RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **STR-T10**

# New Paradigms for the Next Era of Security

**Sounil Yu**

Author
Cyber Defense Matrix
@sounilyu

# $whoami

Former Chief Security Scientist at Major Financial Institution

Mad Scientist → Make New Capabilities

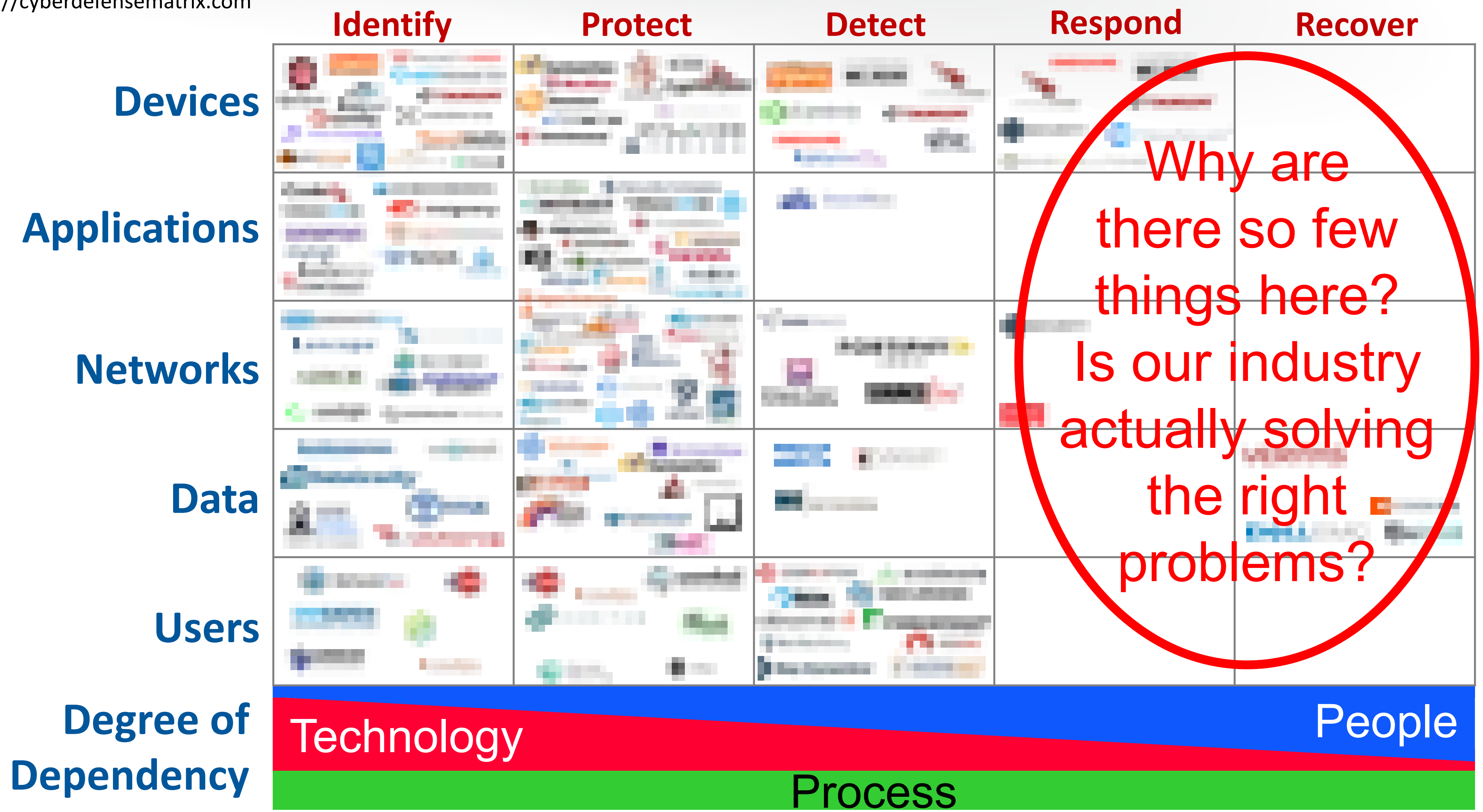
Product Evaluator → Test Market Capabilities

Red Team Lead → Break Capabilities

# Cyber Defense Matrix

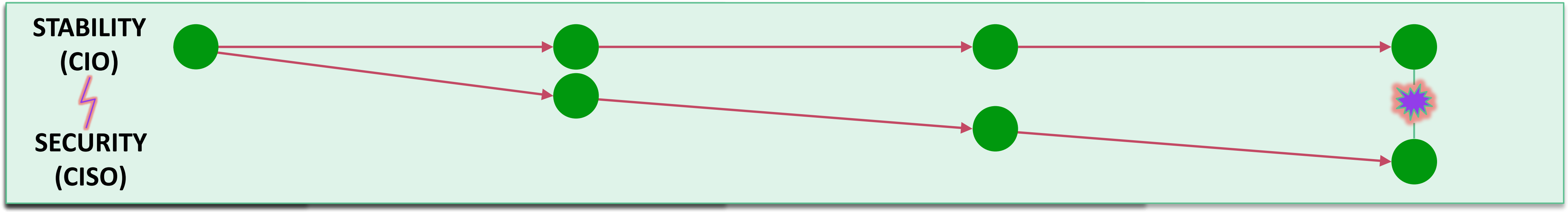
https://cyberdefensematrix.com

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

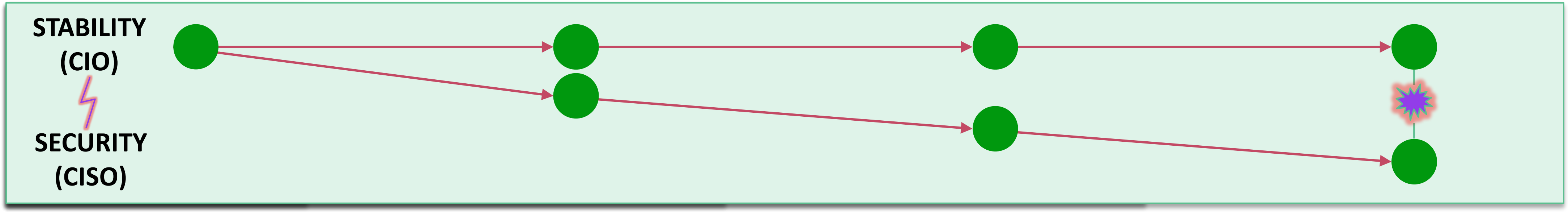


Why are there so few things here? Is our industry actually solving the right problems?

# 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 Cyber Security Framework

| Era | 1980s<br>IDENTIFY | 1990s<br>PROTECT | 2000s<br>DETECT | 2010s<br>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**

↓

**Wikileaks**
**Doxxing**

**Integrity**

↓

**Ransomware**
**#fakenews**

**Availability**

↓

**PDoS, MBR Wiper,**
**Bricking Firmware**

# 2020s: Age of Recovery (or Resiliency)

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

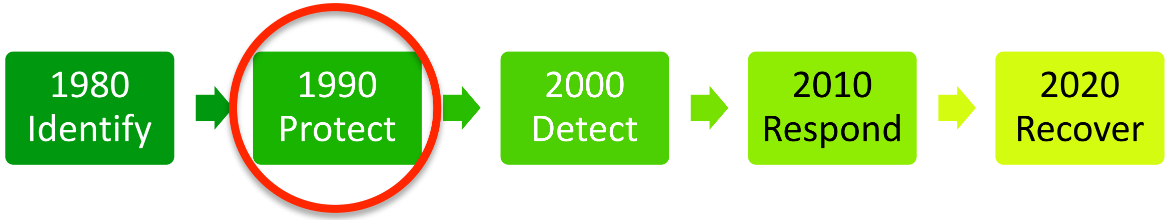
# Forging ahead or regressing back?

Recent advertising campaign from major vendor

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

JOIN THE **PREVENTION** AGE
STOP CYBER BREACHES

- A call to go back to the 1990s?



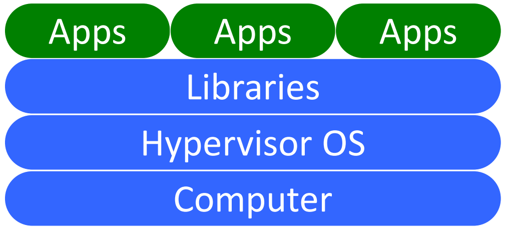
1980 Identify → 1990 Protect → 2000 Detect → 2010 Respond → 2020 Recover

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

# 2020s: Age of Recovery (or Resiliency)

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

SERVERLESS ARCHITECTURE



Apps | Apps | Apps

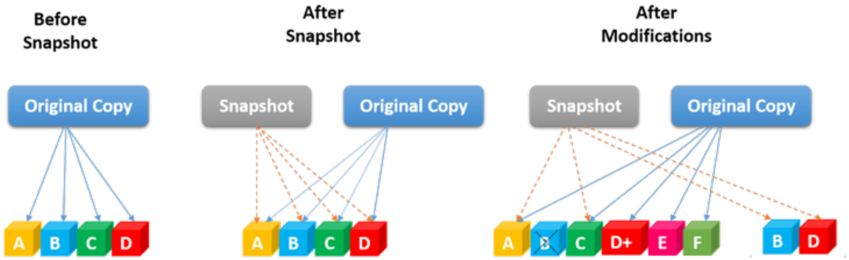
Libraries

Hypervisor OS

Computer

docker

Content Delivery Network

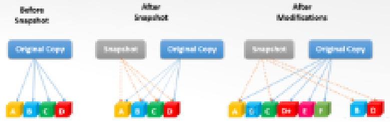


Copy on Write

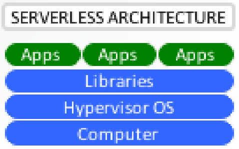
BLOCKCHAIN

# But wait! How are these “security” solutions?

BLOCKCHAIN



docker



## 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

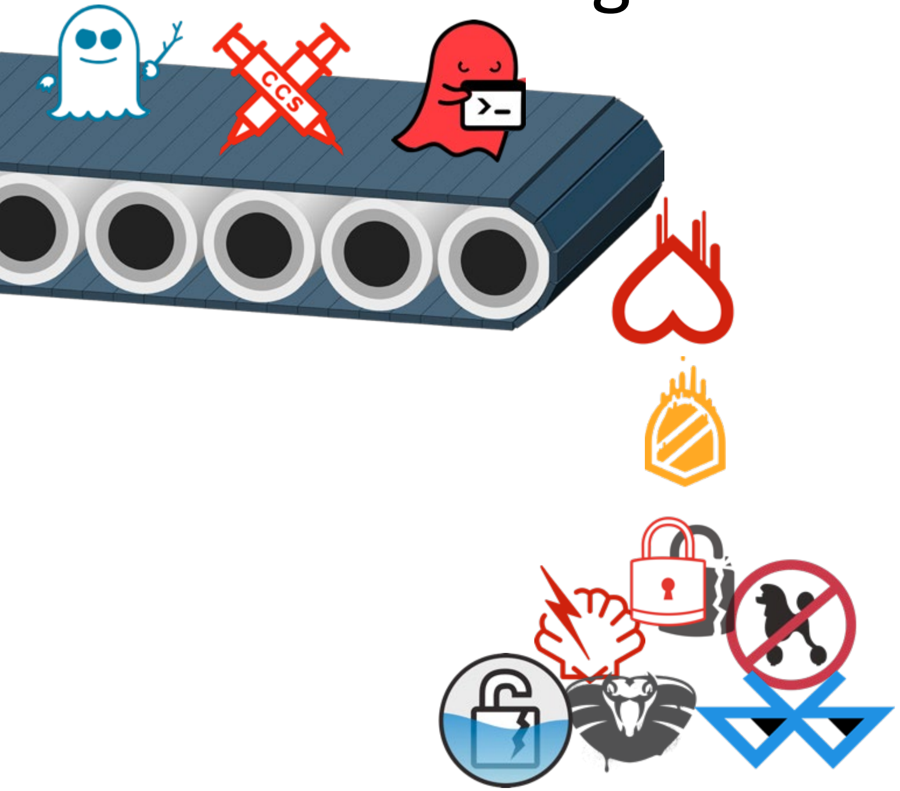
**Confidentiality**

# The Alternative:
# An Endless Conveyor Belt of Vulnerabilities and Threats

**Risk = Likelihood x Impact**

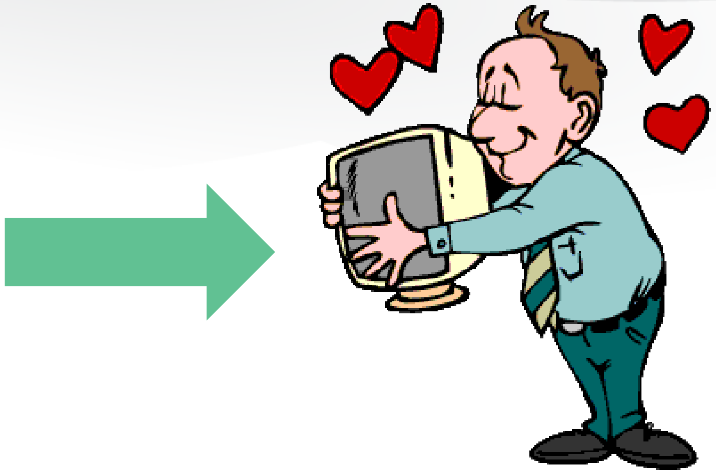
Never Ending Vulns

Never Ending Threats



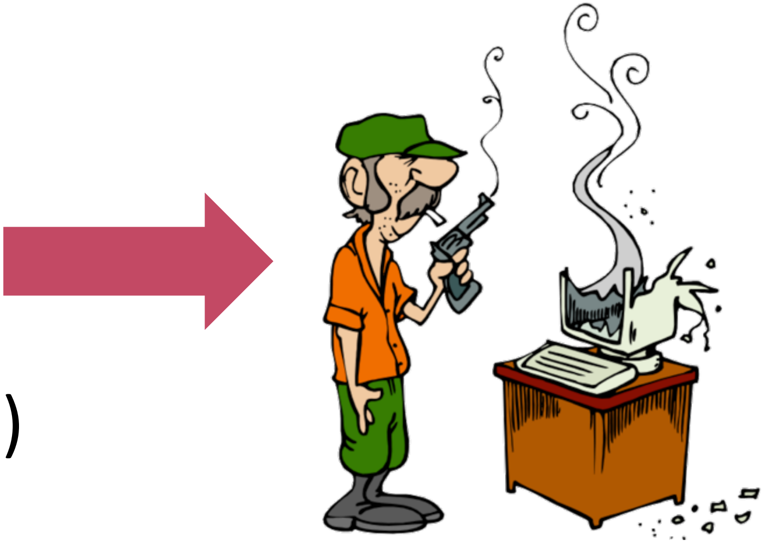
# Pets vs Cattle

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



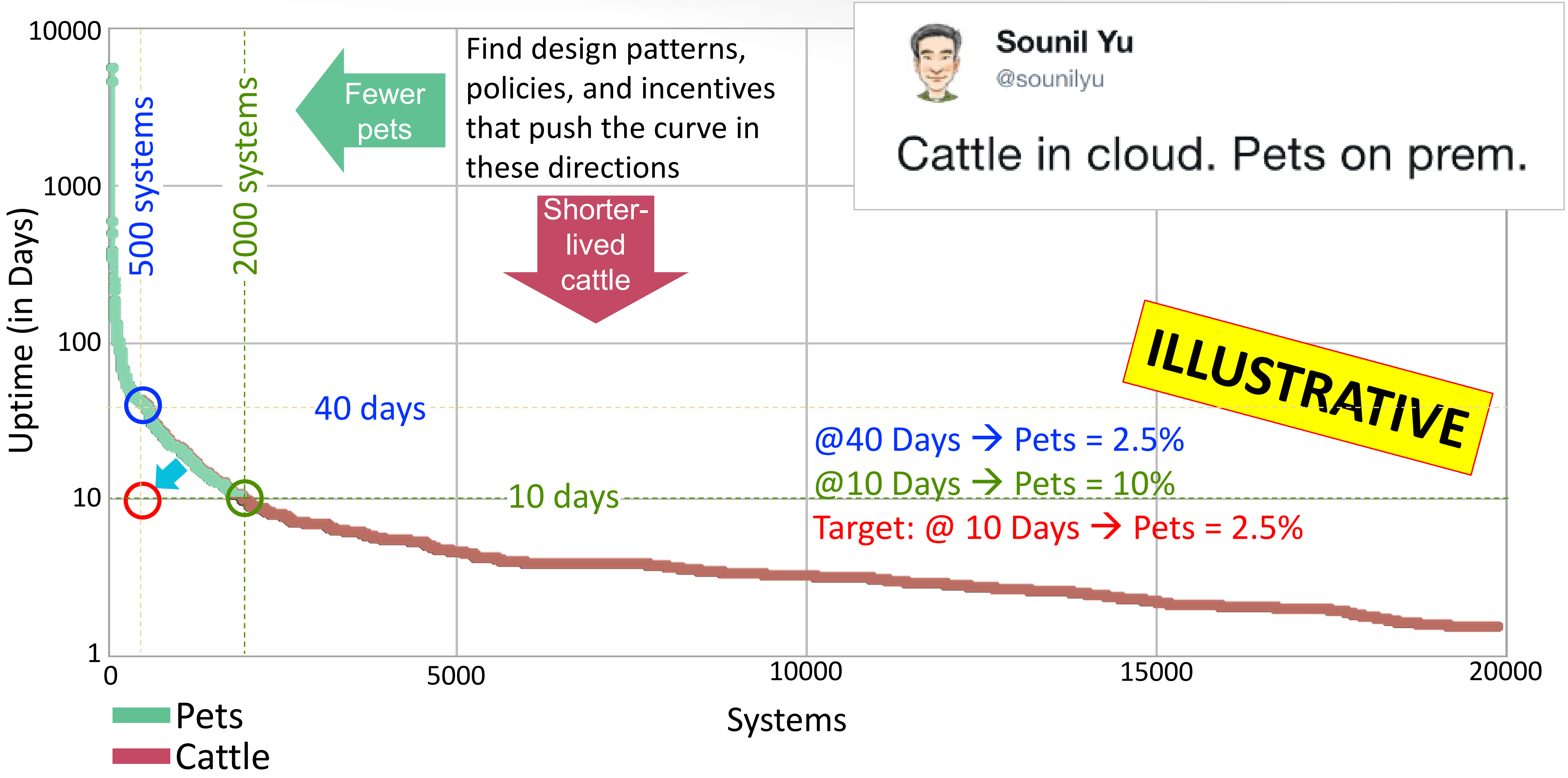
C.I.A.

- Branded with an obscure, unpronounceable name
- Shot when sick
- Eaten/Recycled (sorry PETA)



D.I.E.

# A New Measurement for a New Era: Pets vs Cattle Curve



Fewer pets

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

Shorter-lived cattle

ILLUSTRATIVE

@40 Days → Pets = 2.5%

@10 Days → Pets = 10%

Target: @ 10 Days → Pets = 2.5%

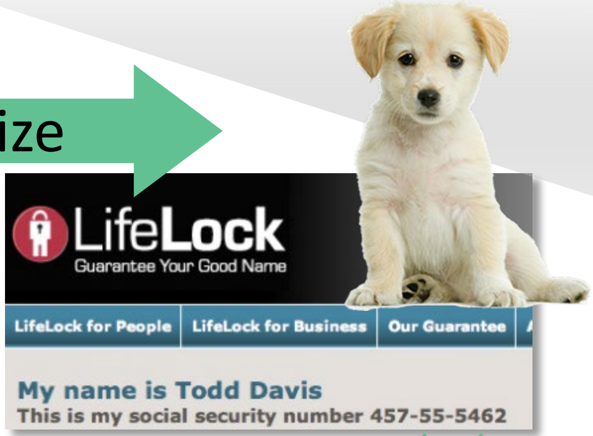
**Sounil Yu**
@sounilyu

Cattle in cloud. Pets on prem.

# 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



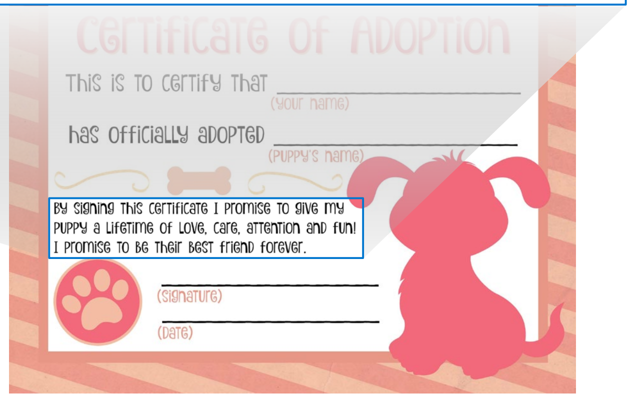
LifeLock

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

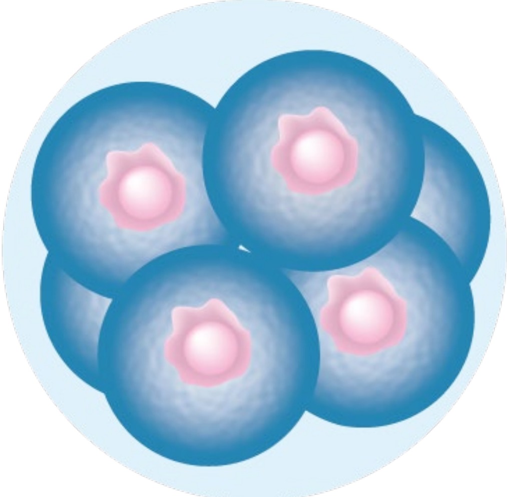
This is to certify that ____________ (your name)

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

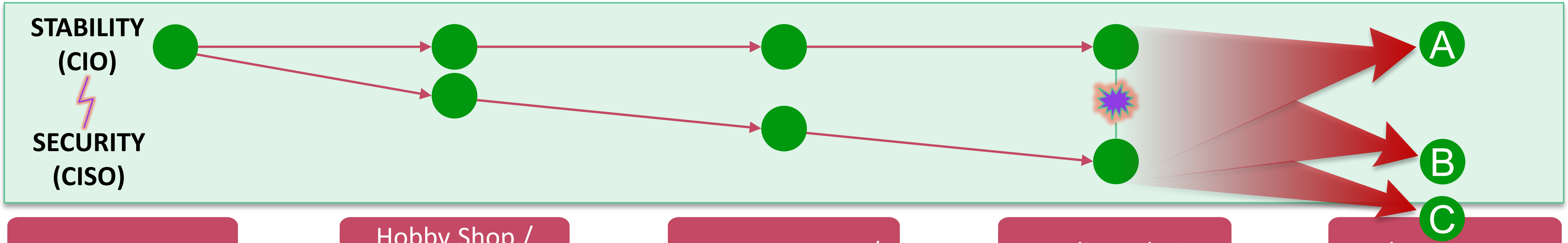
- ssh'ing into a container
- letting an asset live longer than needed
- patching in place

Encourage / Incentivize

# Completing the NIST Cyber Security Framework

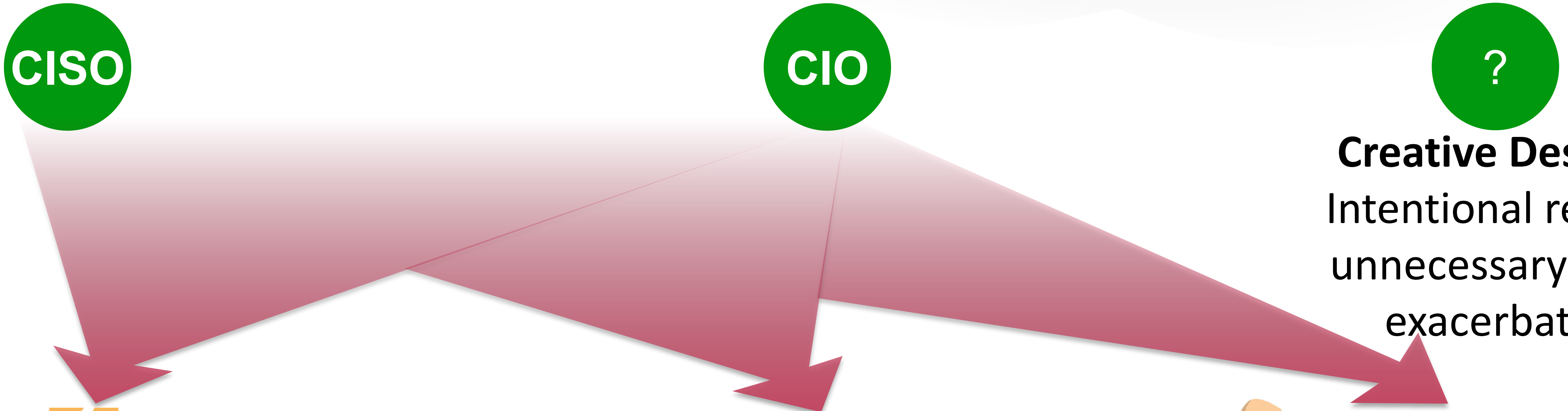
| Era | 1980<br>Identify | 1990<br>Protect | 2000<br>Detect | 2010<br>Respond | 2020<br>Recover |
|---|---|---|---|---|---|
| Core Challenges | What did we buy and how does it support the biz? | Viruses, Server-side Attacks, Insecure Configs | Too many logs and alerts, Client-side attacks | Assume Breach, 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 Resilience vs Anti-Fragility



CISO

CIO

?

**Creative Destruction**: Intentional removal of unnecessary pets that exacerbate fragility

## Fragile

C.I.A.

Volatility causes compounding patchwork and workarounds that create greater fragility

## Resilient

D.I.E.

Volatility results in destruction but no change in configuration

## Antifragile

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

Volatility drives changes in configuration that make it even more DIE-like

Icons made by Nhor Phai and FreePik

# Thoughts and Considerations

- Do our workforce shortage challenges stem more from having too many pets or having too few qualified workers?
- Should cyber pet ownership require licensed cyber veterinarians?
- What factors that result in the creation of more pets and how can that be discouraged?
  - AI/ML creates more data pets
  - GDPR/CCPA punishes for the negligence of data pets

- The more we thinking about securing something, the less we think about how we can live without it
- The security industry is incentivized to have us create more pets

# Summary

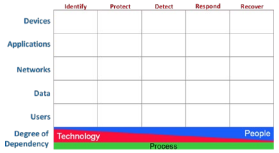
- The next era in IT and Security will manifest **more irreversible attacks** that challenge and undermine our ability to RECOVER
- Better PROTECT, DETECT, and RESPOND capabilities may reduce occurrences of malicious events but are **insufficient against well-executed destructive/irreversible scenarios**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

**Death to CIA! Long live DIE!**

# Applying D.I.E.

- Next week you should:
  - Get uptime measurements and create your own Pets vs Cattle curve
- In the first three months following this presentation you should:
  - Track weekly movement of Pets vs Cattle curve
  - Catalog pet-like and cattle-like design patterns in use within your org
- Within six months you should:
  - Create policies and disincentives that discourage pet creation
  - Create triggers to bring awareness to potential pet owners
  - Discover and provide alternatives to pet-like design patterns

# Questions?



https://cyberdefensematrix.com

sounil@cyberdefensematrix.com

@sounilyu

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

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