

RSA® Conference 2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: HUM-T02

How Behavioral Economics Can Help Make Better Security Decisions

Kelly Shortridge

Senior Principal Product Technologist
Fastly
@swagitda_

Sounil Yu

CISO & Head of Research
JupiterOne
@sounilyu



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 LLC 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.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

A photograph of a brown and white cat sitting on a textured blue surface, looking down at a small lizard on the ground. The cat's front paw is extended towards the lizard. The lizard is brown with a patterned tail.

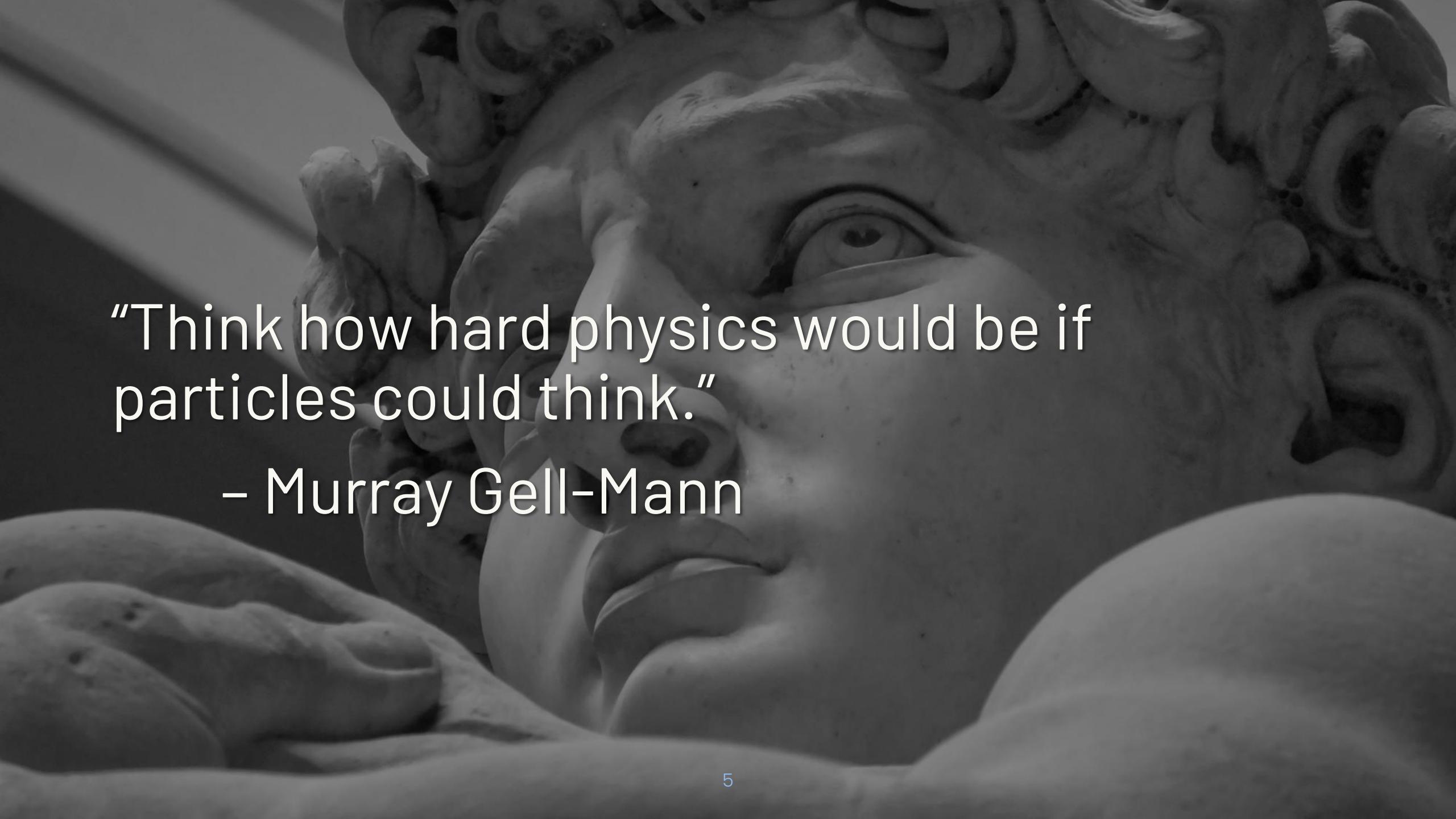
Hi, I'm Kelly
fastly.

A close-up photograph of a Burrowing Owl. The owl has large, bright yellow eyes and a white face with dark brown spots. It is perched on a branch, showing its brown and white patterned feathers. A distinctive feature is its large, reddish-pink gular sac, which it appears to be inflating or using to communicate. The background is a soft-focus green, suggesting a natural, outdoor environment.

Hi, I'm Sounil

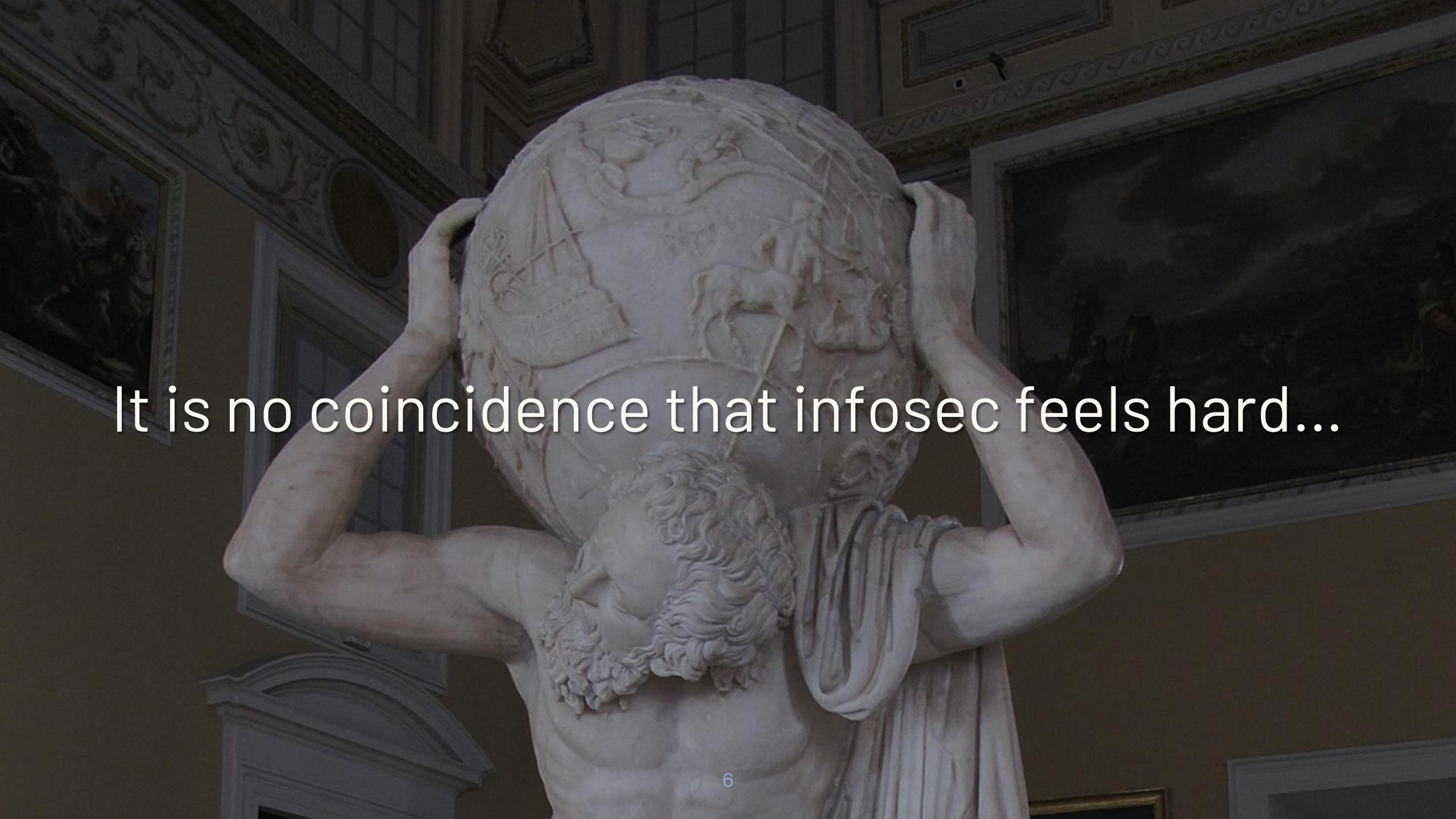


JupiterOne

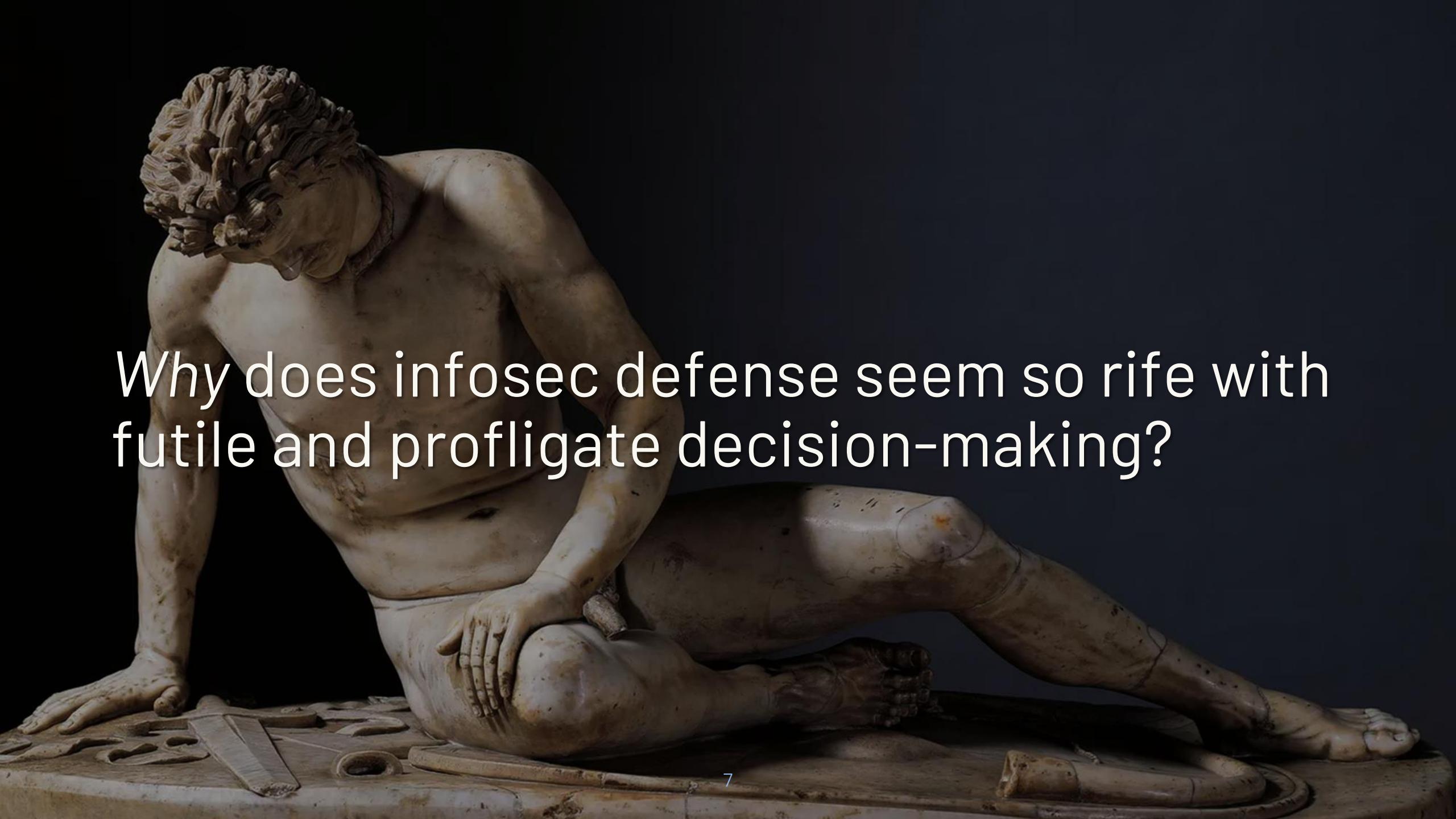


“Think how hard physics would be if particles could think.”

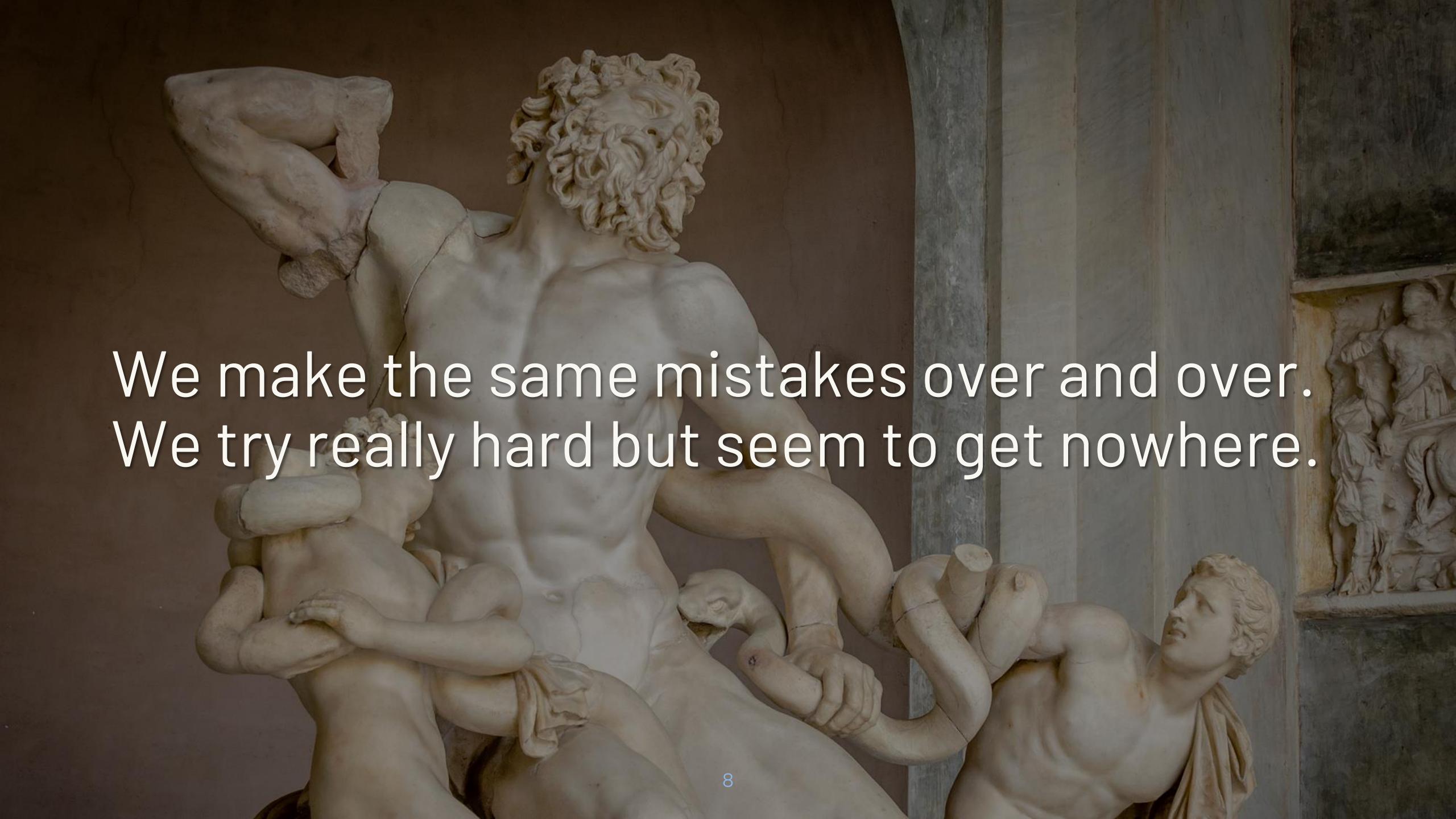
- Murray Gell-Mann

A large, white marble statue of a muscular man, likely a soldier or a deity, is shown from the waist up. He is in a dynamic pose, with one arm raised and bent, holding a circular shield. The shield features a relief of a horse and a temple-like structure. His other arm is bent at the elbow, with his hand near his face. He has curly hair and a determined expression. The background is a dark, ornate room with architectural details like cornices and a painting on the left.

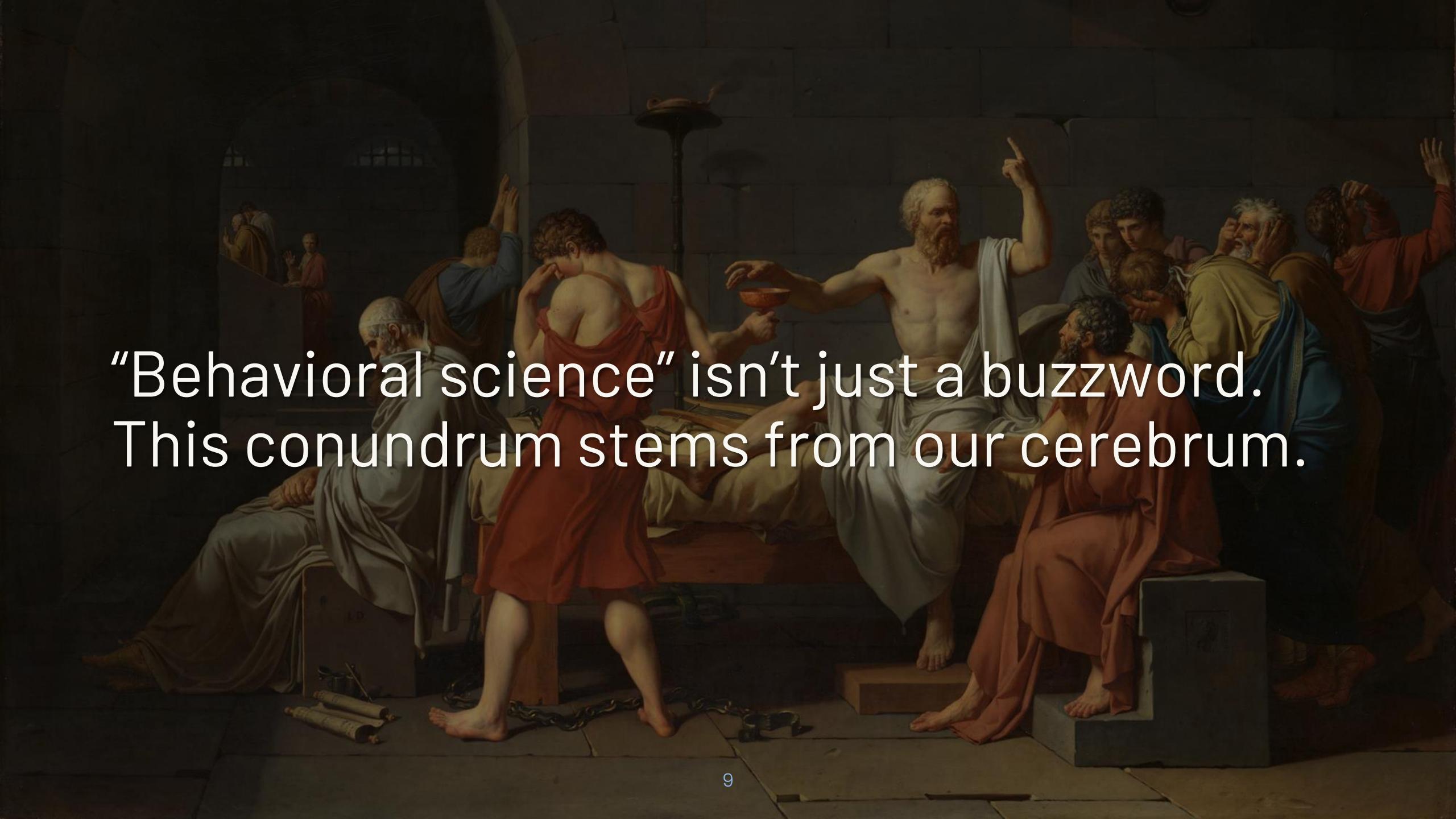
It is no coincidence that infosec feels hard...



Why does infosec defense seem so rife with
futile and profligate decision-making?



We make the same mistakes over and over.
We try really hard but seem to get nowhere.



“Behavioral science” isn’t just a buzzword.
This conundrum stems from our cerebrum.

A painting depicting a scene from a classical epic, likely the Iliad or Odyssey. It shows a multi-oar warship on a dark, choppy sea. In the foreground, several crew members are visible, their faces strained as they row. One man in the center foreground wears a purple cloak and looks towards the stern. Another man in a white tunic stands at the stern, holding a long pole or oar. The ship's hull is dark wood, and its sails are partially unfurled, showing intricate patterns. The background is filled with the turbulent blue and green waves of the sea under a cloudy sky.

Appreciating our brain behavior better is
how we bolster superior security strategy.

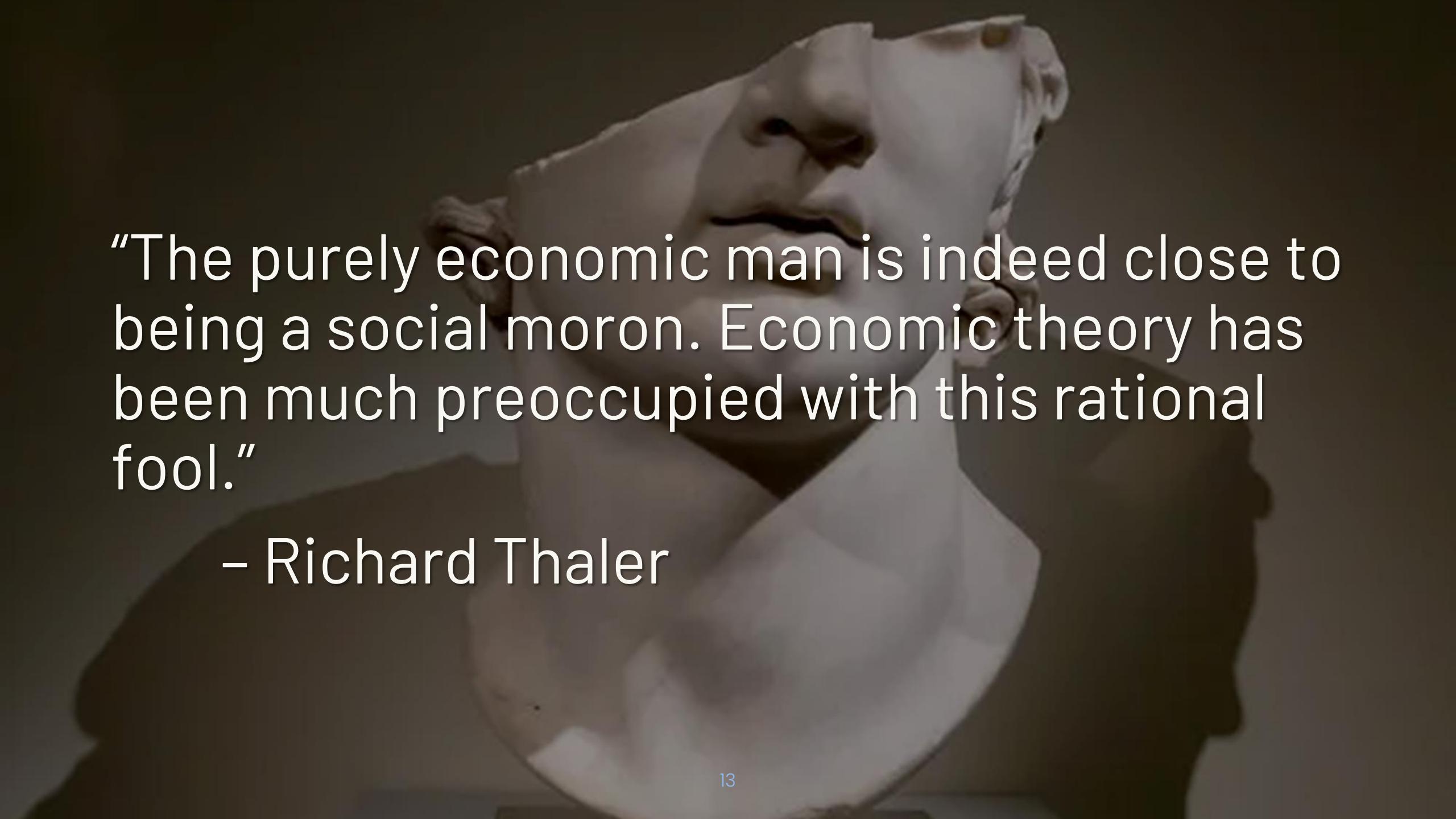
I. How do our brains work?

II. Lizard Brain vs. Philosopher

III. Making better decisions

A close-up photograph of a gecko's head, showing its large, bulging eyes and textured skin. The gecko has a yellow and brown patterned skin. The background is blurred.

I. How do our brains work?



“The purely economic man is indeed close to being a social moron. Economic theory has been much preoccupied with this rational fool.”

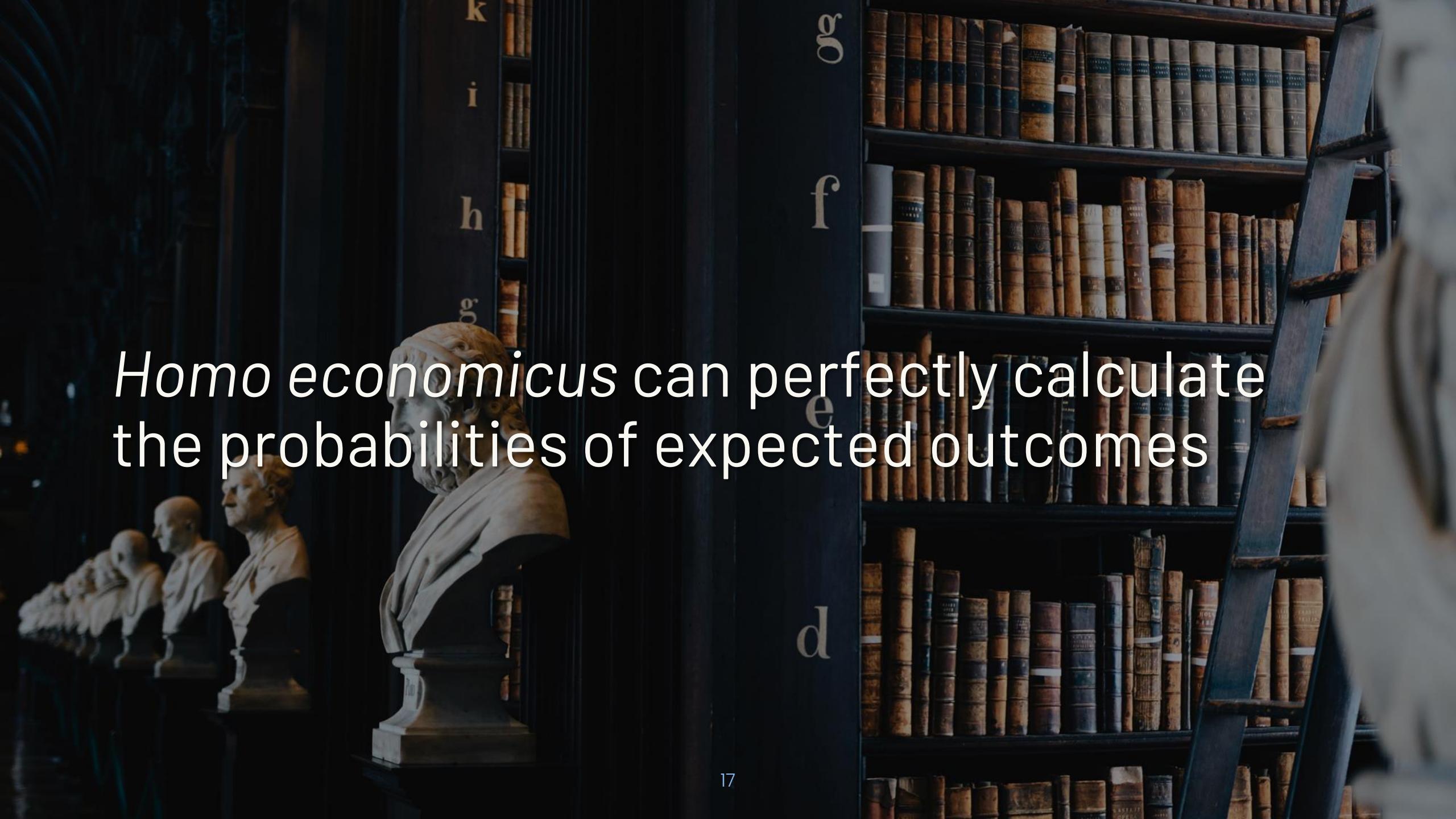
– Richard Thaler

So, what do we mean by rationality here?



Behavioral economics studies how people
actually make decisions vs. classical theory

In theory, every human makes choices to maximize their payoff (expected “utility”)



Homo economicus can perfectly calculate
the probabilities of expected outcomes

In reality, information, attention, and time
are all limited. Our rationality is “bounded.”

A painting of a woman with dark hair, wearing a blue dress, sitting at a desk and holding a book. She is looking upwards and to the right with a thoughtful expression. The background is dark and indistinct.

Every human (even you!) is only *locally*
rational – *global* rationality is a fantasy.

Spoiler: a *lot* of “human error” is a violation of what’s considered “globally” rational...

Understanding how our behavior deviates
from *Homo economicus* matters for infosec

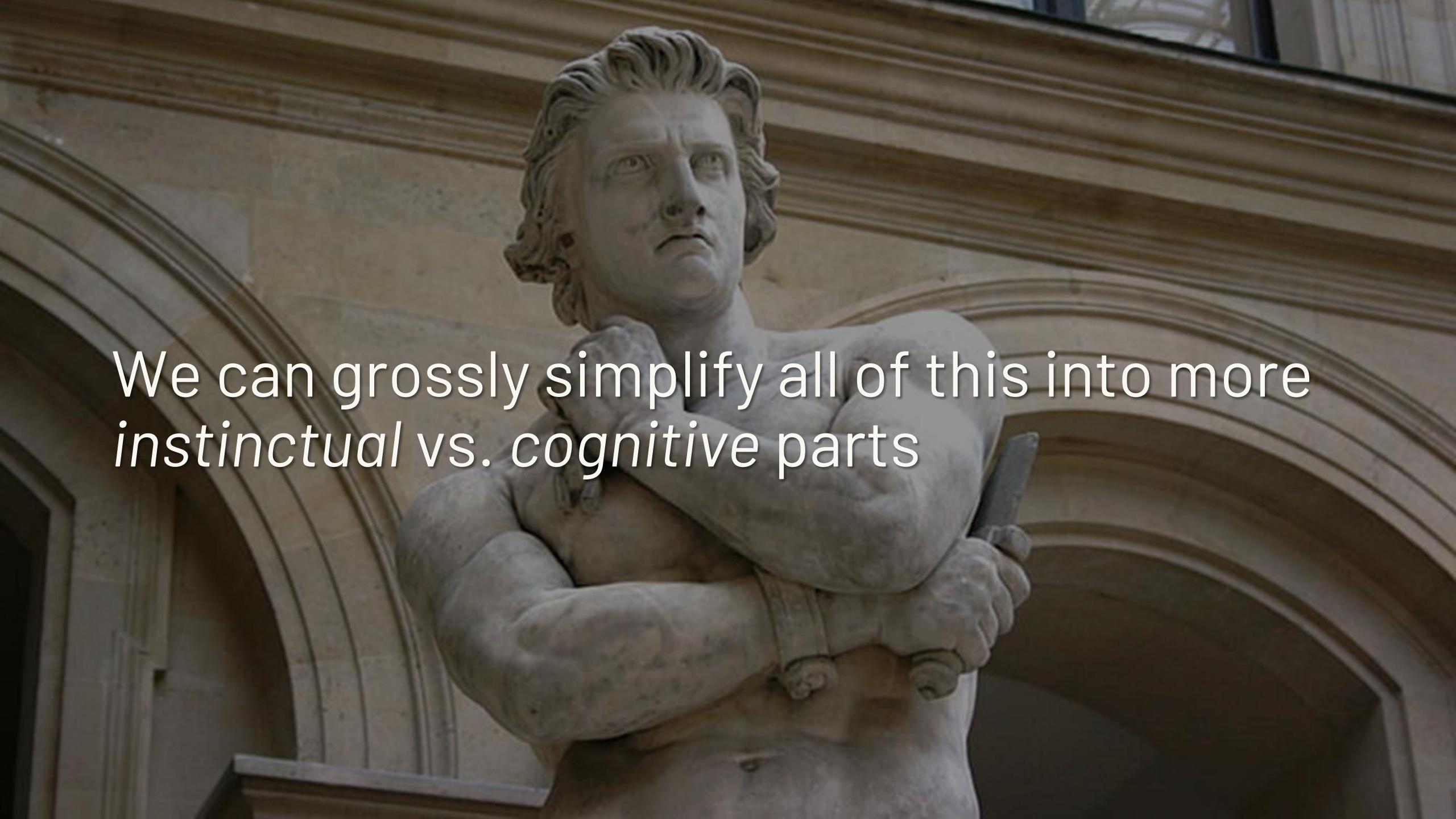


Evolution designed our brains for efficiency,
not for pure logic (or we'd die in the wild)

We were once very simple creatures with
very simple functions (eat food! run away!)



Then we evolved more complex processing
(gossip with tribe! envision the future!)

A detailed statue of a muscular man with curly hair, wearing a loincloth, stands prominently in the center. He is holding a large, circular shield in his left arm, which features a prominent red cross. His right arm is bent, with his hand resting near his shoulder. The statue is set against a background of light-colored, curved architectural elements, possibly a ceiling or a series of arches.

We can grossly simplify all of this into more
instinctual vs. cognitive parts

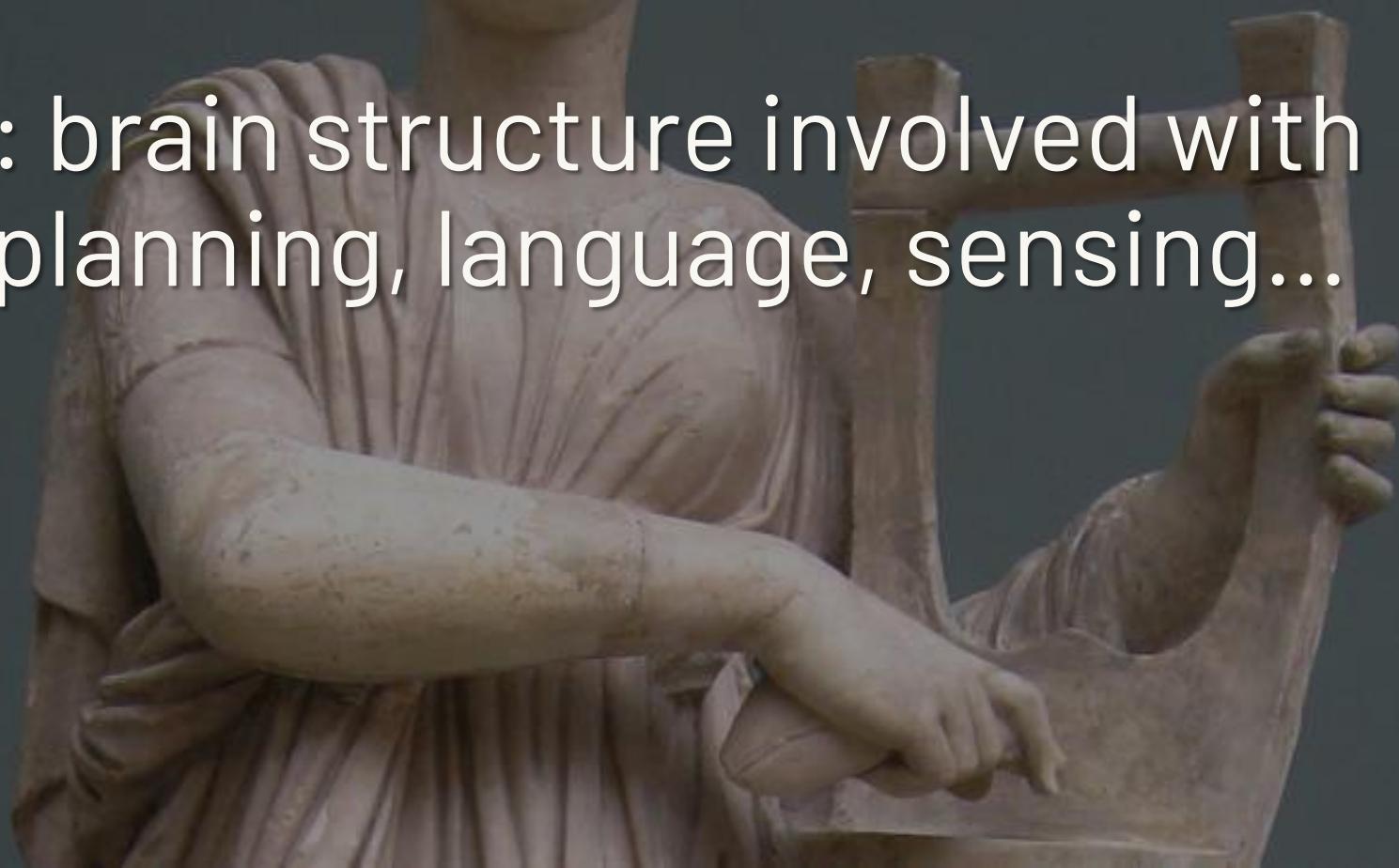
Our ability to imagine the future – and our
future selves – is the most recently evolved

A close-up photograph of a lizard's head, likely a spiny-tailed lizard, showing its yellow and brown patterned scales, a prominent eye, and several sharp spines on its forehead and neck. The background is dark and out of focus.

Protoreptilian brain: self-regulate biological functions to maintain stability for survival

Limbic system: brain structures involved with survival behaviors (fight, feed, f...)

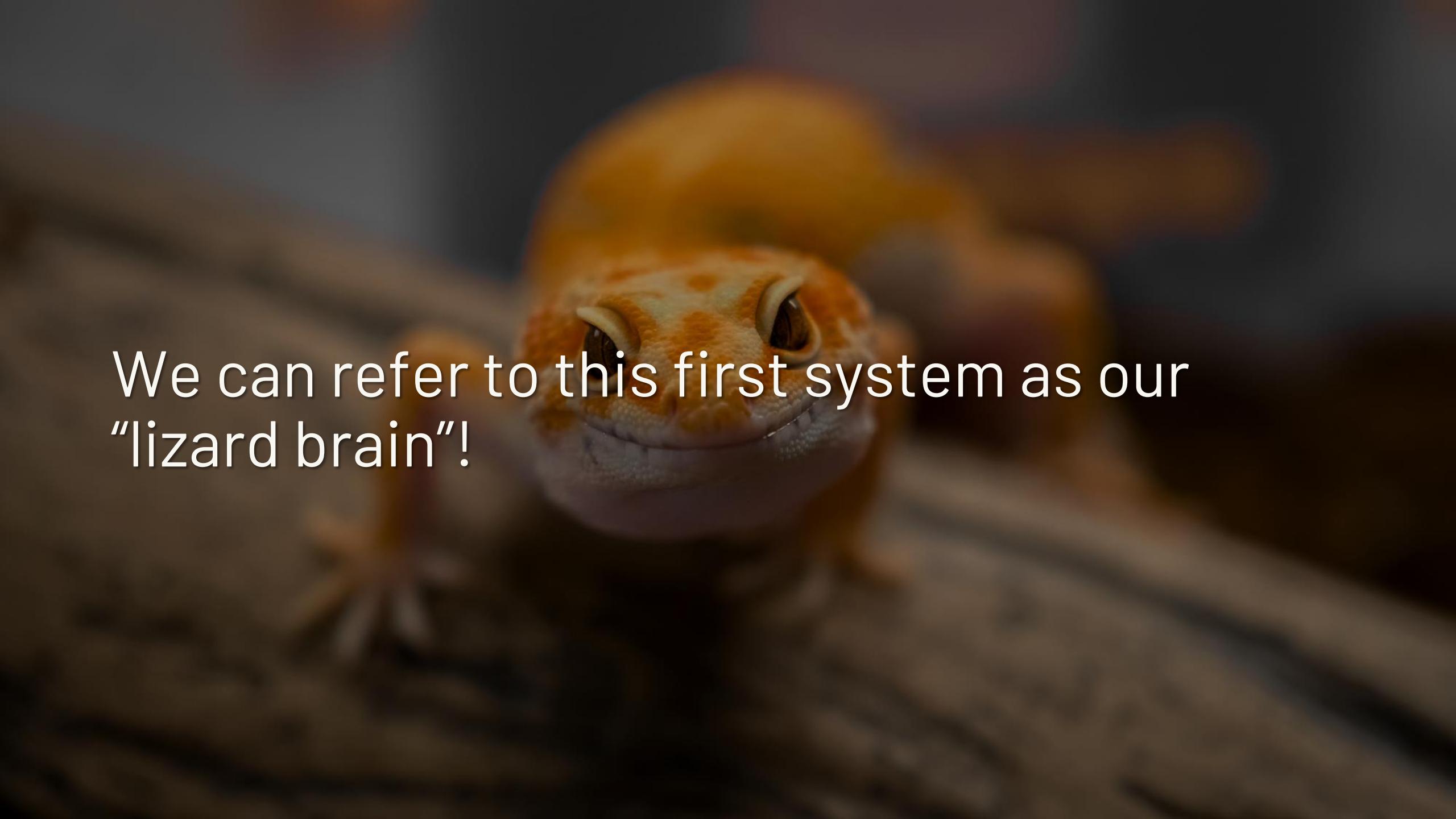
Neocortex: brain structure involved with cognition, planning, language, sensing...



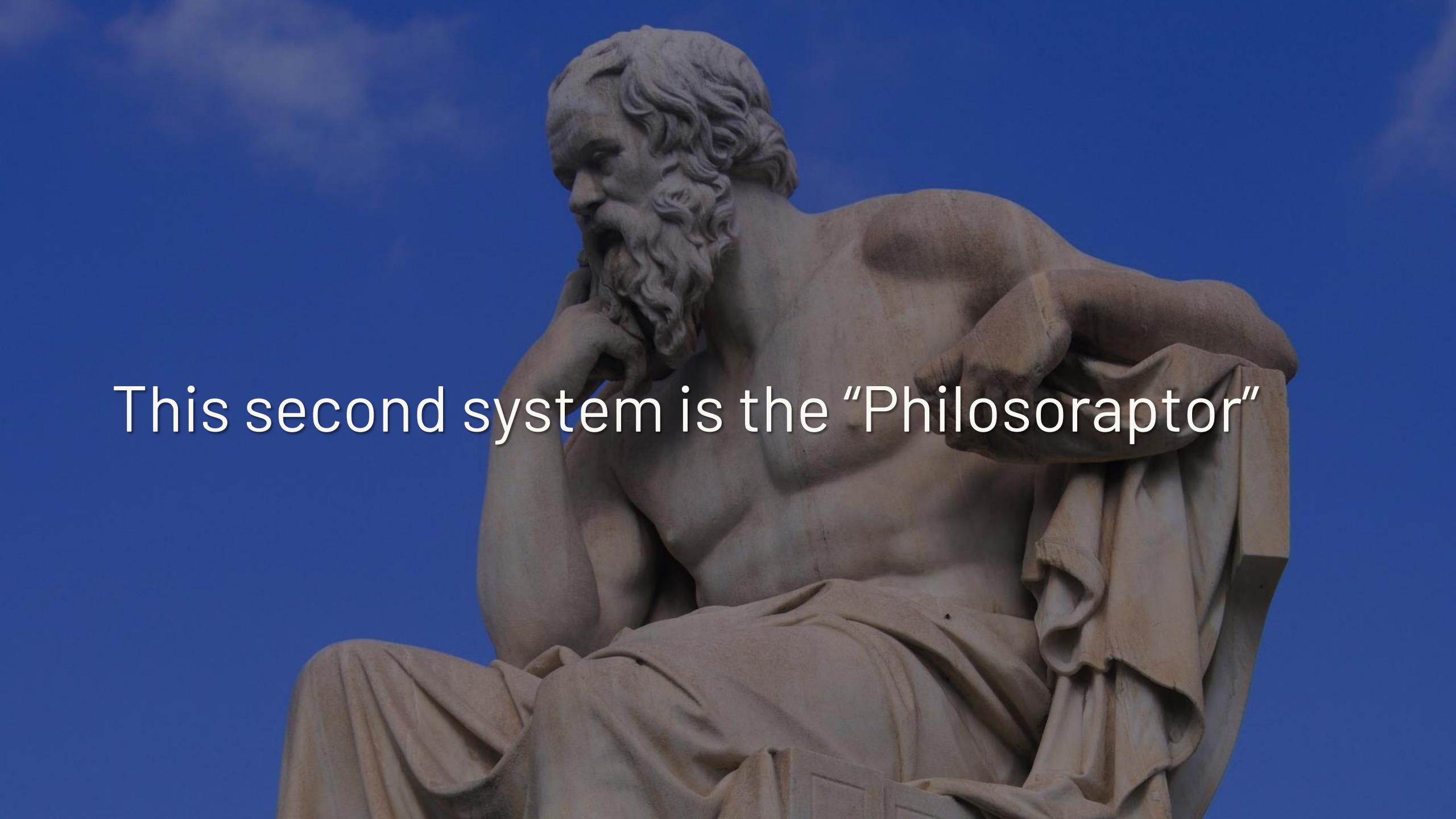
But we usually simplify our brains into two systems for thinking: System 1 & System 2

System 1 = quick, automatic, unconscious;
wants fast, easy, simple thinky thinky

System 2 = effortful thinky thinky; cognition
and purposeful choices vs. instincts



We can refer to this first system as our
“lizard brain”!



This second system is the “Philosopher”

Lizard brain decides to stay up super late
playing video games after a tough week.

Philosoraptor decides to go to bed early and have a refreshing workout in the morning.

As you might suspect, Lizard Brain and
Philosoraptor disagree on infosec choices...

A bronze sculpture of a lizard brain, featuring a small, detailed head and a large, textured, segmented body. The sculpture is positioned in front of a grand, classical building with white columns and a glass roof.

II. Lizard Brain vs. Philosoraptor

How do the Lizard Brain (LB) and Philosoraptor (PR) manifest in infosec?



LB: Heuristics, shortcuts, and folk wisdom

PR: Experimental evidence and analysis



LB: Vulns are predators! They threaten our survival! Eradicate them at all costs!

PR: Non-emotional framing of vulns, use of analogies, focus on impact vs. vague “risk”



LB: Success = no danger ever! Stay safe
within the cave and never leave it

PR: Success = support adaptive cycles,
enable sustainable growth and innovation



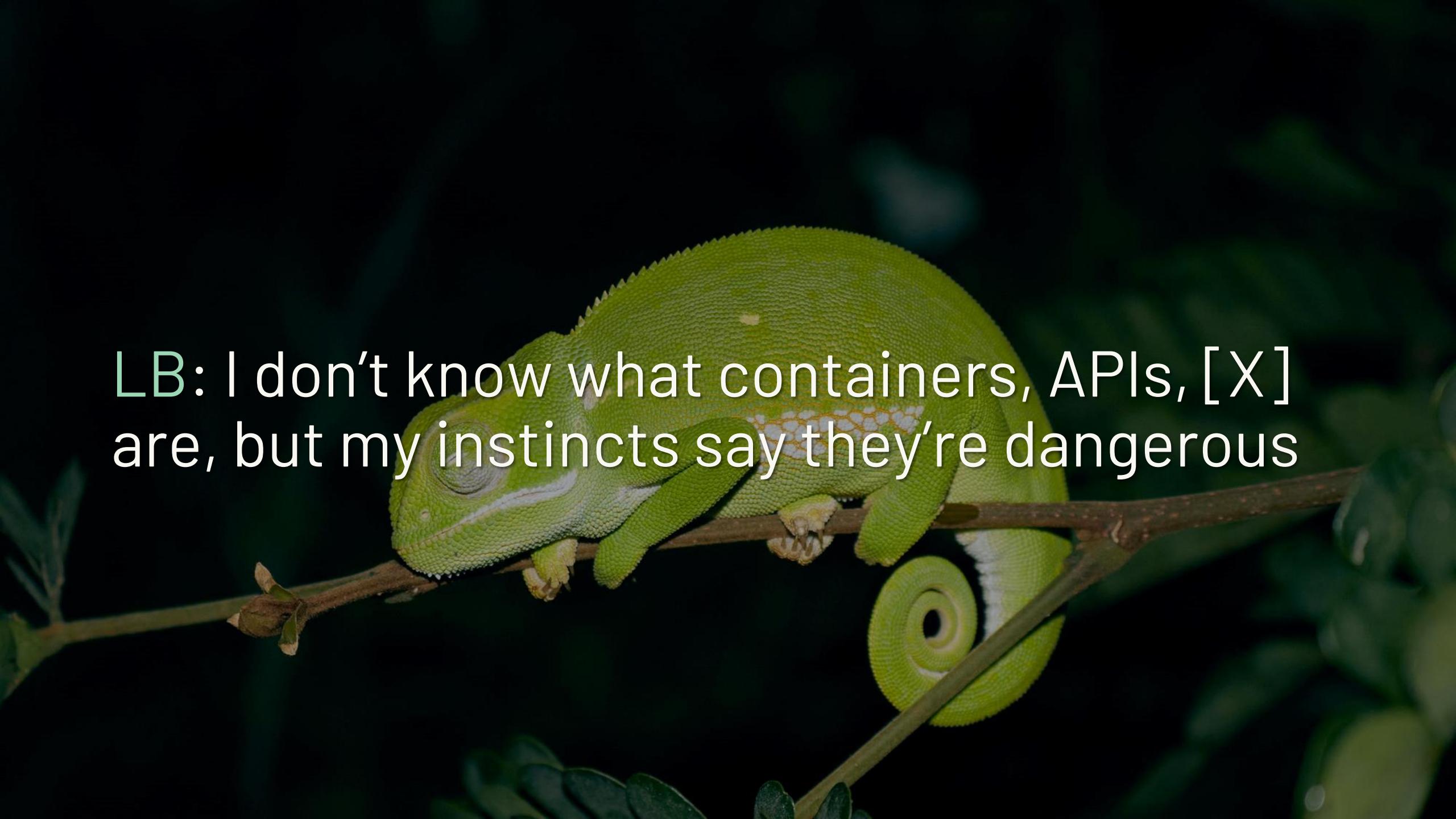
LB: Thoughtful metrics are hard; therefore,
let's use shallow ones for less thinky thinky

PR: Nuanced view of metrics that considers context and complexity of systems



LB: Tribal mindset – Gatekeeping other tribes, hoarding knowledge, bottlenecks

PR: Village mindset – neocortex brain seeks connection and collaboration to build things

A close-up photograph of a bright green chameleon perched on a thin, light-colored branch. The chameleon's body is curved, with its head turned slightly to the left. Its skin has a distinct granular texture. The background is dark and out of focus, making the green color of the lizard stand out.

LB: I don't know what containers, APIs, [X]
are, but my instincts say they're dangerous

PR: Seeks evidence, asks questions with an open mind, ponders new ways to do things



LB: Familiarity = importance. I've heard it a lot and can recall it easily, so it must be true.

PR: Familiarity is successful marketing and doesn't indicate importance or truthfulness.



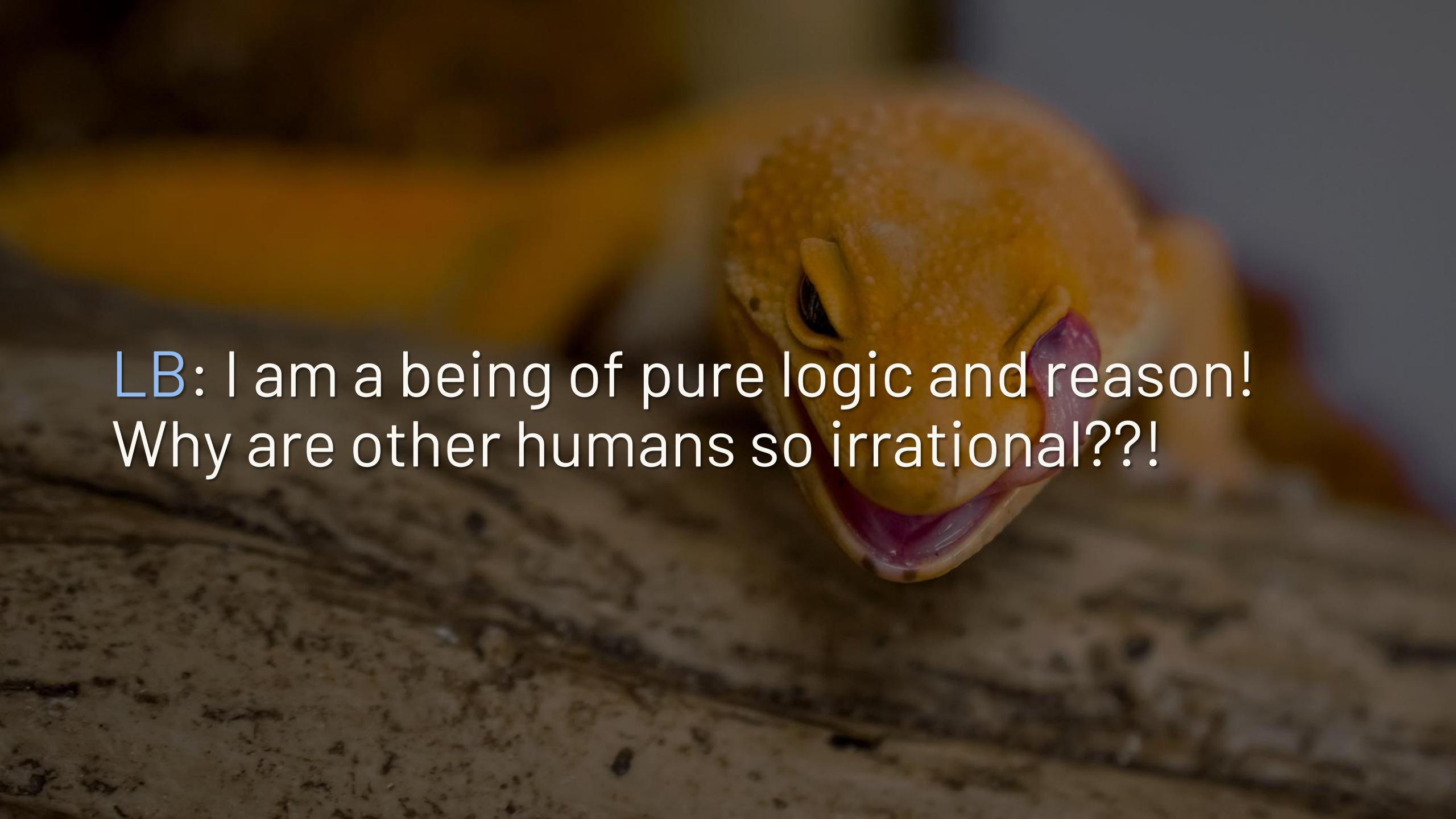
LB: Autonomic nervous system triggers
fight or flight response

PR: Rest and digest response – mindful handling of stress (psychological resilience)



LB: Perfect prevention of failure is the way

PR: Nothing is perfect; what matters is preparing for recovery

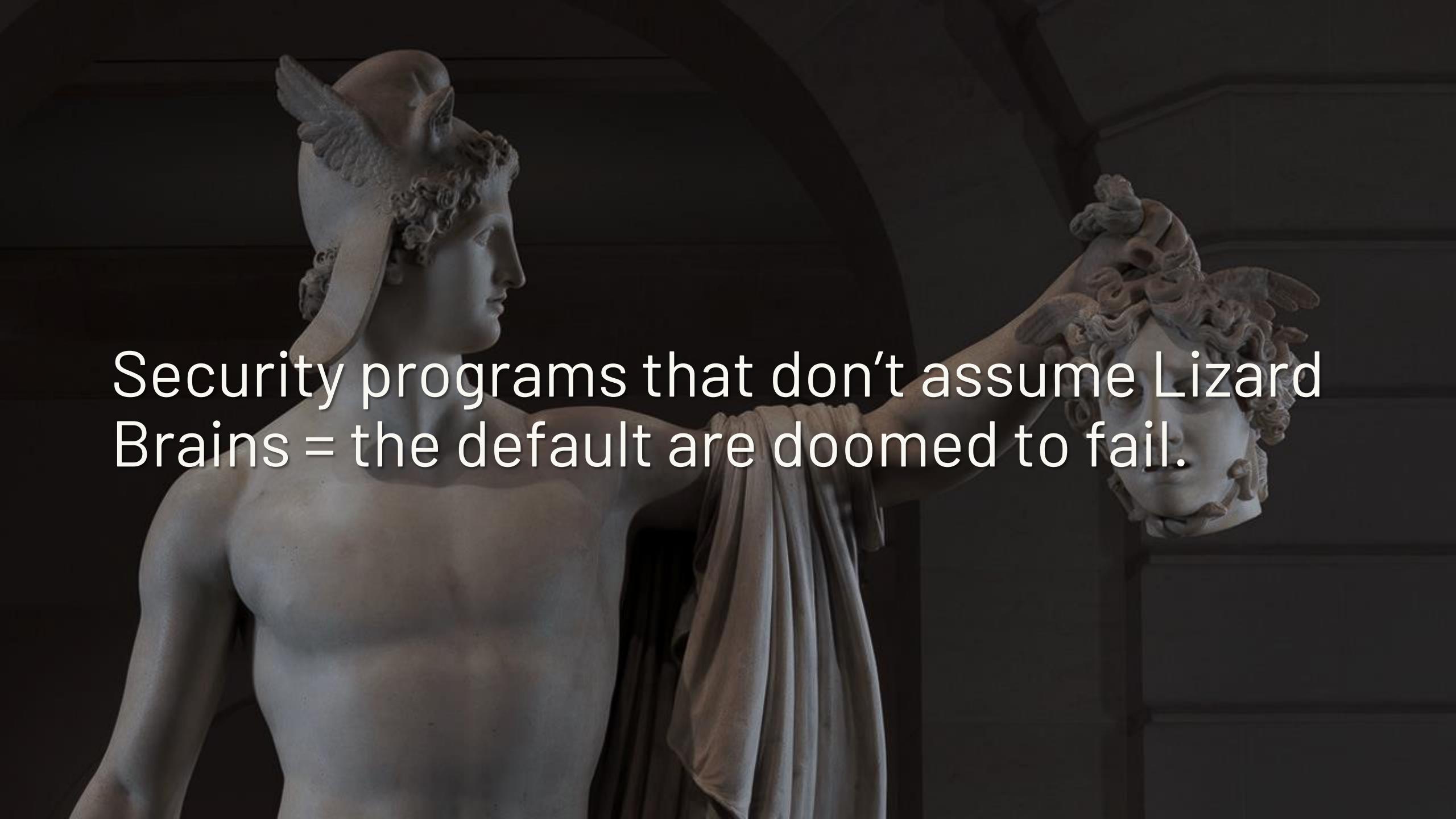


LB: I am a being of pure logic and reason!
Why are other humans so irrational??!

PR: Lizard brains are the default; we can't force humans to change their programming

A dark, moody painting of a figure in a white, flowing robe, possibly Jesus, standing on a rocky shore. The figure is shown from the waist up, looking out over a body of water under a heavy, cloudy sky. The lighting is low, creating strong shadows and highlights on the figure's clothing and the surrounding environment.

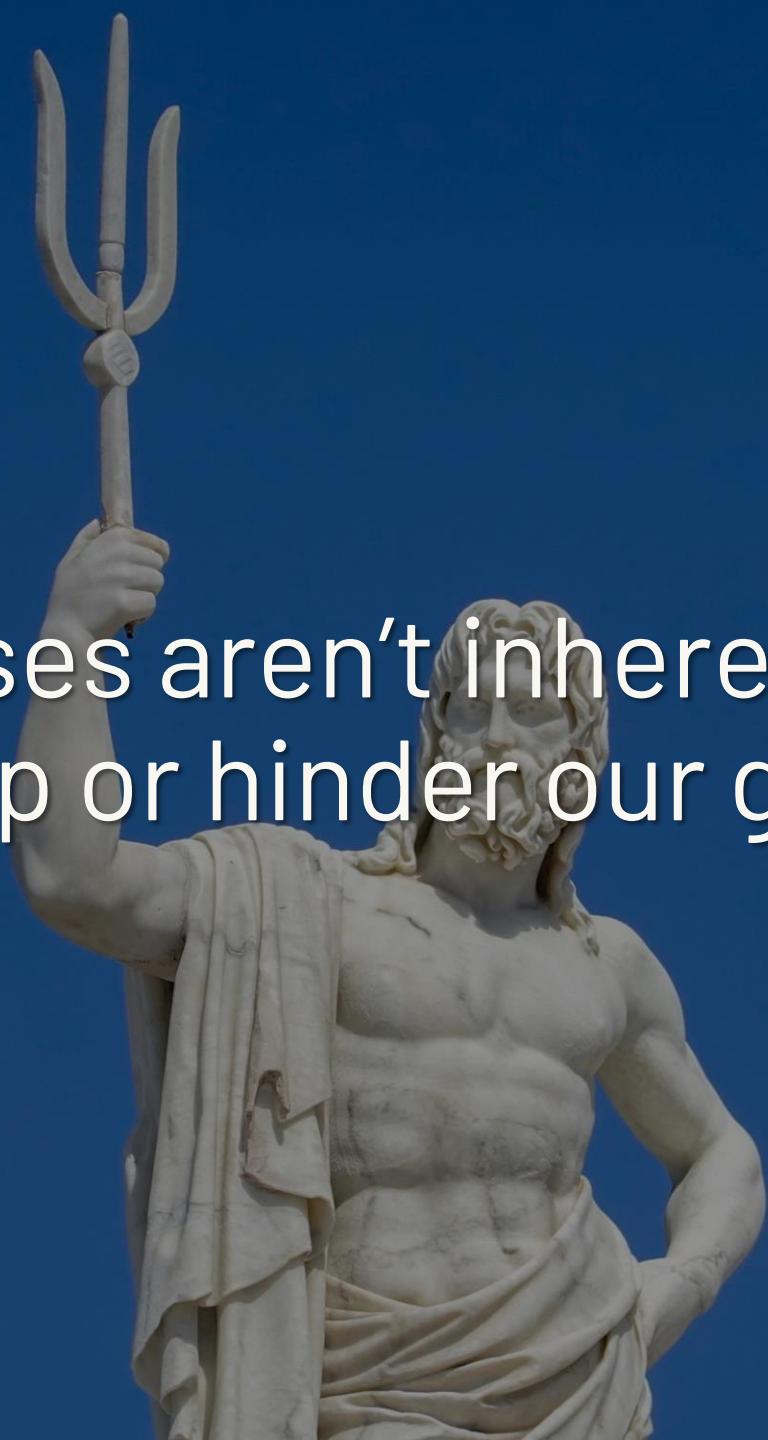
III. Making better decisions

The background is a dark, atmospheric scene featuring two classical stone statues. On the left, a winged Victory (Fame) is shown in profile, her right arm raised. On the right, a Medusa head with a snake for hair and a winged horse (Pegasus) emerging from its mouth is partially visible.

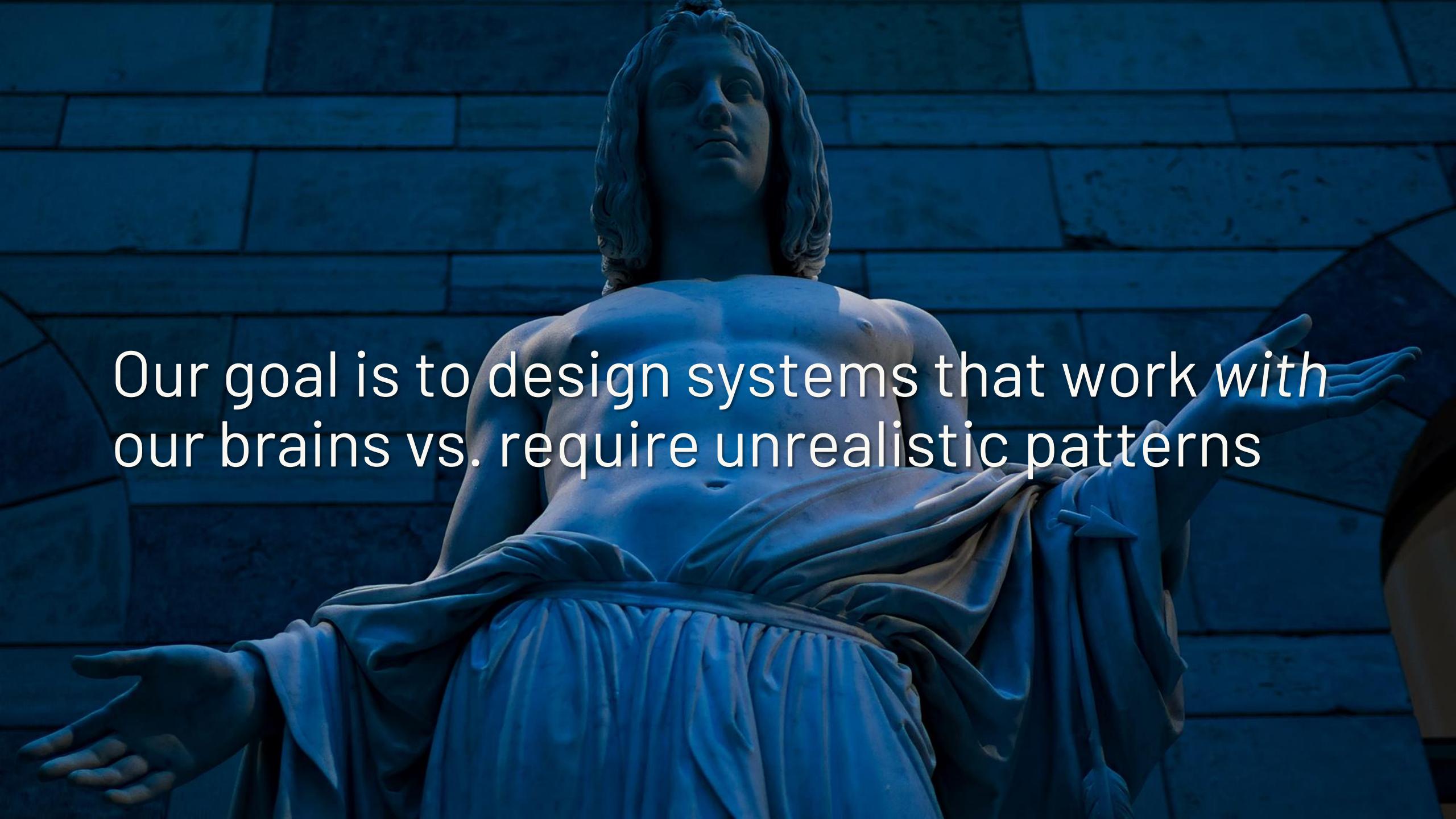
Security programs that don't assume Lizard
Brains = the default are doomed to fail.

(And our Lizard Brains tell us that we really
don't want to fail!)

Cognitive biases aren't inherently bad; they can either help or hinder our goals

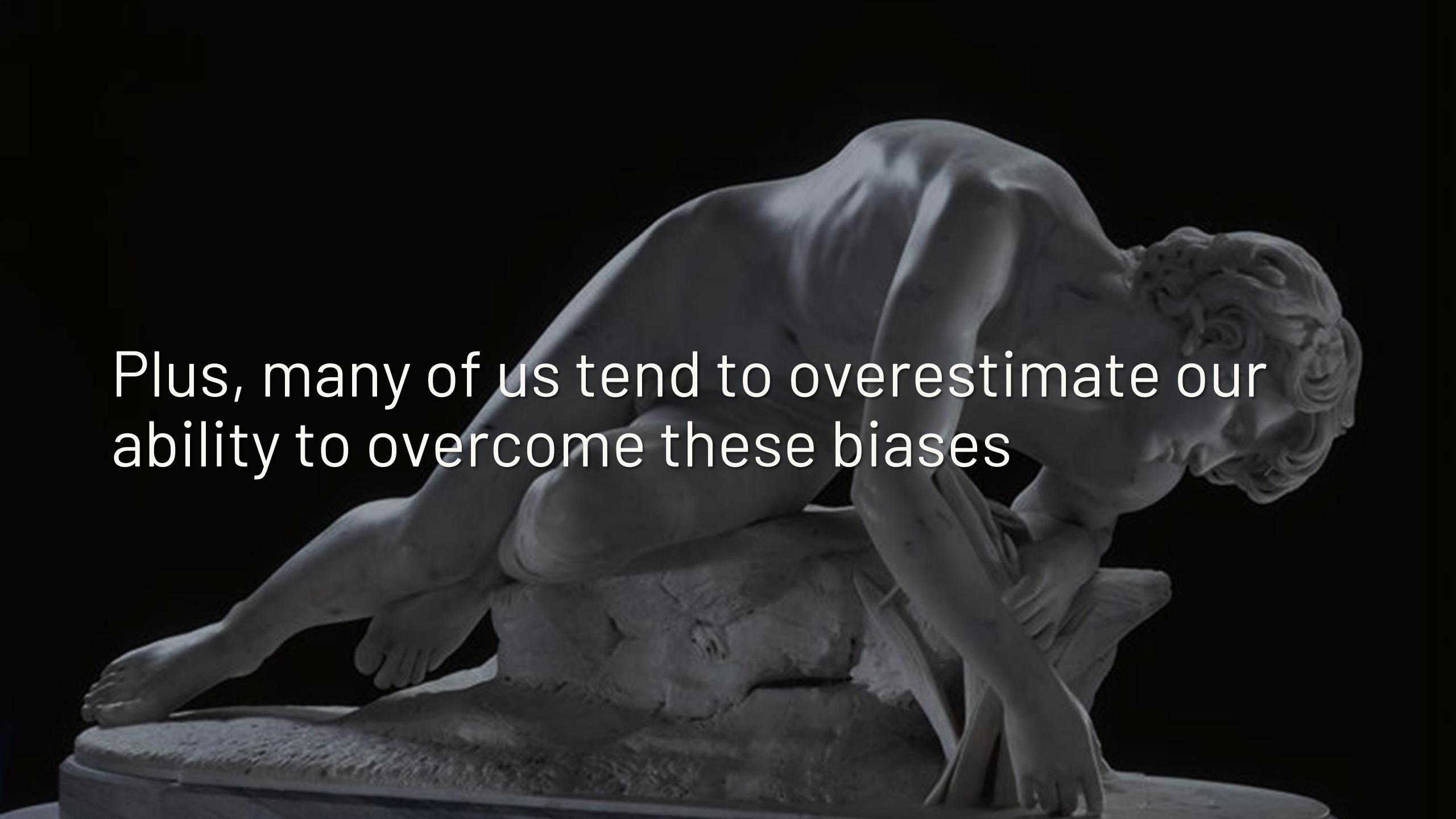


Viewing instincts and emotions as “wrong” thinking will also distort decision-making

A statue of David by Michelangelo, shown from the waist up, looking upwards with arms slightly outstretched.

Our goal is to design systems that work with
our brains vs. require unrealistic patterns

Being aware of cognitive bias isn't enough.
The human brain sucks at self-monitoring.



Plus, many of us tend to overestimate our ability to overcome these biases

(It's still good to be on the lookout, so long
as you remain aware you can be a fool, too)

A classical stone sculpture depicting a woman and a child running away from a large lizard. The woman, on the right, is in a dynamic pose with one arm raised and her body angled back. The child, on the left, is also in motion, looking back over their shoulder. The lizard is shown in a detailed, realistic style, its body coiled and head raised towards the figures. The scene is set against a dark, architectural background with a window visible in the upper right.

We must make the “right way” compatible
with the lizard brain - simple, easy, fast

Repetition and practice turns tasks from
Philosoraptor processes into LB instincts

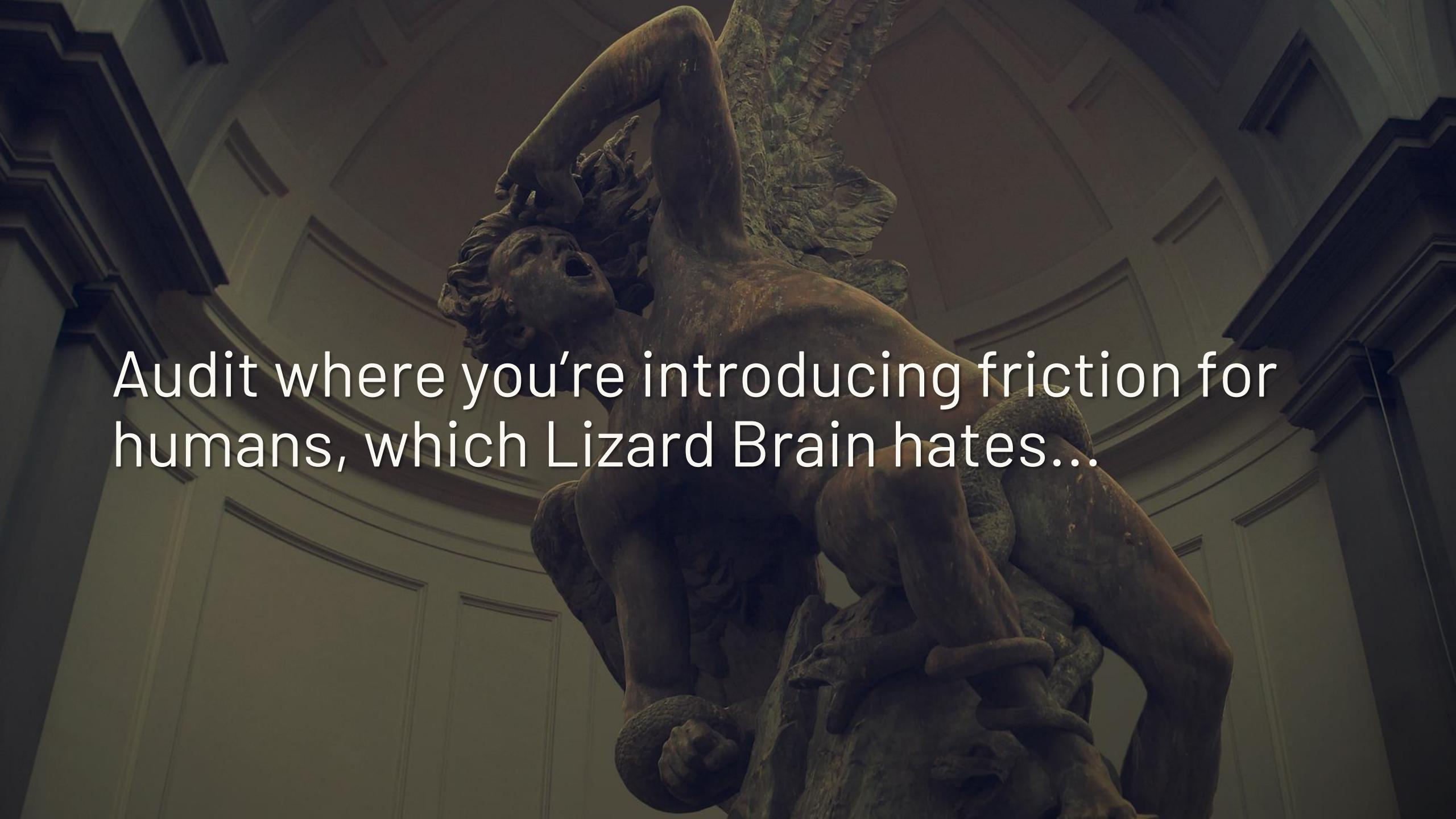
But, repetition needs immediate feedback
in order for it to satisfy the lizard brain

Exploit availability bias for good – ensure
your messages are repeated and pithy



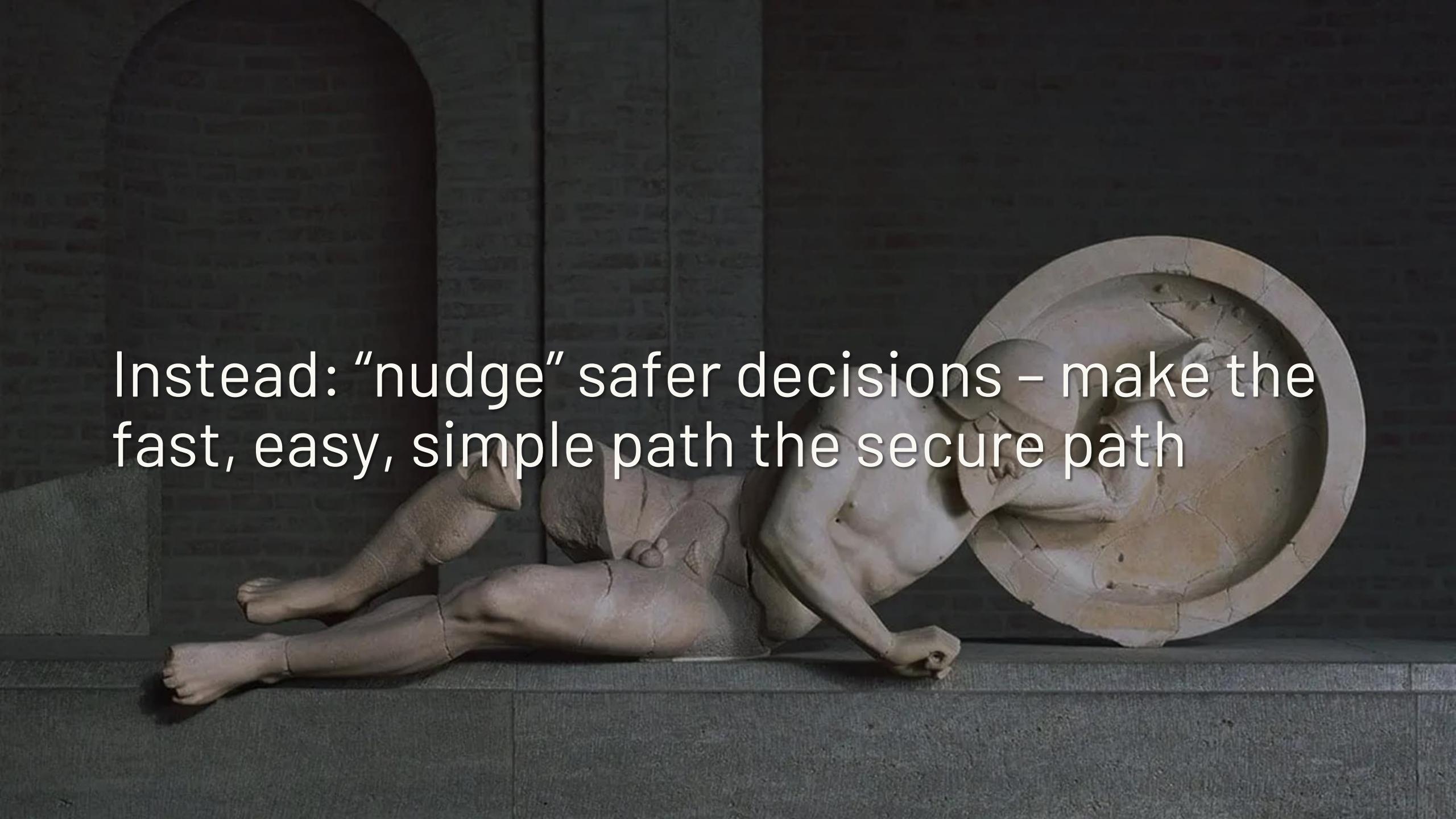
Create your own heuristics... just like we have with Lizard Brain vs. Philosopher :)

Opportunity cost consideration: the “null baseline” is a fast, easy, simple heuristic



Audit where you're introducing friction for humans, which Lizard Brain hates...

Per Richard Thaler: phishing warnings are “sludge”; it’s very natural to ignore them

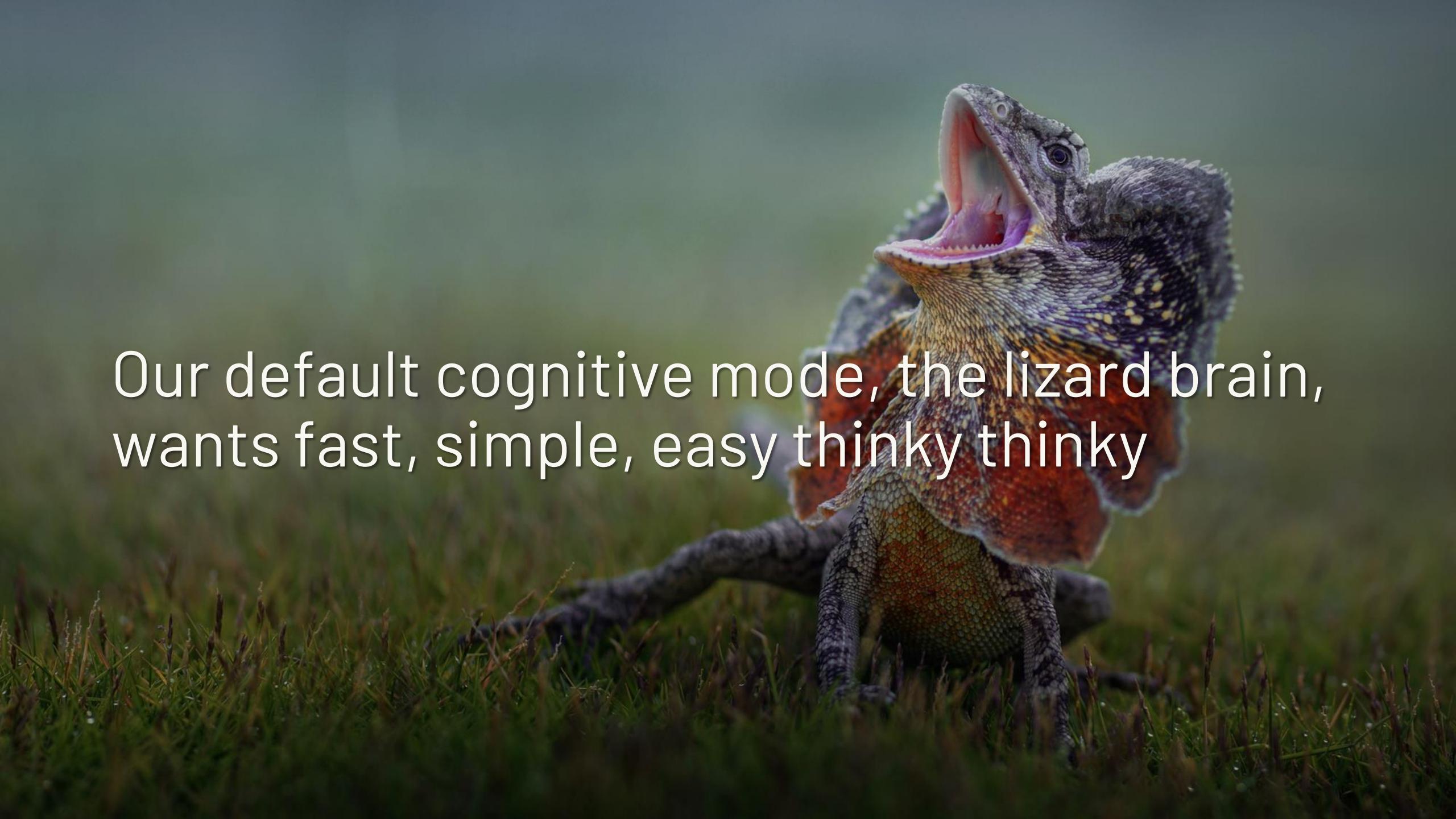
A photograph of a person lying face down on a dark, textured surface, possibly a mat or carpet. The person's body is angled, with their head towards the left and their feet towards the right. They are looking down at a large, circular object, which appears to be a wooden barrel or a circular frame made of wood planks. The lighting is dramatic, with strong highlights on the person's skin and the circular object against the dark background.

Instead: “nudge” safer decisions – make the fast, easy, simple path the secure path

Cognitive biases are chronic, not acute – so
solutions must *manage* rather than “fix”

The background image shows the archaeological site of the Temple of Poseidon at Cape Sounion, Greece. The temple's iconic Doric columns stand silhouetted against a sky filled with warm, orange and yellow hues of a setting sun. The foreground consists of the stone steps leading up to the temple, with some greenery and a few small figures visible.

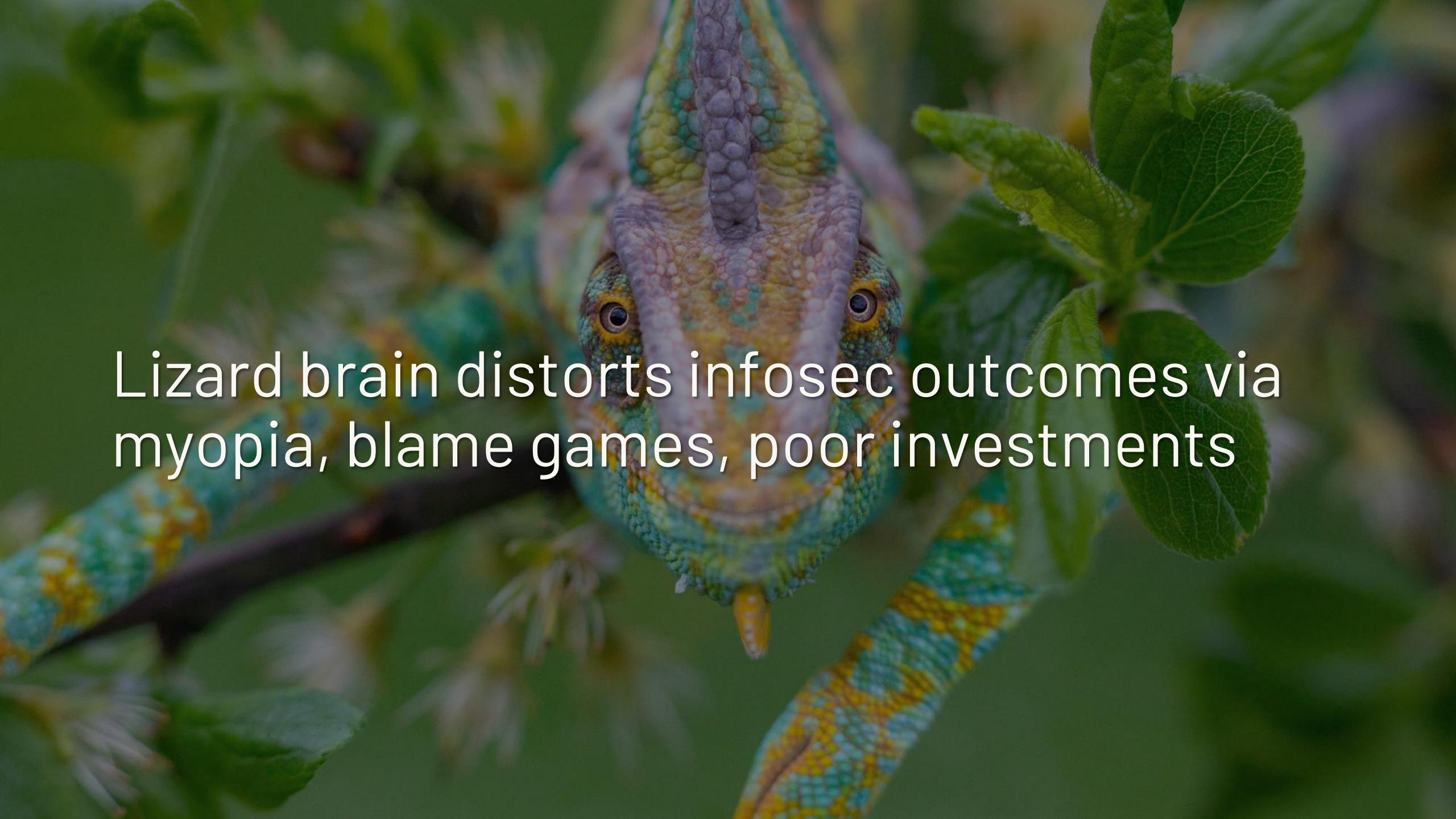
IV. Conclusion

A close-up photograph of a lizard, possibly a frilled lizard, standing in a field of green grass. The lizard's mouth is wide open, showing its tongue and teeth. Its skin is textured with various colors, including shades of brown, orange, and yellow. The background is blurred, making the lizard the central focus.

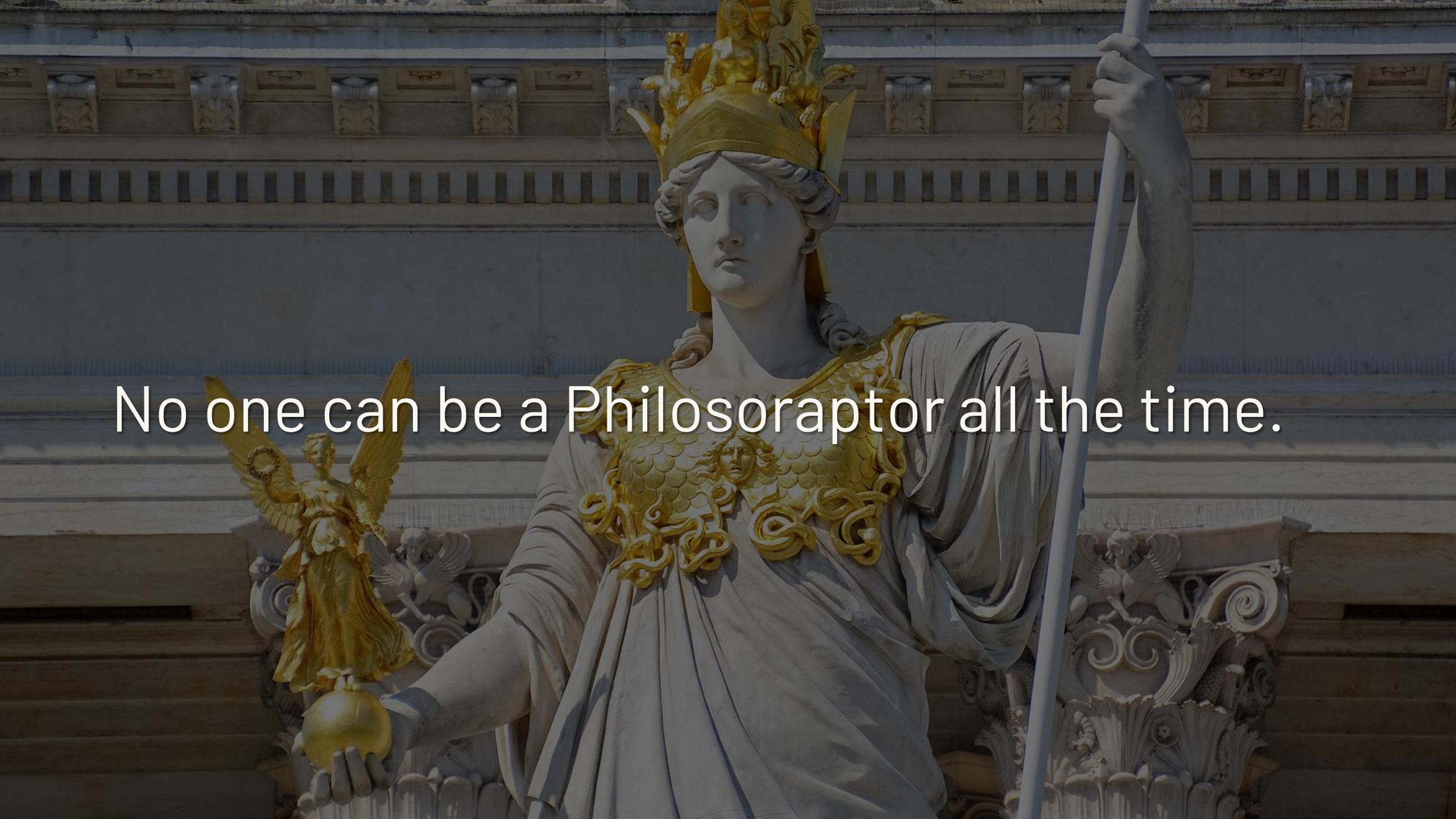
Our default cognitive mode, the lizard brain,
wants fast, simple, easy thinky thinky



Infosec decision making involves a lot of lizard brain because of stress and F.U.D.

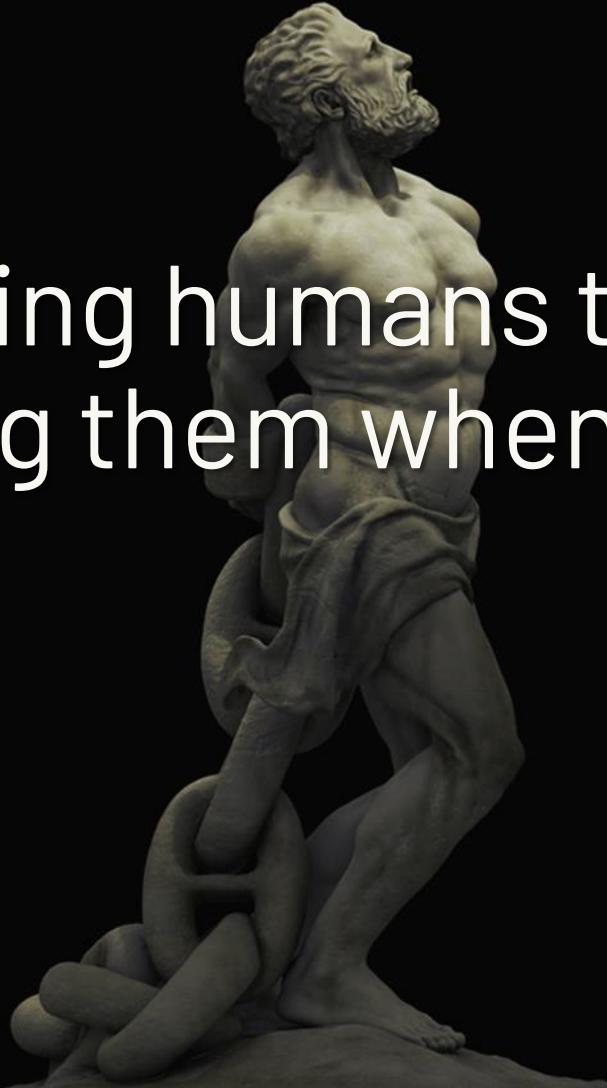


Lizard brain distorts infosec outcomes via
myopia, blame games, poor investments

A large, detailed statue of a classical deity, possibly Athena, stands prominently in the center. She wears an elaborate golden crown and a white robe with gold trim. Her right arm is raised, holding a spear, while her left hand holds a golden sphere. The background features a grand, neoclassical building with intricate carvings and statues.

No one can be a Philosoraptor all the time.

Requiring humans to be “rational” and
blaming them when they’re not is cruel.

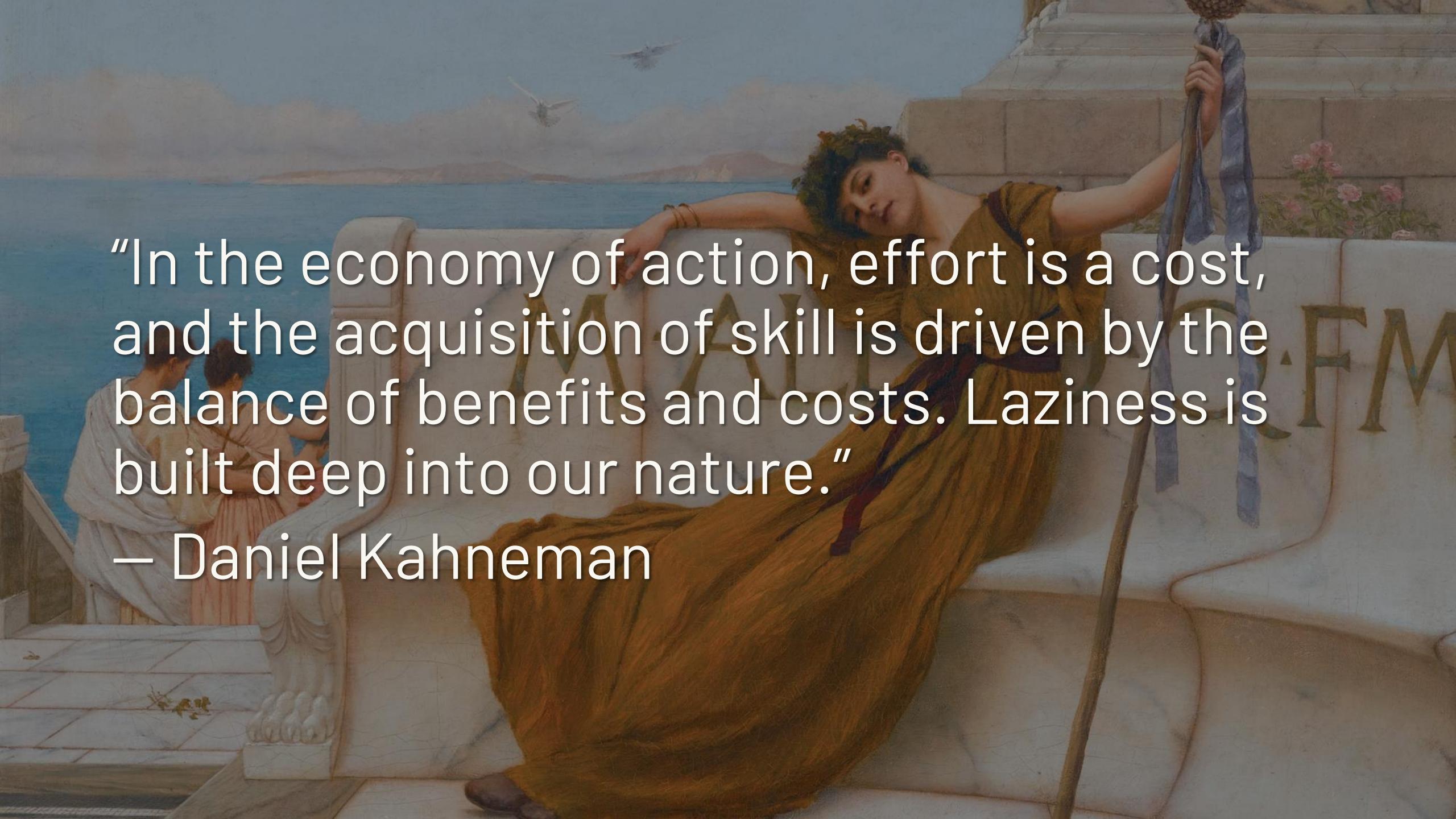


A close-up photograph of a lizard's head, showing its eye and scales, set against a dark background.

We need to design security programs,
policies, and tools for lizard brains instead

A close-up photograph of a lizard with vibrant blue, green, and yellow patterns on its head and neck, perched on a thin, dry branch. The background is a soft-focus, warm-toned landscape.

As security leaders, understand your lizard
brain to optimize your own behavior

A classical painting depicting a woman reclining on a sofa, holding a long staff or spear. She is dressed in a yellow robe and wears a laurel wreath. The background shows a landscape with birds flying over water and distant hills.

“In the economy of action, effort is a cost, and the acquisition of skill is driven by the balance of benefits and costs. Laziness is built deep into our nature.”

– Daniel Kahneman



@swagitda_



@sounilyu



/in/kellyshortridge



/in/sounil



info@kellyshortridge.com



cyberdefensematrix.com