RSAConference™2024
San Francisco | May 6 – 9 | Moscone Center

THE ART OF POSSIBLE

SESSION ID: CLS-T01

CloudSec Hero to Zero: Self-Obsolescing Through Prolific Efficiency

#RSAC

Rich Mogull

Cloud Security Curmudgeon
Firemon/Securosis
@rmogull@defcon.social

Chris Farris

Cloud Security Evangelist
PrimeHarbor Technologies
@jcfarris [@infosec.exchange]

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

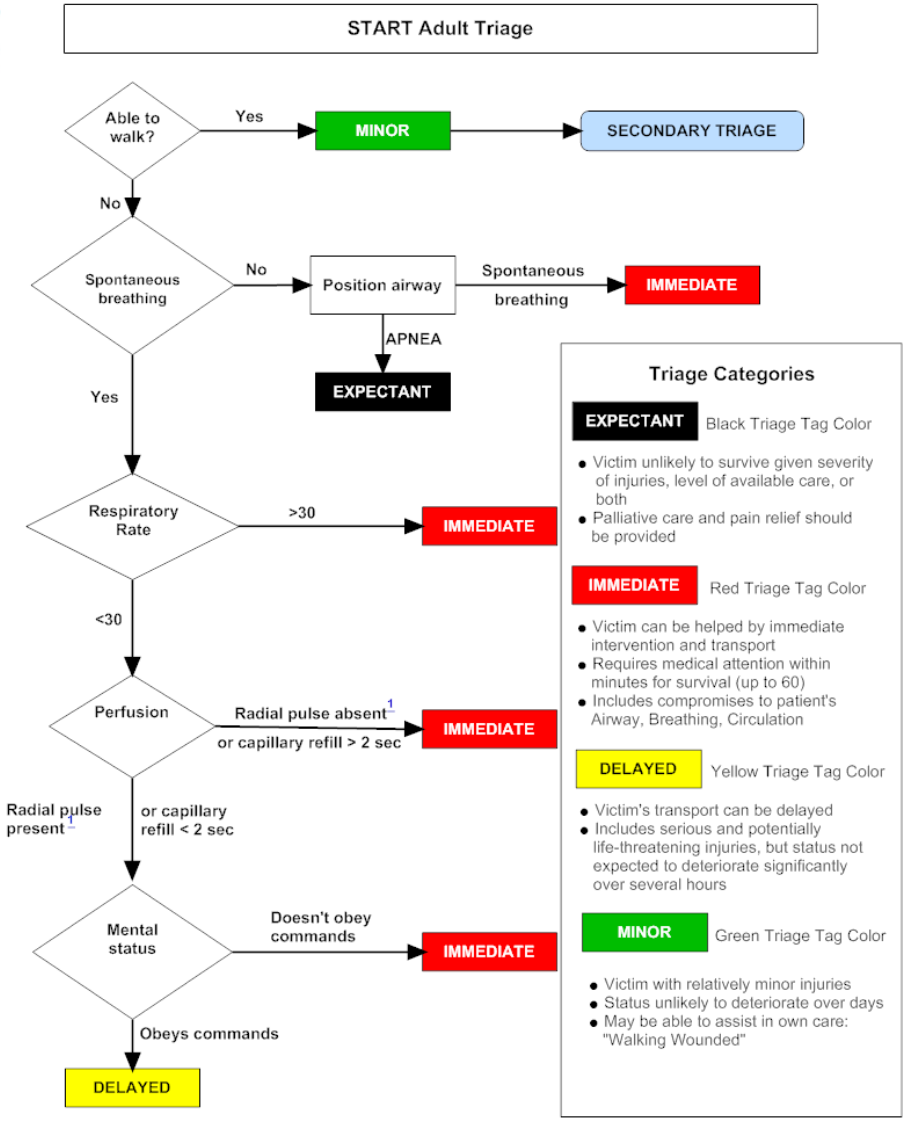
All of this is based on public sources and doesn't reflect incidents that may or may not have occurred at any employer, past, present, or future.


INDIAN PEAKS
EL DORA

Mass Casualty Incident (MCI)

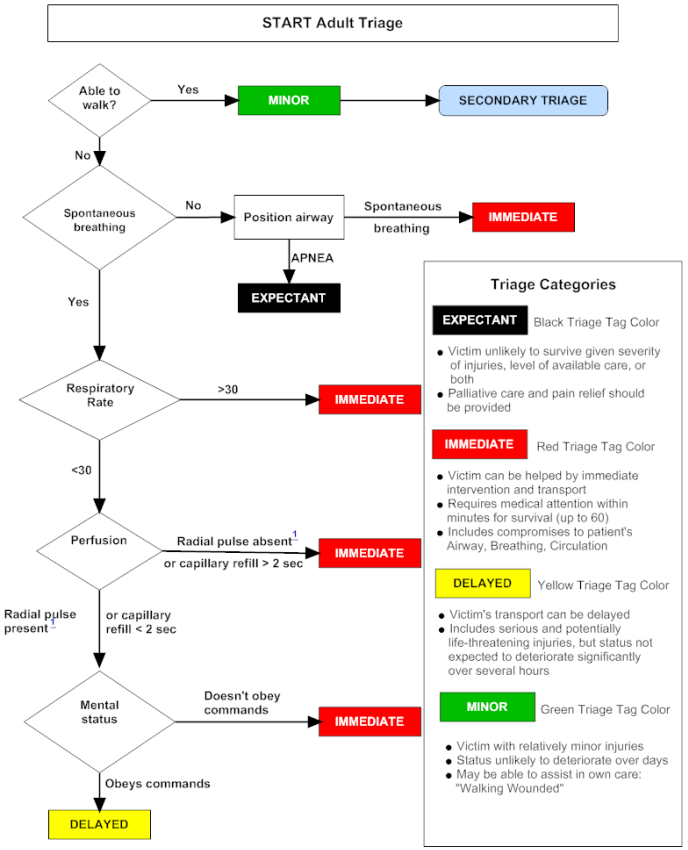
- Any incident that exceeds available resources

START: Simple Triage and Rapid Treatment



FIREMON PrimeHarbor Technologies

START: Simple Triage and Rapid Treatment



You wake up one day and....

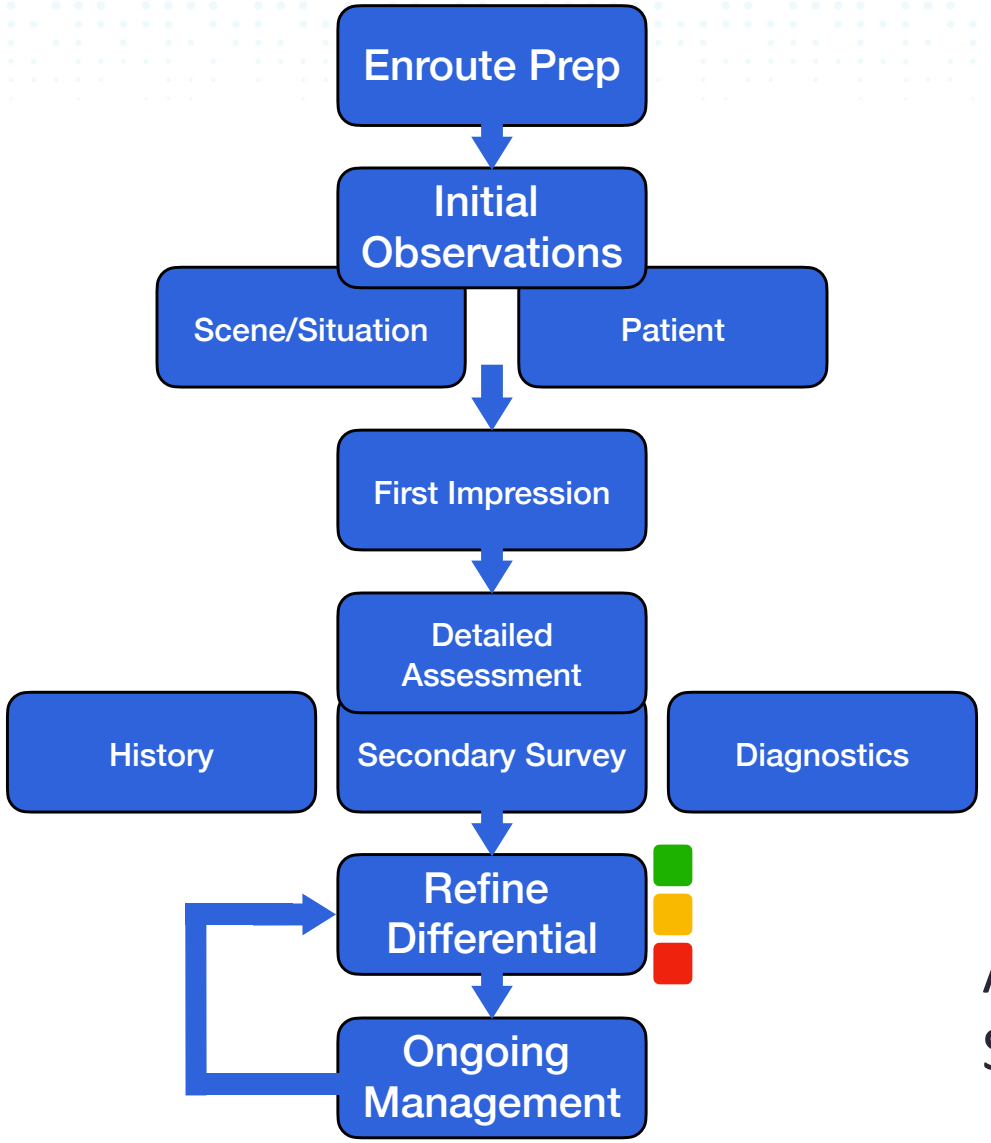
Welcome to your new cloud environment

Day One - what do you do?

- You're the first cloud security hire
- Company has been in business for 15 years
- Been in the cloud for the last 10 years
- Finished their cloud migration 6 months ago
- Internal Audit said they needed a Cloud Security Program
- CISO hired you to make it all better


Now What?

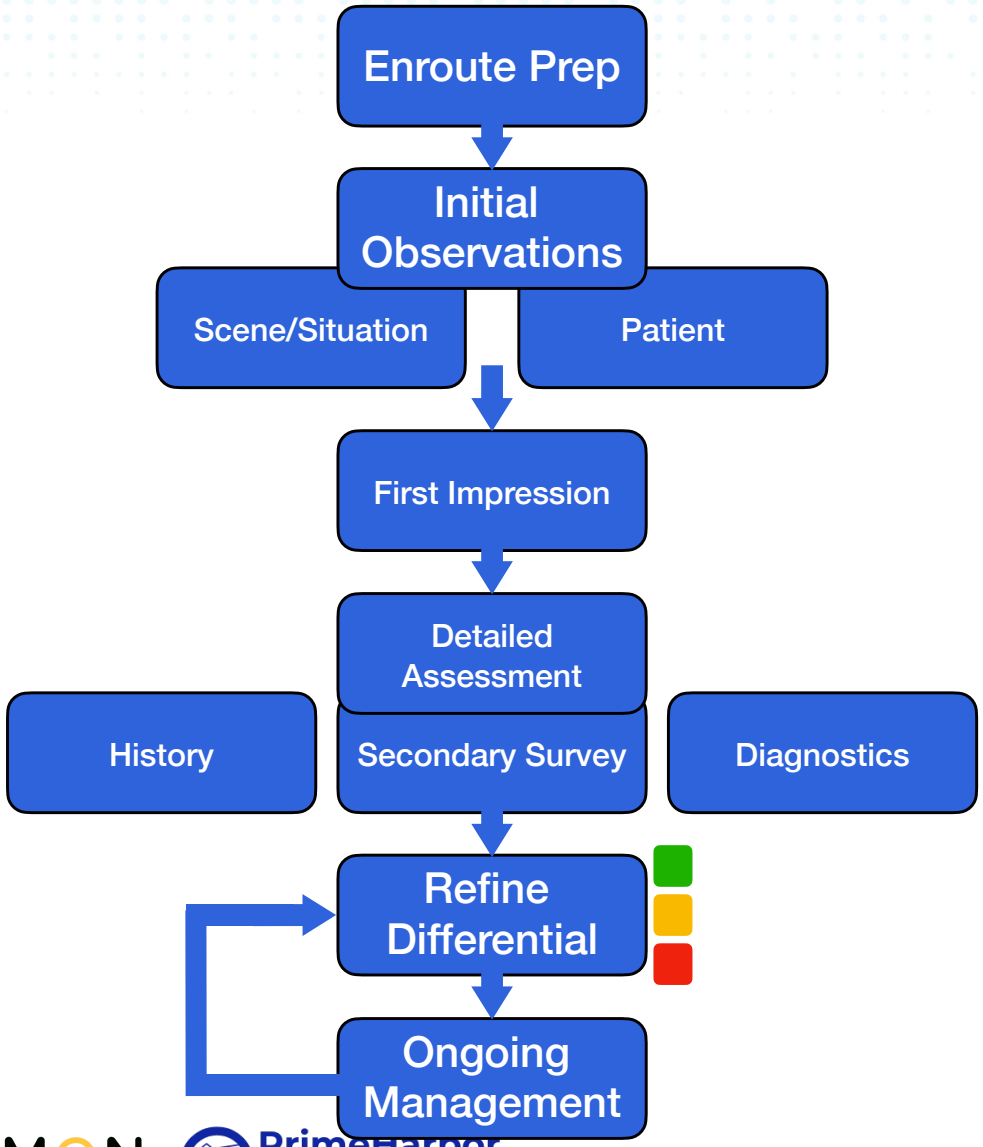
Systemically Taming Chaos

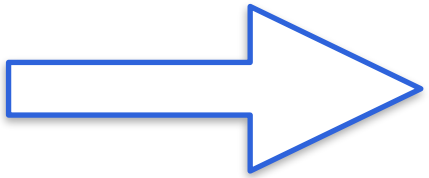


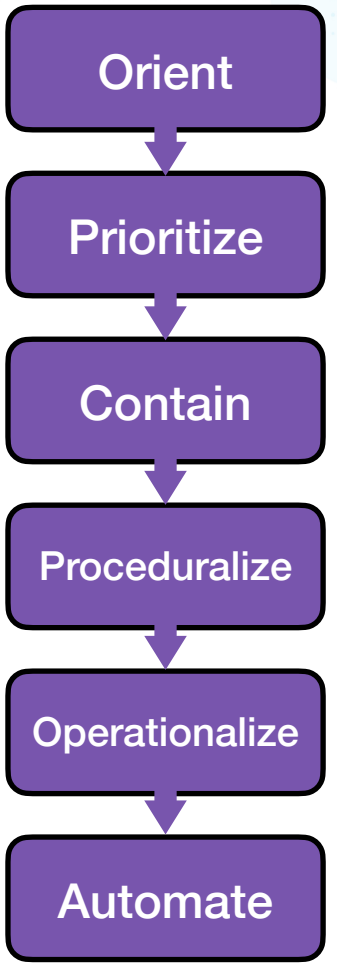
Advanced Medical Life Support (AMLS) Algorithm

FIREMON PrimeHarbor Technologies

Systemically Taming Chaos

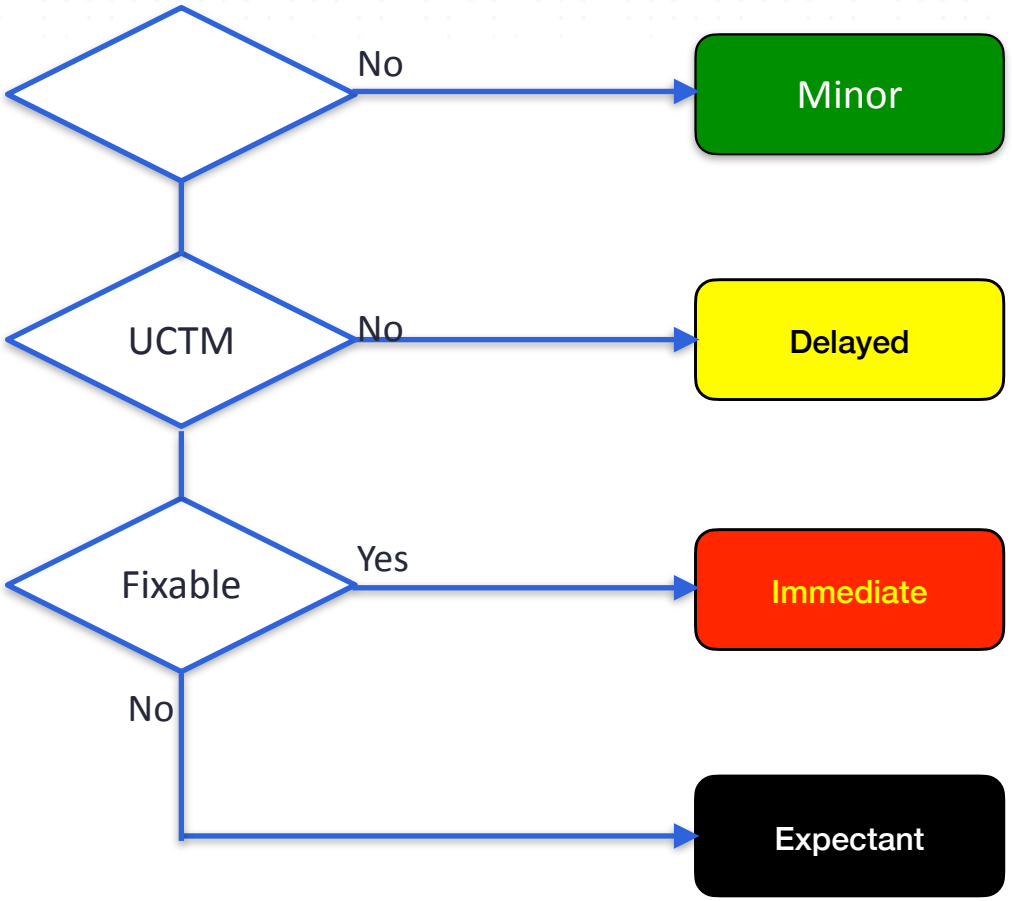






FIREMON PrimeHarbor Technologies

Simple Triage And Rapid ~~Treatment~~ Remediation



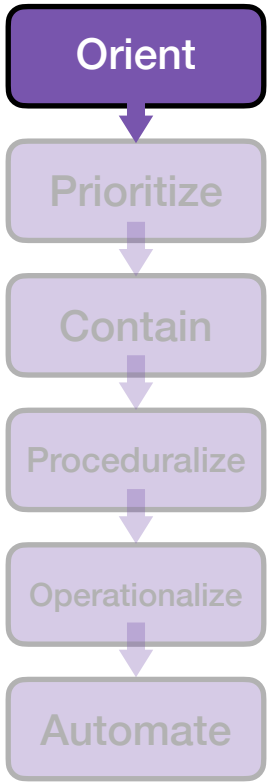
Issues that are regulatory or hard to exploit

These are important, but not heavily exploited, or only after Initial Access

Issues that when resolved immediately reduce risk

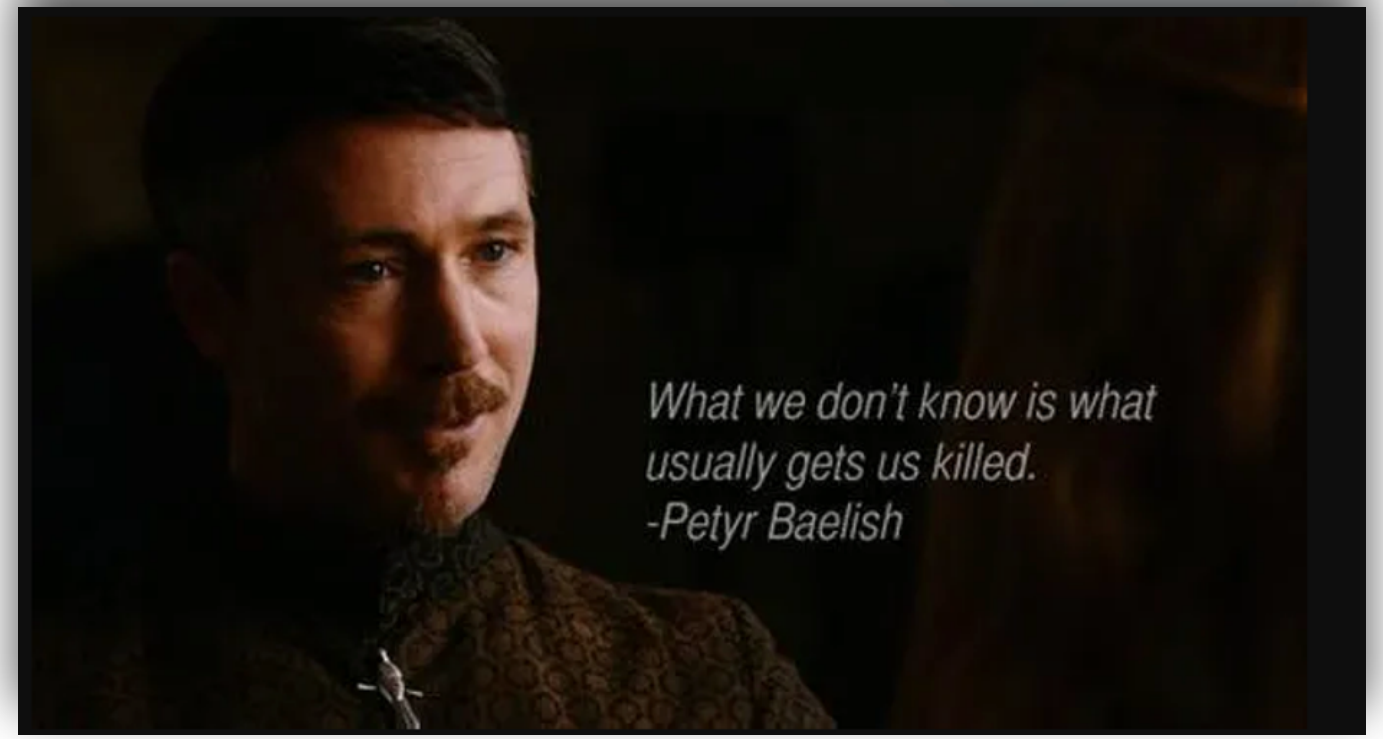
Critical issues that will take herculean efforts to resolve

Week 1


Orient
Prioritize
Contain
Proceduralize
Operationalize
Automate

Step 1: Orient

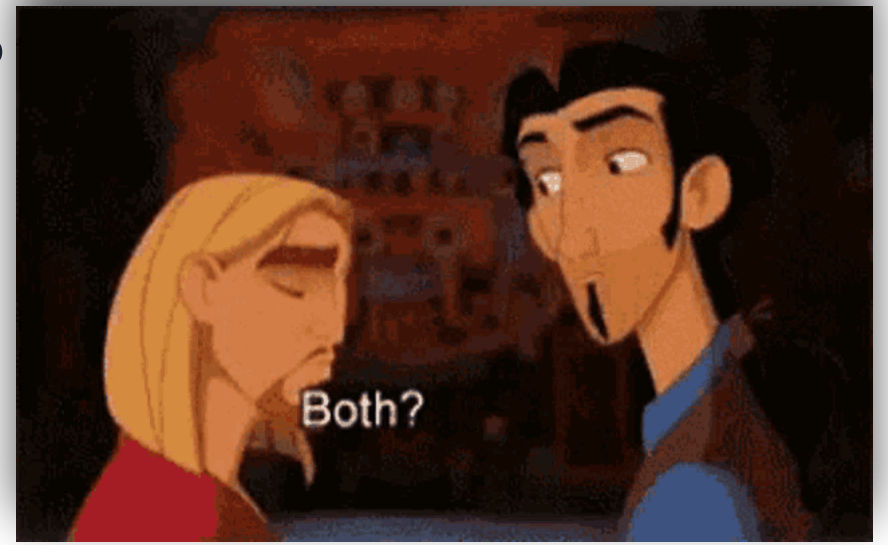
1. Find your Accounts
2. Find your Owners[1]
3. Deploy a CSPM
4. Identify your Telemetry



[1] May take more than a week

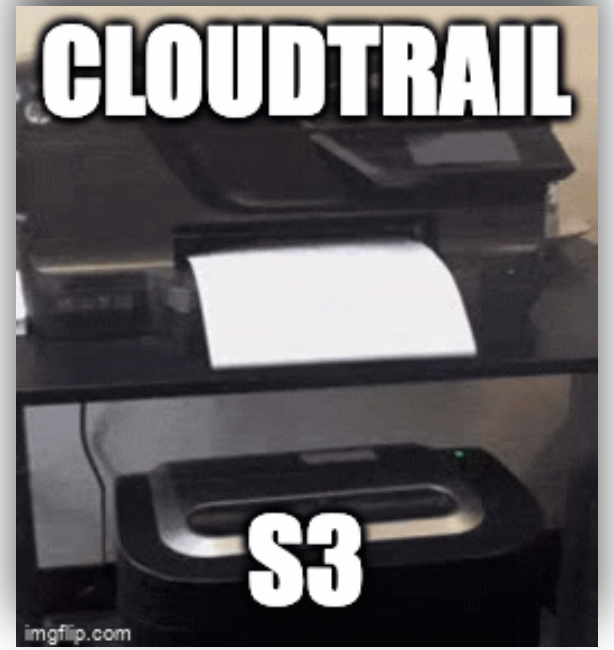
Accounts & Owners

- Find your accounts
  - CIS Critical Control 1 & 2
  - 1.5 is know your cloud accounts
- Owners
  - Who can make a decision about the account?
  - Who can answer technical questions?
  - Both are critical



Telemetry

- Cloud Audit Logs are the #1 priority
  - Credentials are a common threat vector
  - This logs them
- Any CSP threat services that are already running
- IdP logs if they are available



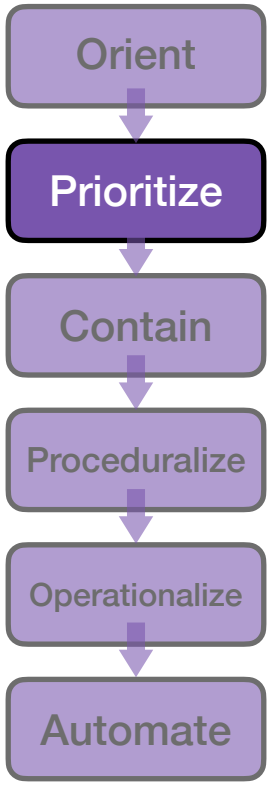
CSPM

- These are your patients
  - Cloud Resources with some form of misconfiguration
  - Resources that shouldn't exist if you're doing cloud right (IAM Users)
- You don't need fancy attack path methodologies here.
- Look at classes of issues, not each finding!
- Start with the Big Gaping Security Holes
  - these are your Immediate concerns
  - We'll discuss later

STARTing Focus

- Move fast
- Focus on information gathering
- Feed into the rest of the cycle AS you get data
  - You don't have to collect everything before making decisions
- Always be prepared to Stop the Bleed
- Use Free and Open Source if procurement can't keep up
  - Consider CSP tools (more later) if needed but be prepared for the bill
  - Vendor trials are a GREAT cheat code

Prioritize with the **Universal Cloud Threat Model**



What is the UCTM?

- We're all in the same public clouds
- We all face the same universal threats
- Many of us can afford to threat model
- Many of us cannot
- Crowd Sourcing!

Why the UCTM

- Address the main gaps in non-cloud threat models:
  - In cloud, infrastructure and applications are often deeply entangled
  - In public cloud the Internet-facing attack surface now includes the administrative management plane
  - In public IaaS, nearly all organizations run on the shared infrastructure of three primary cloud service providers followed by a slightly-large set of secondary providers

90/90

The *Universal* Cloud Threat Model identifies the commonalities faced by all organizations equally based on their cloud usage, regardless of size, vertical, or nationality.

Threat Actors have **Objectives**
against **Targets** using **Attack Vectors**
that are observed by defenders as **Attack Sequences**

Clue®

Parker Brothers Detective Game

Threat Actors

- State-nexus threat actors




- Cybercriminals & financially motivated threat actors

- Hacktivists & cause-motivated threat actors

- Insider threats
- Script-kiddies, reputation builders, 80s-style hackers

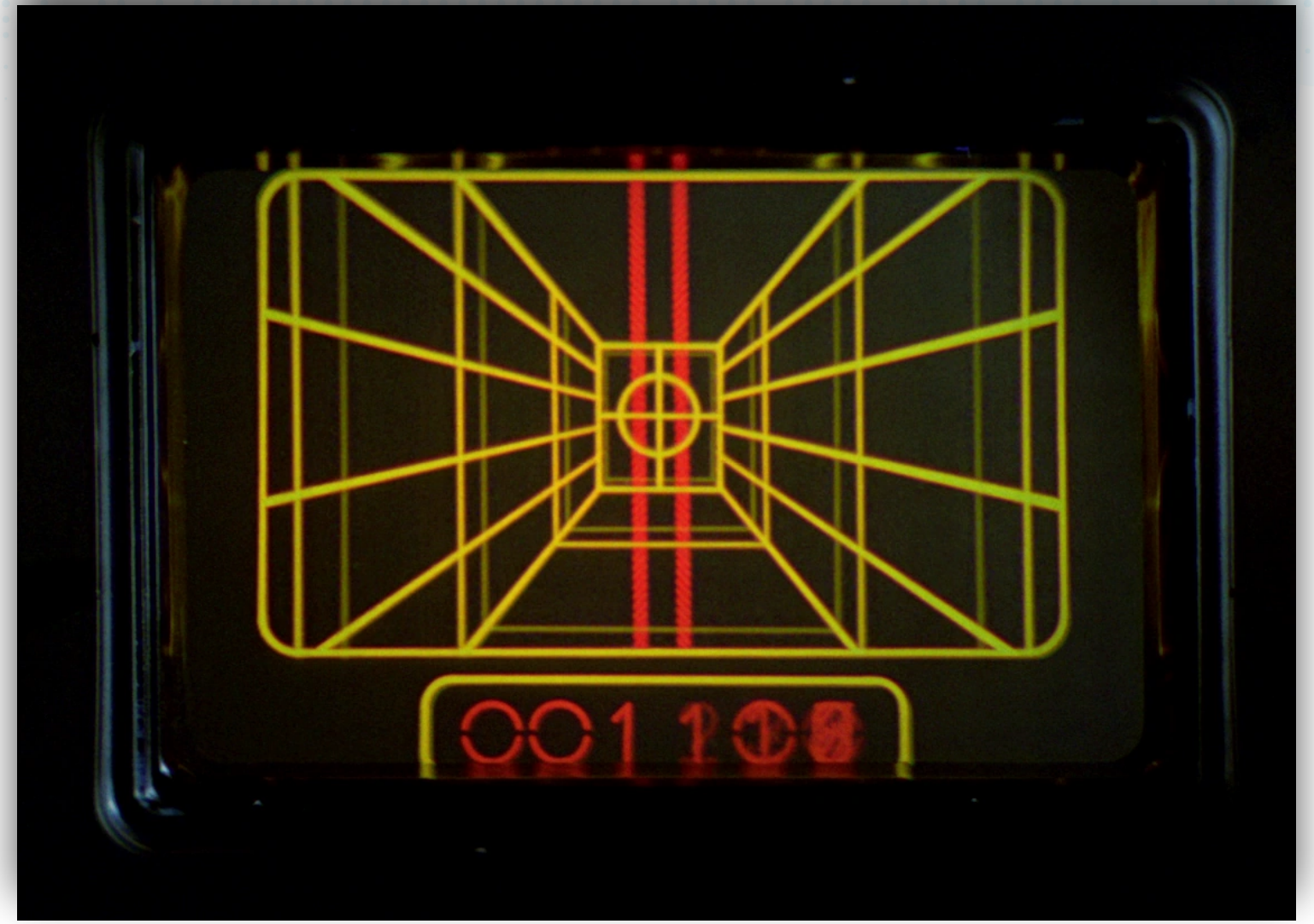
- Rich's Cat. He's a legitimate turdhole.

Objectives

- Financial Gain from:
  - CryptoMining
  - Spam
  - Ransomware (encryption or deletion)
  - threat of sensitive information disclosure (blackmail)
  - selling Sensitive Data on black market
- Leveraging Cloud Infrastructure for:
  - Financial attacks against others
  - Geo-Political attacks against others
- Denial of Service Attacks
- Industrial espionage
- Nation-state espionage

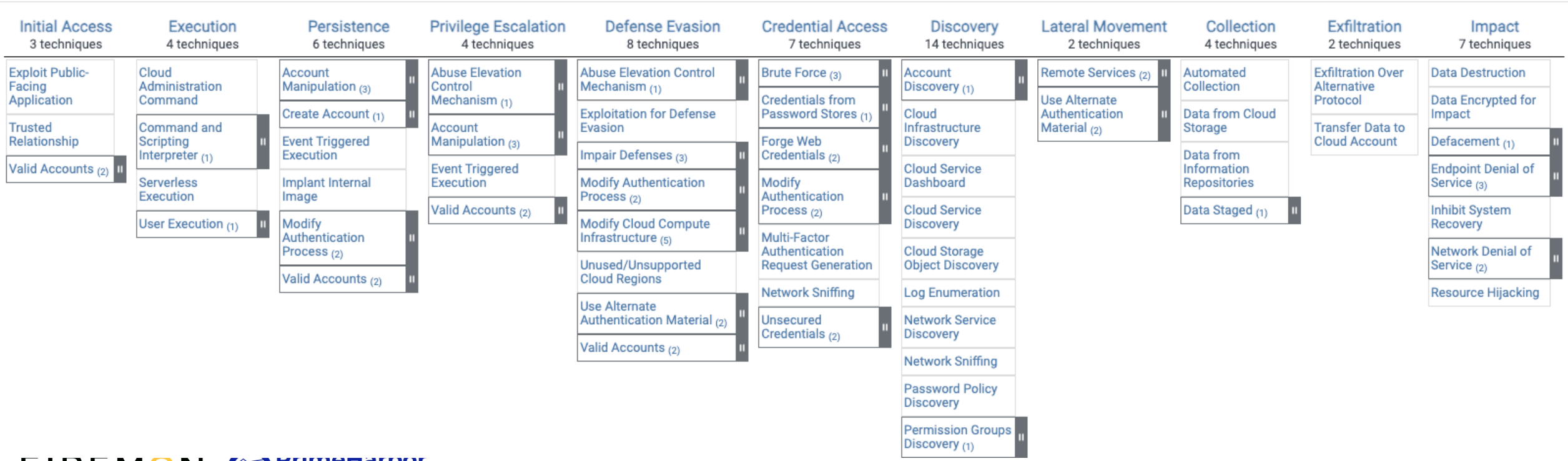
Targets

- Data
- Compute
- Network
- Pipelines
- Supply Chain



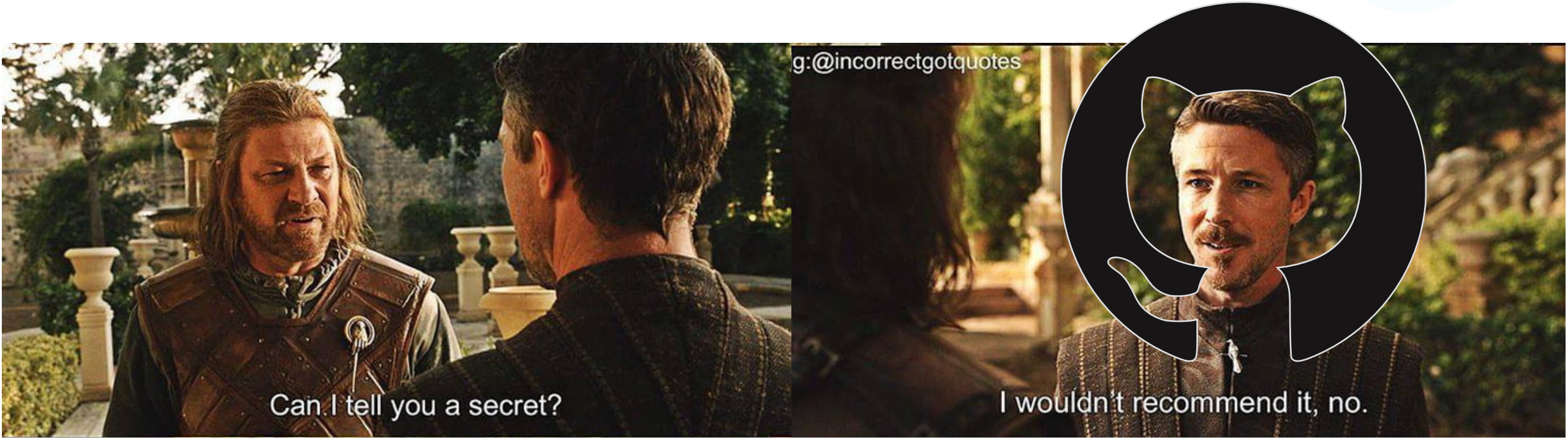
Attack Vectors

- These are the things to defend against
- Involve credentials, network exposure, misconfigurations




For the Cloud is Dark
And Full of Terrors

VECTOR: Lost, stolen, or exposed credentials



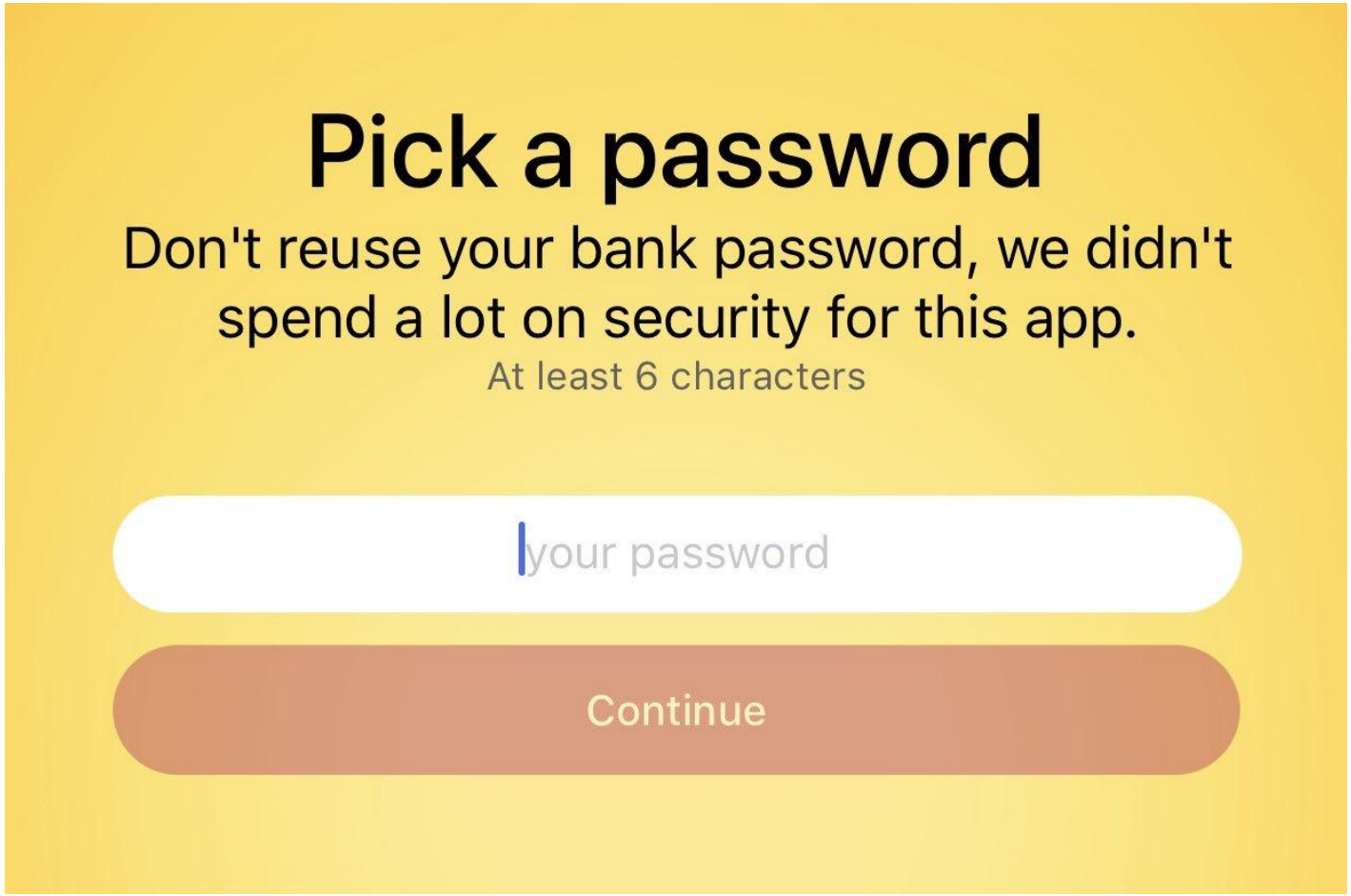
VECTOR: Publicly Exposed Resources

ACHIEVEMENT UNLOCKED!

S3 Bucket Negligence Award

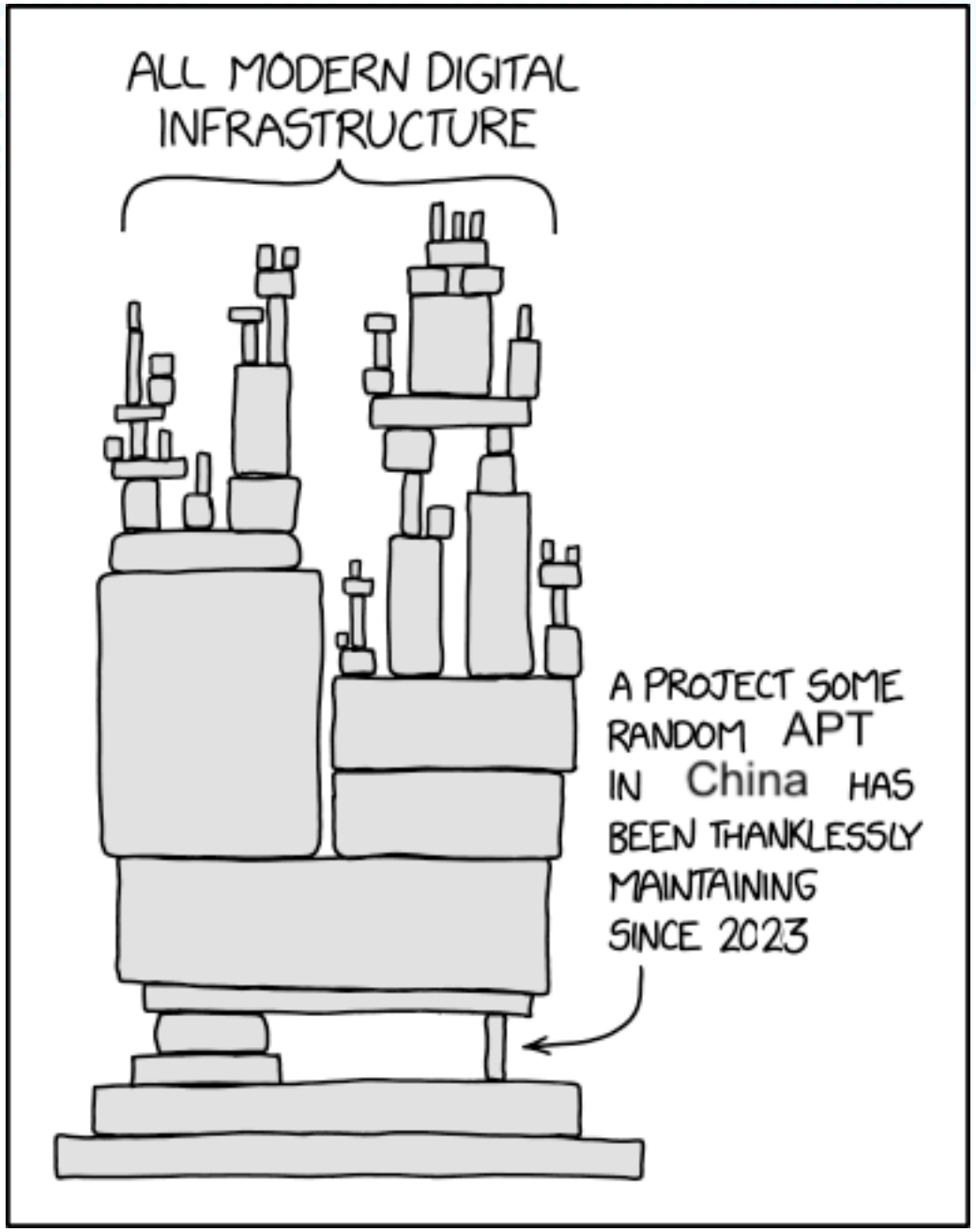
You have failed to adequately safeguard the data with which you were entrusted. You have failed those who relied upon you.

VECTOR: Credentials exposed via application security flaws



VECTOR: Unpatched vulnerabilities and zero-days in overly exposed systems

VECTOR: Supply Chain



FIREMON PrimeHarbor Technologies

VECTOR: Domain Takeover

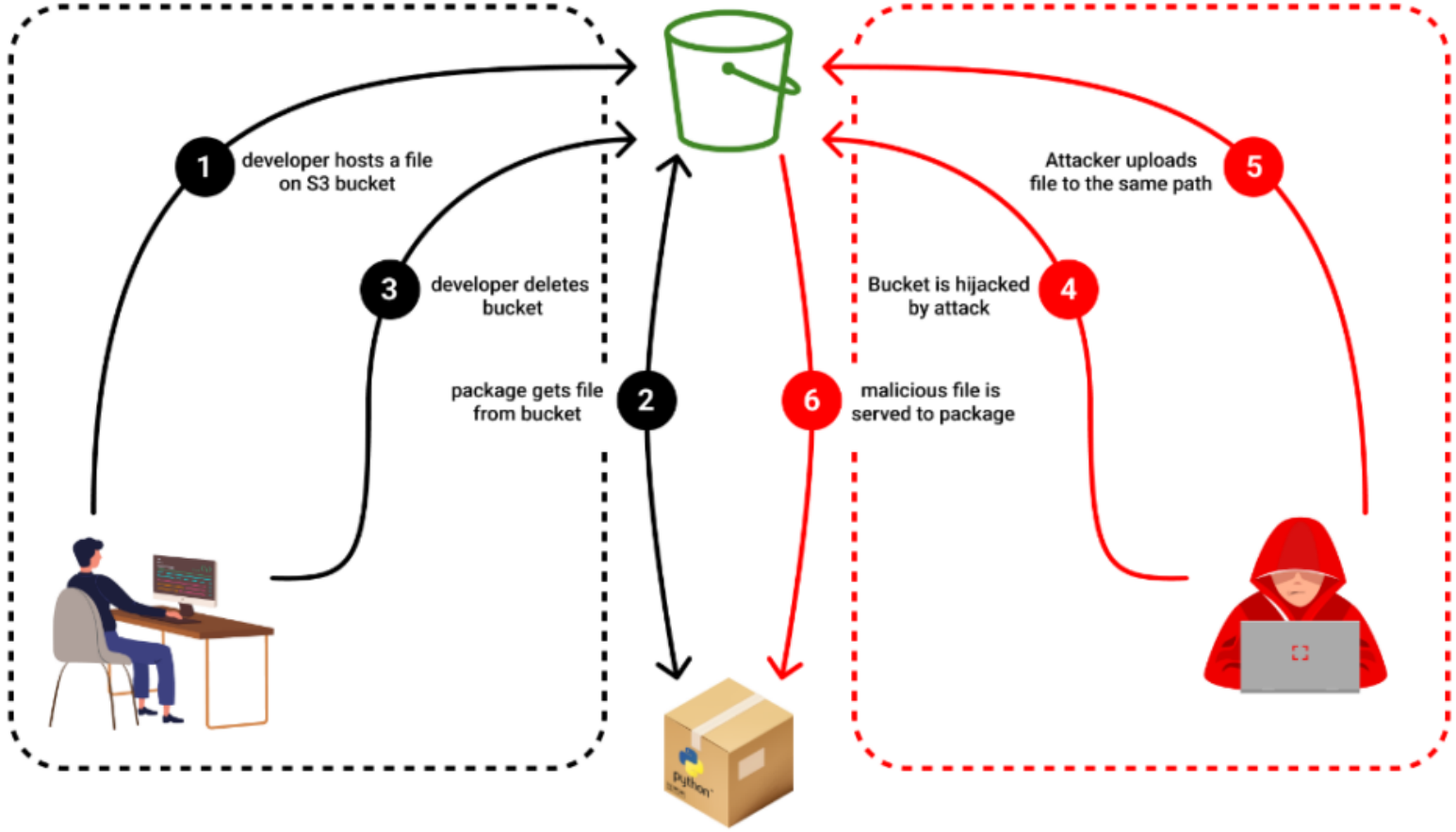
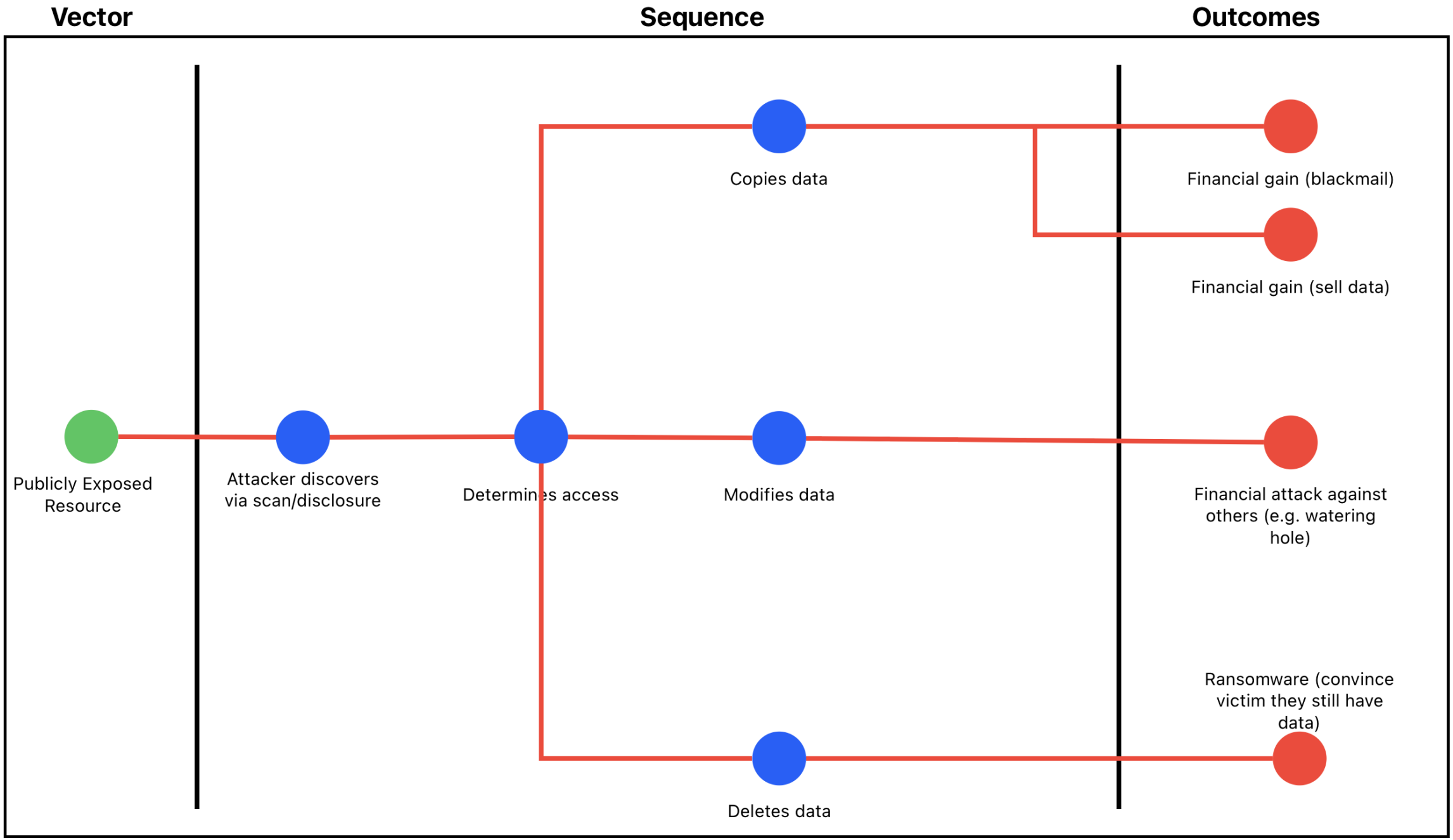


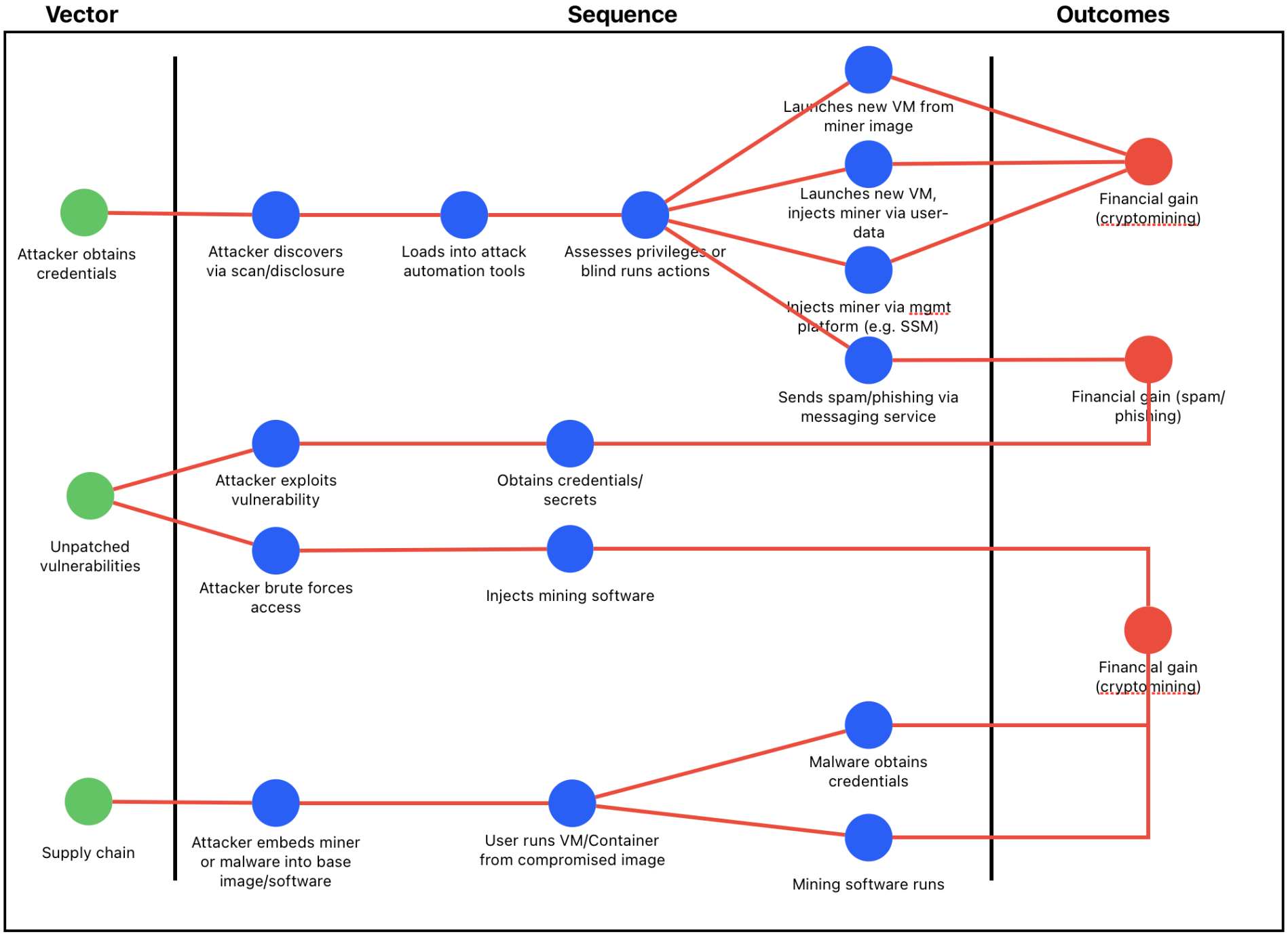
Image courtesy of Checkmarx -
Hijacking S3 Buckets: New Attack Technique Exploited in the Wild by Supply Chain Attackers


“two cozy bears in a midnight blizzard” (DALL-E 2)

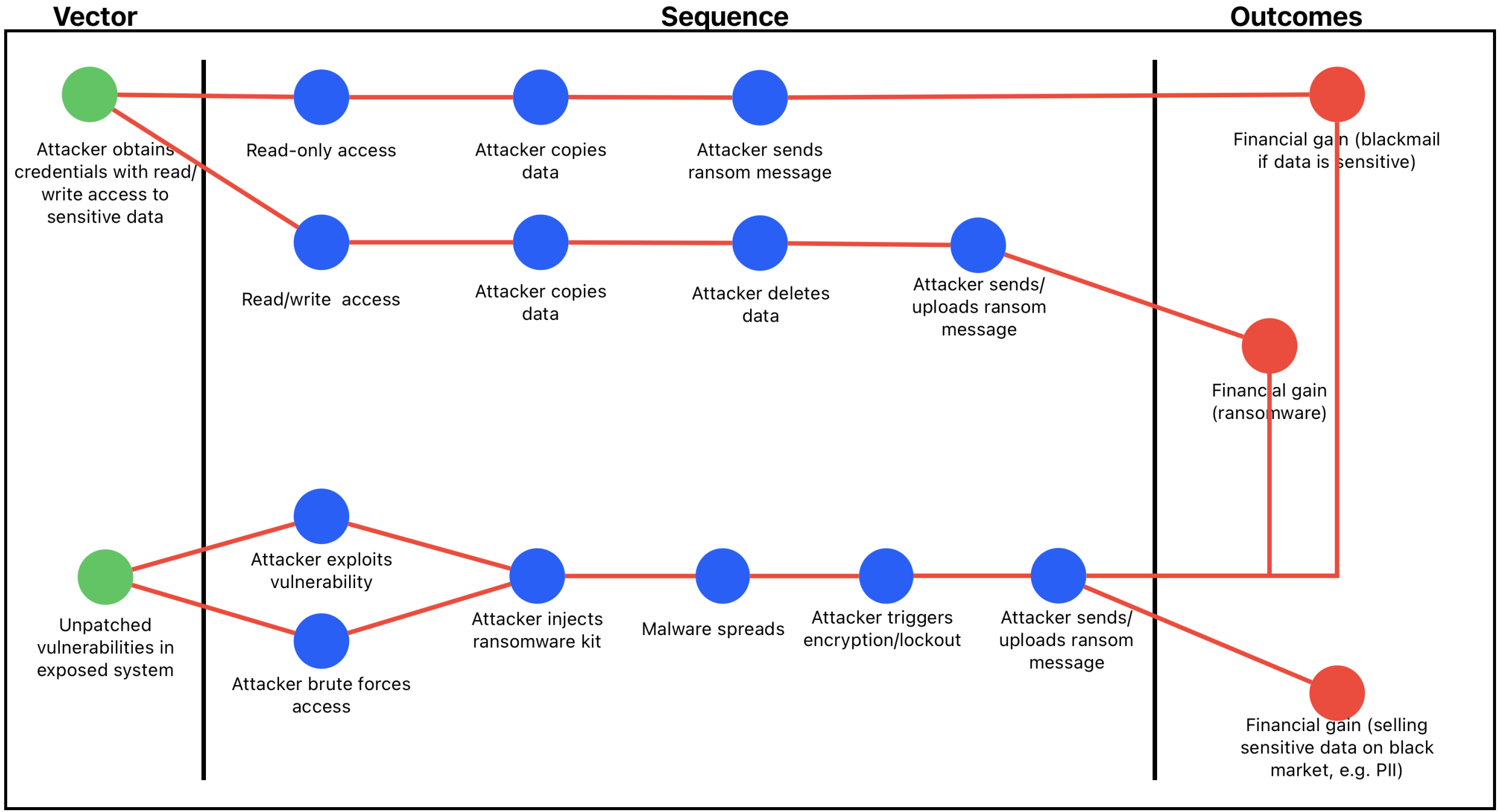
Threat Actor Copies/Alters a Public Data Resource



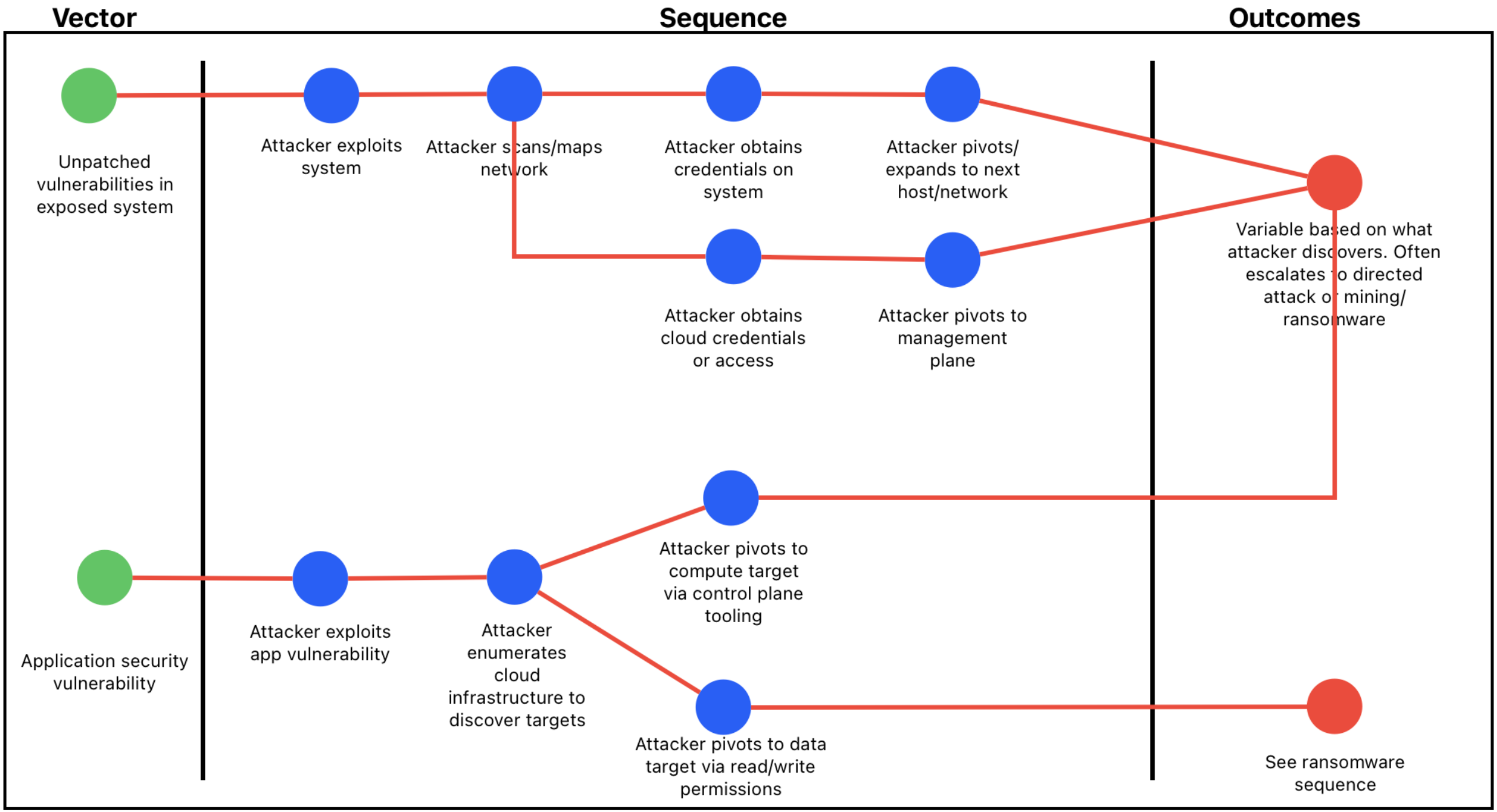
Threat Actor Hijacks Resources for Cryptomining, Spam, or Phishing

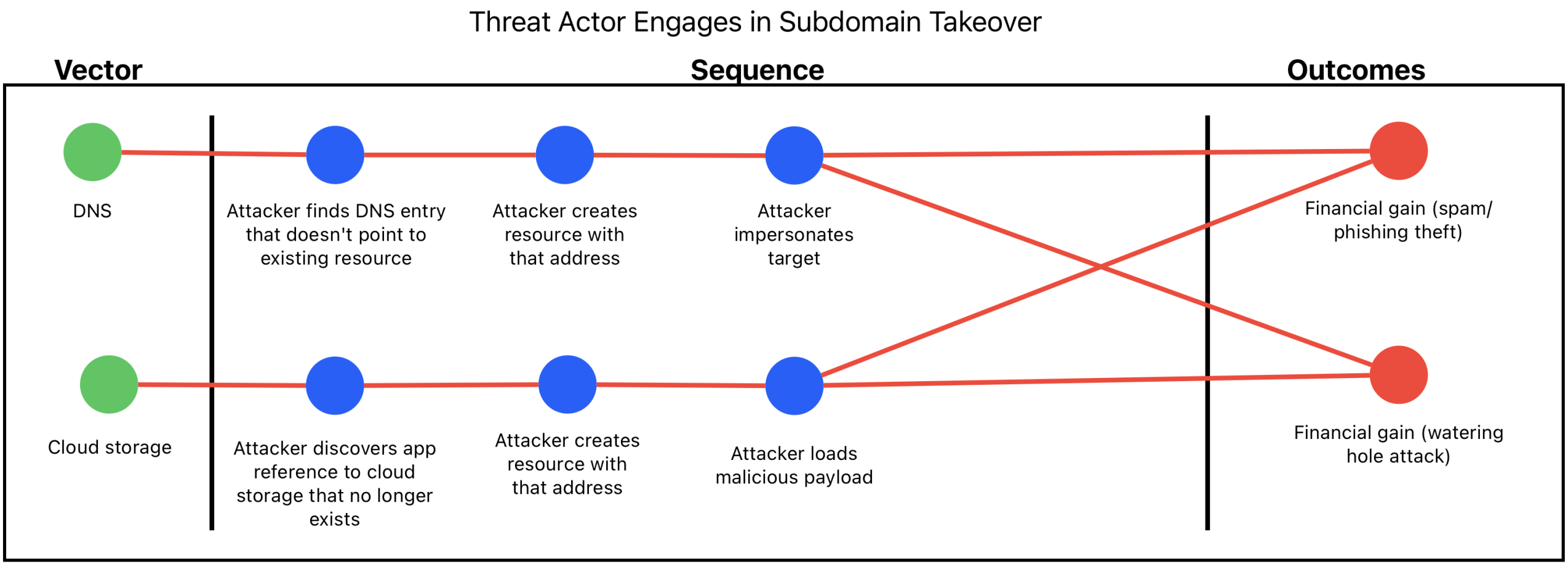


Threat Actor Engages in Ransomware

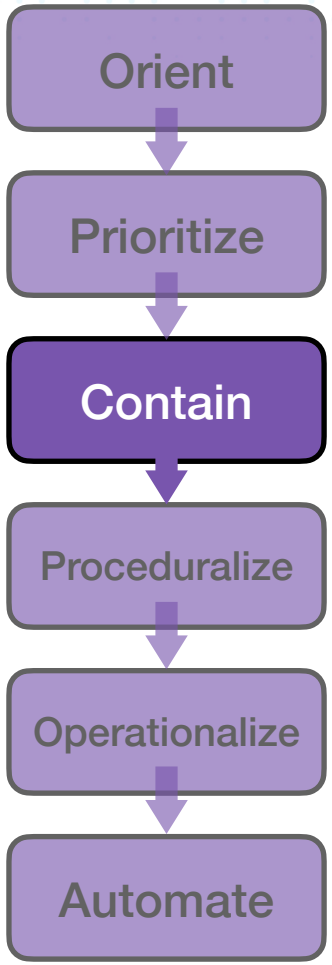


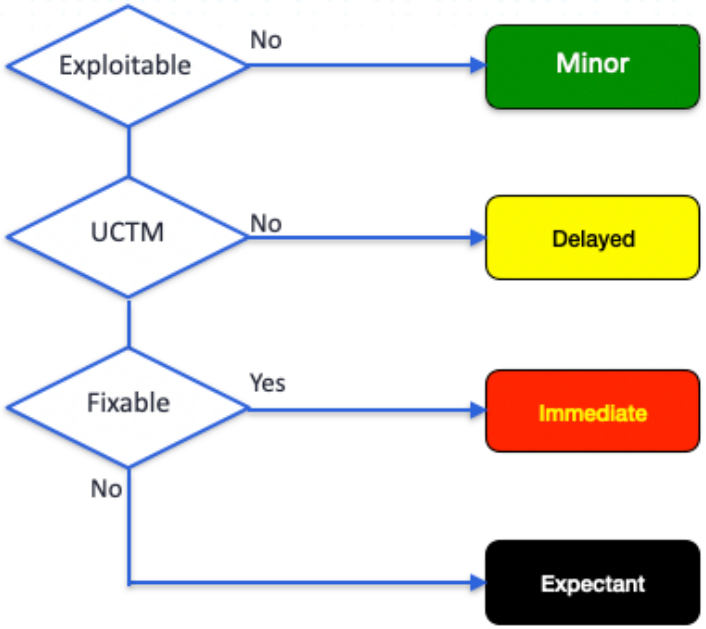
Threat Actor Engages in Lateral Movement




Threat Actor Engages in Subdomain Takeover
Vector
Sequence
Outcomes
DNS
Attacker finds DNS entry that doesn't point to existing resource
Attacker creates resource with that address
Attacker impersonates target
Financial gain (spam/ phishing theft)
Cloud storage
Attacker discovers app reference to cloud storage that no longer exists
Attacker creates resource with that address
Attacker loads malicious payload
Financial gain (watering hole attack)

What's a Big Gaping Security Hole™?



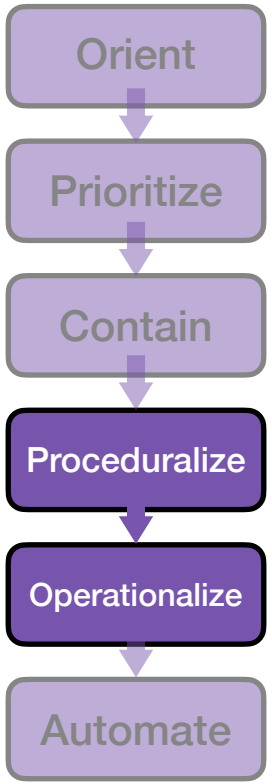


Examples:

- Root Access Keys
- Public Write/List Buckets
- 3389 open to the world
- Missing MFA
- Access Keys from the Obama Administration

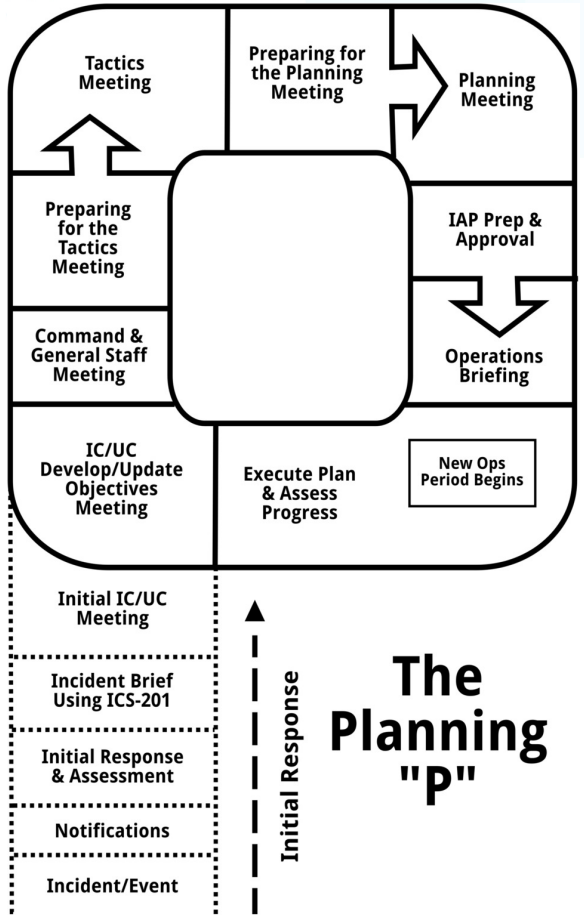
FIREMON PrimeHarbor Technologies

Setting up incident command (and beyond)



After your initial response

- You should have:
  - Identified and analyzed initial telemetry
  - Closed the BGSHs
  - Prioritized using the UCTM
  - Begun playing politics (ICS 400 FTW)
- Now you
  - Start the planning cycle
  - Implement procedures and guardrails based on prioritization
  - Begin transitioning into daily operations vs. crisis mode



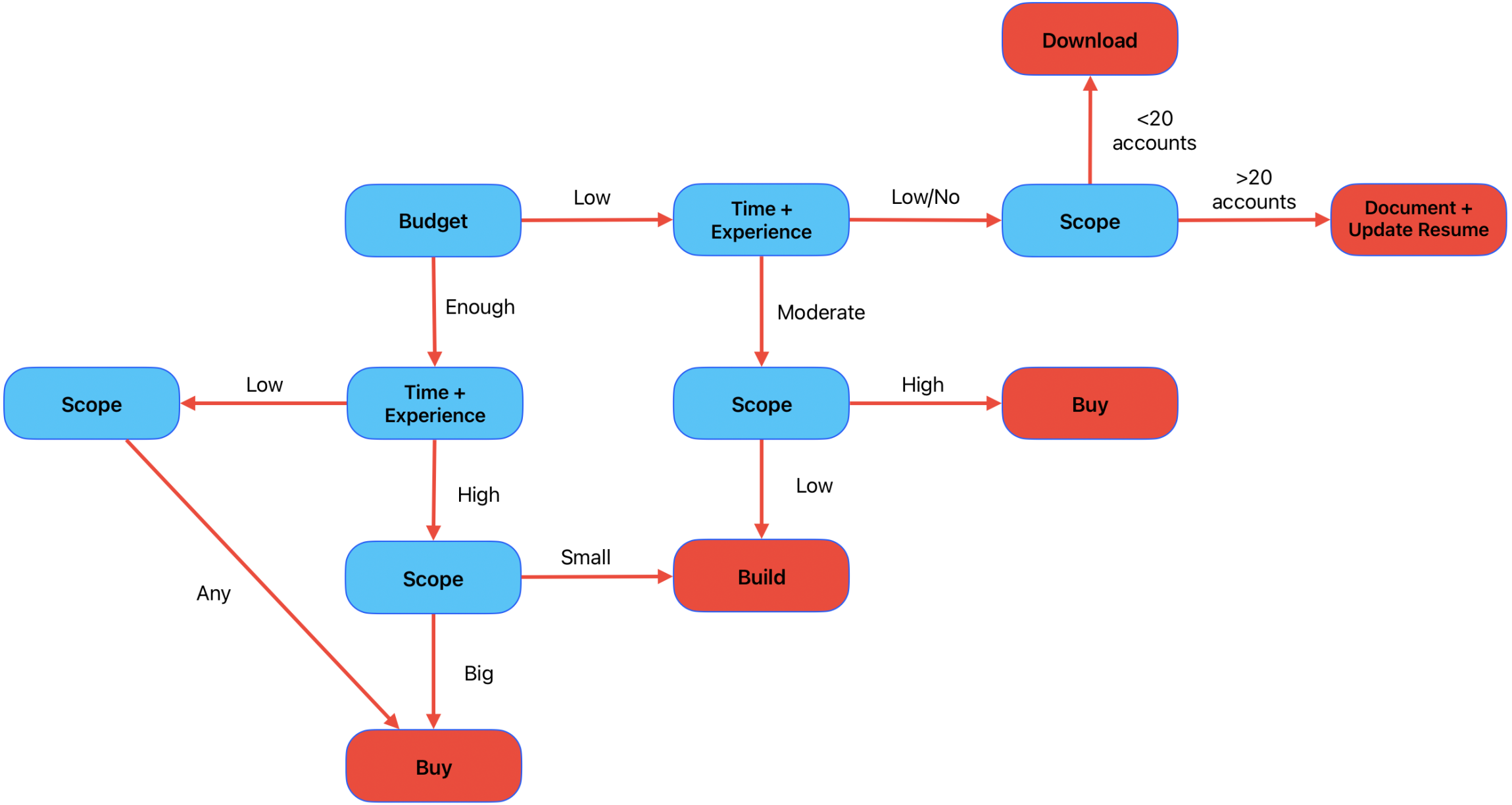
What other tools do you need?

- CSPM (permanent)
- Inventory
- Cloud API Logging
  - And event (e.g. GuardDuty/Defender) handling
- Identity Federation
- Secrets Scanning!
- SBOM

Cloud Providers are not your friend!

- In all providers, Security is an up-charge
- They're typically not as good as what you'll see on the show floor
- But...
  - No procurement process
  - Less setup
  - (Usually) Better than nothing
- Often you have no choice

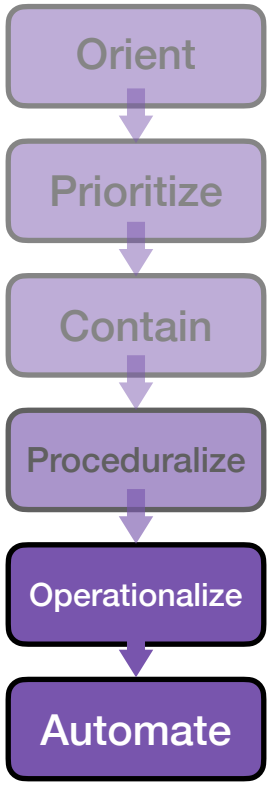
Build vs Buy vs Download



Transition Period

- Slowly move from reactive to engaging with teams
- Begin putting in initial guardrails for the BGSHs
  - Detective with alerting
  - Preventative with policies (SCPs/Azure Policy/etc.)
- Now the politics get fun

Moving from Pandemic to Endemic



Find your systemic issues

- Wide open security groups?
  - Lack of VPN, no RFC1918 connections
- Lots of IAM Users?
  - No centralized identity system
- Public Buckets?
  - User education
  - Lack of understanding of IAM and cloud APIs

You're not Ike

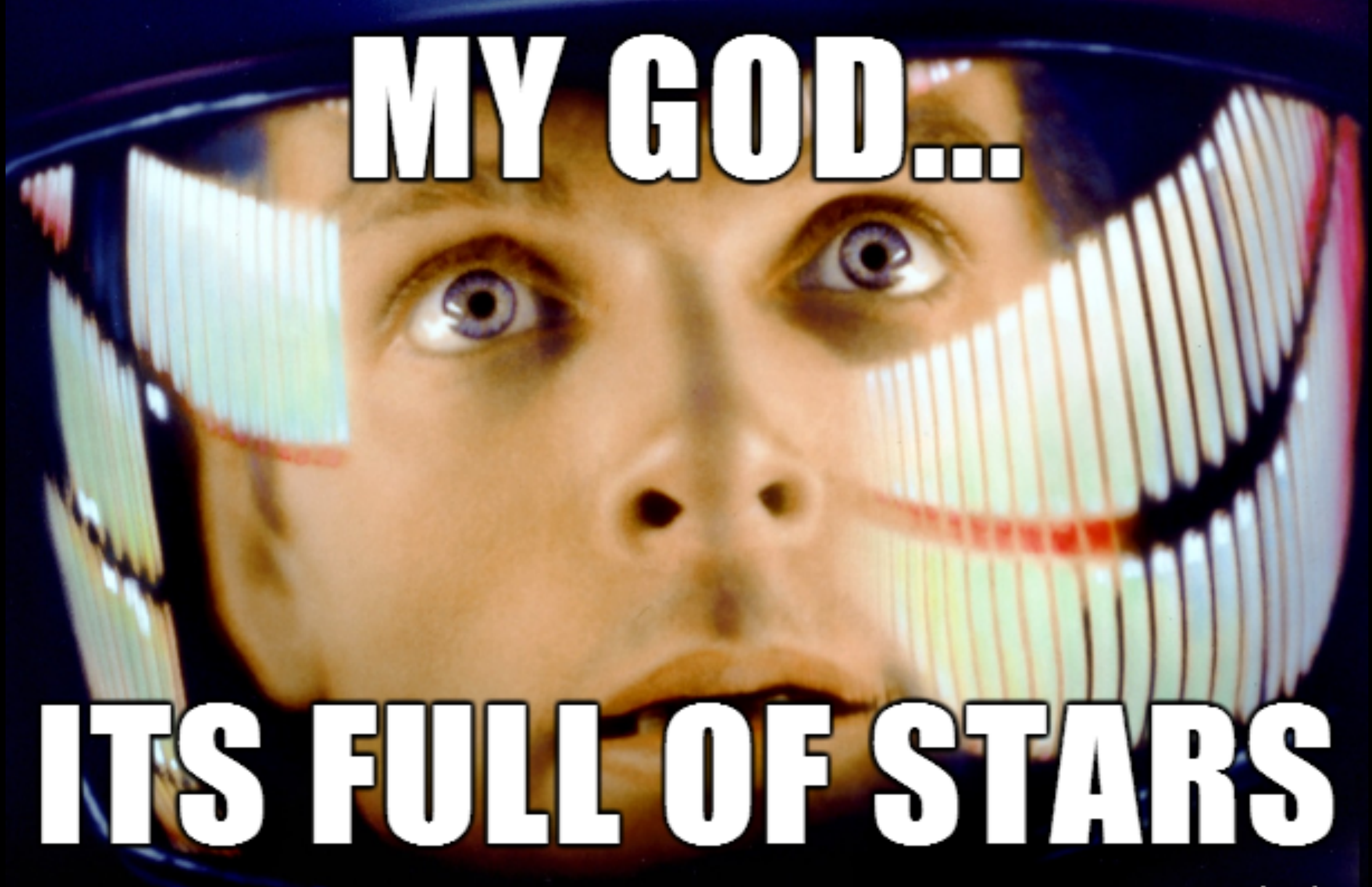
- Don't start with paved-roads
- Clear the path first - remove obstacles
  - Get an centralized identity system
  - Get VPN/RFC1918 routing working
  - Write a Baseline (https://pht.us/baseline)
- Then focus on guard-rails

Extend the Cloud Threat Model

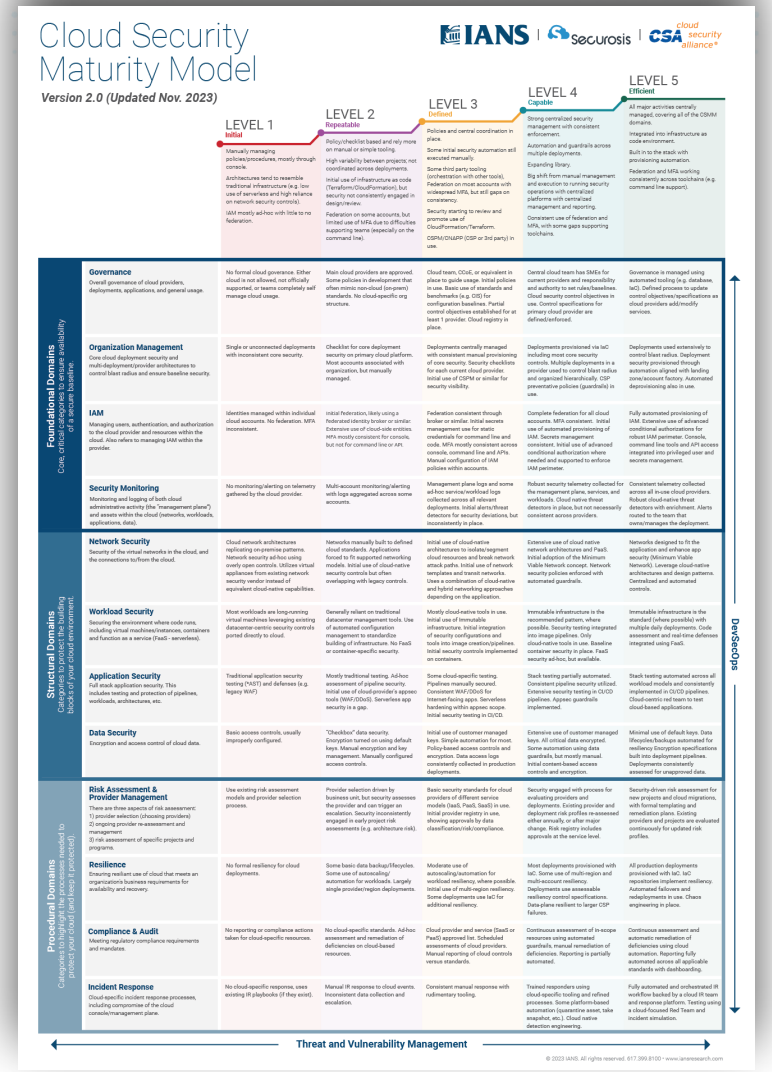
- What threat actors want to target you?
- What are their objectives and motivations?
- What do you have that they want? (Targets)
- Now go brainstorm how they'd do it!

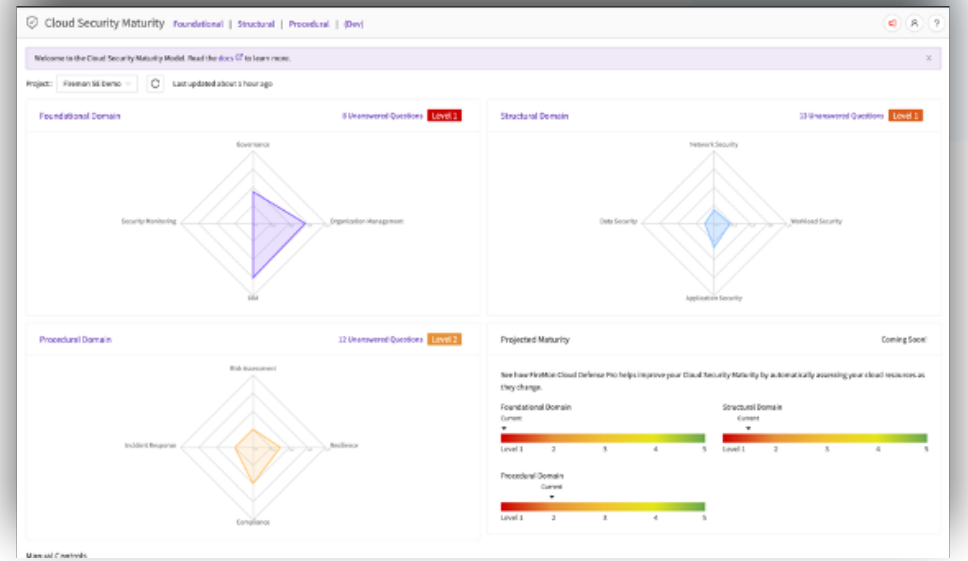
Unique Adversaries & Threats

- Auditors
- Mergers & Acquisitions
- Those other Nation-State Actors


MY GOD...
ITS FULL OF STARS

Measure Twice, breach never

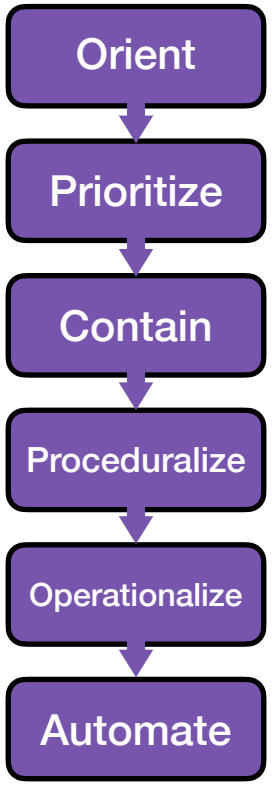




https://www.iansresearch.com/resources/cloud-security-maturity-model

FIREMON PrimeHarbor Technologies

Putting it all together



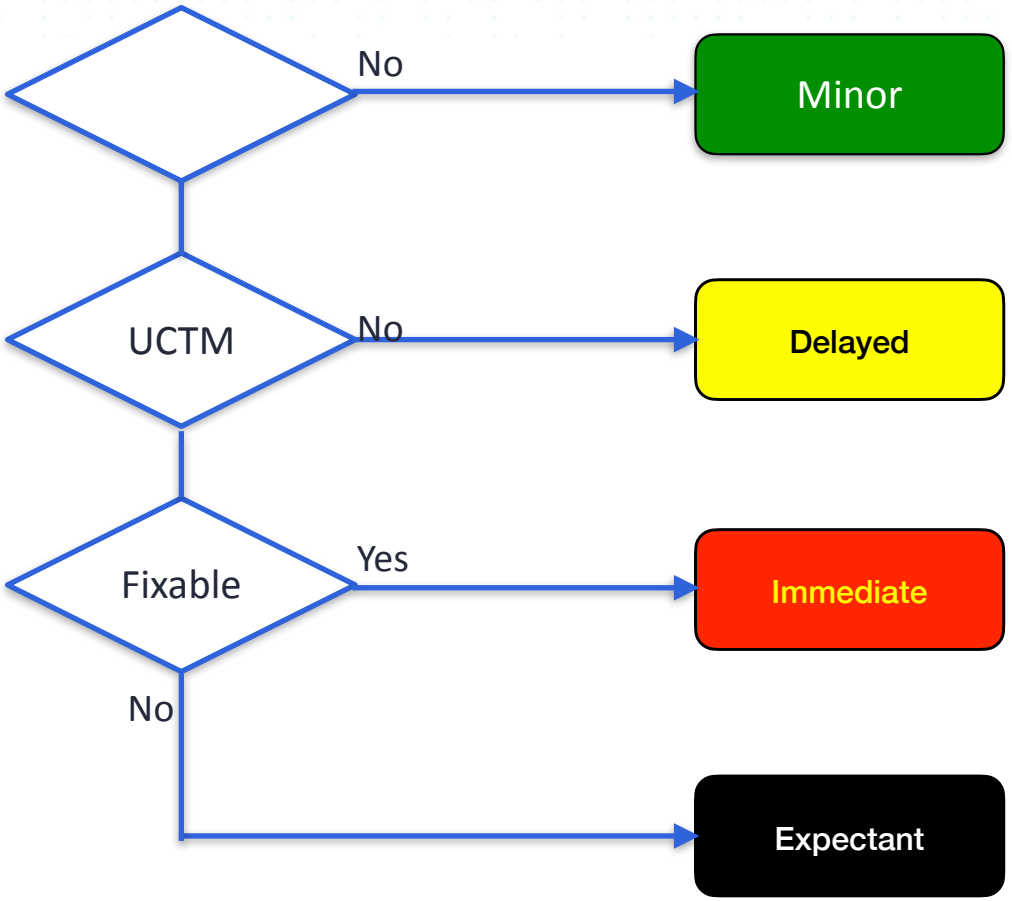

DON'T PANIC

Apply the Universal Cloud Threat Model

Threat Actors have **Objectives**
against **Targets** using **Attack Vectors**
that are observed by defenders as **Attack Sequences**

https://pht.us/uctm

Apply START to prioritize your issues.



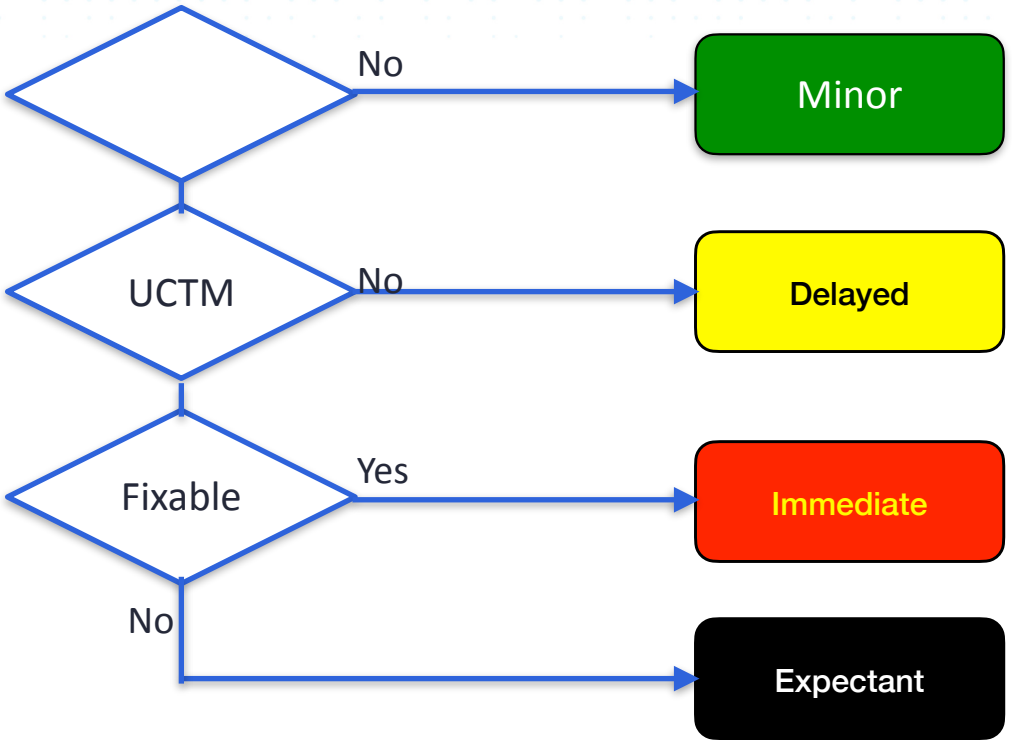
Issues that are regulatory or hard to exploit

These are important, but not heavily exploited, or only after Initial Access

Issues that when resolved immediately reduce risk

Critical issues that will take herculean efforts to resolve

Apply START to prioritize your issues.



Issues that are regulatory or hard to exploit

These are important, but not heavily exploited, or only after Initial Access

Issues that when resolved immediately reduce risk

Critical issues that will take herculean efforts to resolve

Then start to Implement GuardRails

Questions?

Rich Mogull

@rmogull (rarely there anymore)

@rmogull@defcon.social

https://securosis.com

https://slaw.securosis.com

https://defense.firemon.cloud

Chris Farris

@jcfarris

@jcfarris@infosec.exchange


https://www.chrisfarris.com

https://primeharbor.com


https://breaches.cloud

https://pht.us/uctm