Confidence Predicts Accuracy !

…….and other lies about Cloud Security

About Me

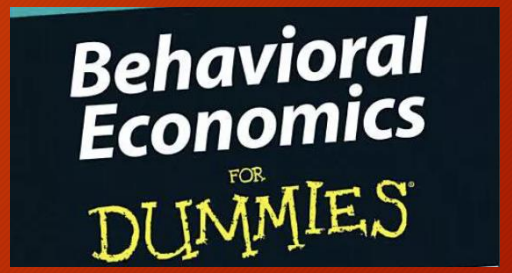
Kat Traxler

Principal Security Researcher

My fwd:CloudSec Journey

AWS S3 Exfiltration with the Replication Service

2022



2025

GCP Privilege Escalation

2020

Service Agent Exploitation in GCP

2024

Confidence Predicts Accuracy ?

ACT 1

Thinking Fast and Posture Perfect

ACT 2

Thinking Slow and Understanding Cloud Risk

ACT 3

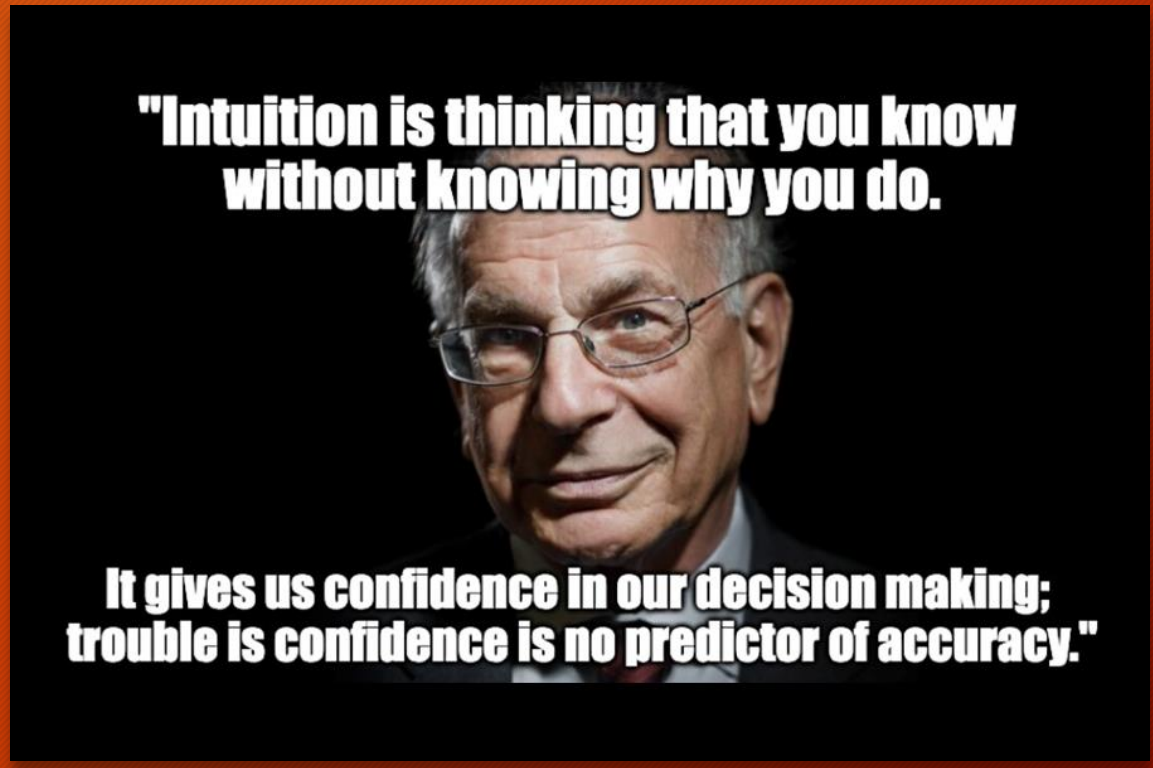
The More Things Change, The More They Stay the Same

Act 1: Thinking Fast

……And Pursuing Posture Perfect

Challenging Our Gut Instinct

- Thinking, Fast and Slow 2011
- Daniel Kahneman

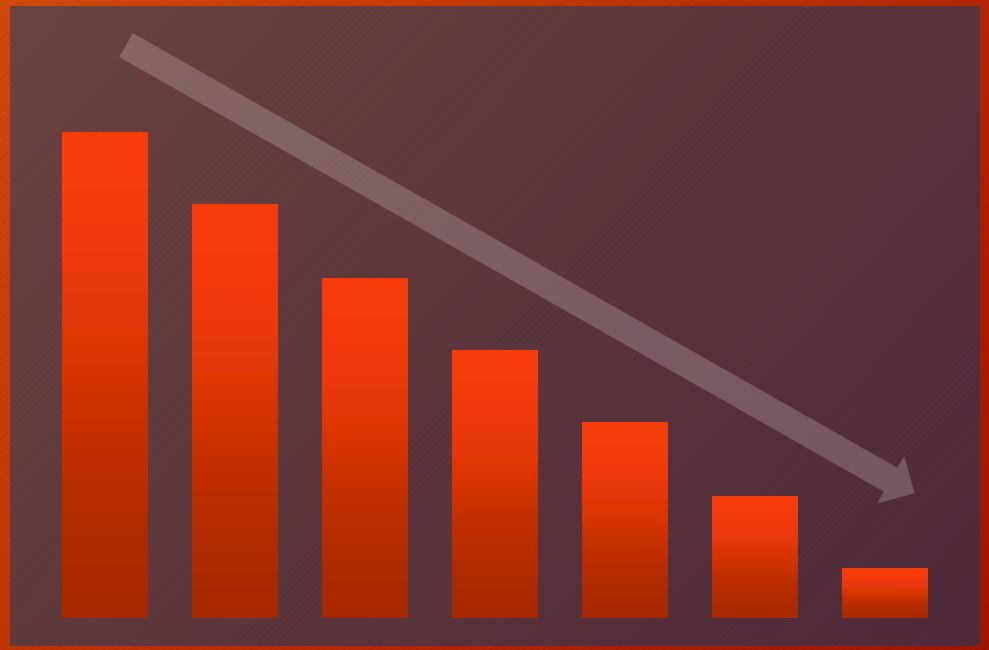


The **measure of success** for System 1 is the coherence of the story it manages to create.

Thinking Fast and Posture Perfection

Misleading Metrics

Overemphasis on metrics that are easily measured, frequently reported, or emotionally resonant,



Examining Supporting Evidence - Part 1

Only a Slice of the Story

61%

of organization have a root user or account owner without MFA

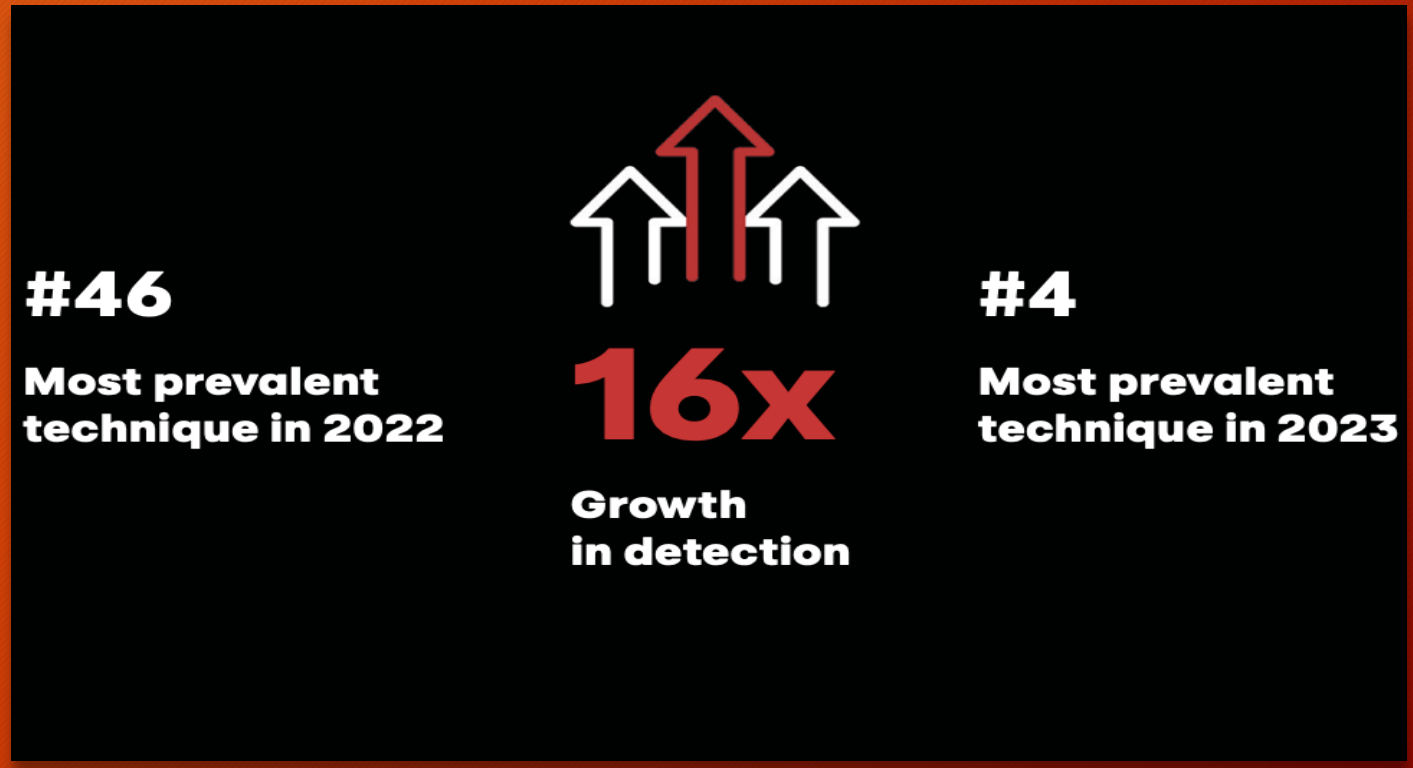
Cherry Picking Data

82%

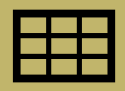
of AWS SageMaker users have a notebook exposed to the internet

Examining Supporting Evidence – Part 1

Identifying year-to-year trends from Threat Reports, is a **minefield due to data instability**.



What You See Is All There Is (WYSIATI)



WYSIATI means that System 1 doesn't look for information it doesn't have.

It takes the limited data presented and expertly weaves it into a coherent and plausible story.

Act 2: Thinking Slow

……And Understanding Cloud Risk

Opportunity Cost of Getting It Wrong

We spend our brain power working towards posture perfect **leaving no excess capacity** to tackle risk from other angles

Thinking Slow with Deliberative Reasoning

Instinctive processes for making decisions is often wrong

Slow and deliberate thinking is needed to judge the most effective activities in reducing cloud risk

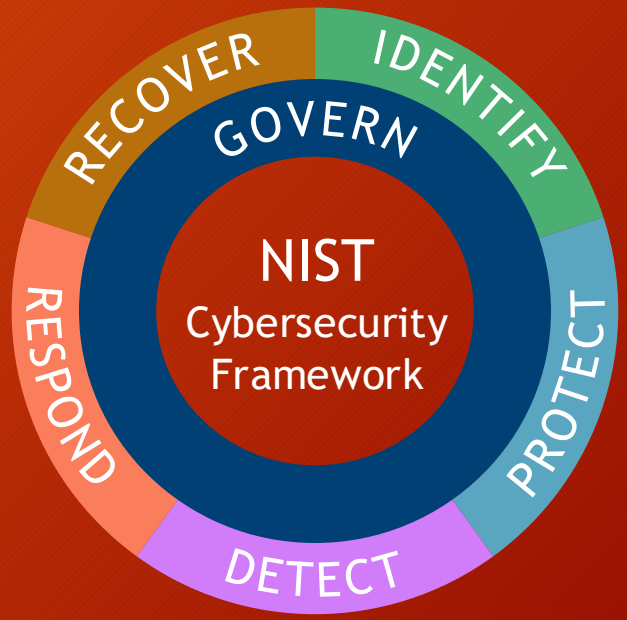
Frameworks As Our Guide

A good framework forces a deliberate, step-by-step analysis.

It forces the lazy System 2 to wake up and follow a logical path.

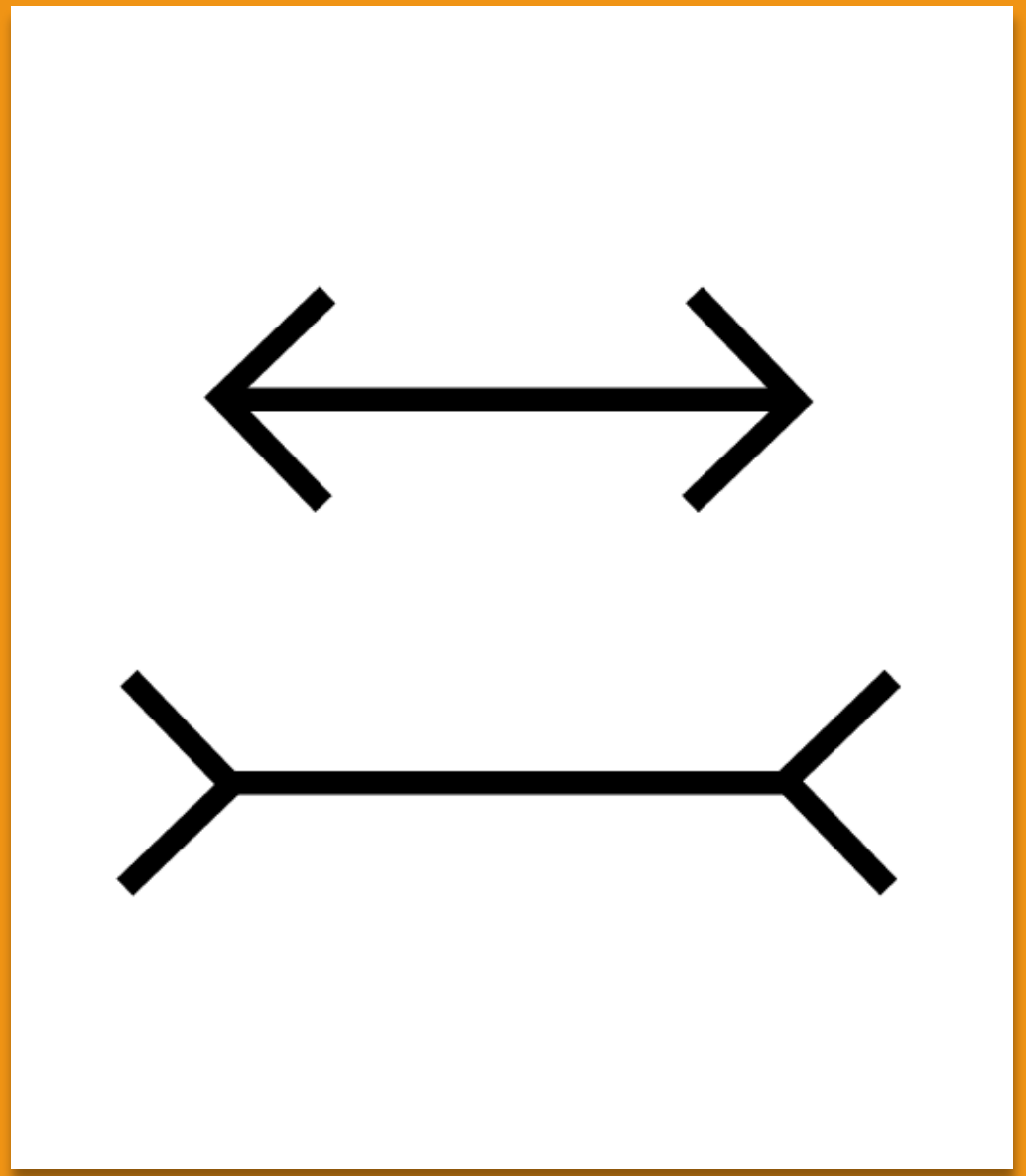
The NIST Framework for Structured Thinking

A tool like NIST helps us adopt the “OUTSIDE VIEW” and ask, "What happened when other people were in this situation before?"



The NIST Framework for Structured Thinking

The very existence of the **'Detect'** and **'Respond'** functions are a direct challenge to this illusion.



Act 3: The More Things Change

……The More They Stay The Same

Why Are We Pursing Posture Perfect ?

- “….because its the **first thing** to do?”
- “….because it’s the **easiest thing** to do”
- “….because it’s the **simplest** activity to measure?”
- “….because **everyone else** is doing it?”

Cloud Isn’t a New Department

Enterprise Security Capabilities

Mission

Enable business through risk reduction and protect the organization's assets, data, and operations from security threats.

What's new with the cloud ?

- How does a team's mission grow, change or morph with the introduction of the cloud?
- What new areas of focus does the team need in order to fulfill their stated mission?

What stays the same ?

- The more that changes the more that stays the same right?
- Are their ways of working a practitioner can expect to stay consistent between on-premises and cloud worlds?

New Tools?

Definitely

Given an expanded scope, are there any new tools either free, commercial, custom or open-source that need to be adopted to carry out the mission?

New Mindset or Skillset ?

- What new skills should practitioners learn to adapt to the changing landscape?
- How should they think differently about the attack surface in order to meet the challenges of the cloud

“A throughline exists between the patch levels of applications, operating systems and the resource configuration status in the cloud”

The **natural evolution** of a Vulnerability Management Program

The Evolution of Vuln Management - **Posture**

The Next 15 Years Can’t Look Like the Last

A select few are tasked with ‘Cloud Security’:

Exposure to cloud risk only is minimally addressed despite burning a lot of calories

Getting Off the Hamster Wheel

Recognize	Recognize the diminishing returns of ANY single-pronged strategy
Use	Use frameworks like NIST to engage System 2's deliberate brain
Don't create	Don't create a siloed 'Cloud Security Team'

The Power of Now

We overvalue immediate rewards and undervalue future ones

THANK YOU