> – Ryan McGeehan
>
> https://medium.com/starting-up-security/you-dont-need-a-chief-security-officer-3f8d1a76b924

Completing the NIST CSF

Era	1980 Identify	1990 Protect	2000 Detect	2010 Respond	2020 Recover
Core Challenges	What did we buy and how does it support the biz?	Viruses, Server-side Attacks, Insecure Configs	Too many logs and alerts, Client-side attacks	Assume Breach, Raging Fires, Too Many Privileges	Ransomware, MBR Wiper, DDoS, Firmware Bricking
Solutions	Asset Mgt, Systems Mgt Tools	Anti-Virus, Firewalls, Secure Configs	IDS, SIEM	Incident Responders & IR Tools (EDR, SOAR)	Distributed, Immutable, Ephemeral (DIE!!!) Systems
IT / Security Tension					
Security Team Composition & Focus	None	Hobby Shop / Vulnerability Mgt	Sec Ops Center / Threat Mgt	Dedicated Biz Unit / Risk Mgt	Choose Your Own Destiny

Fragility vs Resiliency vs Antifragility

Destiny A

(C.I.A)

Harm mitigated through bolt-ons and workarounds that create instability

Destiny B

(D.I.E.)

Harm results in destruction but no change in configuration

Destiny C

D.I.E. + Chaos Engineering + Creative Destruction

Harm finds unknown pets and removes them to make system even more DIE-like

Chaos Engineering Redefined:
Intentional discovery of unknown pets that exacerbate fragility

Creative Destruction Redefined:
Intentional removal of known pets that exacerbate fragility

Secure (CIA) != Resilient (DIE)

WTH does that mean?!

Secure your resilience.

RSA Conference 2022
June 6-9 | San Francisco

Summary

- The next era in IT and Security will manifest **more irreversible attacks** that challenge and undermine our ability to RECOVER
- Better PROTECT, DETECT, and RESPOND capabilities may reduce occurrences of malicious events but are **insufficient against well-executed destructive/irreversible scenarios**
- Our best countermeasure is to **avoid pet creation** (that requires CIA) and **promote cattle creation** (built to DIE)

Death to CIA! Long live DIE!

Questions?

@sounilyu

sounil@cyberdefensematrix.com

https://cyberdefensematrix.com

https://www.linkedin.com/in/sounil

https://www.slideshare.net/sounilyu/presentations