# HACKS & HOPS

# SPONSORED BY:

FRSECURE®

OSTRA CYBERSECURITY

RECON™ INFOSEC

red canary™

rubrik

SentinelOne®

# EVENT SCHEDULE

## Check-In | 12:00 PM

## Welcome | 12:30 PM

John Harmon, FRSecure CEO
Special words from Evan Francen

## Speaker Features | 1:00 – 2:00 PM

Dave Gold - 1:00 PM
Exploring Generative AI & LLMs

Dr. Anmol Agarwal - 1:30 PM
Transforming Data Privacy

Jeremy Vaughan - 2:00 PM
Threat Hunting - The Key to Security

## Break | 2:30 – 3:00 PM

## Speaker Features | 3:00 – 3:30 PM

Andrew Cook - 3:00 PM
Threat Hunting: The Key to Security

Oscar Minks – 3:30 PM
Real-world Attacker Techniques:
Protect Yourself

## Panel Discussion | 4:00 – 4:40 PM

## Networking & Happy Hour | 5:00 - 6:30 PM

## JOHN HARMON

FRSecure | CEO

## EVAN FRANCEN

FRSecure | Founder

# WELCOME TO HACKS AND HOPS 2024!

Evan Francen – FRSecure Founder

John Harmon – FRSecure CEO

SECURITY EXPERTS ON A MISSION

# WE ARE ON A MISSION:

## To fix the broken information security industry

SECURITY EXPERTS ON A MISSION

# WHAT ARE WE WORKING ON?

## FRSecure

- Growing like crazy
- Leveling up methodologies
- Awesome humans doing awesome work
- CISSP Mentor Program

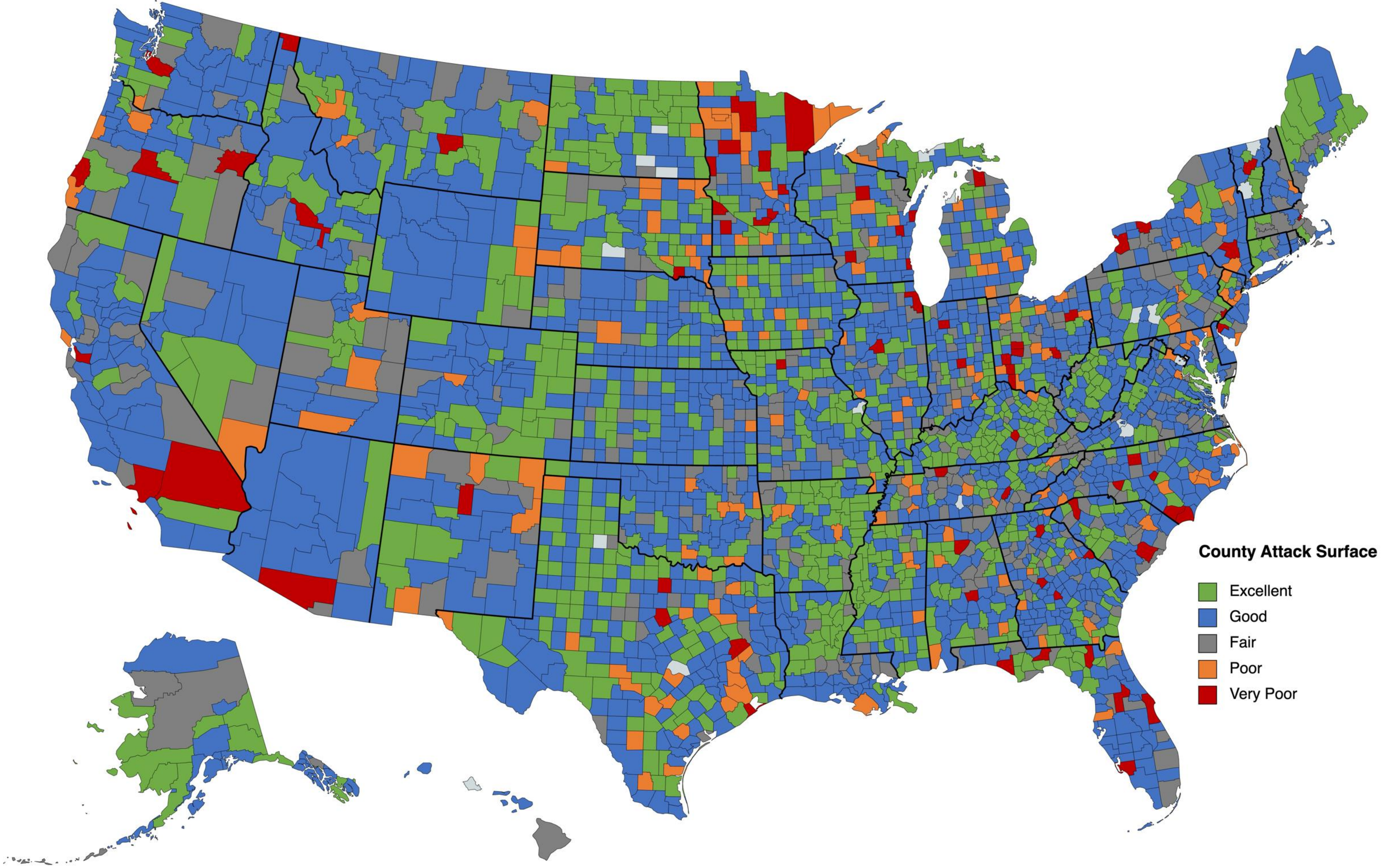
## cVCISO

- We need help!
- ~50,000 companies will need a vCISO in the next five years
- Awesome community of cVCISO’s
- Next class - October

SECURITY EXPERTS ON A MISSION

# SO, EVAN DID A THING…

## Why?



Created with mapchart.net

SECURITY EXPERTS ON A MISSION

# MIRRORED DEFENSE

## Attack Surface Intelligence

- Works for any context
- Launching soon – help us test and improve
- Go see Seth at the booth
- Free trial

SECURITY EXPERTS ON A MISSION

# MANY THANKS!

## It takes a village...

- Sarah Ronkainen and the FRSecure Marketing Team
- All of our sponsors and speakers
- Our partners and supporters
- YOU!

Enjoy the day!

# JUDY HATCHETT

## WiCyS | President

Judy Hatchett is an experienced CISO with over two decades of cybersecurity expertise and currently serves as President of WiCyS Minnesota. She has a relentless commitment to safeguarding digital landscapes.

Moderator

# DAVE GOLD

## Sentinel One | Field CTO

With more than 20 years in Information Security, Dave Gold is America's Field CTO at SentinelOne. Prior to this, he has held various roles in engineering and product management. He has an MBA from the Carlson School of Management and a BA in Political Science/International Relations from Carleton College.

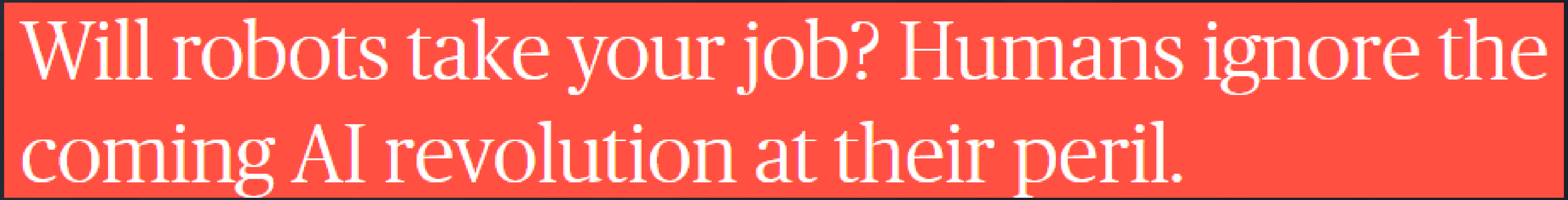
Topic: Exploring Generative AI & LLMs

# AI IN SECURITY:
# FROM HYPE TO REALITY

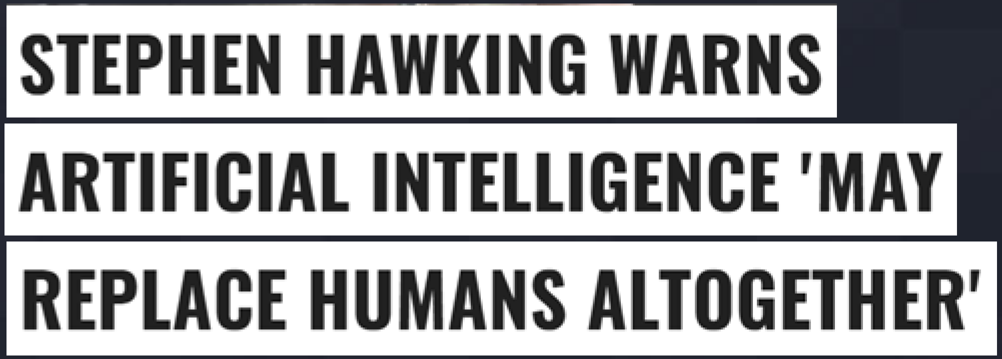
5 Ways AI will both challenge and change the cybersecurity landscape

AMERICAS FIELD CTO
SENTINELONE

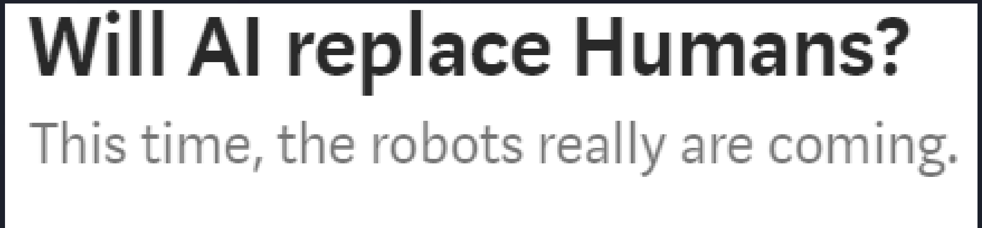
FRSECURE



Will robots take your job? Humans ignore the coming AI revolution at their peril.

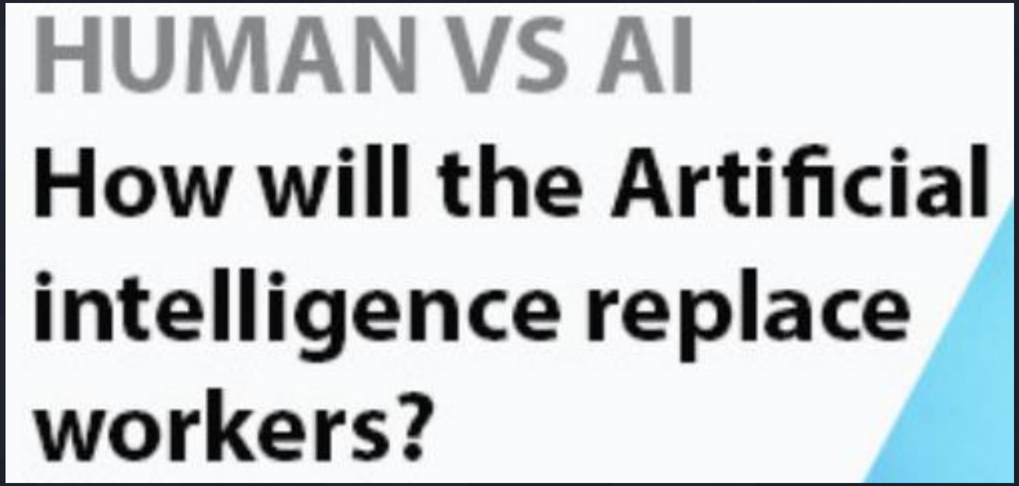


STEPHEN HAWKING WARNS ARTIFICIAL INTELLIGENCE 'MAY REPLACE HUMANS ALTOGETHER'



Will AI replace Humans?

This time, the robots really are coming.



HUMAN VS AI

How will the Artificial intelligence replace workers?

LEARNING TO WORK WITH ROBOTS

AI WILL CHANGE EVERYTHING. WORKERS MUST ADAPT—OR ELSE.

# CHALLENGES WE HEAR FROM CUSTOMERS

### Rapidly Expanding Attack Surfaces

Stealthy, advanced threats that continue to evade even the best defenses

### Complex Multi-Vendor Security Stack

Increasing level of complexity as vendor footprint expands without integrated workflows

### Manual Triage & Investigation

Disconnected, alert-centric tools with alerts that lack context and correlation

### Cybersecurity Skills Shortage

Lack of skilled SecOps practitioners with insufficient domain expertise

### Reactive Processes & Flows

Manual orchestration of responses that happen at individual control points and at human speed

# SOME DATA POINTS

**3.4 Million**

Security Pros Needed

(ISC2 2022 Workforce study)

**76%**

Enterprises prioritized Budget for AI/ML

(Forbes)

**67%**

Security Analysts experience stress & anxiety

(IBM)

**67%**

Daily Alerts are not investigated

(Capgemini Research Institute)

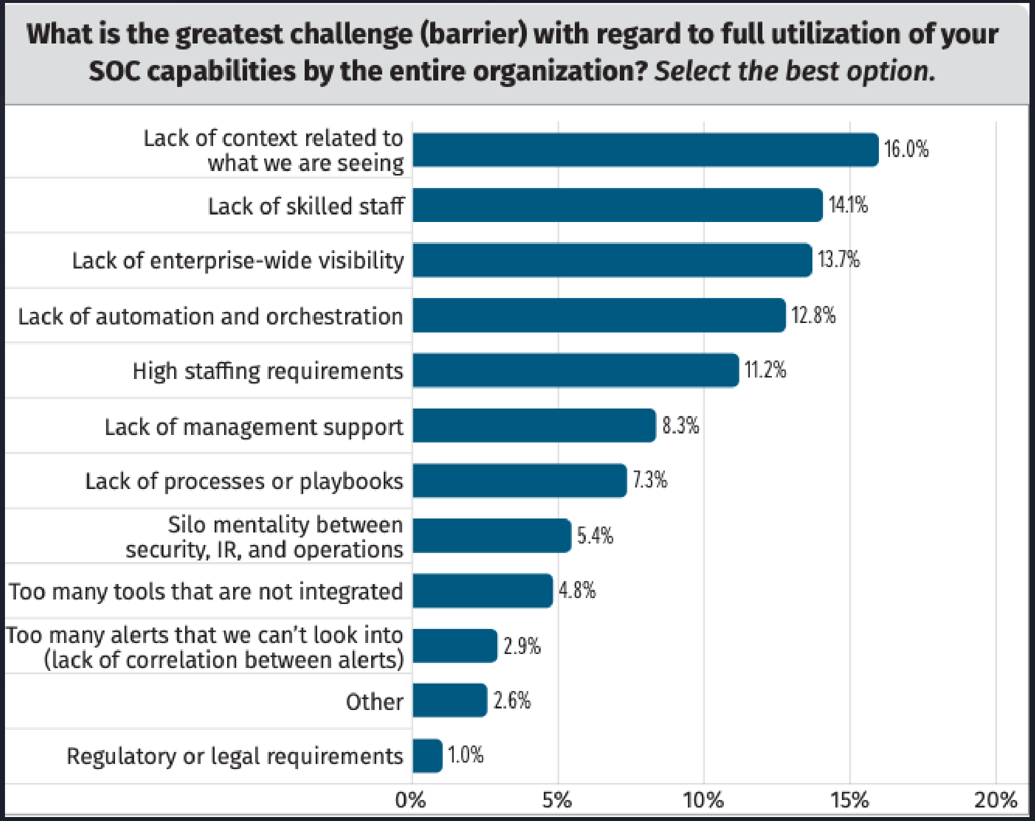
**79 Zettabytes**

Data created by 2025

**4.5K**

Average security events per day

(Source: Damballa)



**What is the greatest challenge (barrier) with regard to full utilization of your SOC capabilities by the entire organization? *Select the best option.***

Source: SANS 2023 SOC Survey

# IS AI THE NEXT INDUSTRIAL REVOLUTION?

**1st** (1750-1850)
Mechanization - Steam Power

**2nd** (1850-1930)
Mass Production - Energy

**3rd** (1930-2000)
Automation - Compute

**4th** (2000-2020)
Robotization
Cyber Physical Systems (IOT)

**5th** (2020 - ???)
Artificial Intelligence
Human Robot Collaboration

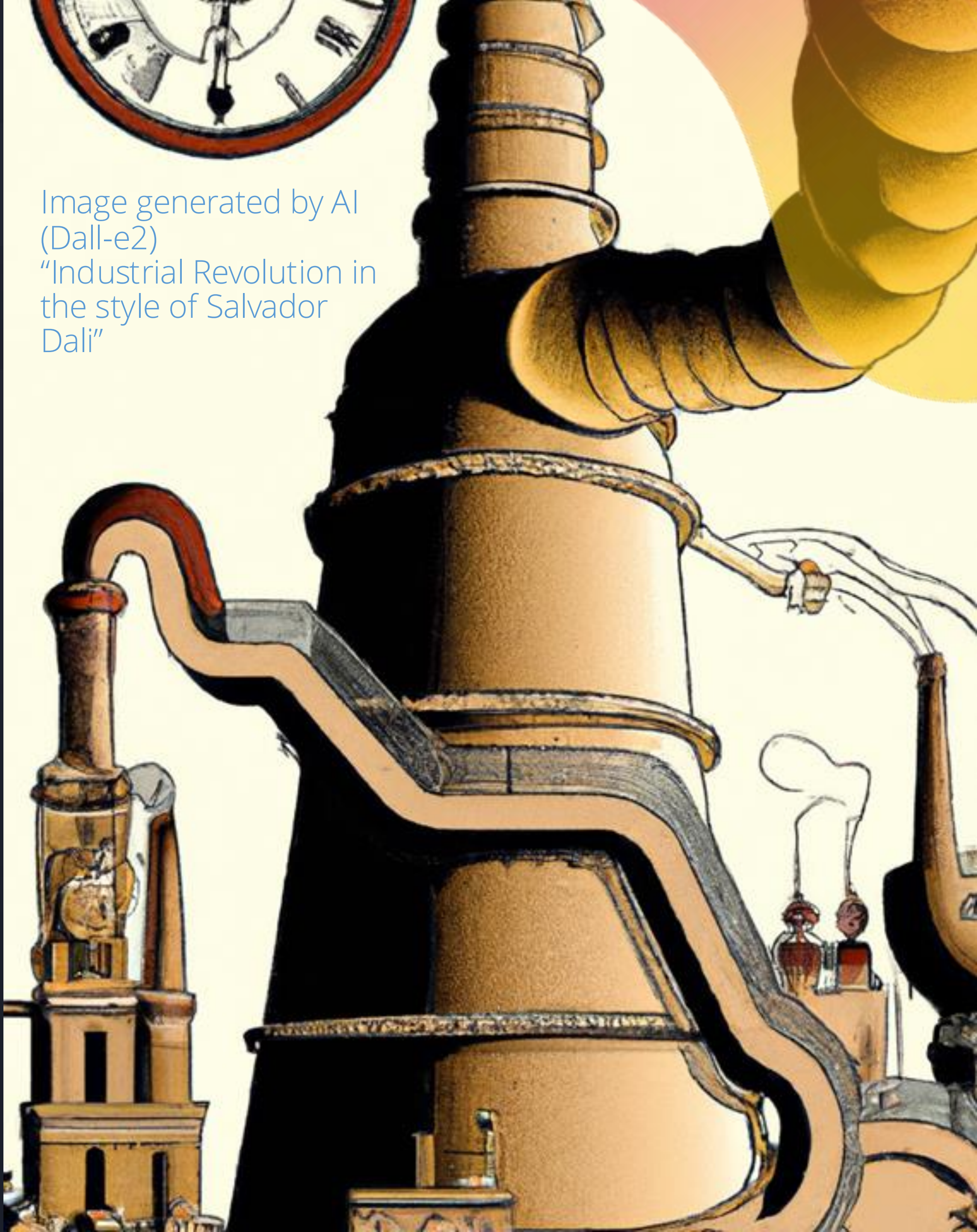


Image generated by AI (Dall-e2)
"Industrial Revolution in the style of Salvador Dali"

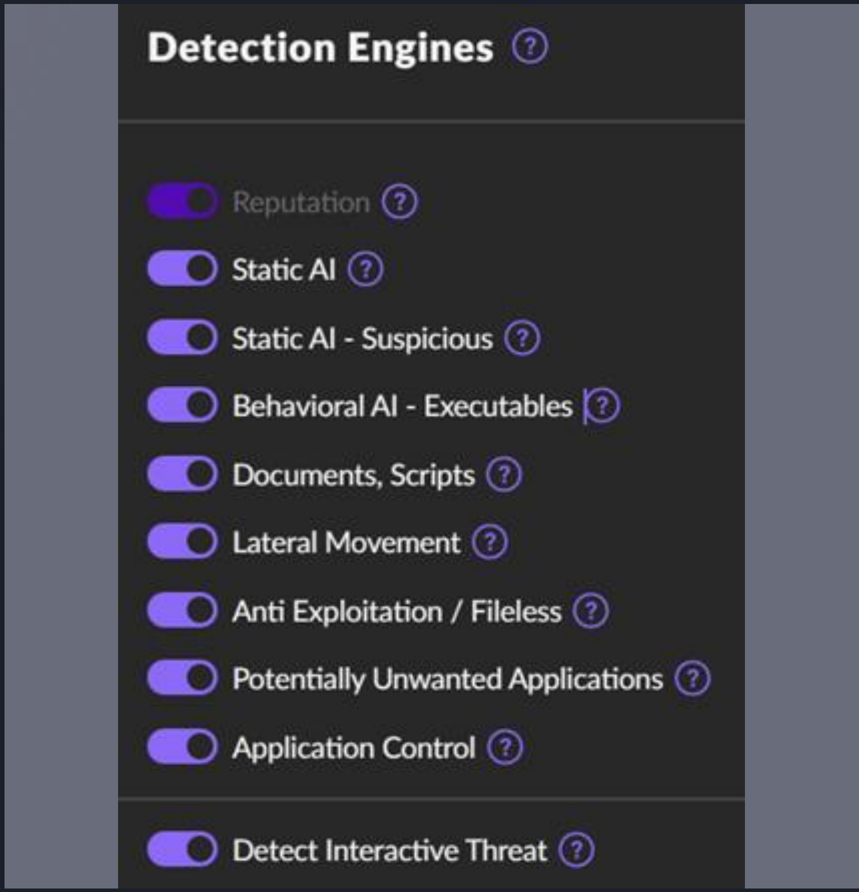
# 5 Ways AI/ML Can Change Cyber Security

Image generated by AI (Dall-e2) "AI vs. AI"

FRSECURE

# 1. BEHAVIORAL AND ANOMALY DETECTION

- Machines can continuously monitor vast amounts of data
- Specialized Machine Learning Models for specific behaviors
- Anomalies
- Predictive Analytics
- Insider Threats & User Behavior
- Autonomous Real-Time Protection from Zero Days



**Detection Engines** ?

- ● Reputation ?
- ● Static AI ?
- ● Static AI - Suspicious ?
- ● Behavioral AI - Executables ?
- ● Documents, Scripts ?
- ● Lateral Movement ?
- ● Anti Exploitation / Fileless ?
- ● Potentially Unwanted Applications ?
- ● Application Control ?
- ● Detect Interactive Threat ?

# 2. THREAT HUNTING

- Threat hunting is very manual today and requires knowledge and context
- Natural language processing
- Proactive hunts based on threat intelligence
- AI can provide continuous hunting
- Threat hunting requires a human to know what to look for - AI can do this automatically

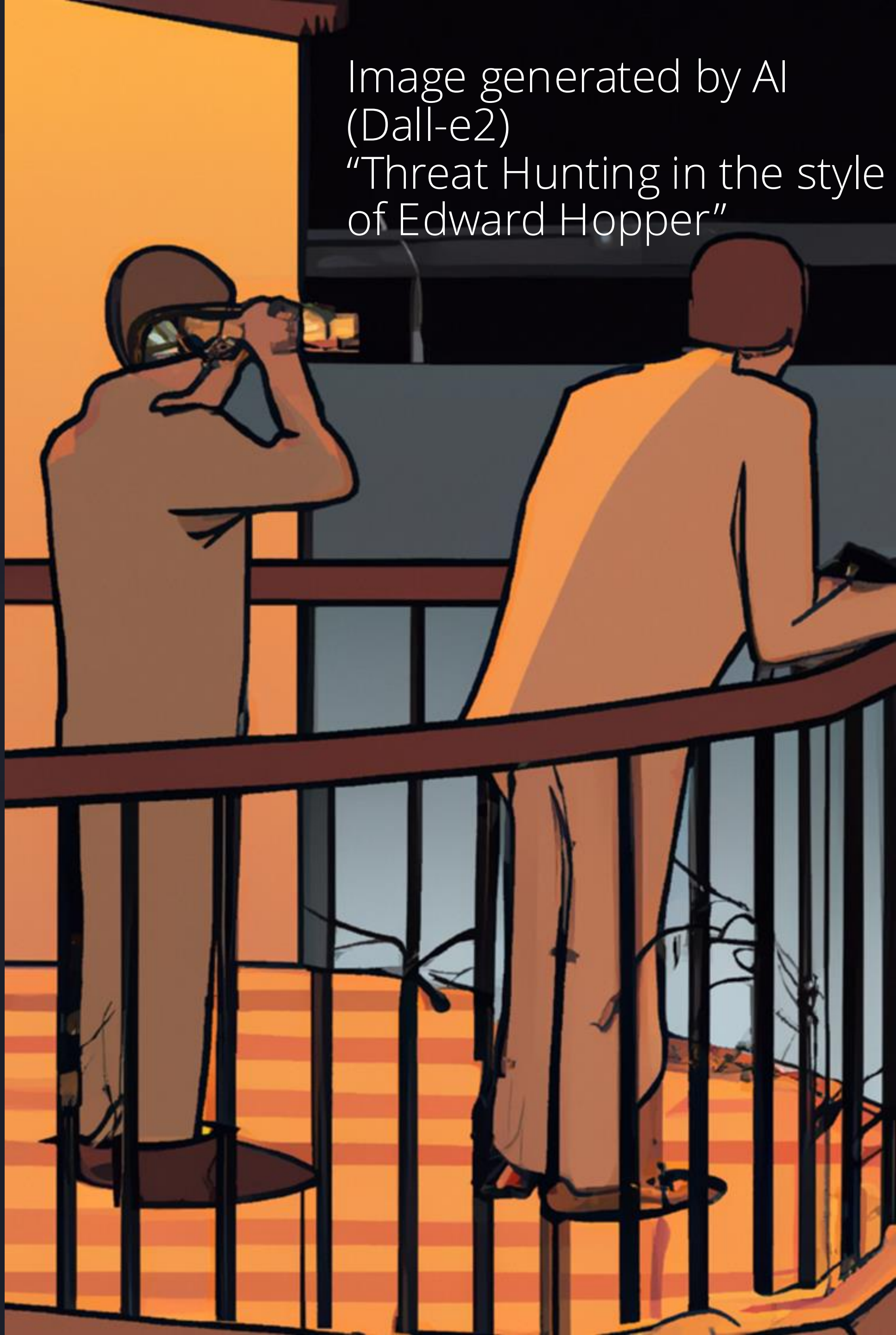


Image generated by AI (Dall-e2)
"Threat Hunting in the style of Edward Hopper"

# 3. AUTOMATION

## ELIMINATE TIME CONSUMING AND ROUTINE TASKS

- Tier 1 Triage

## AUTOMATED RESPONSE AND MITIGATION

- Reduce MTTR

## IOC EXTRACTION

- Automatically extract IOC and feed to other systems

## THREAT INTELLIGENCE SHARING

- Intel gets stale quickly
- Consume much faster

Image generated by AI (Dall-e2) “Intelligent Automation”

# 4. VULNERABILITY MANAGEMENT

## ANALYZE LOTS OF FACTORS TO PRIORITIZE

- Asset Inventory
- Contextual Understanding
- Risk-Scoring Algorithms

## BREACH RISK PREDICTION

## PENETRATION TESTING

- Simulate Social Engineering Attack

## AUTOMATED PATCHING

Image generated by AI (Dall-e2) "Cyberpunk Automation"

# 5. INCIDENT RESPONSE

## INCIDENT RESPONSE

- Prioritize Alerts
- Identify False Positives

## LLMS IMPROVE INCIDENT RESPONSE

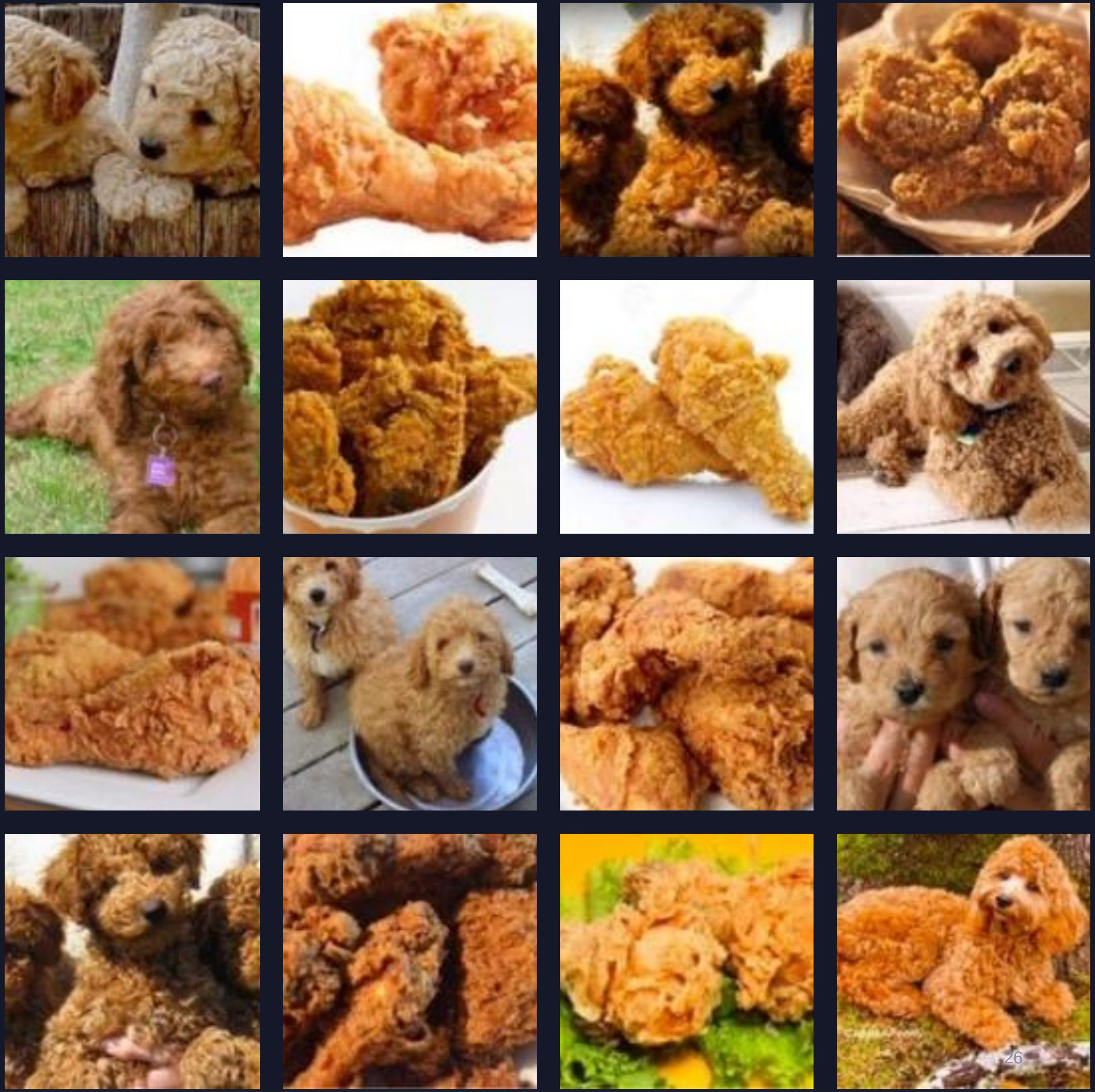
- Increased Accuracy
- Reduced Costs
- Improve Efficiency / Force Multiplication
- Enhanced Visibility
- Context

Image generated by AI (Dall-e2)
“Incident Response hacker cyber punk”

# 5 CHALLENGES WITH AI/ML

# Can AI Tell the Difference?

90%



# 1. PRIVACY & SECURITY

## PRIVACY

- Models trained on personal or company intellectual property
- Surveillance and Monitoring
- Use by law enforcement agencies

## BIAS & DISCRIMINATION

## SECURITY

- Data Theft
- Data Poisoning

Image generated by AI (Dall-e2)
"Face with hands over eyes on a poster in a futuristic subway"

# 2. THE USE OF AI/ML IN CYBER ATTACKS

**AI Powered Bots**

Looking for Vulnerabilities

**Automated Phishing**

Trained to bypass

**AI Created Malware**

Lower barriers to entry

**Deep Fakes**

Fraud & Deception

**Data Poisoning**

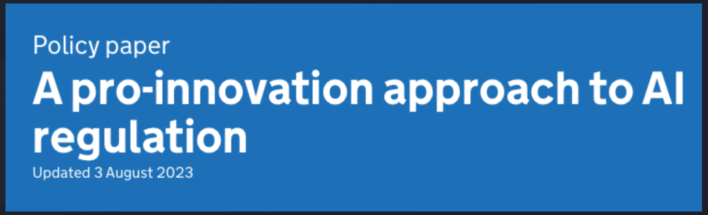
Confuse Defenses

# 3. REGULATORY UNCERTAINTY

## AI Bill of Rights (USA)

- Safe & Effective Systems
- Algorithmic Discrimination Protections
- Data Privacy
- Notice and Explanation
- Human Alternatives, Considerations, and Fallback

## United Kingdom

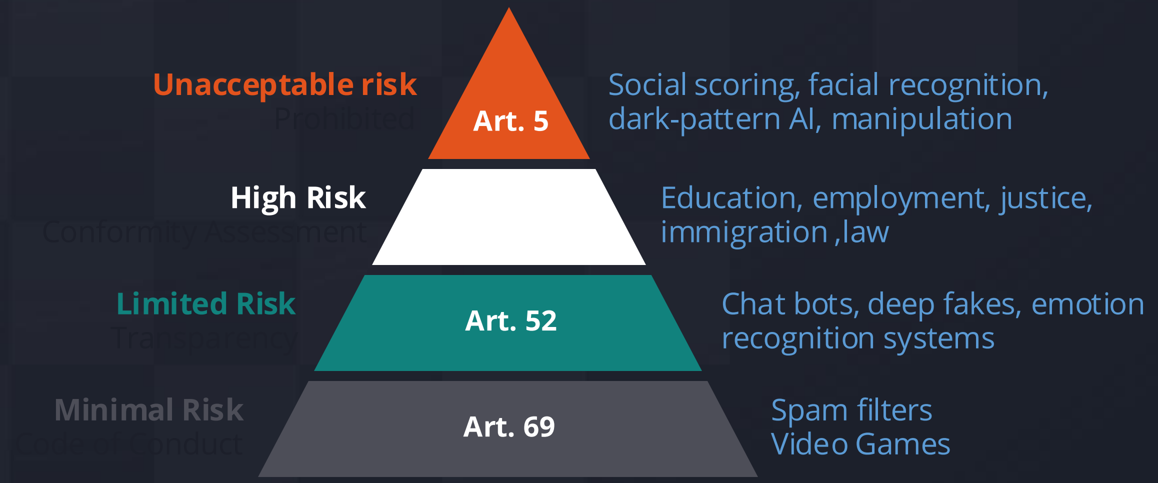


Policy paper

**A pro-innovation approach to AI regulation**

Updated 3 August 2023

## European Union AI Act



Unacceptable risk
Prohibited
Art. 5
Social scoring, facial recognition, dark-pattern AI, manipulation

High Risk
Conformity Assessment
Education, employment, justice, immigration ,law

Limited Risk
Transparency
Art. 52
Chat bots, deep fakes, emotion recognition systems

Minimal Risk
Code of Conduct
Art. 69
Spam filters
Video Games

## China’s Deep Synthesis Provisions

| | |
|---|---|
| Data security & personal information protection | Transparency |
| | Technical Security |

FRSECURE

# 4. COSTS

- Compute (GPU)
- Environmental costs (natural resources)
- Will need AI/ML expertise on team
- Larger models aren’t necessarily better
- Can reduce costs by leveraging multiple smaller models that are optimized for specific tasks

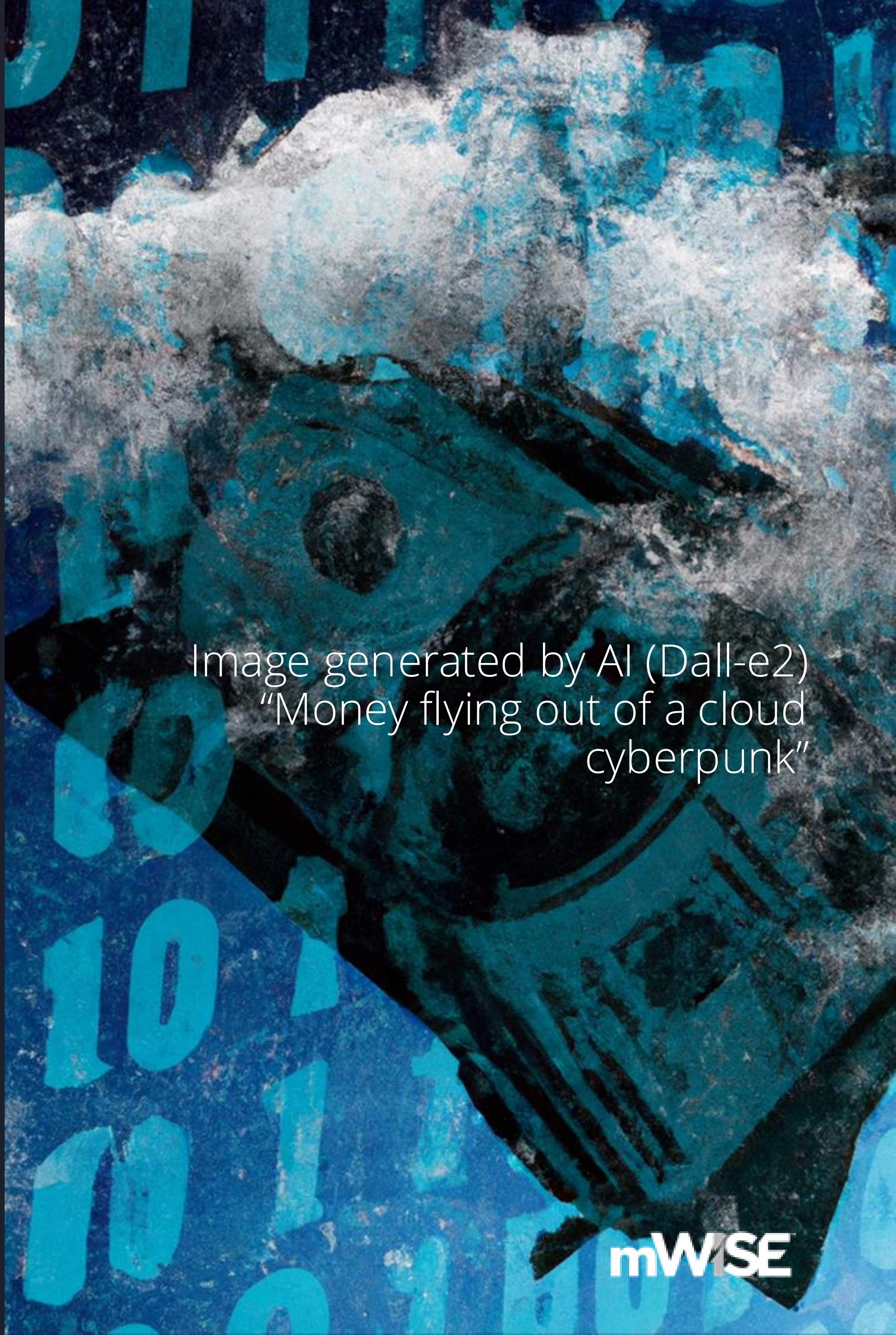


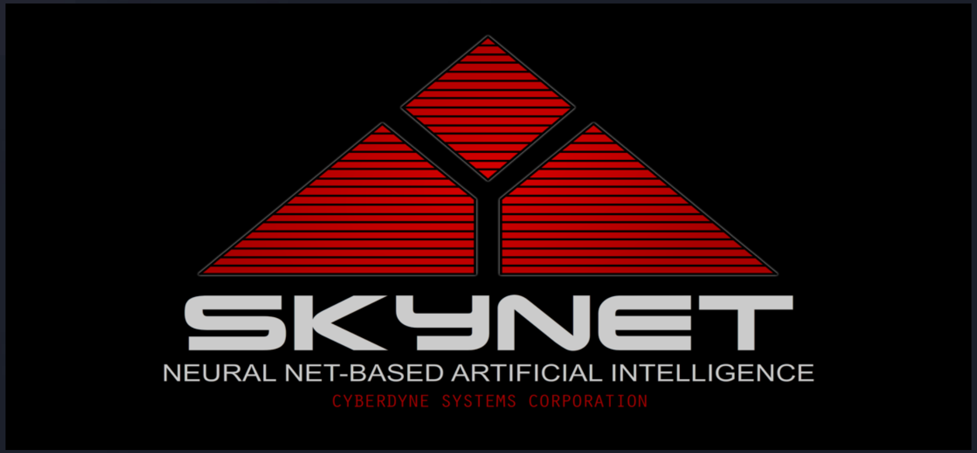
Image generated by AI (Dall-e2)
“Money flying out of a cloud cyberpunk”

# 5. ACCURACY

- Hallucinations
- Data poisoning
- False positives
- Only as good as the training data
- Cyber automation requires a highly accurate model

Image generated by AI (Dall-e2)
"A target with lots of arrows in the bullseye in Times Square "

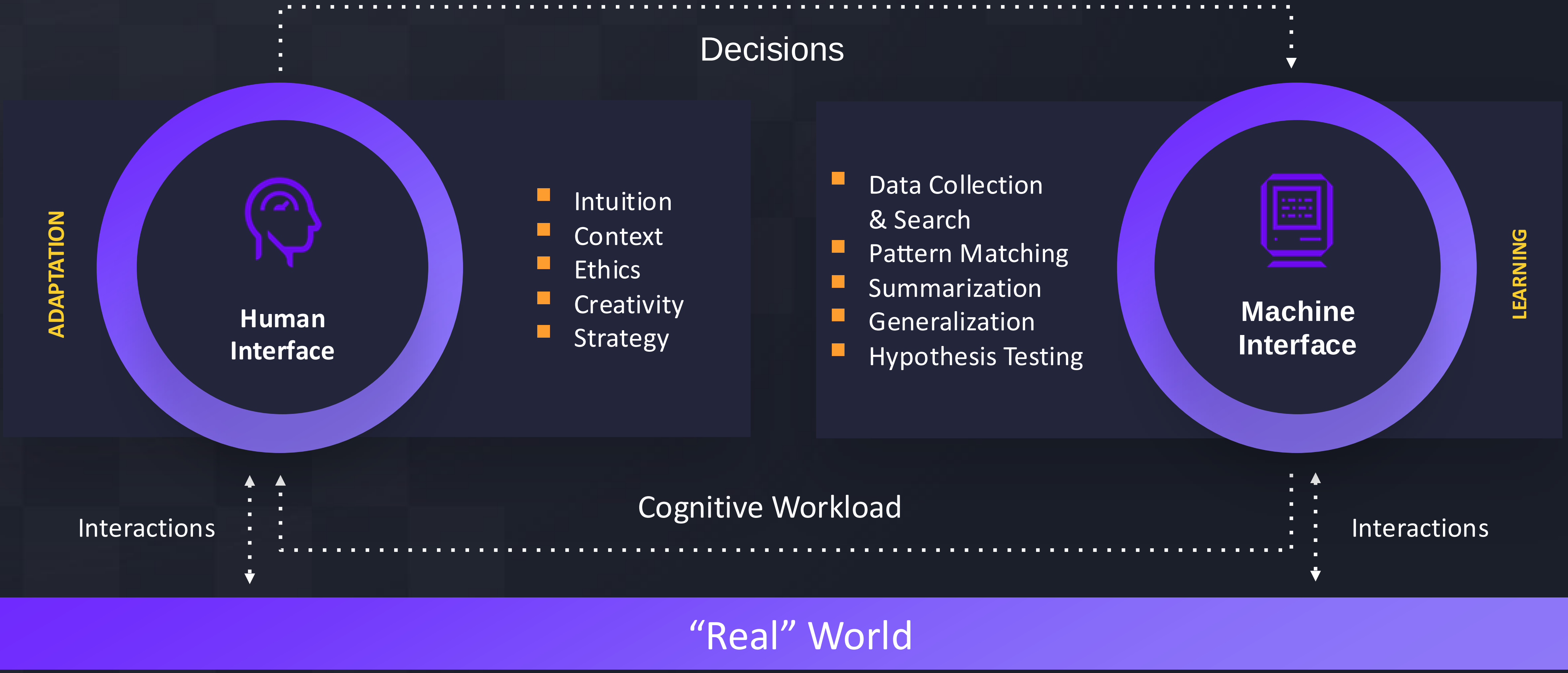
# WHAT'S NEXT ?


SKYNET
NEURAL NET-BASED ARTIFICIAL INTELLIGENCE
CYBERDYNE SYSTEMS CORPORATION

# WILL AI REPLACE HUMANS IN CYBER SECURITY?

- **Already have a shortage of Cyber Security Expertise**
- **AI can process massive amounts of data**
- **Humans move from reactive to proactive**
  - Threat Hunting
  - Strategic Planning
  - Mitigation Strategies
- **Humans will shift focus**
  - Industrial Revolution = Realignment of jobs
  - Build, maintain, direct, optimize autonomous systems
  - Need more ML/AI, Data expertise

# A TIME & PLACE FOR MACHINES



- Intuition
- Context
- Ethics
- Creativity
- Strategy

- Data Collection & Search
- Pattern Matching
- Summarization
- Generalization
- Hypothesis Testing

# BENEFITS OF HUMAN-MACHINE TEAMING

## Simplified Triage

- Natural Language Queries
- Automate Data Gathering
- False-Positive Reduction
- Signal from Noise
- Reduced Complexity

## Integrated Response

- Conformity of Actions
- Designed for Repeatability
- Improve Confidence
- Reduce MTTD & MTTR

## Staff Efficiencies

- Reduce FTE Requirements
- Automate / Replace Tier 1
- Analyst Coaching
- Reduce Alert Fatigue

# HOW TO START YOU AI JOURNEY

- Identify **Data Sources** & a consolidated **Data Platform**
- Select Right Use Cases - **Highest Benefit, lowest costs**
- **Collaborate** on Threat Intelligence
- Use **Automation** as much as possible
- **Train** Cyber Analysts to be AI-Ready
- Implement **Governance** Program for AI

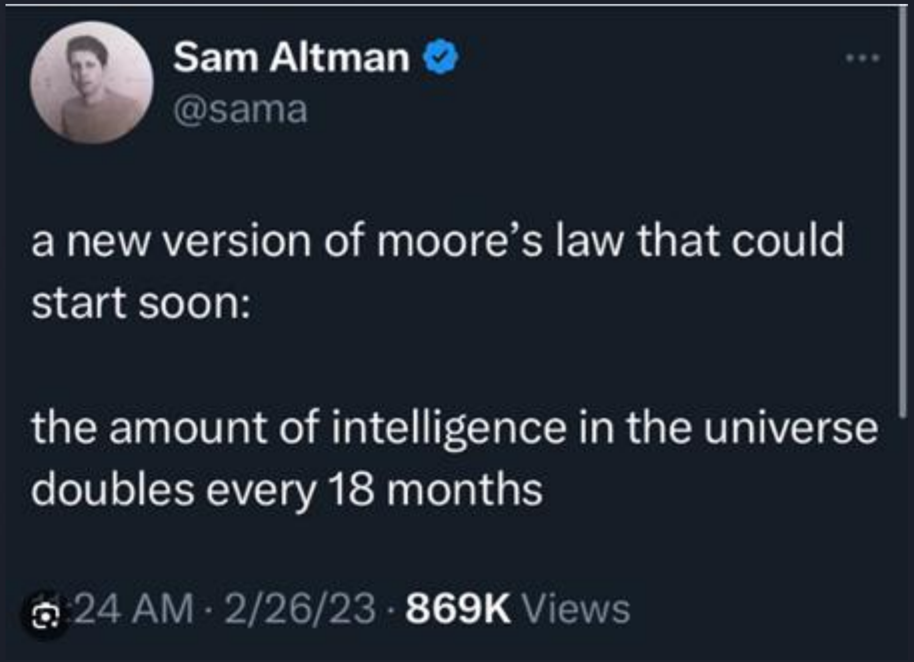
Image generated by AI (Dall-e2)
“AI on a journey digital art”

# AI REQUIRES THE RIGHT DESIGN

1. Helpful - reduce the customer’s burden
2. Correct - deliver accurate, up-to-date responses
3. Responsive - enable SecOps at the pace of conversation
4. Safe - respect trust, geo, and security boundaries
5. Transparent - show work and sources, costs and value
6. Adaptive - get better with use and feedback
7. Comprehensive - one familiar way to get all the work done

# KEY TAKEAWAYS

- AI holds immense potential for defending (and attacking).
- Advancements in ai significantly enhance cybersecurity.
- Adopt a holistic approach with ai powered solutions and human expertise
- Stay vigilant and continually advance defensive AI.
- Collaboration is vital to develop effective countermeasures.



**Sam Altman**
@sama

a new version of moore's law that could start soon:

the amount of intelligence in the universe doubles every 18 months

:24 AM · 2/26/23 · **869K** Views

# Thank You!

Image generated by AI (Dall-e2)
“A speaker on stage with a large audience of people raising hands to ask questions”

FRSECURE

# DR. ANMOL AGARWAL

## Alora Tech | Expert Researcher

Dr. Anmol Agarwal is a senior security researcher specializing in AI security. She holds a doctoral degree in cybersecurity analytics. She is a renowned speaker and has spoken at many events about AI and cybersecurity. In her free time, she enjoys mentoring others in the community and traveling.

Topic: Transforming Data Privacy

HACKS & HOPS® an FRSECURE® EVENT SERIES

FRSECURE®

# Privacy Enhancing Technologies and Federated Learning

DR. ANMOL AGARWAL

# About Me

- Sr. Security researcher working in AI/ML security
- Adjunct professor teaching ML
- Doctorate in cybersecurity analytics
- Founder/Speaker/Consultant

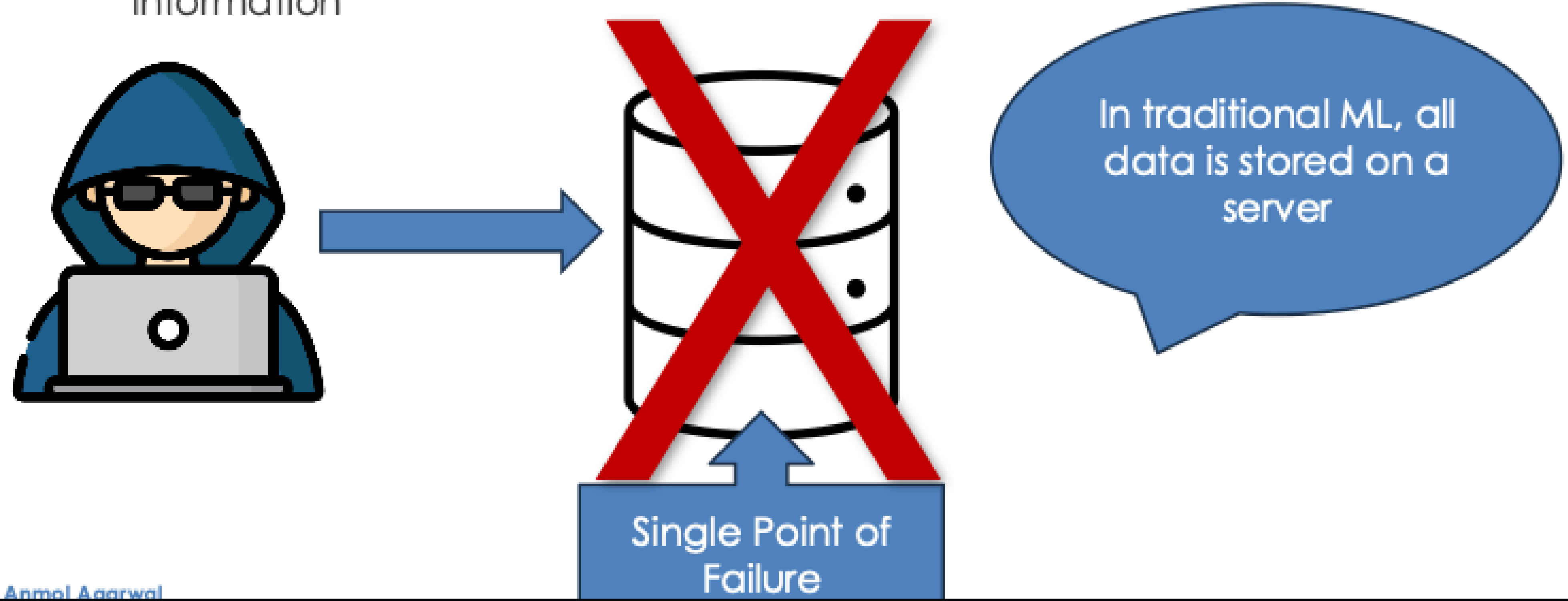
QR code = my LinkedIn

# What is Data Privacy?

- Protection of personal data
  - Only authorized people should have access to personal data

# Some Issues With Data Privacy

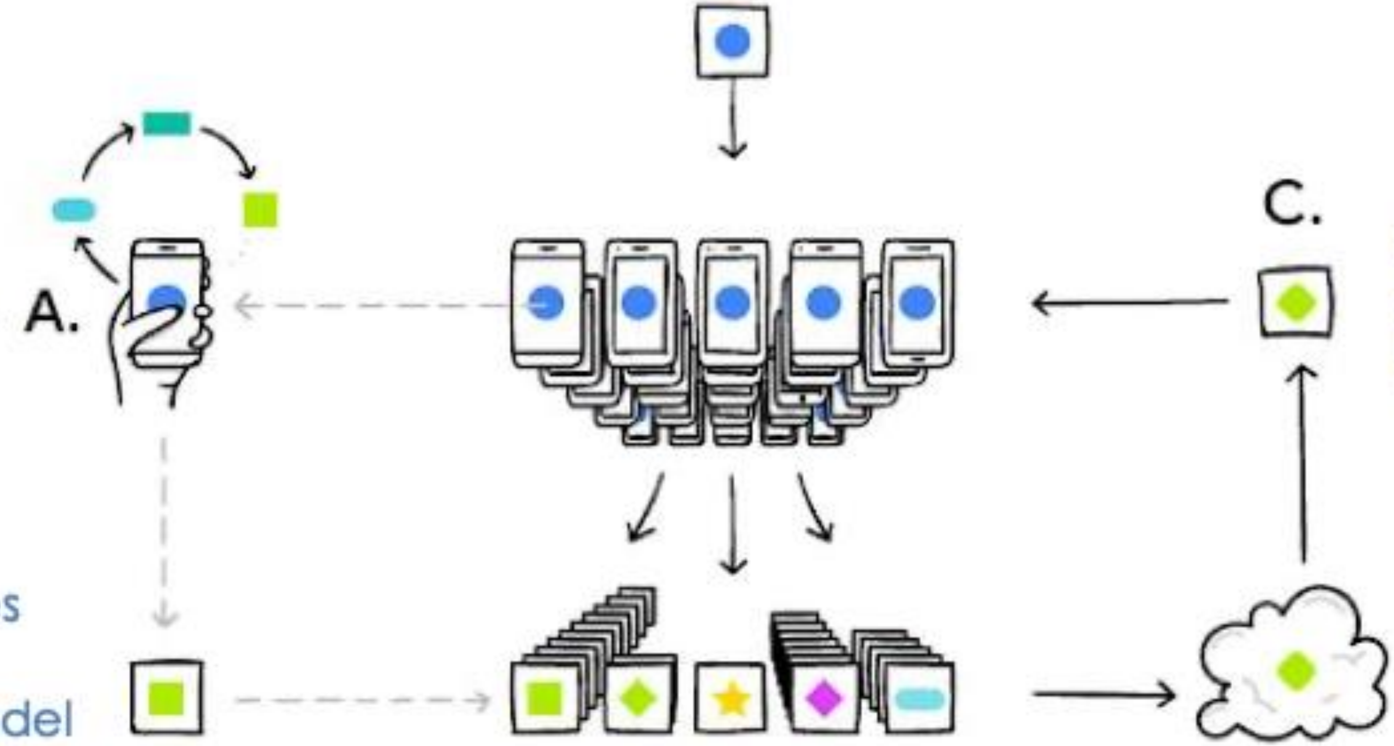
- In some cases, Machine Learning can be attacked and reveal private information



In traditional ML, all data is stored on a server

Single Point of Failure

# Federated Learning!



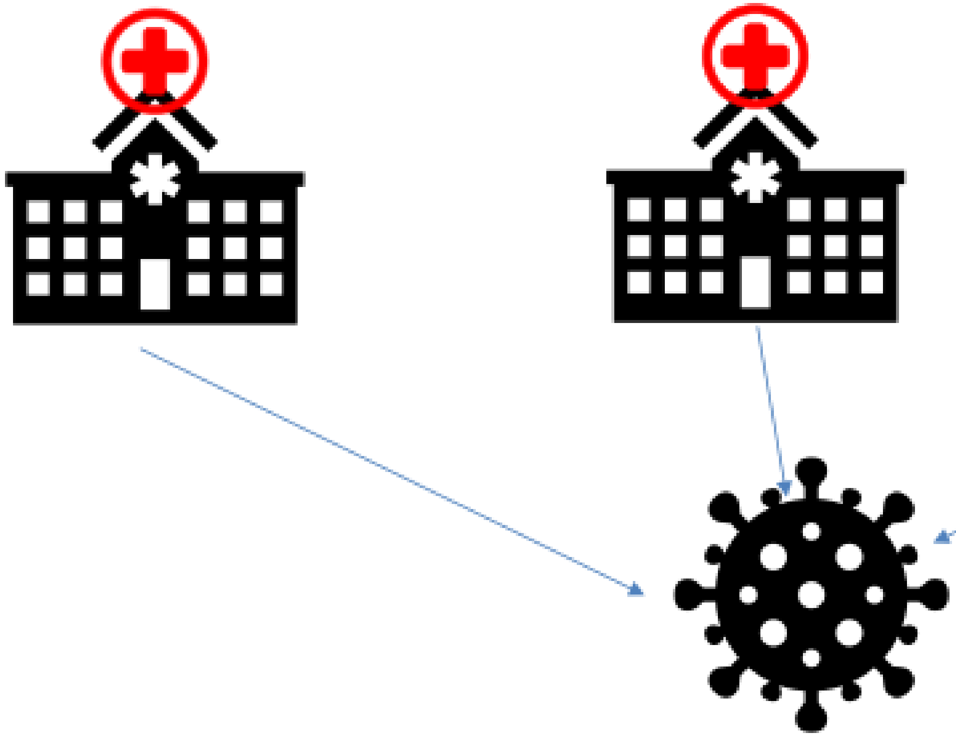
A. Data stored locally on client

Device completes training, sends update to ML model

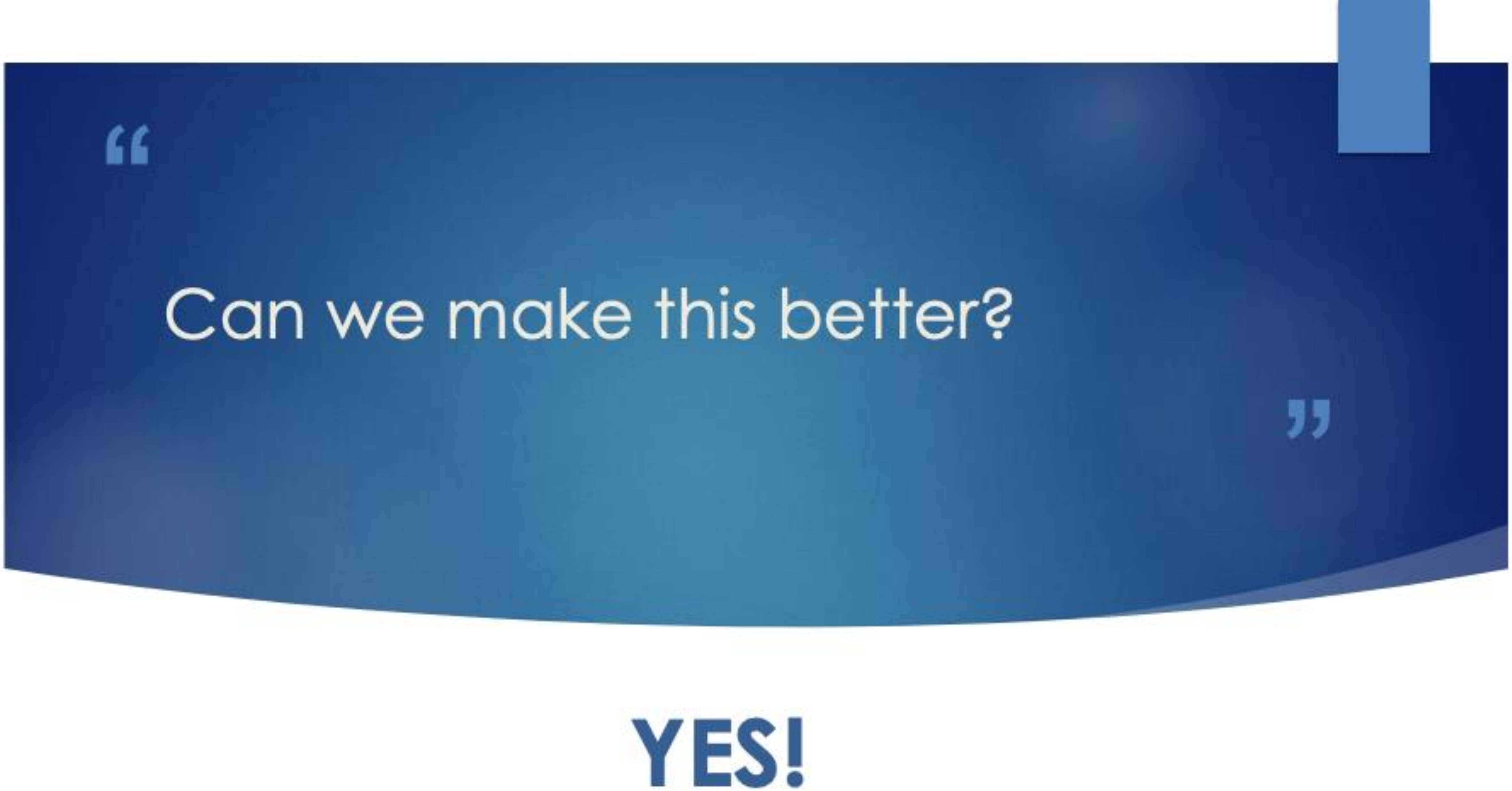
B. All updates from clients sent to server (aggregation)

C. Server sends new ML model based on updates to selected clients

# Federated Learning In Healthcare

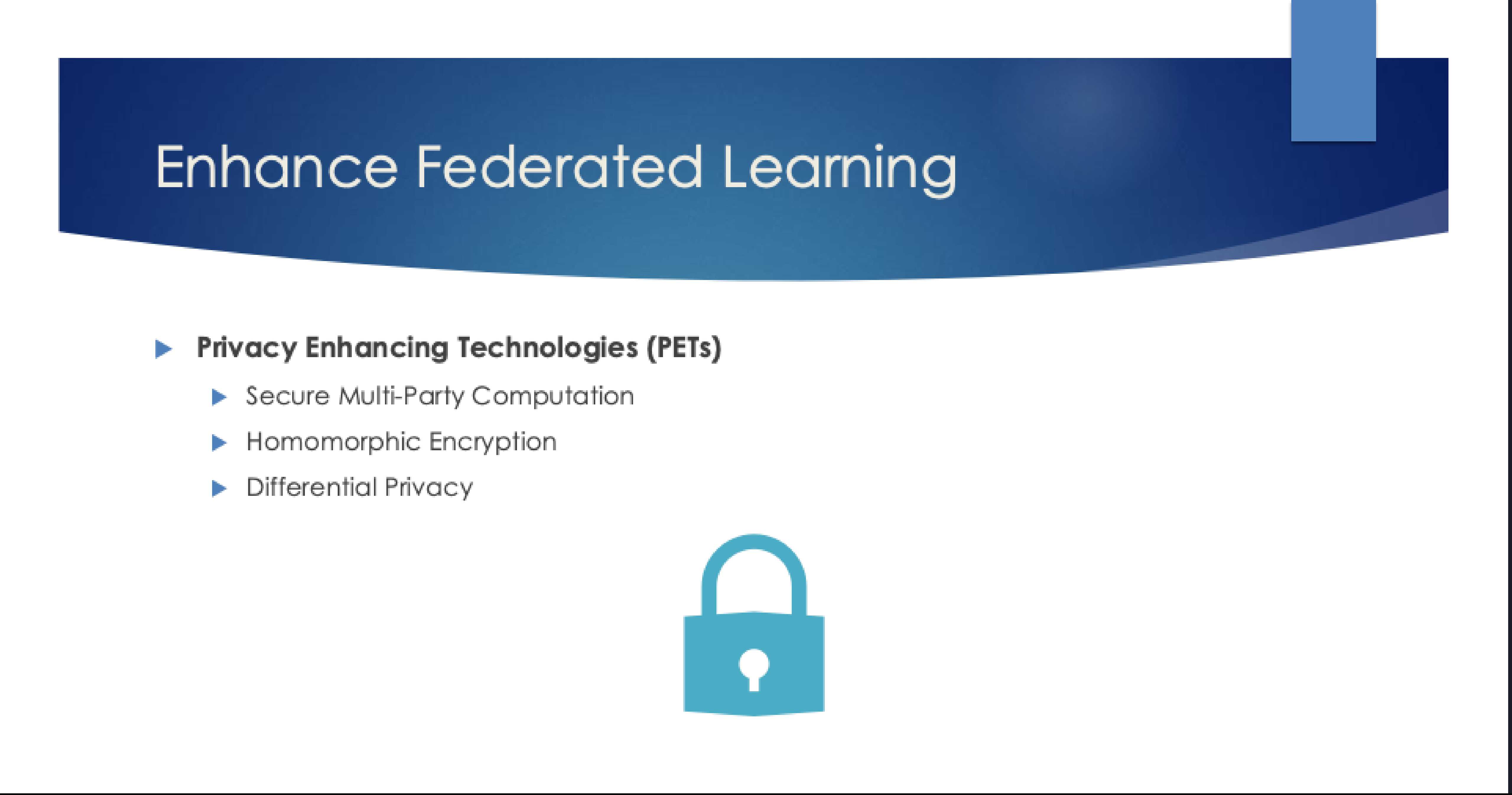


Learn from multiple hospital data
Preserve patient privacy



“Can we make this better?”

YES!



# Enhance Federated Learning

- **Privacy Enhancing Technologies (PETs)**
  - Secure Multi-Party Computation
  - Homomorphic Encryption
  - Differential Privacy

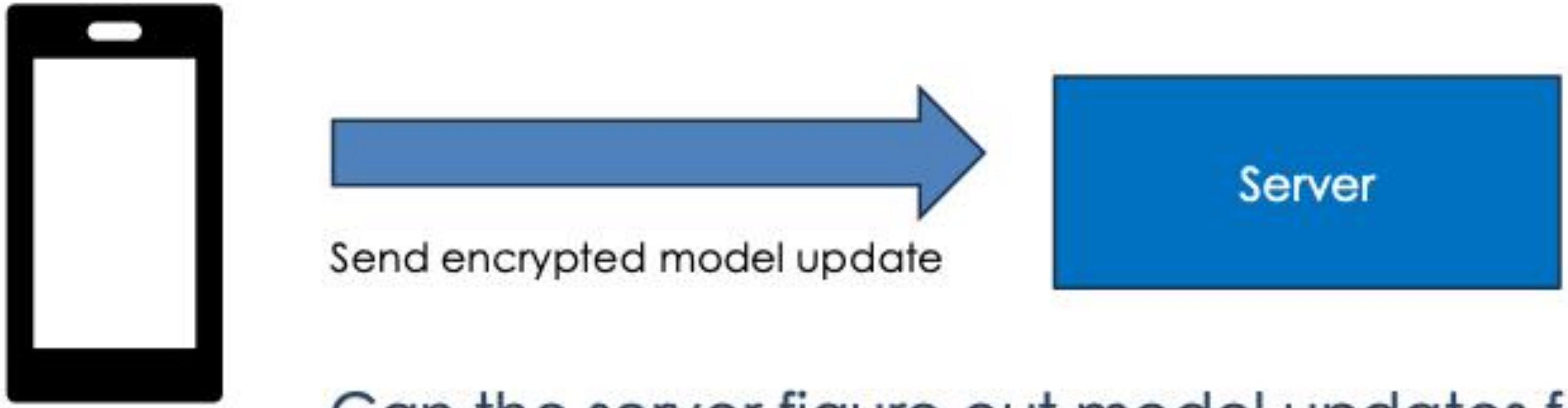
# Privacy Enhancing Technologies (PETs)

- **Secure Multi-Party Computation** – No participant learns anything about other participants

Secret sharing

# Privacy Enhancing Technologies (PETs)

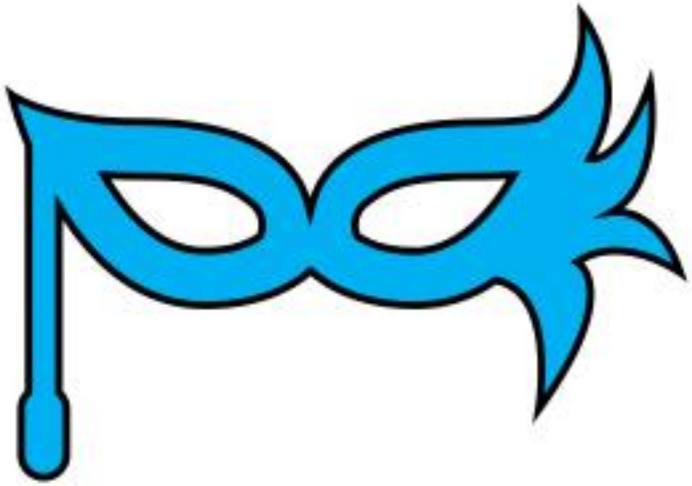
- **Homomorphic encryption (HE)** – perform computations only on encrypted data without unencrypting it

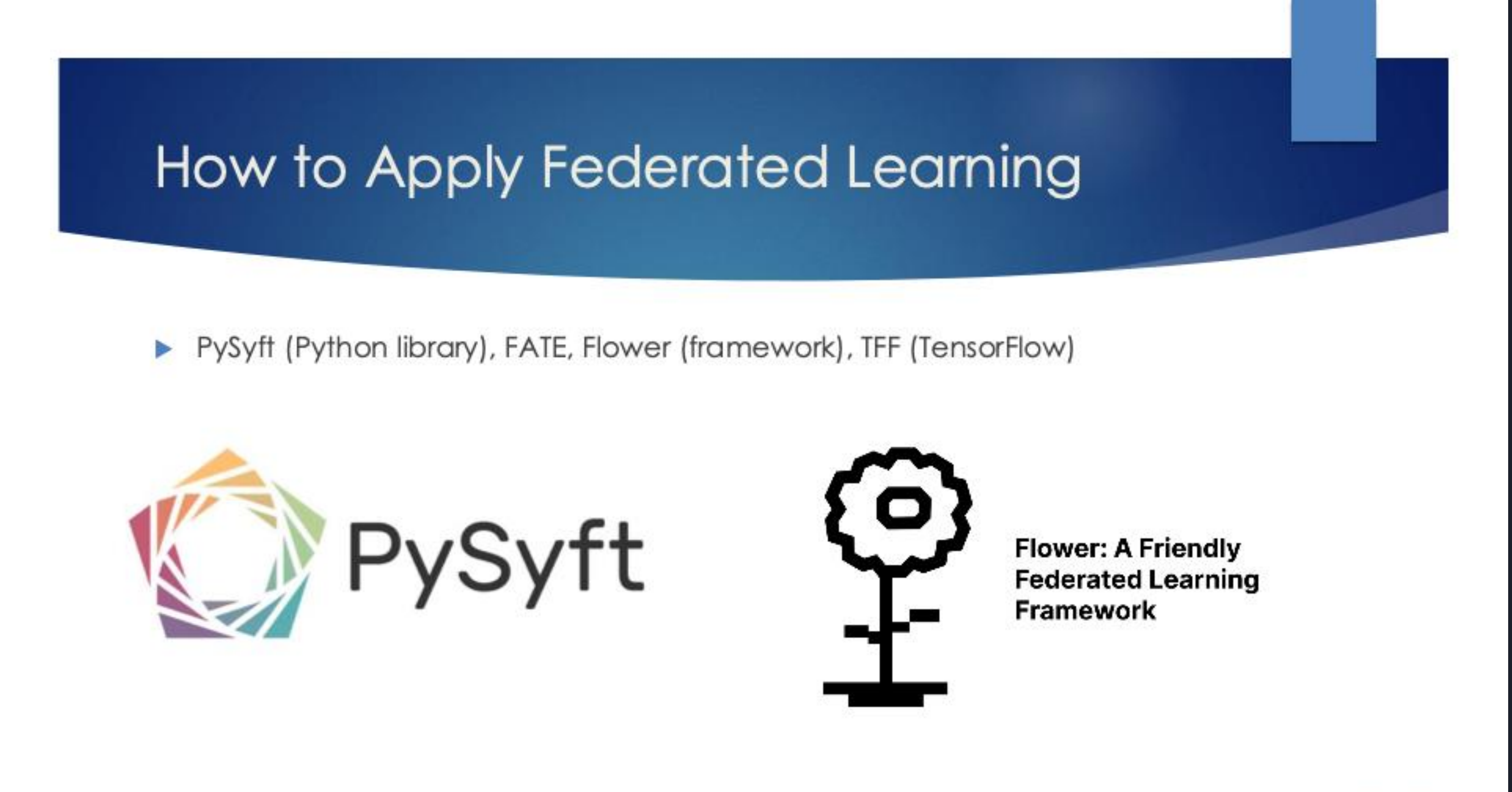


Can the server figure out model updates for each client?

# Privacy Enhancing Technologies (PETs)

- **Differential privacy** – Mask the data used by the model, add noise to data inputs and models. Used in medical applications
- Add noise to less important features to preserve accuracy





# How to Apply Federated Learning

- PySyft (Python library), FATE, Flower (framework), TFF (TensorFlow)

PySyft

Flower: A Friendly Federated Learning Framework

# Any Questions?

Contact me on Linkedin: anmolsagarwal

Email: anmol@aloratech.com

# References (Research Papers)

- Mosaiyebzadeh, F., Pouriyeh, S., Parizi, R. M., Sheng, Q. Z., Han, M., Zhao, L., ... & Batista, D. M. (2023). Privacy-enhancing technologies in federated learning for the internet of healthcare things: a survey. *Electronics*, *12*(12), 2703.
- Mugunthan, V., Polychroniadou, A., Byrd, D., & Balch, T. H. (2019, December). *Smpai: Secure multi-party computation for federated learning*. In *Proceedings of the NeurIPS 2019 Workshop on Robust AI in Financial Services* (Vol. 21). Cambridge, MA, USA: MIT Press.
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7523633/

# JEREMY VAUGHAN

## Start Left Security | Founder & CEO

Jeremy Vaughan, a product security leader, co-founded Start Left™ Security to empower developers with an all-in-one program for secure software creation. Their AI-powered platform integrates with development workflows to ensure secure products from the ground up.

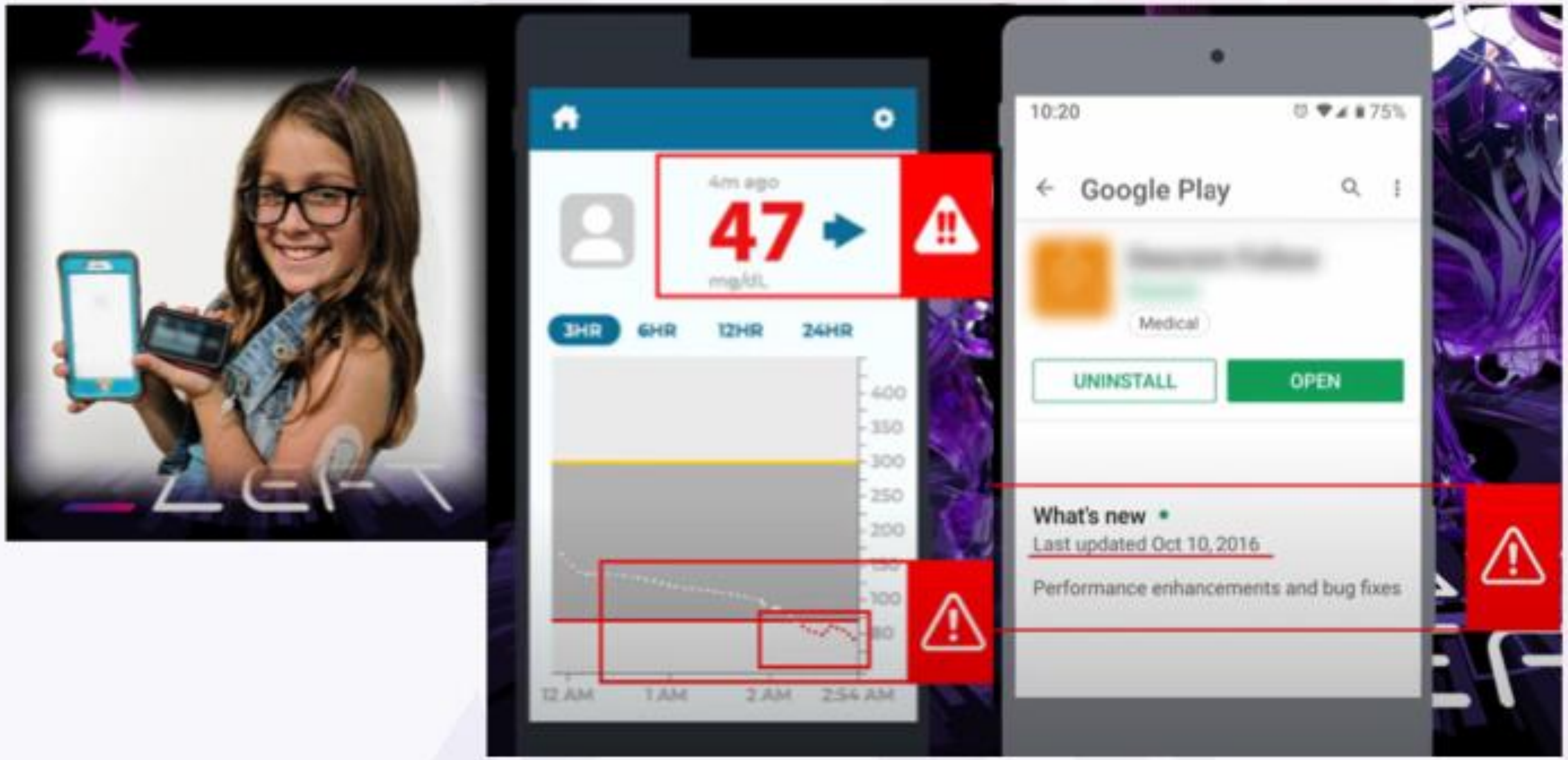
Topic: Developers & Defense

# Scaling Your **Security Champions**

*If Our Developers Are Our Front Line of Defense, Why Do We Put Them Last?*

START LEFT®

# What Happens When…
# **Developers Are Left Out**



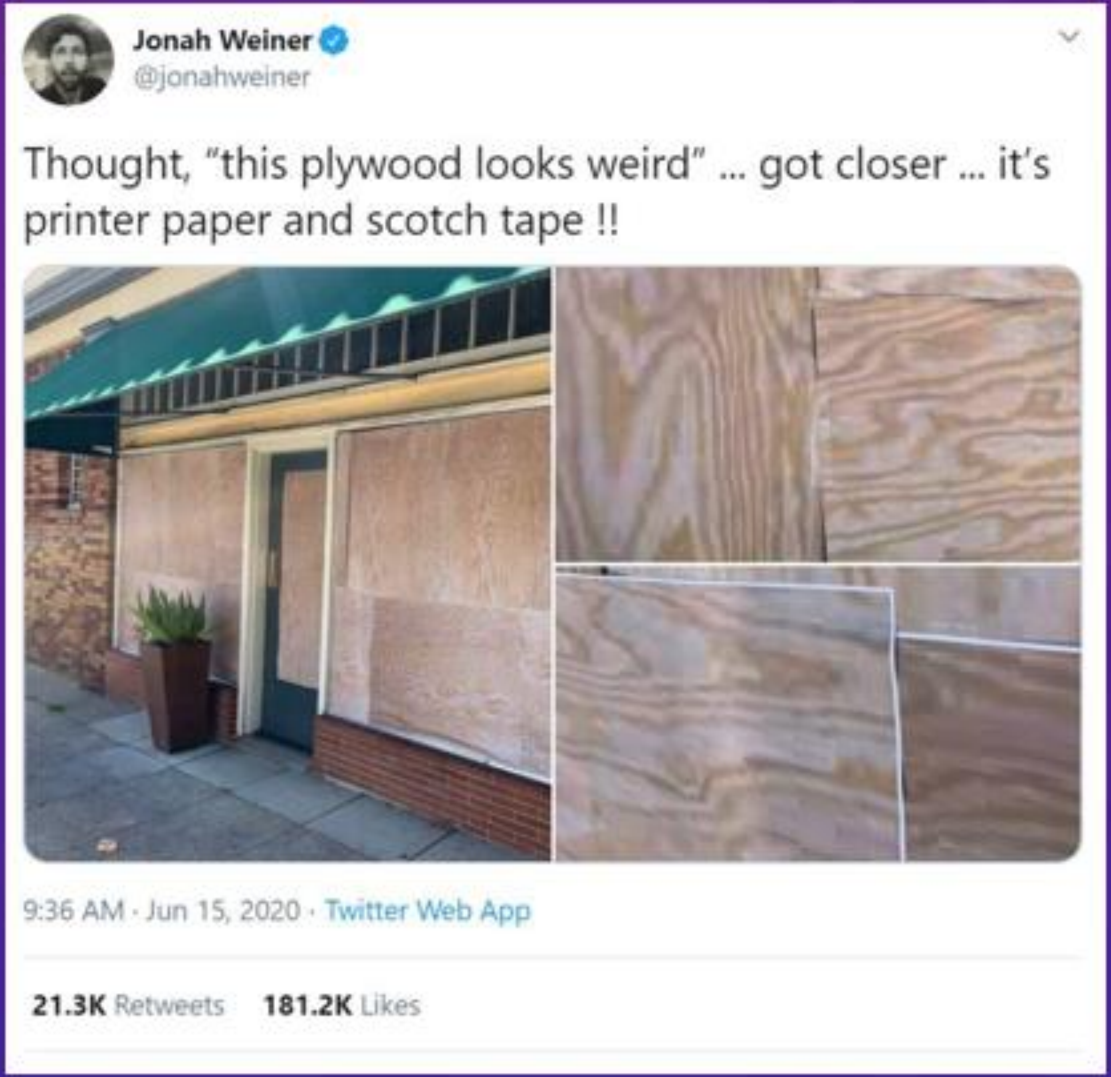
What's new

Last updated Oct 10, 2016

Performance enhancements and bug fixes

# Cybersecurity is ~~broken.~~ incomplete.

WE DON'T HAVE A CYBERSECURITY PROBLEM.
WE HAVE A SOFTWARE QUALITY PROBLEM.



Jonah Weiner @jonahweiner

Thought, “this plywood looks weird” ... got closer ... it’s printer paper and scotch tape !!

9:36 AM · Jun 15, 2020 · Twitter Web App

21.3K Retweets 181.2K Likes

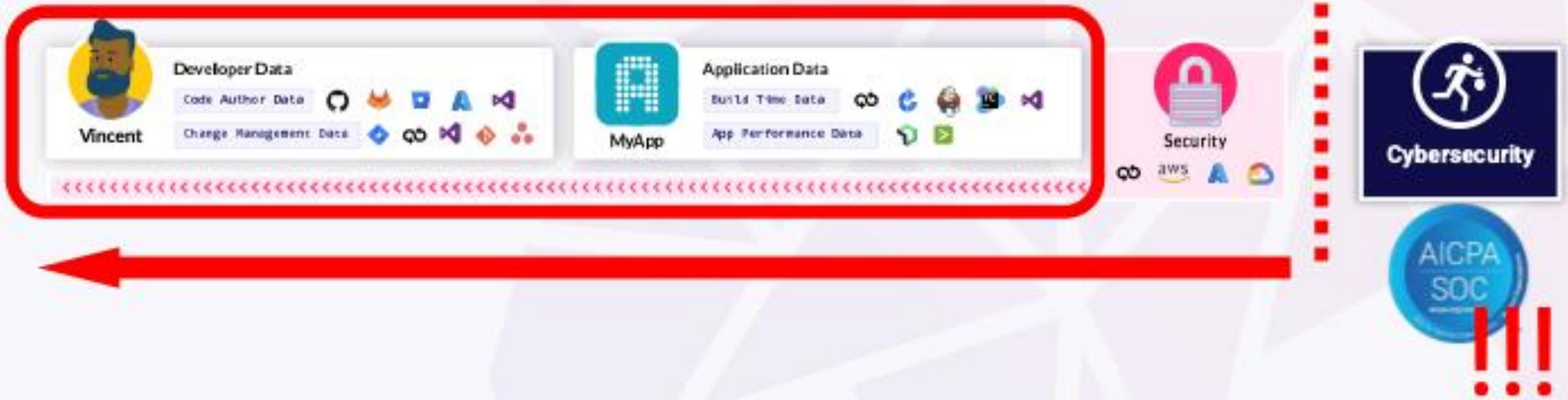
| Traditional 💀 | Modern |
|---|---|
| Vulnerability-Centric | Program-Centric |
| Tool-Heavy | Unified Platforms |
| Compliance-Driven | Culture-Driven |
| Siloed | Integrated |
| Asset-Focused | People-Focused |

Vs

WHAT
DOES EVERY
~~HOARDER~~ CISO
HAVE IN COMMON?
MANY THINGS
imgflip.com

# Introduction to
# **The Paradox**

Why Not Build In Quality, Resilience, Integrity Into The System?



Vincent

Developer Data

Code Author Data

Change Management Data

MyApp

Application Data

Build Time Data

App Performance Data

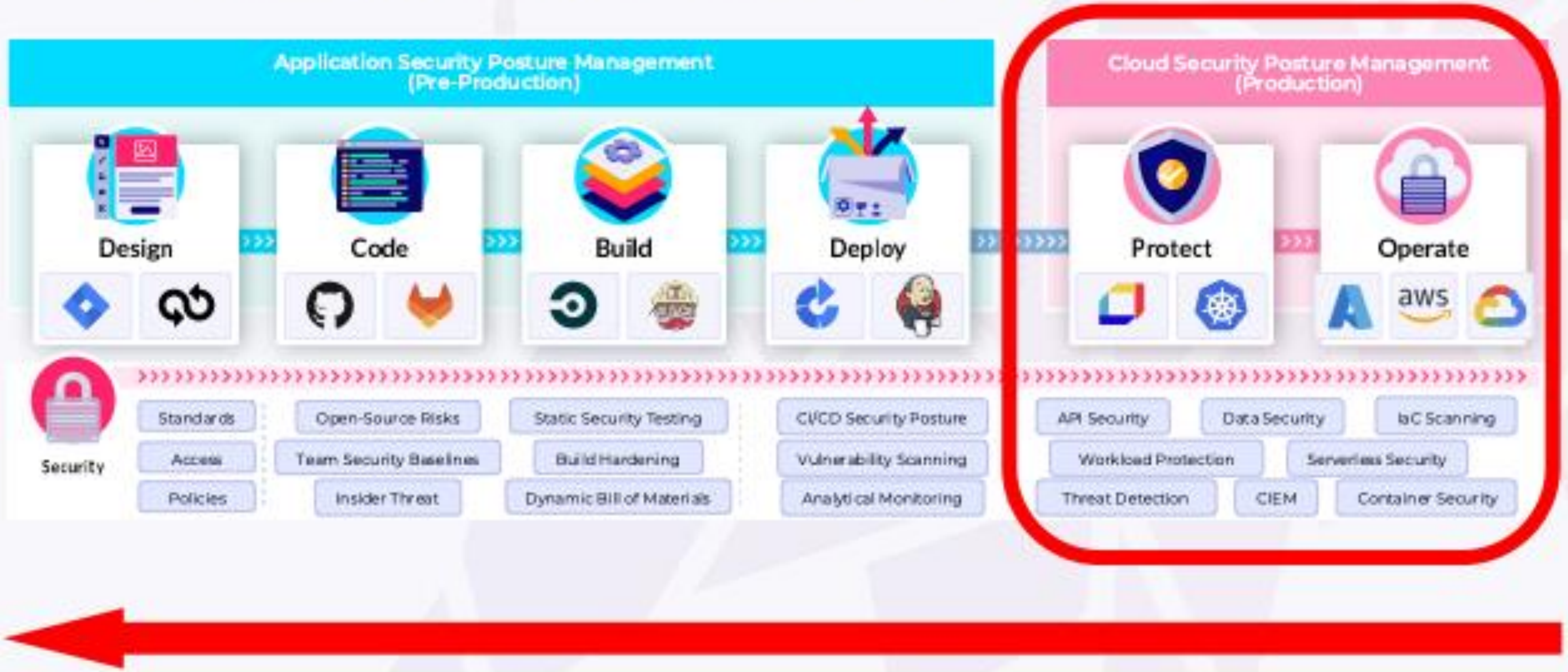
Security

Cybersecurity

# How Do We Handle **Risks From The Future?**

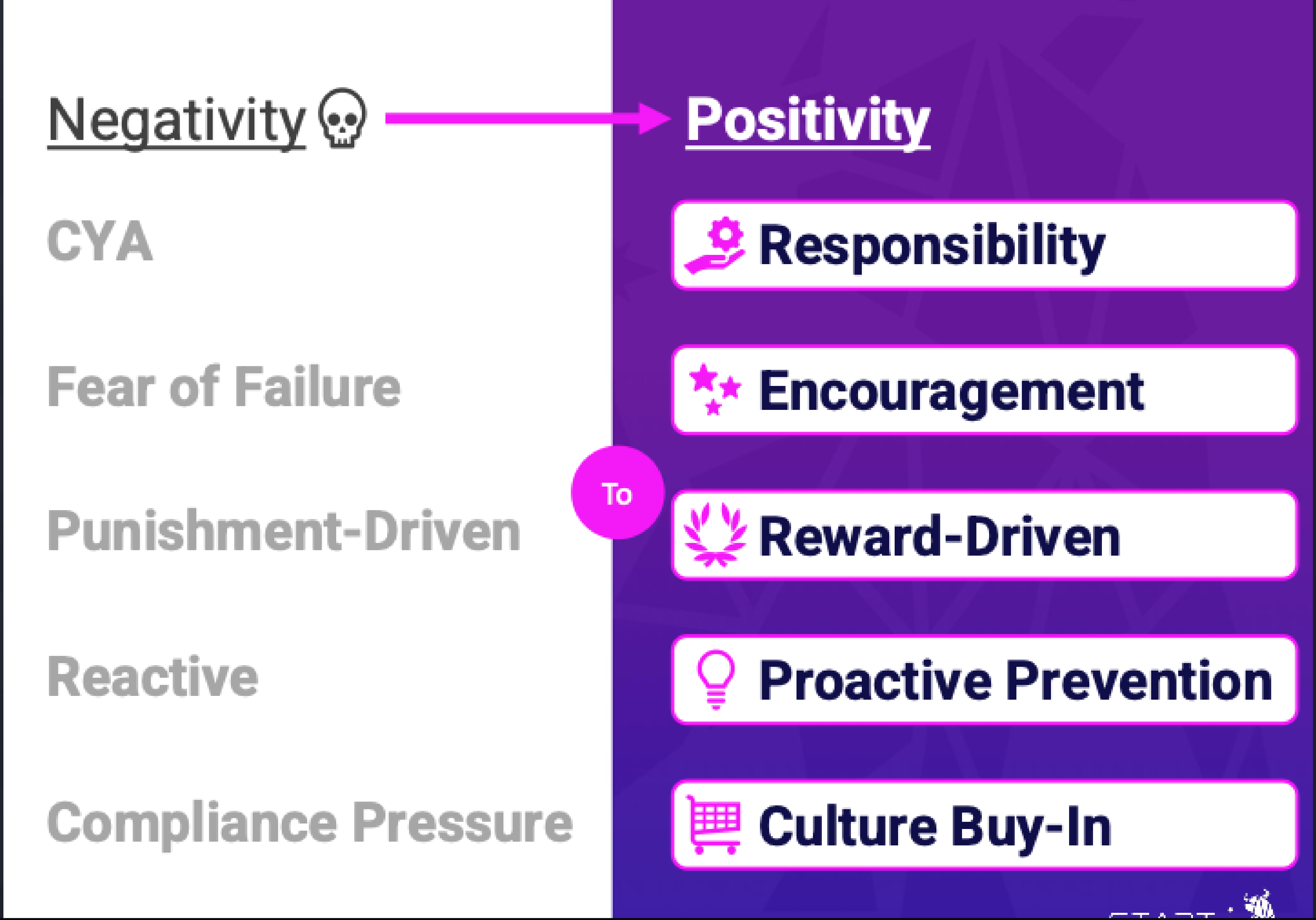
# The Flawed Legacy of CSPM:
# **Why Shift Left Isn't Enough**

## The Illusion of Integration: Misaligned Silos & Conway's Law



# The Flawed Legacy of CSPM: **Why Shift Left Isn't Enough**

Conway's Law



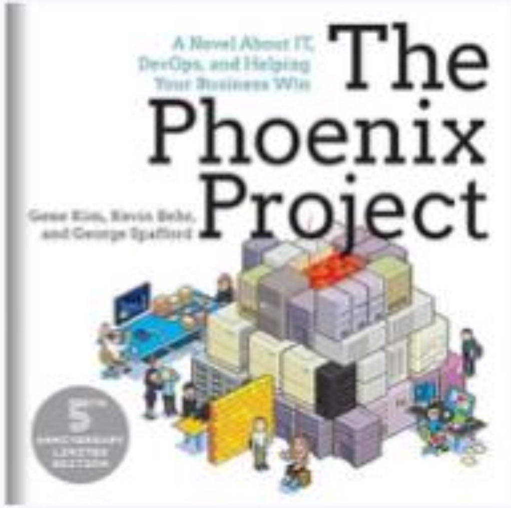
## Negativity 💀 → Positivity

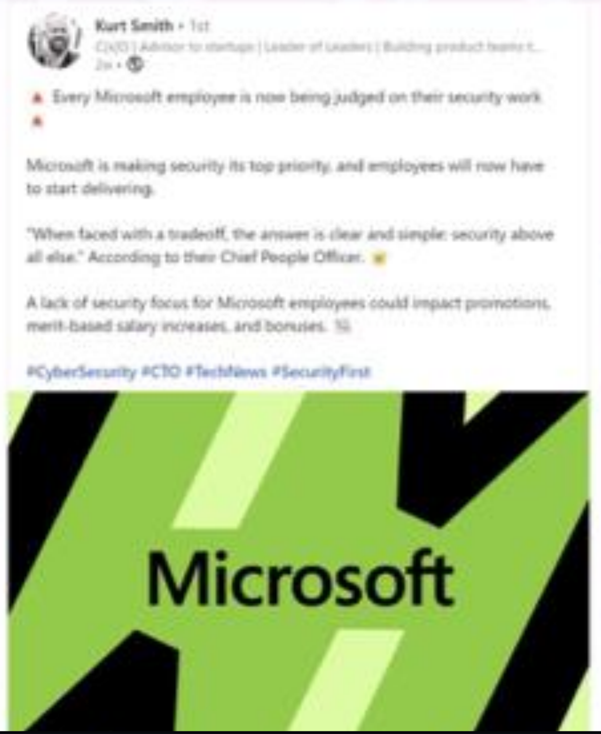
| Negativity | | Positivity |
|---|---|---|
| CYA | To | Responsibility |
| Fear of Failure | | Encouragement |
| Punishment-Driven | | Reward-Driven |
| Reactive | | Proactive Prevention |
| Compliance Pressure | | Culture Buy-In |

SECURITY MANAGERS BE LIKE
SPENT $200K ON A NEW SECURITY TOOL
JUST REALIZED IT IS NOT THE SOLUTION

# High-Performing DevOps Teams: **The Foundation of High-Quality Software**

## The Need for Product-Focused DevSecOps


A Novel About IT, DevOps, and Helping Your Business Win
The Phoenix Project
Gene Kim, Kevin Behr, and George Spafford
5th Anniversary Limited Edition


Kurt Smith • 1st
CXO | Advisor to startups | Leader of Leaders | Building product teams t...
2w •

▲ Every Microsoft employee is now being judged on their security work
▲

Microsoft is making security its top priority, and employees will now have to start delivering.

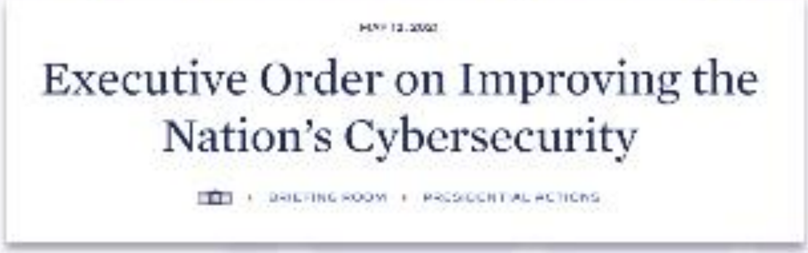
"When faced with a tradeoff, the answer is clear and simple: security above all else." According to their Chief People Officer.

A lack of security focus for Microsoft employees could impact promotions, merit-based salary increases, and bonuses.

#CyberSecurity #CTO #TechNews #SecurityFirst

# What Happens When...
# **Developers Are Left Out**

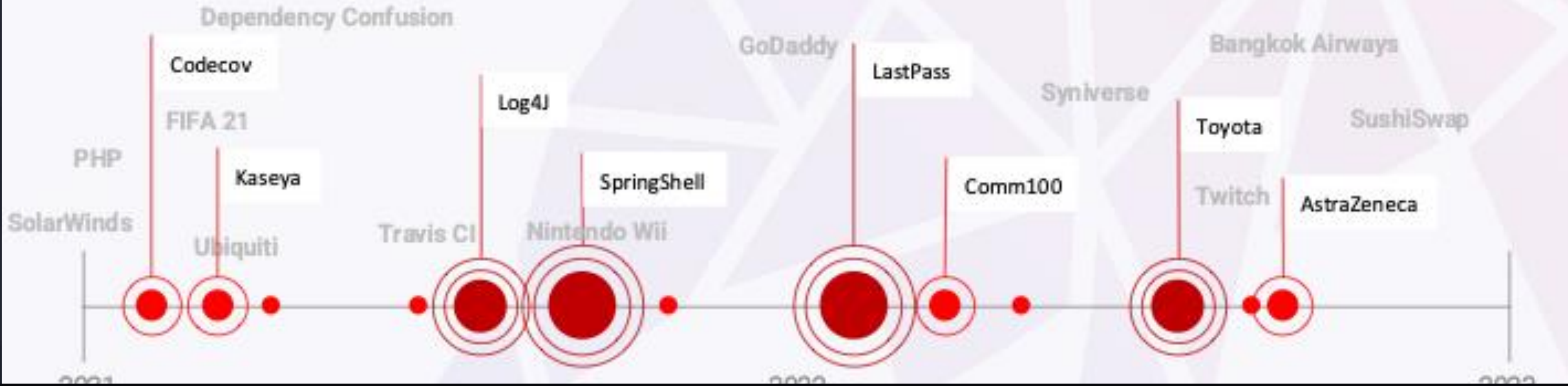
## The Consequences of NOT Empowering Developers



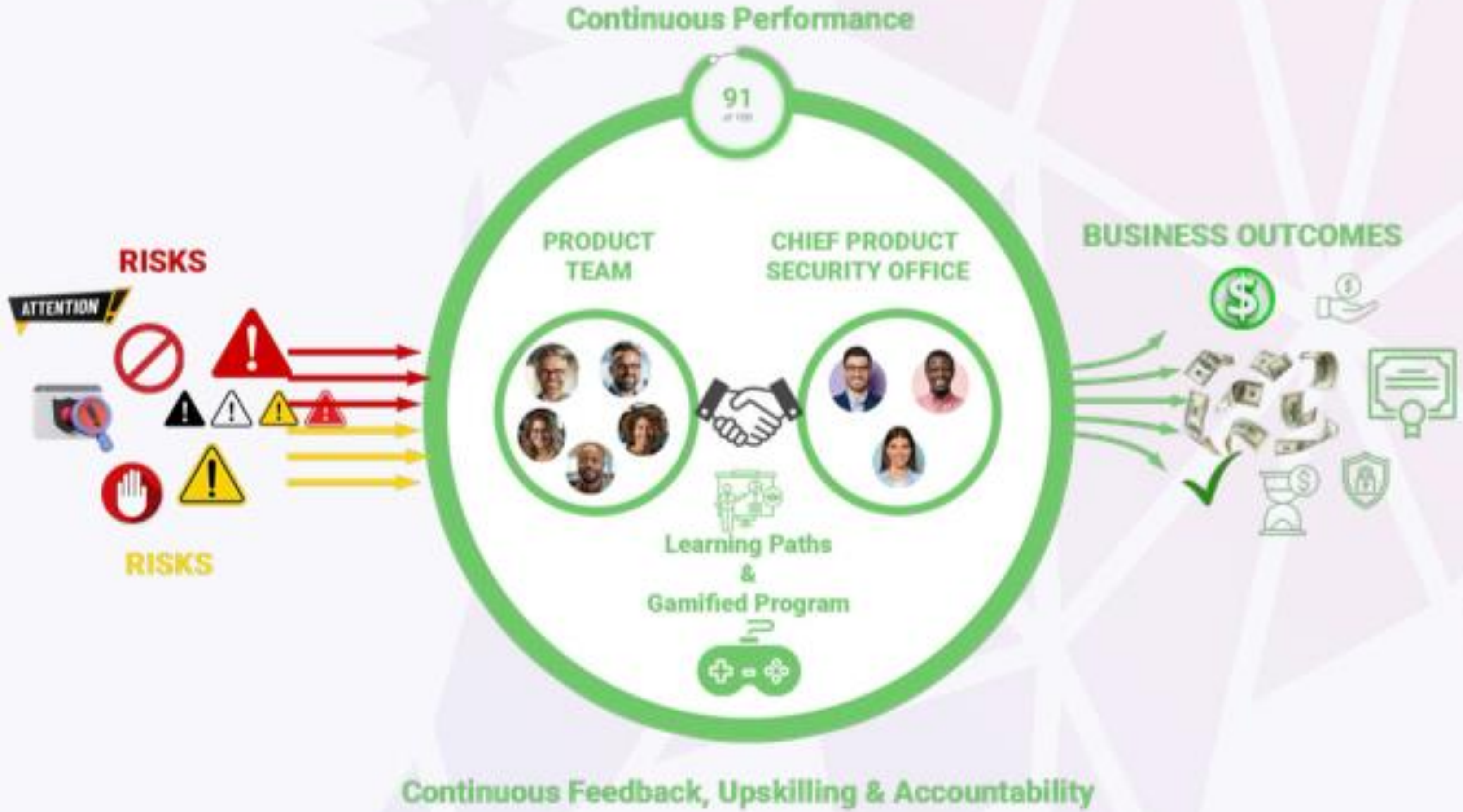
MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM • PRESIDENTIAL ACTIONS



# Organizational Communication,
# **Cultural & Behavioral Change**



Continuous Performance

RISKS

PRODUCT TEAM

CHIEF PRODUCT SECURITY OFFICE

BUSINESS OUTCOMES

Learning Paths & Gamified Program

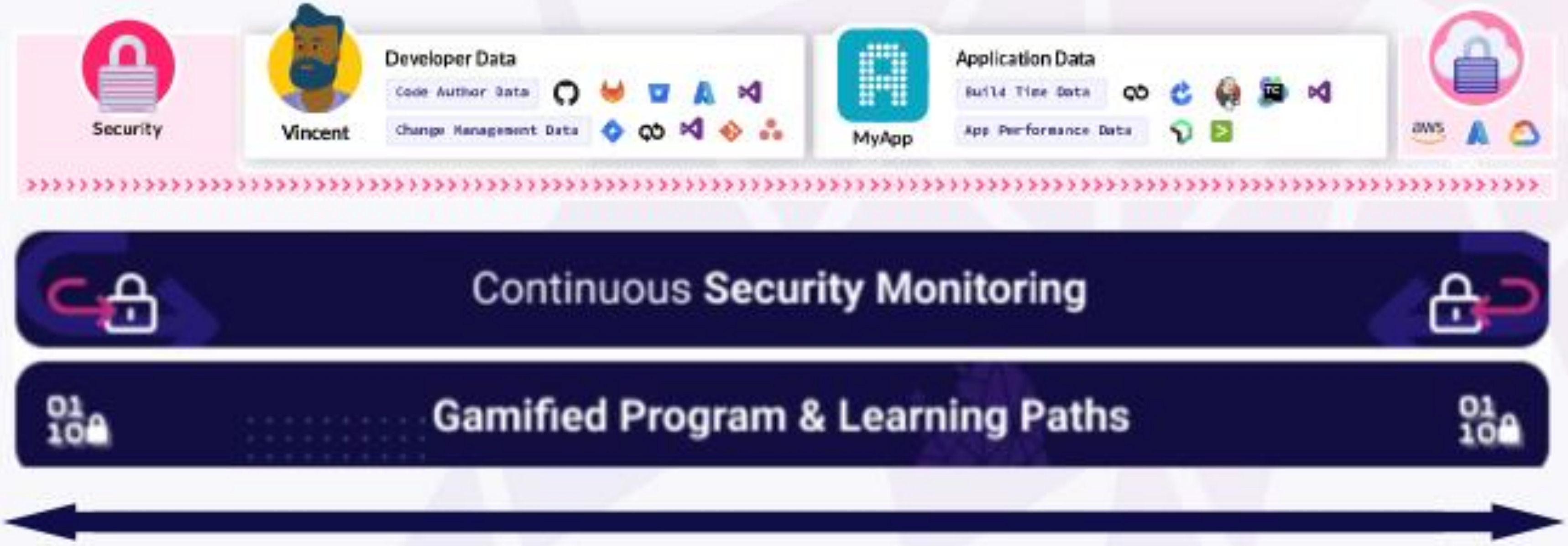
RISKS

Continuous Feedback, Upskilling & Accountability

# Empower Your Champions, **Optimize Security Excellence**

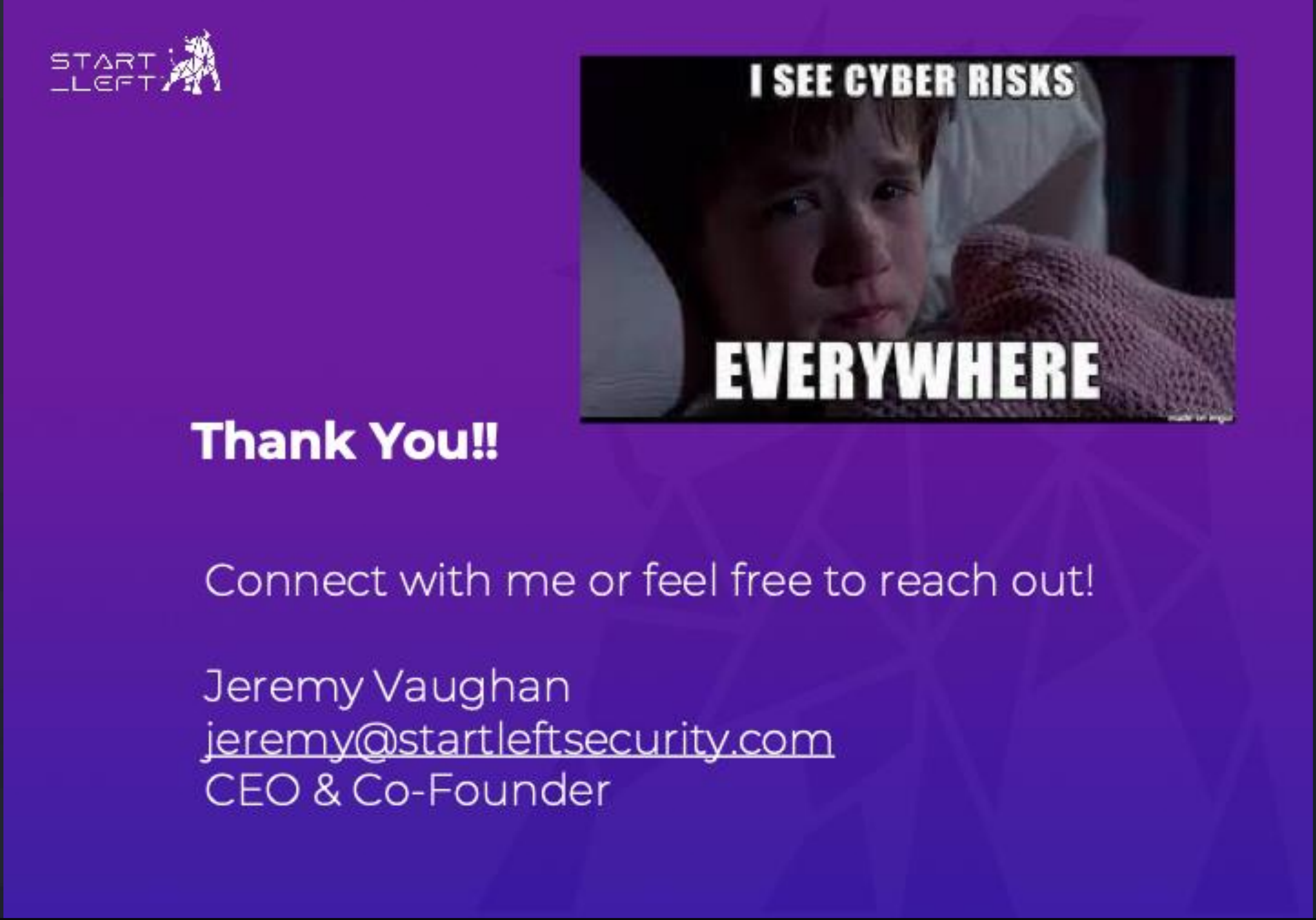
# Security Champions:
# Developers As The Front Line of Defense

## Aligning Everything & The Developer's Role



Continuous **Security Monitoring**

**Gamified Program & Learning Paths**


START
_LEFT
I SEE CYBER RISKS
EVERYWHERE

## Thank You!!

Connect with me or feel free to reach out!

Jeremy Vaughan
jeremy@startleftsecurity.com
CEO & Co-Founder

# BREAK

FRSECURE

# ANDREW COOK

## Recon Infosec | CTO

With over a decade of cybersecurity experience, Andrew is responsible for the delivery of threat hunting, incident response, and security operations to Recon's customers. As a former Air Force officer, Andrew has participated in national-level operations and exercises and provided real-world emergency response to state-level cyber incidents.

Topic: Threat Hunting – The Key to Security

RECON™
INFOSEC

# THREAT HUNTING THE KEY TO ENTERPRISE SECURITY

Andrew Cook
CTO, Recon InfoSec

TAGITM South Texas Regional - 2024

# WHO AM I?

## BACKGROUND

### Air Force Cyberspace Operations Officer ✓

Contributor to Air Force cyber doctrine on threat hunting. Founding operator, weapons and tactics officer for the nation’s first defensive cyber weapons system.

### TX Air National Guard ✓

Instructor and incident responder for one of the first national guard Cyber Protection Teams. Responded to statewide emergencies from hurricanes to ransomware.

### Consultant and Incident Responder ✓

Protected and guided organizations around the world through through training, consulting, and incident response. First threat hunt of the DHS RVA program.

### CTO, Recon InfoSec ✓

Finding and stopping bad guys ever day with a world-class Managed Detection and Response service.

# What is Threat Hunting?

Threat hunting is a methodology, a mindset, and an analogy.
It is a philosophy of defensive cyber security.

## Definition

Any proactive effort to find threats that are already inside your environment.

## Threat-Centric Mindset

Assumed breach: We are already compromised. Relentless pursuit and discovery of threats. Indignant.

## Methodology

Proactive, not reactive. Hypothesis generation, forensic state analysis, stack-analysis, and more...

## Analogy

Derived from the military's “hunter-killer” concept. Other analogies include hygiene, vegetables, and sports.

# BECOME A THREAT HUNTER

## KNOW THE THREAT

- READ!
  - Incident reports
  - Technical threat analyses
  - CISA advisories
- MITRE ATT&CK TTPs
  - Tactics
  - Techniques
  - Procedures
- David Bianco's "Pyramid of Pain"
  - Behaviors, not hashes

## KNOW YOUR ENVIRONMENT

- What threats target my industry?
- If I was a threat actor, how would I get in? Where would I hide?
- What are my public-facing exposures?
- What detection tools do I have? What are their weaknesses?
- What telemetry and artifacts do I already have to identify potential threats?

# Driving Organizational Change

# Threat Hunting as Applied to…

Positioning threat hunting as the central pillar of your security program creates a dynamic and adaptive security posture and culture that is well equipped to handle today's changing threats.

### Information Technology Teams

What can the IT team do to start threat hunting?

### Security Operations Teams

Why is threat hunting *the* key indicator of a high performing SOC?

### Users

Are your users threat hunters or victims?

### Leadership Teams

How should leaders think about decisions related to threats?

# A THREAT HUNTING IT TEAM

IT teams have the best understanding of their network.

- Set aside time for threat hunting.
- For every misconfiguration, missing control, or new vulnerability, ask: “how could I tell if this was exploited?”
- Spot check systems as you interact with them.

**But wait! I don’t have any tools!**

You probably have more than you think and even more is available for free and open source:

- PowerShell, Excel, and Pivot Tables
- Microsoft Sysinternals, including Sysmon and Autoruns
- Hayabusa Windows Event Log Analyzer
- SANS Hunt Evil Poster

# A THREAT HUNTING SECOPS TEAM

Threat hunting is the #1 indicator of high performing SOC

- Measure threat hunting performance.
- Threat hunts should improve daily ops:
  - New detections and more visibility
  - Better analysts and improved workflows
- As daily ops improves, threat hunting needs to mature.

## What about my outsourced security team?

Challenge them and use threat hunting as your litmus test.

- How often do your analysts threat hunt? Is it included?
- What are they using to measure their threat hunts?
- Do your analysts also create their own detections?
- Does every analyst threat hunt?

# A THREAT HUNTING USER BASE

Users are just trying to do their jobs hassle. Unfortunately, the bad guys get a vote.

- Use realistic threats and scenarios in your training.
- Encourage users to report suspicious activity.
- Abundantly award “true positives” and correct action.
- Shift mindsets from prey/victim to threat hunter

## Who are my most targeted users?

Prioritize converting your most heavily targeted users:

- Executive decision makers
- Finance and accounting
- Human Resources
- Sales

Make sure they know *why* threats are interested in them!

# A THREAT HUNTING LEADERSHIP TEAM

Leaders set the tone and control the budgets.

- Encourage, do not discourage, threat hunting!
- Ask productive questions as new threats hit the news.
- Prioritize realistic threats and contextualize compliance
- Prepare for the inevitability of a breach with executive tabletops and reviews.
- Hire/Train and empower threat hunters

**Hope for the best, prepare for the worst.**

History is riddled with organization's that never expected to be breached. Even the most secure and prepared can fall victim. Compliance-driven thinking without context can lead to expedited shortcuts that fail to adequately address major concerns.

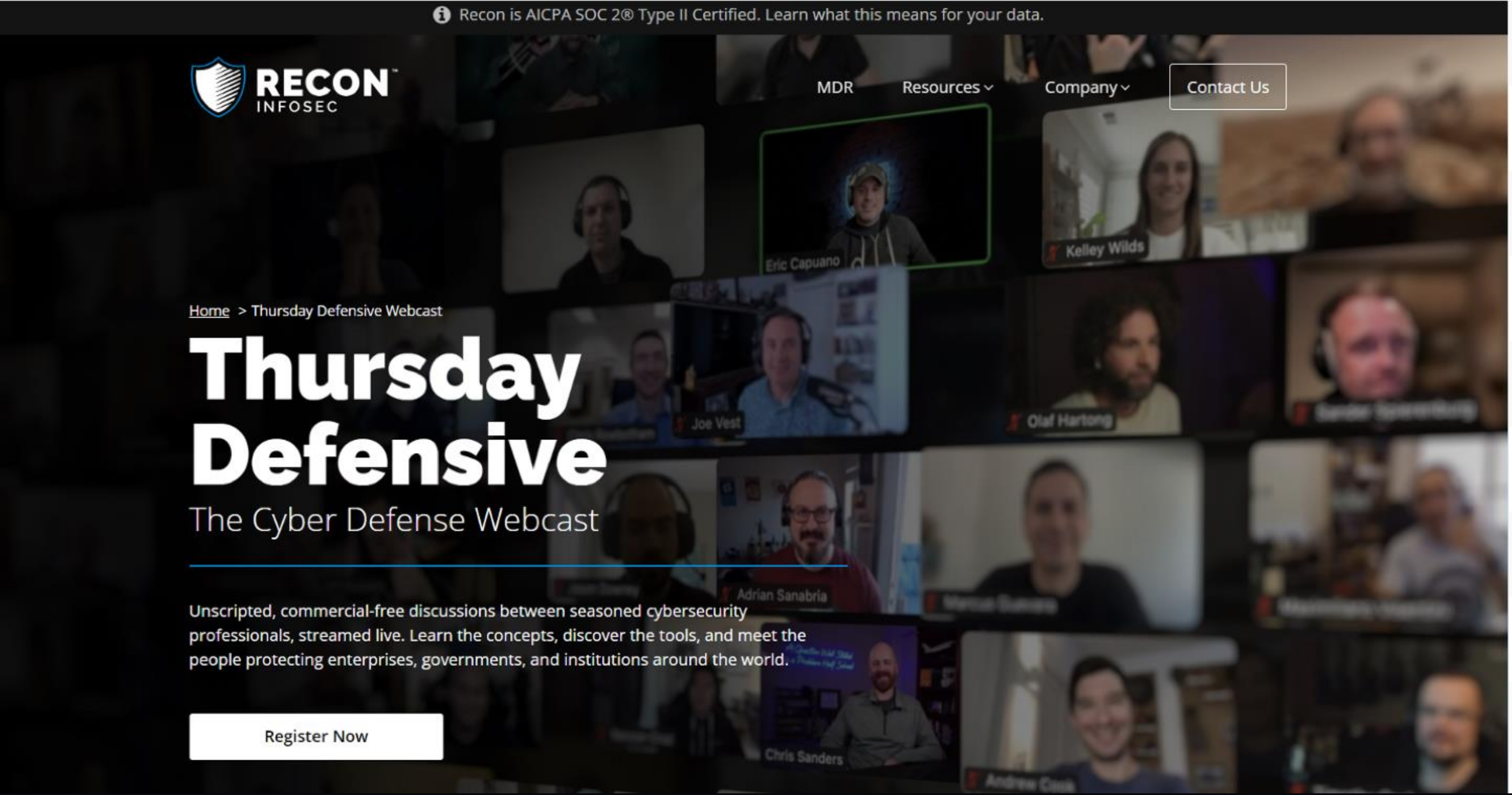
# Key Takeaways
# Become a Threat Hunting Organization

Start Threat Hunting

Cultivate a Threat Hunting Mindset and Culture

Use Threat Hunting to Drive Improvement and Priorities

Everyone can be a Threat Hunter



Recon is AICPA SOC 2® Type II Certified. Learn what this means for your data.

Home > Thursday Defensive Webcast

# Thursday Defensive

## The Cyber Defense Webcast

Unscripted, commercial-free discussions between seasoned cybersecurity professionals, streamed live. Learn the concepts, discover the tools, and meet the people protecting enterprises, governments, and institutions around the world.

Register Now

# QUESTIONS?

**Email me!**

**Andrew Cook**
**acook@reconinfosec.com**

# OSCAR MINKS

## FRSecure | President

Oscar brings almost 20 years' experience in information security to his role as President of FRSecure. He has experience managing Incident Response programs, Cyber Defense programs, Vulnerability Management programs, and more.

Topic: Real-World Attacker Techniques – Protecting Yourself

# STATE OF THE UNION: ANNUAL INFORMATION SECURITY REPORT

Oscar Minks, President

FRSecure

# INTRO

## Oscar Minks – CTO FRSecure

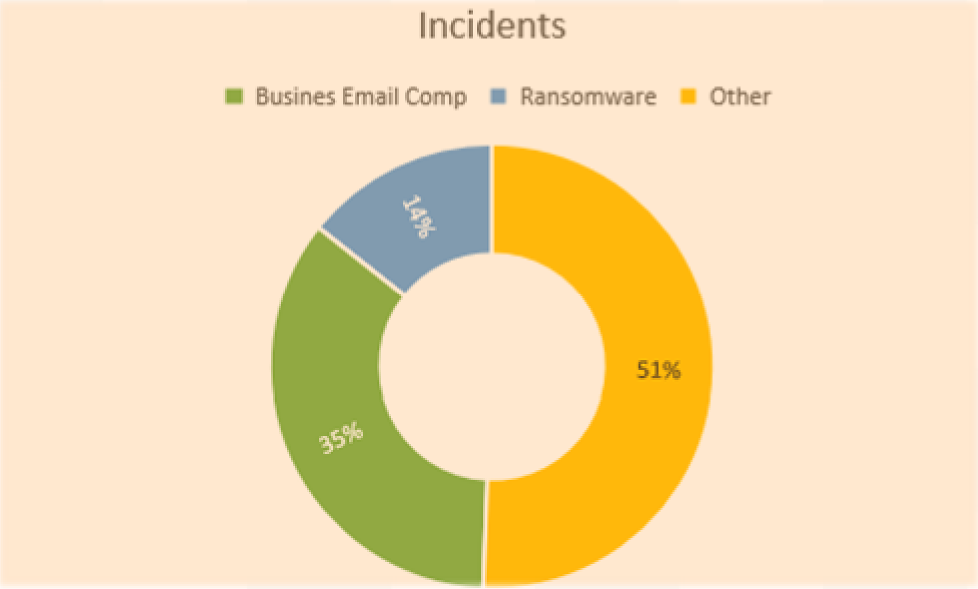
- FRSecure President
- Kentucky born and raised, Montana bound!
- I like helping people; hacking things; stopping hackers; fishing and playing music
- 20 Years in the industry/ MS in Info Sec/ GCFA, GREM
- Very happy to be here!

# KEY LEARNINGS – TL:DR (DPA)

1. Financial Impact and Frequency of Cyber Security Incidents Continue to Rise!
2. Social Engineering Remains King!
3. You doing better at MFA implementation, but it's not enough.  Conditional Access IS the new MFA!
4. Dwell time is reducing for impactful cyber events!
5. Malware Drive-By Download attacks are very prevalent!
6. Encryption-less Ransomware being observed – Get better at Ex-Fil Detection!
7. Less C2; More COTS!
8. It all starts with education – Security is a Life Skill!

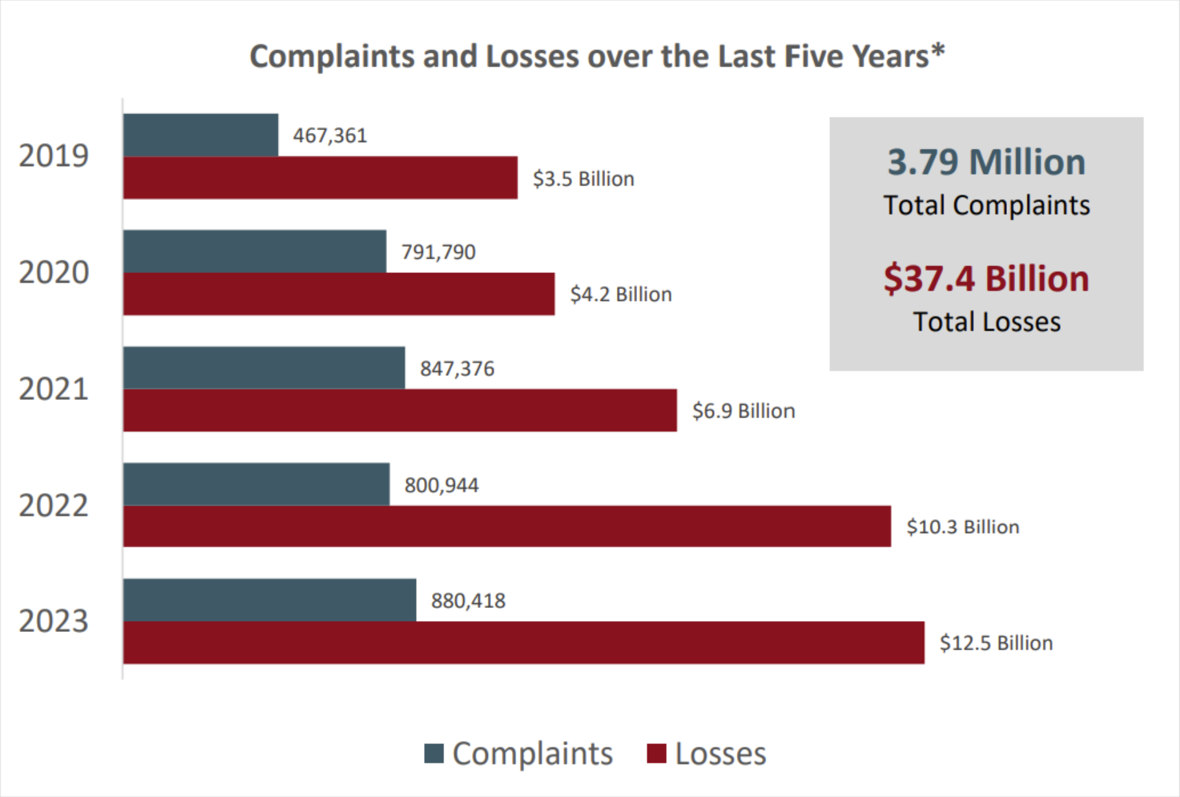
# ABOUT THE DATA

- 77 Incident Response Engagements
    - Business Email Compromise, Ransomware, Pre-Ransom and Internal Compromise
    - Information has been anonymized
    - Data logged on controls, Root Cause, Exploits, etc..
- This is our Analysis, Interpretation, and a Recommendations!
- Goal – Reduce Frequency and Impact of Security Incidents!



# IR OVERVIEW

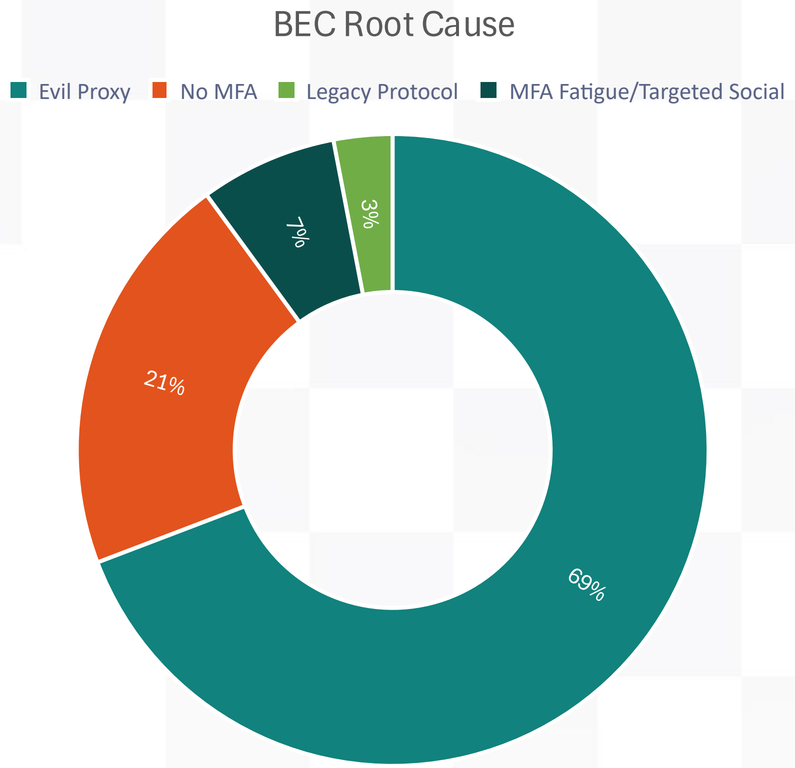
- Attacks and Financial loss is on the rise
  - 17.5% Increase in Financial Loss
  - 9% Increase in Complaints
- This data can be used to Educate HOW attacks are happening
- Learn and implement
- Have fewer incidents
- Minimize impact of negative incidents



*IC3 Annual Report 2023 – ic3.gov*

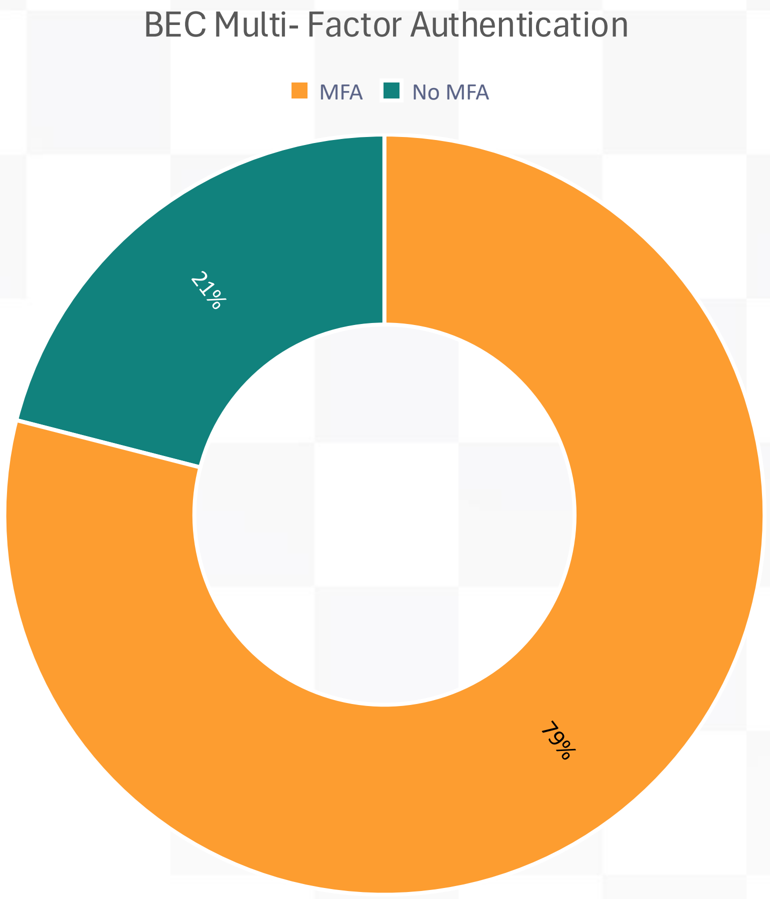
# BUSINESS EMAIL COMPROMISE ROOT CAUSE

- Social Engineering Remains King
- Technology Evolves and Humans remain the weakest link
  - Most organizations have implemented regular Social Engineering tests
    - Have you tested the efficacy?
    - Do you continue to modify and improve?
    - Don’t make it status quo!
  - Make your Information Security Training Valuable!
  - Information Security as a life skill!
  - Leaders must set the tone!



# MFA INSIGHTS

- MFA – Great Job!
  - In 2023 Report:
    - 73% of BEC victims did not have MFA
    - In 2024 – 79% DO have MFA!
    - Don’t put it in Cruise – still have work to do!
- We warned…..MFA – Not a silver bullet

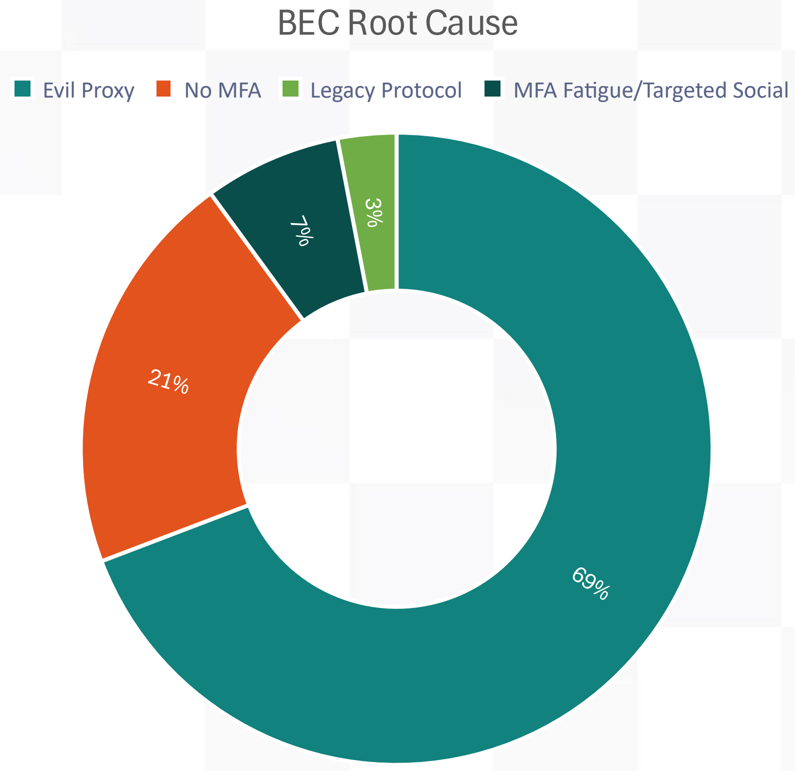


# *2023 MFA DEFEAT TECHNIQUES REMINDER*

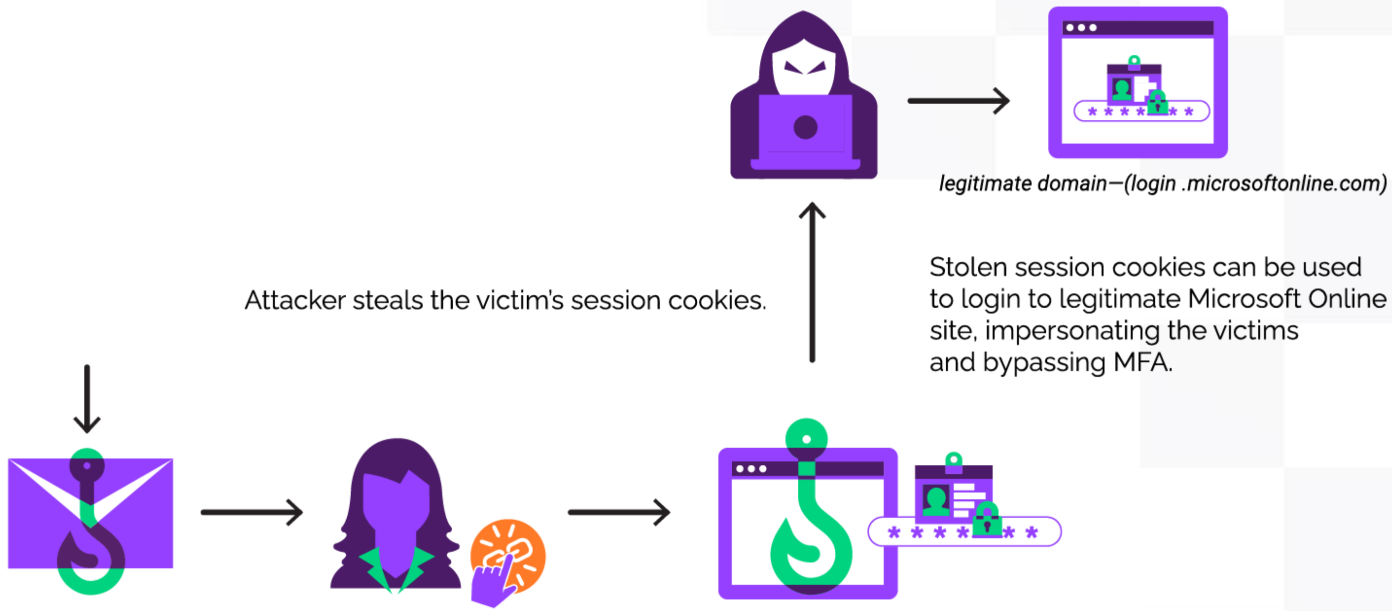
- ***MFA Fatigue Attacks***. *The attacker utilizes a set of compromised credentials to target the victim with approve requests, and then tricks the end user into approving the push notification. This is usually either the result of a well timed attack, or by overloading the victim with multiple notifications.*
- ***Help-Desk social engineering.*** *Attackers are able to identify internal helpdesk contacts, and use compromised employee information to masquerade as the employee to eventually trick the helpdesk analyst into updating the employee's phone number where one time passcodes will be delivered.*
- ***Legacy protocols.*** *Legacy protocols do not support MFA, so the attacker was easily able to circumvent the MFA requirement and gain access to the victim tenant.*
- ***Defense Recommendation. Do not utilize push approvals and SMS one-time passcodes; and sunset/disable all legacy protocols.***

# EVIL PROXY - A NEW PLAYER ENTERS THE CHAT!

- Expected evolution of the attacker.
- New play on an old trick!
  - MitM w/ MFA Defeat!
- Accounted for 69% of all BEC's



# EVIL PROXY - A NEW PLAYER ENTERS THE CHAT!



legitimate domain—(login .microsoftonline.com)

Attacker steals the victim's session cookies.

Stolen session cookies can be used to login to legitimate Microsoft Online site, impersonating the victims and bypassing MFA.

Victim receives phishing email with Indeed link.

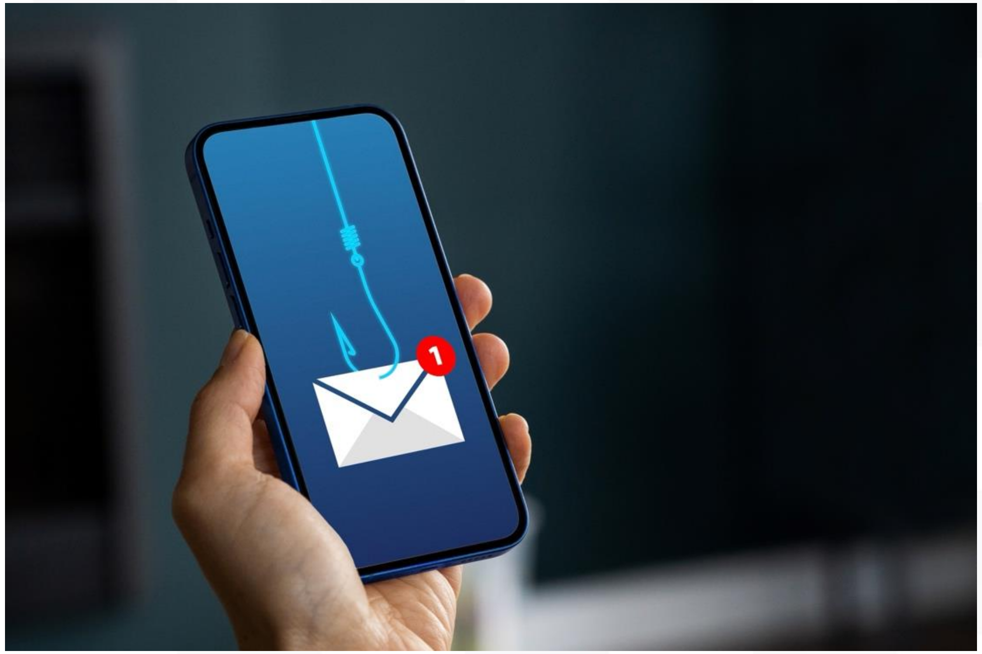
Victim clicks on the Indeed link inside the mail redirecting the victim to the phishing page.

The phishing site acts as a reverse proxy, proxying the request to the actual website. The attacker intercepts the legitimate server's requests and responses.

https://www.menlosecurity.com/blog/evilproxy-phishing-attack-strikes-indeed

# BUSINESS EMAIL COMPROMISE

- **Persistence and Evasion**
    - Mailbox Offloading
    - Auto Deletion
    - Third Party Application Authorization
        - PerfectData Software
            - Legit application used for backup



# BEC - HOW DO WE DEFEND THE TACTIC

- **Conditional Access is the New MFA!**
- Do NOT stop what your doing w/ MFA!
  - Expand utilization of Conditional Access!
  - Device Access Authorization
    - detail
  - Application Access Authorization
    - detail
  - Geo-Fencing, Risky Users, etc.

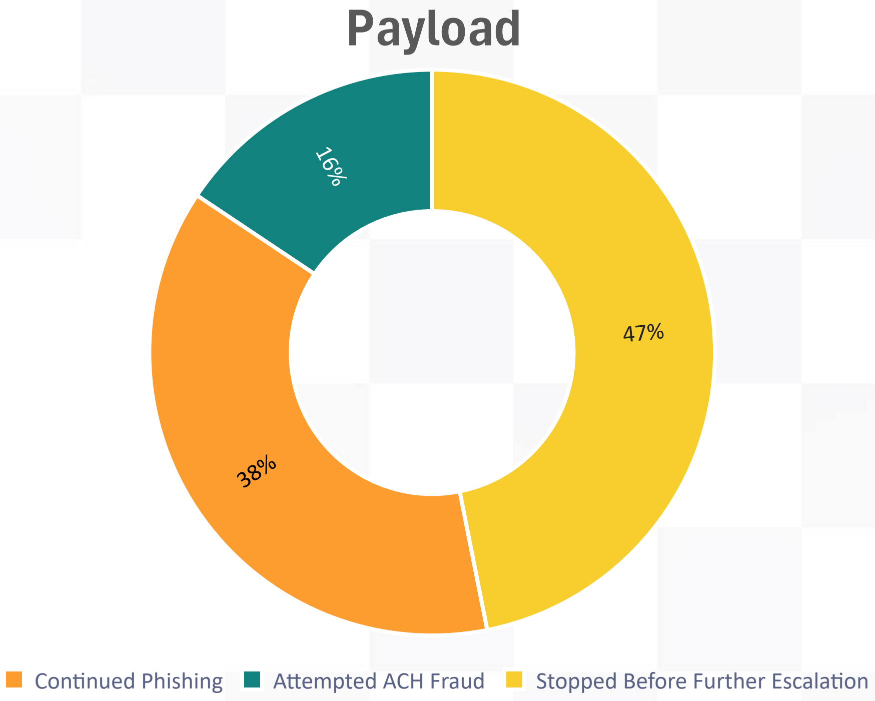
# BEC - HOW DO WE DEFEND THE TACTIC

- Be Prepared – Train more and Train More Effective!
  - It ALL starts with the People!
  - Leaders have to set the tone!
  - Information Security Knowledge as a Life Skill!
    - Home habits convey to business!
- Have a plan and know how to Respond!
  - MTTR is Critical!

FRSECURE ANNUAL INFORMATION SECURITY REPORT

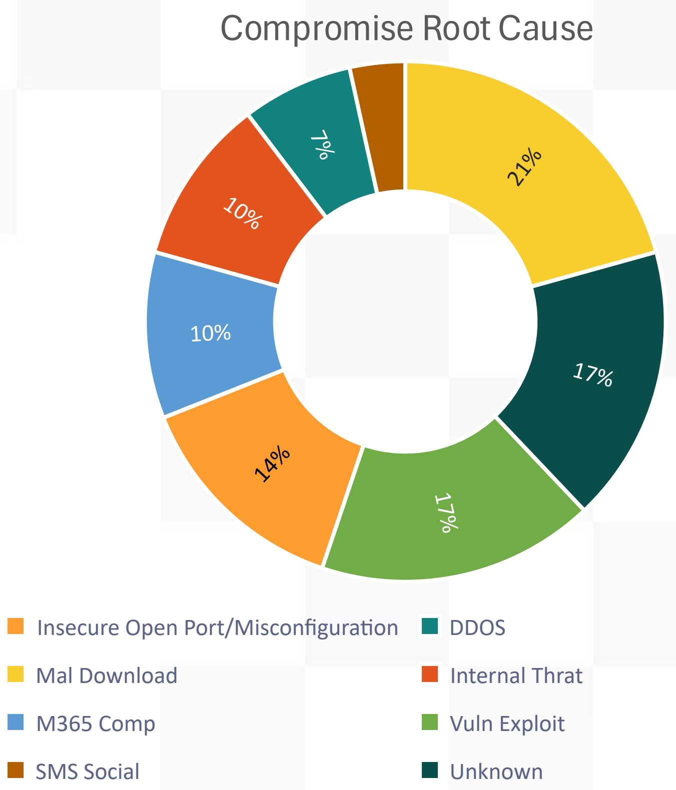
# BUSINESS EMAIL COMPROMISE

- **The Payload:**
  - 16% Attempted ACH
  - 38% Continued Phishing
  - 47% Nothing – Client was prepared and responded quick!
  - Be prepared to Minimize Damage!
    - Internal Capability or a Partner!



# RANSOMWARE AND INTERNAL COMPROMISE

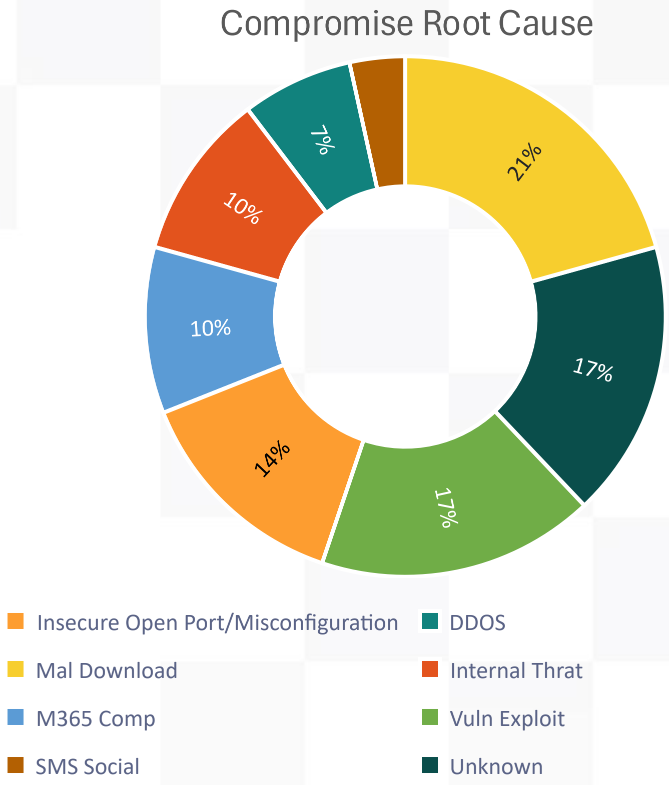
- < 20% of all cases resulted in encryption
  - FRSecure was notified post fact in all instances.
  - Being prepared is pretty important…..



# VULNERABILITY EXPLOITS, OH MY!

- Vulnerability Exploits, Oh My!
  - 33% of cases in 2023
  - 17% in 2024
  - Trend is to be expected, we were peaking in 2022; Year of the 0-Day
  - Don't Lower your guard!

- Positive Improvements
  - Historically we observed exploits of old vulns (<12 Months)
  - All but 1 we're recently released
  - We are observing improvement in Patch Management!



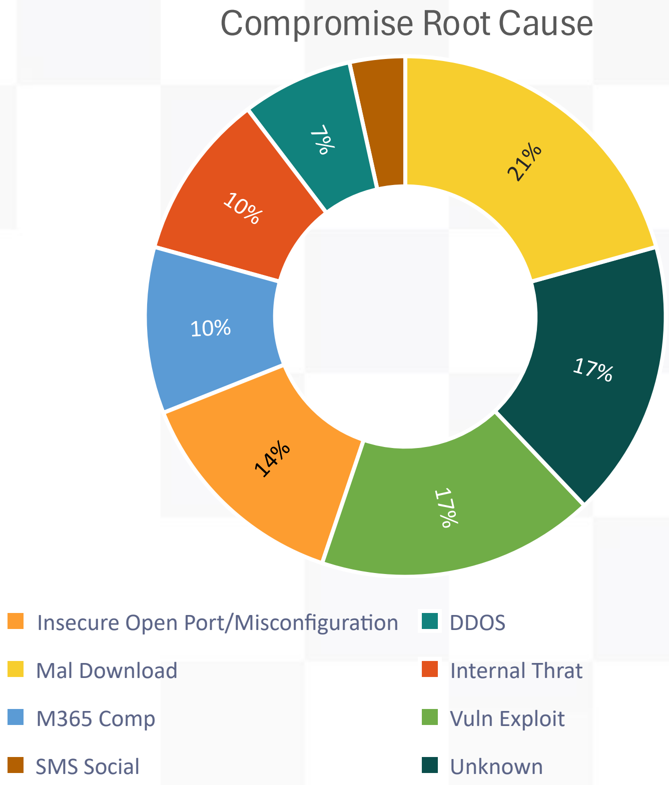
# VULNERABILITY EXPLOITS, OH MY!

| *CVE* | Description | Publish Date | CISA KEV |
|---|---|---|---|
| CVE-2023-3519 | Citrix ADC and Gateway Unauthenticated RCE | 7/19/2023 | Yes |
| CVE-2023-4966 | Citrix Netscales ADC and Gateway Sensitive Information Disclosure | 10/10/2023 | Yes |
| CVE-2023-24998 | Apache Commons FileUpload Exploit | 2/20/2023 | No |
| CVE-2022-41040, CVE-2022-41082 | Microsoft Exchange Privilege Escalation - ProxyNotShell | 10/2/2022 | Yes |
| CVE-2024-1709 | Connectwise server Authentication Bypass vulnerability | 2/21/2024 | Yes |
| CVE-2024-4040 | CrushFTP Auth Bypass and RCE | 4/26/2024 | Yes |

FRSECURE ANNUAL INFORMATION SECURITY REPORT

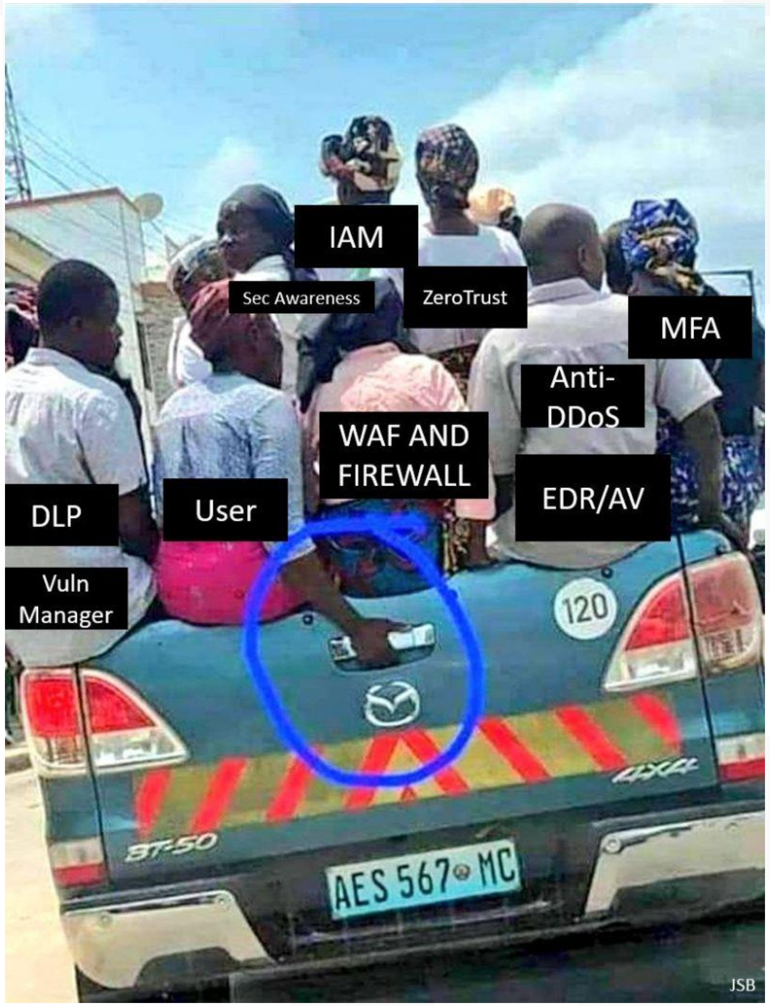
# VULNERABILITY EXPLOITS, OH MY!

- Stay Diligent on your Vulnerability Management Programs!
- Tune in to the CISA KEV
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Understand – A Patch is Not Enough!
  - If the system is already Compromised – A patch Does Not Remediate!
  - Review the systems for IoC's
  - Determine Proper Remediation Patch

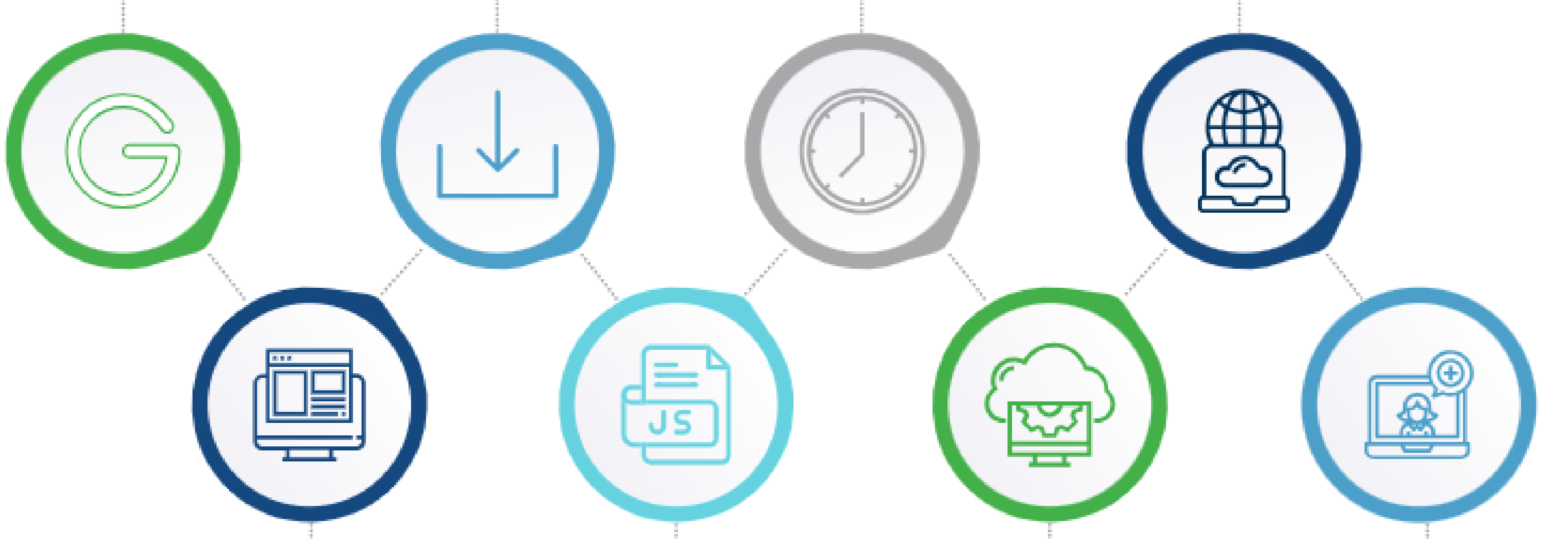


# MALWARE DRIVE-BY DOWNLOAD ATTACKS

- 21% of Ransom/Pre-Ransom Attacks
  - 2 Led to Ransom Deployment
  - 4 Contained before Escalation
- Source of Downloads?
  - Search for tools – WinDirStat
  - Malicious Forum/Reddit/Search Result Links
- Will My EDR Catch it?
  - Not Always
  - Attackers are GREAT at Defense Evasion!



# MALWARE DRIVE-BY DOWNLOAD ATTACKS



Victim searches for "xxx agreement template"

Search engine provides a compromised website

Victim is provided with a link to download a zip file name "xxx agreement template.zip"

Victim executes first-stage GootLoader JavaScript file

Second-stage JavaScript file and scheduled task are created

SystemBC and Cobalt Strike installed for remote access

Threat Actor remotely accesses the network

Sensitive files are identified and exfiltrate via FileZilla

Source: https://www.kroll.com/en/insights/publications/cyber/deep-dive-gootloader-malware-infection-chain

# RANSOMWARE WITHOUT ENCRYPTION

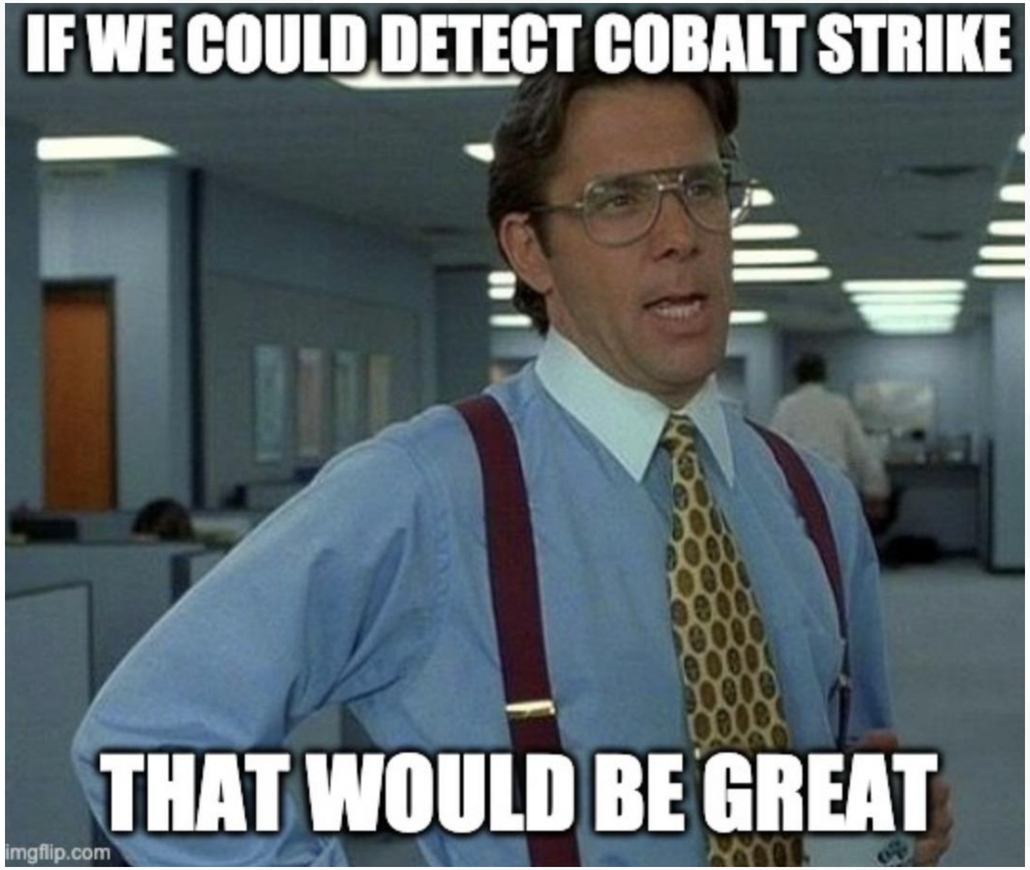
- New Trend Observed in 2023
  - Data Ex-Filtration Only – NO Encryption!
  - Fast Attacks – Dwell Times < 24 Hours
  - Threat to release or sell data and notify public for non-payment!
- Threat Actors acted fast!
  - Dwell times < 24 hours!
- How to identify?
  - Normalize traffic egress; Investigate Anomalies!
  - Block file-transfer apps from your organization!
    - FileZilla, Rclone
    - Application Allow-Listing!
  - Alert on usage of compression tools!
    - WinRAR

# LESS CUSTOM C2'S – MORE COTS

- Custom C2 utilization
  - Cobalt Strike still being utilized
  - Observed in 5 Cases
  - EDR getting better (not Great) at detection!

- Significant Uptick in COTS Products
  - Connectwise ScreenConnect
  - Anydesk
  - RDP (VPN Compromised first)

- Why?
  - Sometimes – they are already in your environment!
    - Application Audit! Relics from old MSP's
  - EDR does NOT Identify as Malicious!



# RANSOMWARE – EARLY DETECTION AND RESPONSE ARE IMPORTANT!

- Full Encryption – Ruh Roh
  - All reported POST fact
  - Dwell Times are Reducing!
    - 7 hours (smash and grab) to 23 Days
    - Peak in last report was 9 Month's
  - We are getting better at detection – Attackers are moving faster!
    - Early Detection and Swift Response are Key!
  - Even though Dwell is reducing….
    - We Still observed Backup Destruction in successful campaigns.
    - Get your backups Offline!
    - Test your Backups!
  - Data Ex-Filtration 60% of cases!

I DON'T ALWAYS THINK ABOUT CYBERSECURITY...
BUT WHEN I DO, IT'S USUALLY TOO LATE.
imgflip.com

# INGRESS UNKNOWN?  LOGS NEEDED!

- Know Normal – Find Evil!
  - What does this mean?
- Creatures of habit
  - IP’s; Time; Fingerprint
- Time-Stamps are important – NTP
- M365 – Familiarize w/ Risky Users
- Require approval for new Devices or Authorized Apps (OAUTH)

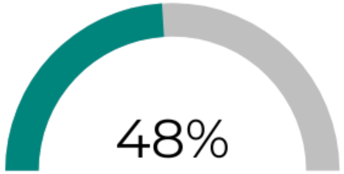
# INGRESS UNKNOWN? LOGS NEEDED!

- Pro Tips!
  - Enable Script Block Logging across the domain
  - Don’t assume the identified compromised user – is the only compromised user
    - Most cases we find multiple accounts compromised.

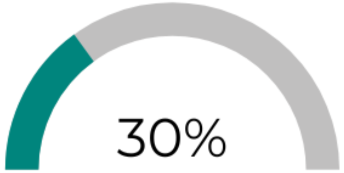
FRSECURE ANNUAL INFORMATION SECURITY REPORT

# CYBER INSURANCE IS NOT YOUR IR PLAN

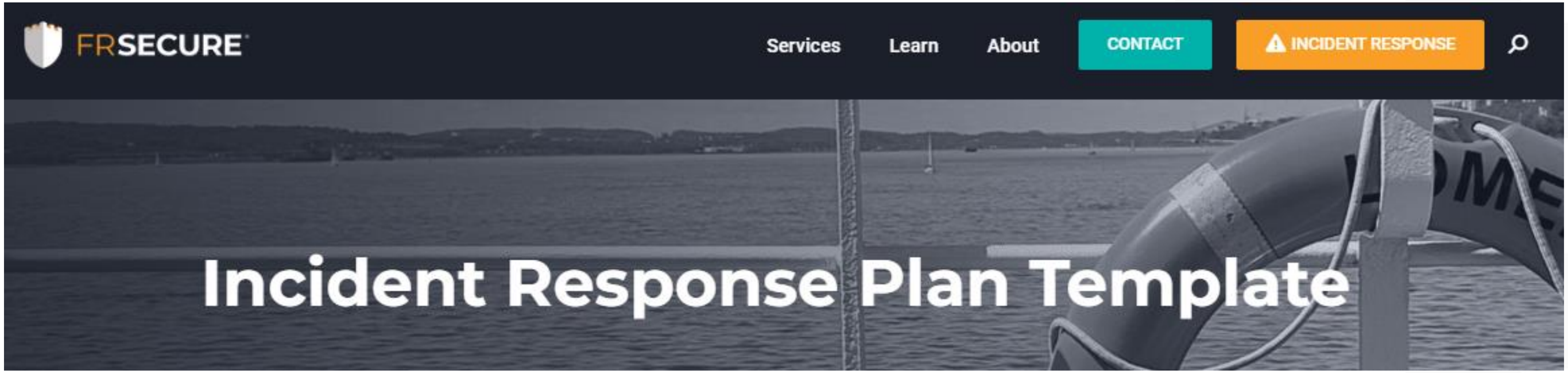
- Preparedness is key!!



of organizations assessed have defined a formal incident response plan.



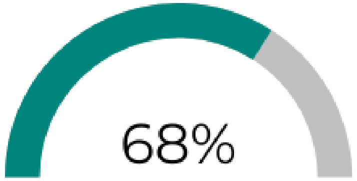
of organizations assessed are testing their incident response plan on a periodic basis.



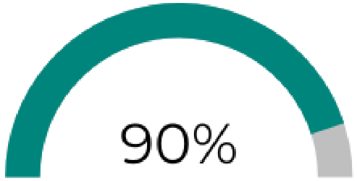
Incident Response Plan Template

FRSECURE ANNUAL INFORMATION SECURITY REPORT

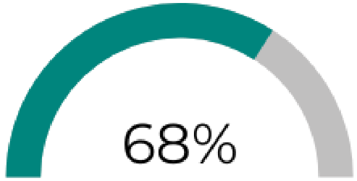
# CYBER INSURANCE IS NOT YOUR IR PLAN



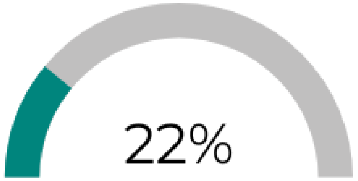
of organizations have engaged their insurance provider pre-incident.



of organizations observed have a cyber insurance policy.



of organizations have cyber insurance, breach counsel, and vendors are in their IR plan.



of organizations document how and when to notify insurers of cyber incidents.

- You’re doing it wrong!
  - Not an IR Plan
  - Engage Insurance BEFORE an incident
    - Know your breach coach
    - Agree upon a vendor (you CAN use yours)
    - Document in your IR plan HOW to engage

# QUESTIONS?

- Feel free to get in touch:

- ominks@frsecure.com
  - Projecthyphae.com
  - FRSecure.com
  - The HackleBox Podcast

# PANEL DISCUSSION

**Evan Francen, Michael Kennedy, Megan Larkins, Brad Nigh**

Moderated by Judy Hatchett

FRSECURE

## EVAN FRANCEN

**FRSecure | Founder**

Sunsets and Snowdrifts

## MEGAN LARKINS

**FRSecure | Co-Host**

Unsecurity

## MICHAEL KENNEDY

**Ostra | Founder**

Sunsets and Snowdrifts

## BRAD NIGH

**FRSecure | Co-Host**

Unsecurity

# THANK YOU!

Please enjoy our networking happy hour!

FRSECURE