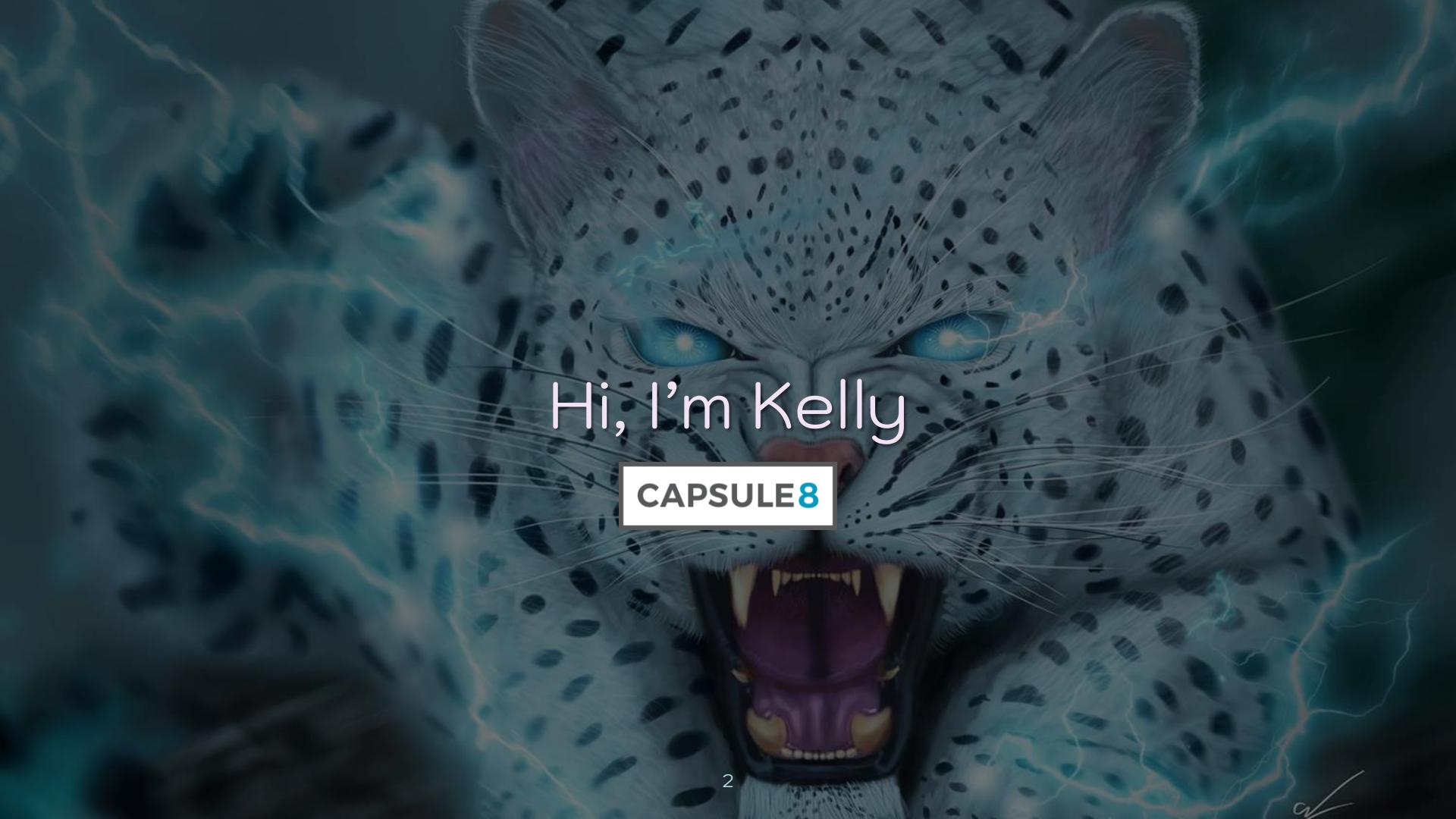


# Controlled Chaos

The Inevitable Marriage of  
DevOps & Security

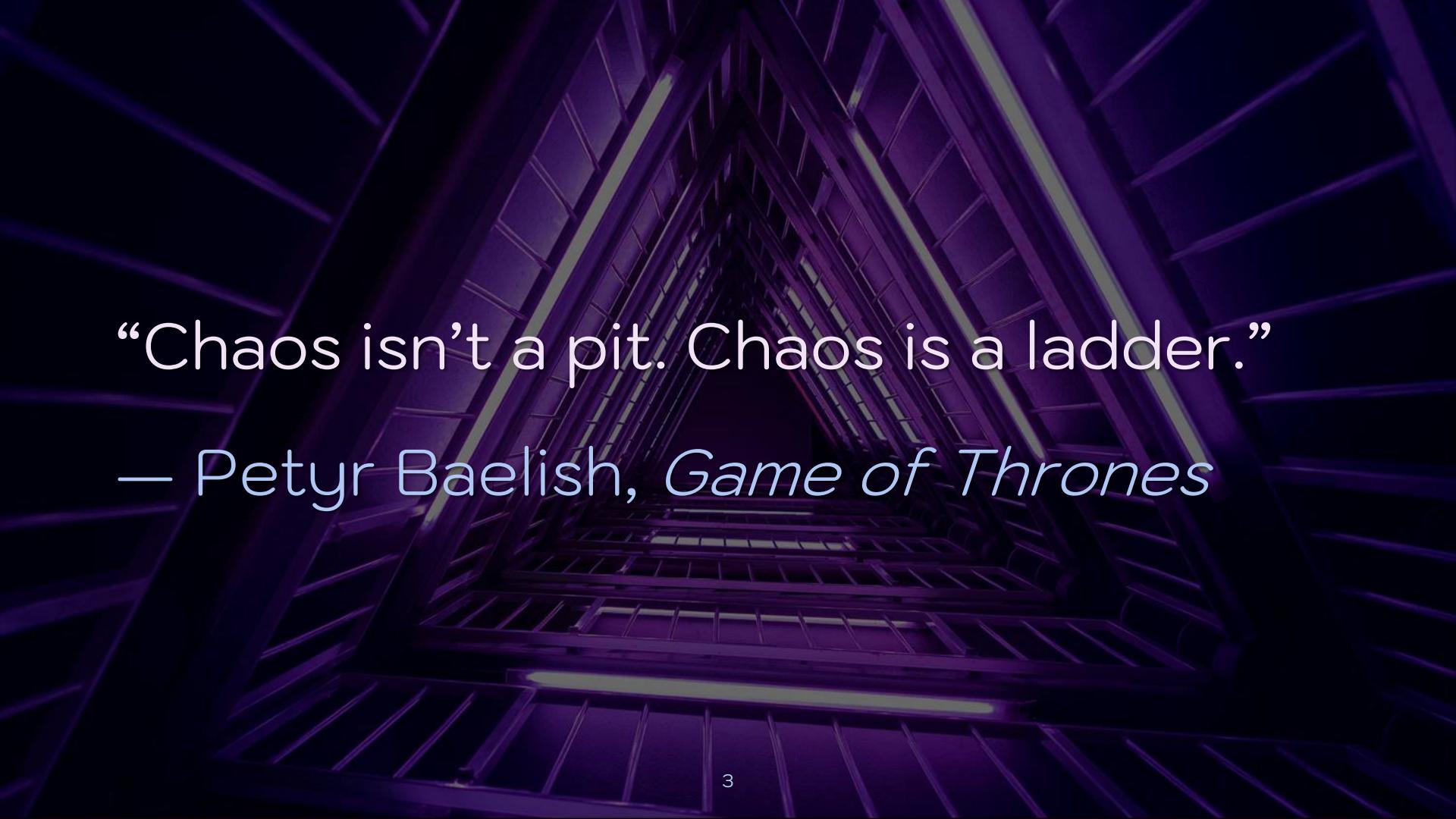
Kelly Shortridge (@swagitda\_)

S4x20



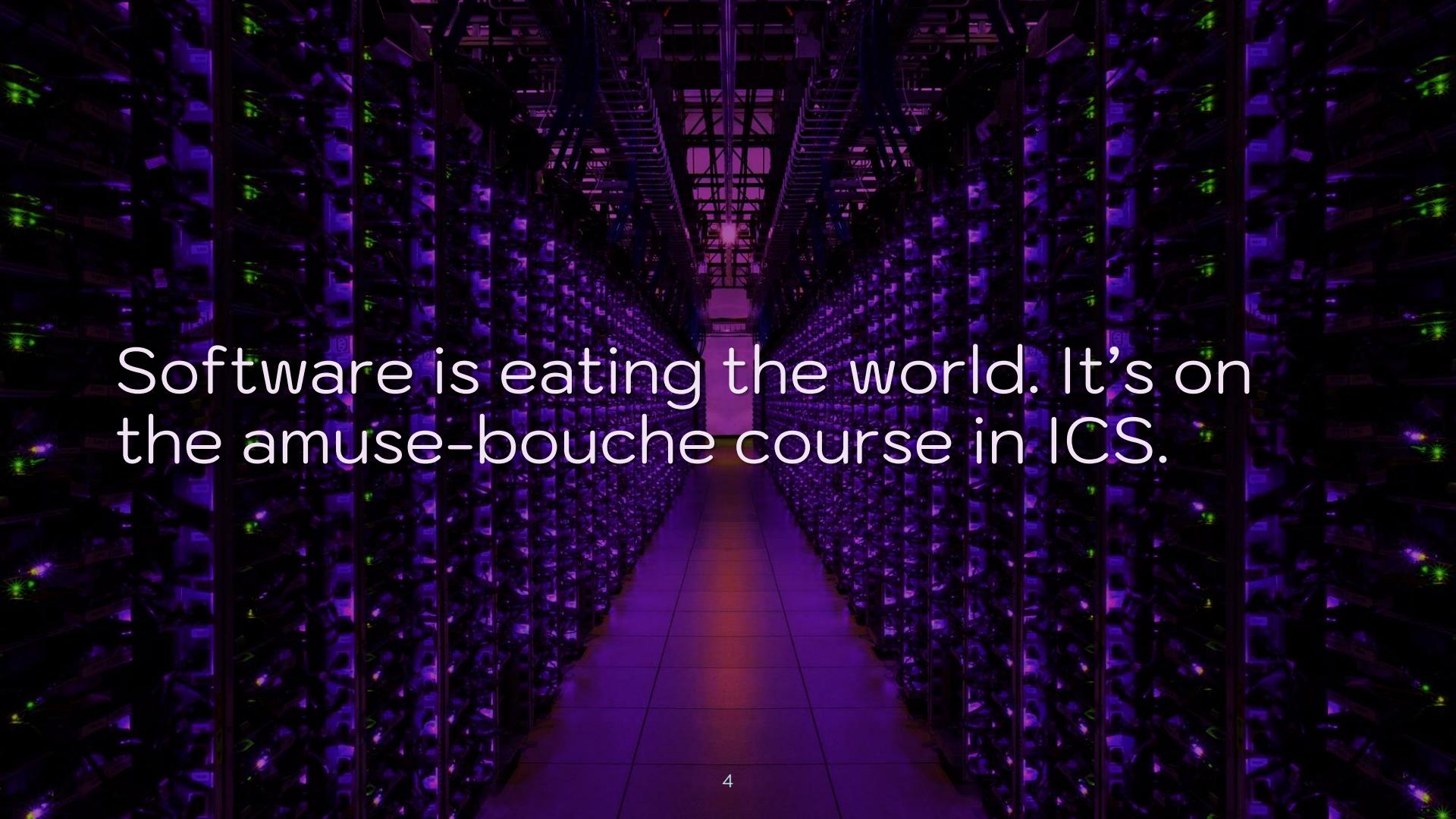
Hi, I'm Kelly

CAPSULE8

The background of the slide features a perspective view of a long, dark corridor. The floor is marked with several glowing blue rectangular lights. The ceiling has a grid of recessed lights, and the walls are made of dark panels. The overall atmosphere is mysterious and futuristic.

“Chaos isn’t a pit. Chaos is a ladder.”

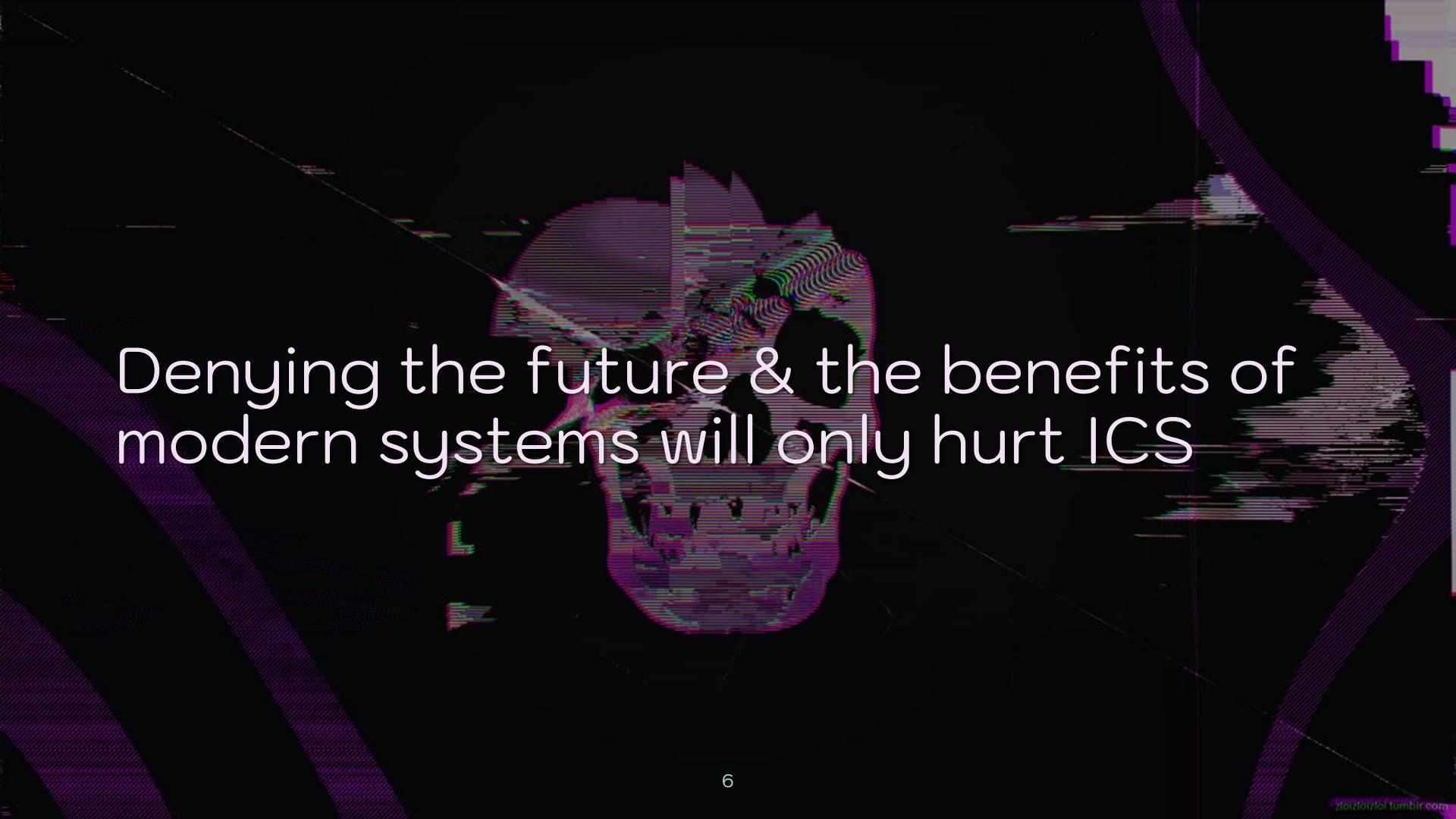
– Petyr Baelish, *Game of Thrones*

A dark server room with rows of server racks. The racks are illuminated from within, showing glowing green lights and internal components. The floor is made of grey tiles, and the overall atmosphere is dimly lit by the glow of the servers.

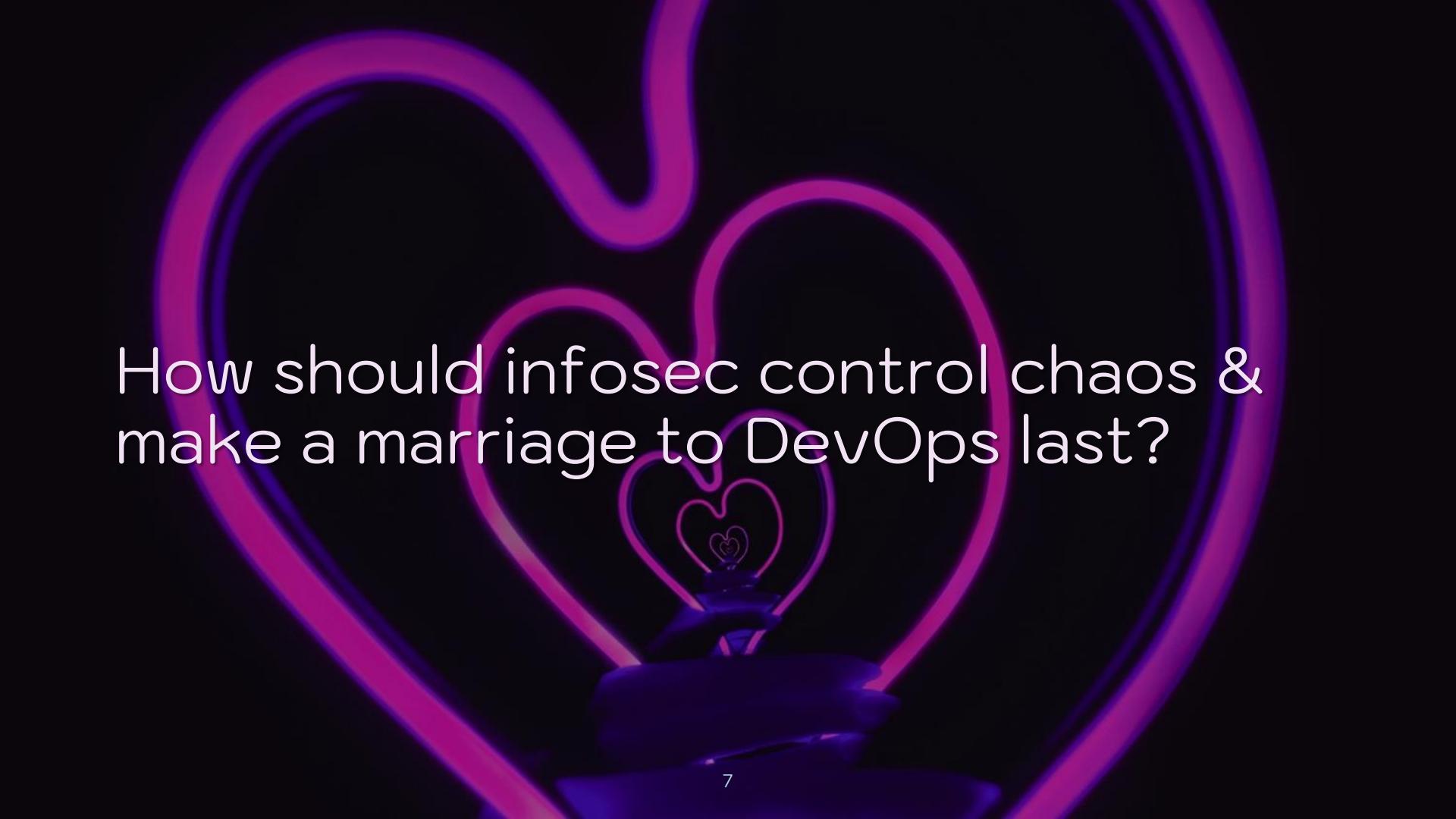
Software is eating the world. It's on  
the amuse-bouche course in ICS.

Infosec has a choice: marry DevOps  
or be rendered impotent & irrelevant





Denying the future & the benefits of  
modern systems will only hurt ICS

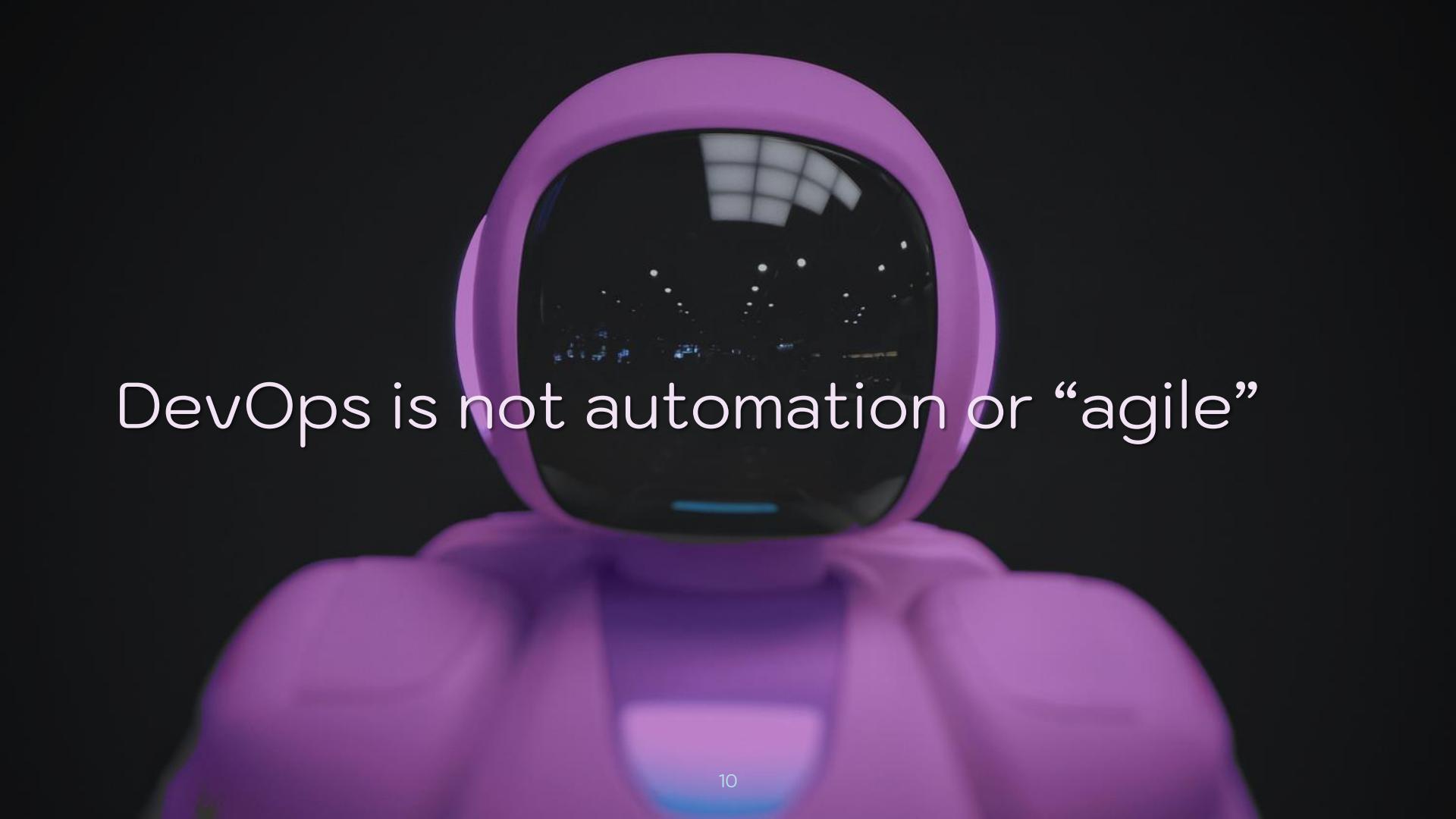
A hand holds a glowing pink and purple heart-shaped light-up stick against a dark background. The light from the stick creates a series of concentric heart shapes that radiate outwards. The central heart is the brightest and most prominent.

How should infosec control chaos &  
make a marriage to DevOps last?

1. DevOps Dominion
2. The Metamorphosis
3. Time to D.I.E.
4. A Phoenix Rises



# DevOps Dominion



DevOps is not automation or “agile”

DevOps is a mindset that unifies responsibility and accountability.



Infosec can join DevOps or take a  
back seat to the future of systems

# Chaos & resilience is infosec's future



What are DevOps's priorities?

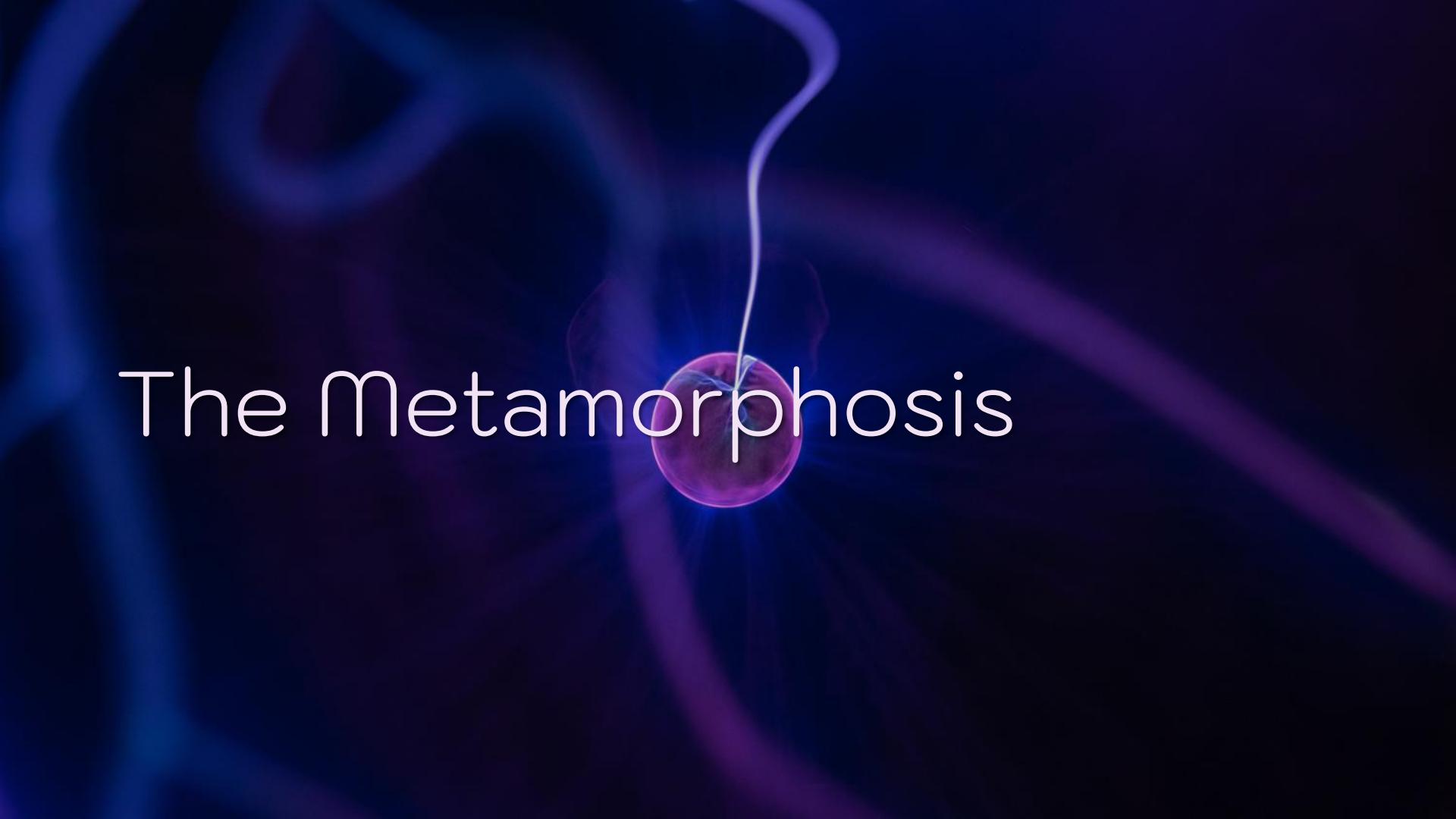
Optimization of software delivery  
performance so tech delivers value



Stability & speed don't conflict –  
resilience & innovation are bffs

Security drives stronger DevOps  
results. Now ICS security must evolve.

# The Metamorphosis



Partitioning of responsibility &  
accountability engenders conflict

After this evolution, DevOps will be held accountable for security fixes



What goals should infosec pursue in this evolution?

And... why should infosec goals  
diverge from DevOps goals?



Infosec has arguably failed, so “this is how we’ve always done it” is invalid

# The Security of Chaos

HURT ME

“Things will fail” naturally extends  
into “things will be pwned”

Security failure is when security controls don't operate as intended



What are the principles of chaotic security engineering?

1. Expect that security controls will fail & prepare accordingly

2. Don't try to avoid incidents – hone your ability to respond to them

What are the benefits of the chaos / resilience approach?



Benefits: lowers remediation costs & stress levels during real incidents

Benefits: minimizes service disruption  
& improves confidence

A glowing pink spiral lightbulb against a black background.

Benefits: creates feedback loops to foster understanding of systemic risk

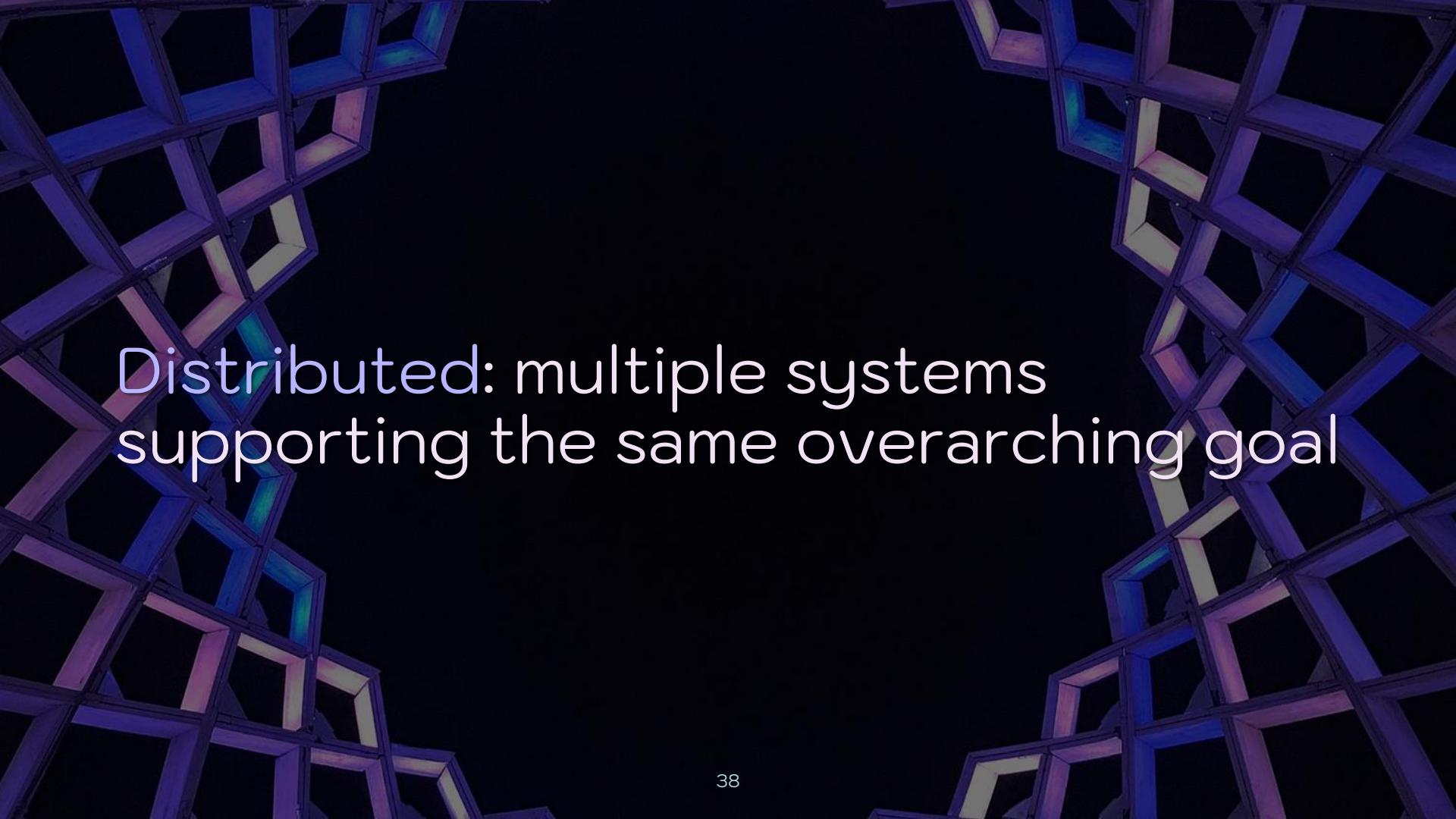
What other ways can infosec become more strategic?



Time to D.I.E.

We need a model promoting qualities  
that make systems more secure

Enter the D.I.E. model: Distributed,  
Immutable, Ephemeral

The background of the slide features a dark, black space filled with numerous glowing, translucent blue and purple 3D cubes. These cubes are arranged in a way that suggests depth and perspective, creating a sense of a vast, interconnected network or a complex data structure. They are illuminated from within, casting soft shadows and highlights that give them a three-dimensional appearance.

Distributed: multiple systems  
supporting the same overarching goal

Distributed infrastructure reduces risk of DoS attacks by design

The background of the slide features a complex, abstract geometric pattern composed of numerous small triangles. These triangles are primarily colored in shades of blue and purple, creating a sense of depth and perspective. The pattern is organized into larger, irregular shapes that overlap each other, giving it a organic, almost molecular appearance.

**Immutable:** infrastructure that  
doesn't change after it's deployed

Servers are now disposable “cattle”  
rather than cherished “pets”



Immutable infra is more secure by design – ban shell access entirely

Unlimited lives is better for security  
than game over upon death

The background of the slide features a dynamic, abstract pattern of swirling, billowing smoke or ink droplets against a black background. The colors used are primarily shades of red, pink, and blue, which interact with each other to create a sense of depth and movement. The smoke forms various shapes, from tight, rounded clouds to more open, wispy patterns, filling the frame.

Ephemeral: infrastructure with a very short lifespan (dies after a task)

Ephemerality creates uncertainty for attackers (persistence = nightmare)



Installing a rootkit on a resource that  
dies in minutes is a waste of effort



ICS attacks take months to plan;  
ephemerality constantly disrupts it

Optimizing for D.I.E. reduces risk by  
design & supports resilience



# A Phoenix Rises

Harness failure as a tool to help you  
prepare for the inevitable

Game days: practice risky scenarios

Prioritize game days based on potential business impacts



Decision trees: start at target asset,  
work back to easiest attacker paths

Determine the attacker's least-cost path (hint: it doesn't involve Oday)

A statue of David by Michelangelo, illuminated with blue and red light against a dark background.

Architecting chaos

Begin with “dumb” testing before  
moving to “fancy” testing

Think digital twins, analytics services,  
or O365... *not* field-level SCADA

# Controlling Chaos: Distributed

Distributed mostly overlaps with availability in modern infra contexts

The background of the slide features a dark, abstract design. It is filled with numerous small, glowing blue and white circular particles of varying sizes, resembling bokeh or distant stars. Interspersed among these particles are several bright, thin, diagonal light rays that radiate from the bottom left towards the top right, creating a sense of depth and motion.

Chaos Monkey: inject random  
instances failures to test resilience

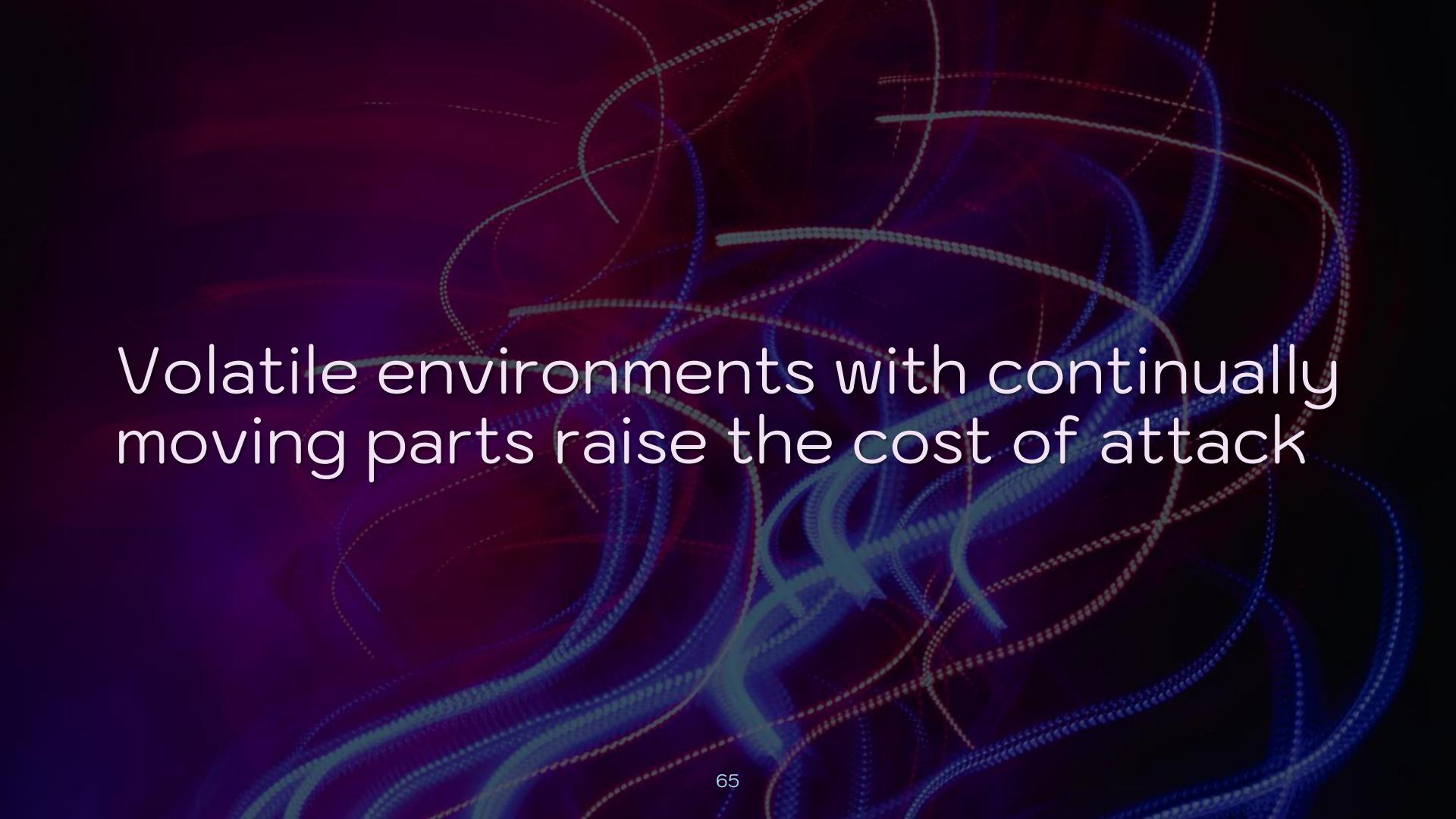
Infosec teams can use these tools but  
make attackers the source of failure

A woman stands in the center of a futuristic, glowing purple tunnel. The tunnel walls are lined with glowing blue and purple panels, and the floor is a bright white semi-circle. The perspective is looking down the length of the tunnel, which disappears into the distance.

Multi-region services present a fun opportunity to mess with attackers

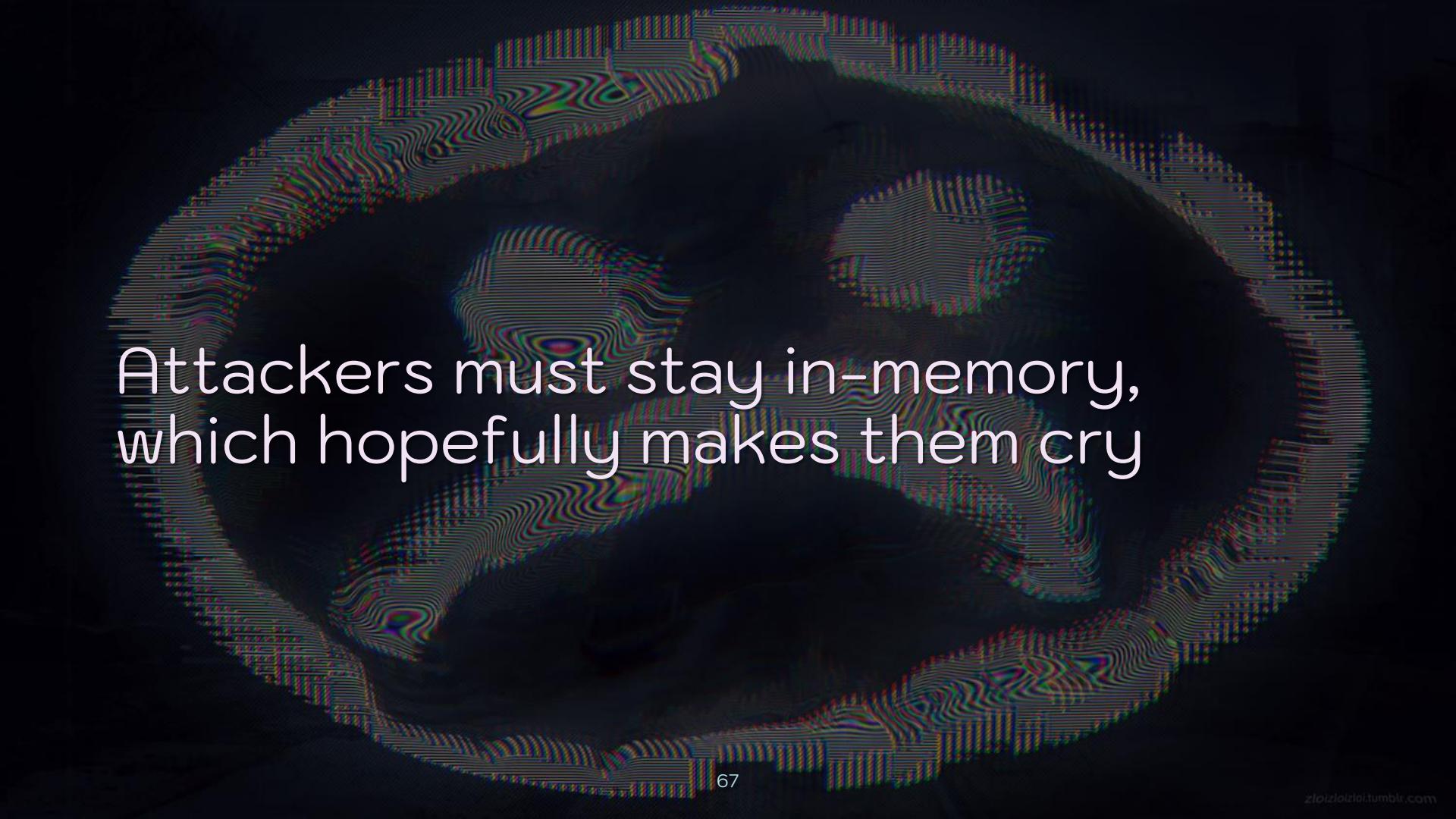
Shuffle IP blocks regularly to change  
attackers' lateral movement game

# Controlling Chaos: Immutable



Volatile environments with continually moving parts raise the cost of attack

Create rules like, “If there’s ever a write to disk, crash the node”

The background of the slide features a complex, abstract pattern of wavy, colorful lines in shades of blue, green, and red, set against a dark, almost black, background. The lines form several concentric, undulating shapes that create a sense of depth and motion.

Attackers must stay in-memory,  
which hopefully makes them cry

Metasploit Meterpreter + webshell:  
Touch passwords.txt & kaboom



Infosec teams can build Docker images with a “bamboozle layer”

Mark garbage files as “unreadable” to craft enticing bait for attackers



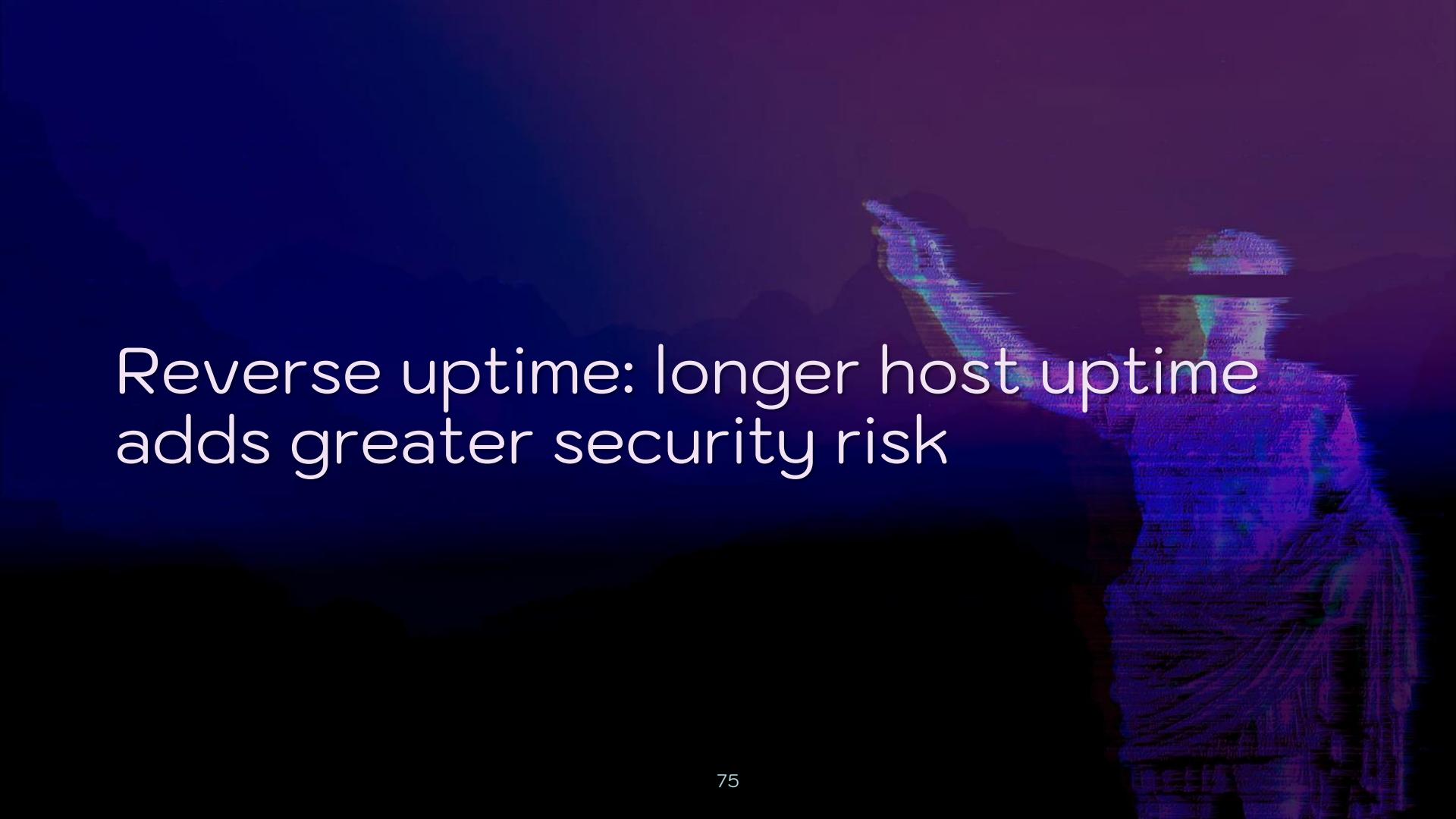
Potential goal: self-healing edge devices with immediate reversion

Test: inject attempts at writing to disk to ensure detection & reversion



# Controlling Chaos: Ephemeral

Most infosec bugs are state-related  
– get rid of state, get rid of bugs



Reverse uptime: longer host uptime  
adds greater security risk



Test: retrograde libraries, containers,  
other resources in CI/CD pipelines

Leverage lessons from toll fraud –  
cloud billing becomes security signal



Test: exfil TBs or run a cryptominer  
to inform billing spike detection

# Conclusion

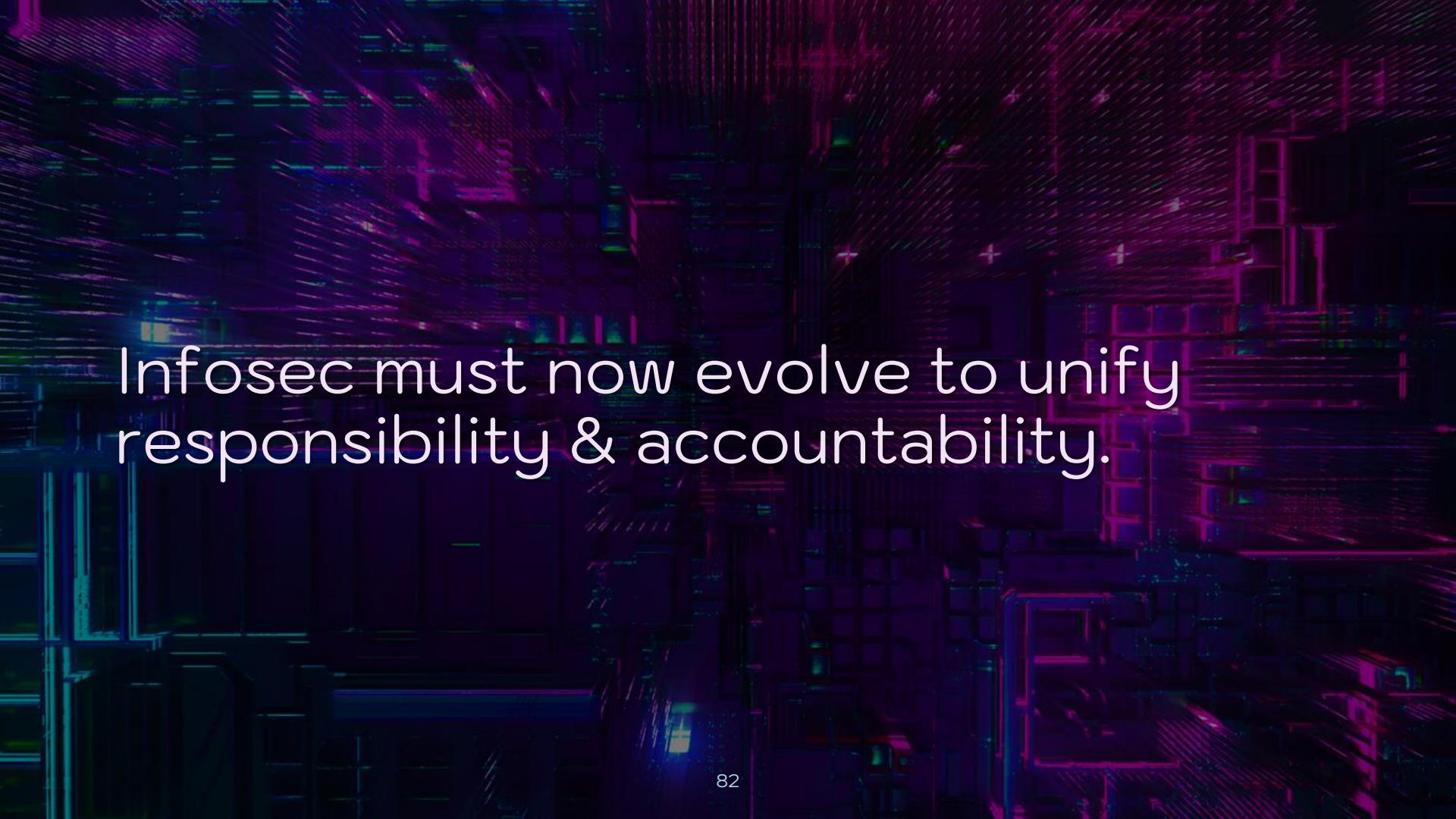




Security cannot gatekeep DevOps.  
It must marry it.

The background of the slide features a dark, abstract design composed of overlapping geometric shapes. It includes large, semi-transparent red and purple triangles and trapezoids that create a sense of depth and movement. In the center, there is a faint, thin-lined rectangular frame.

Chaos/resilience are natural homes  
for infosec & represent its future.



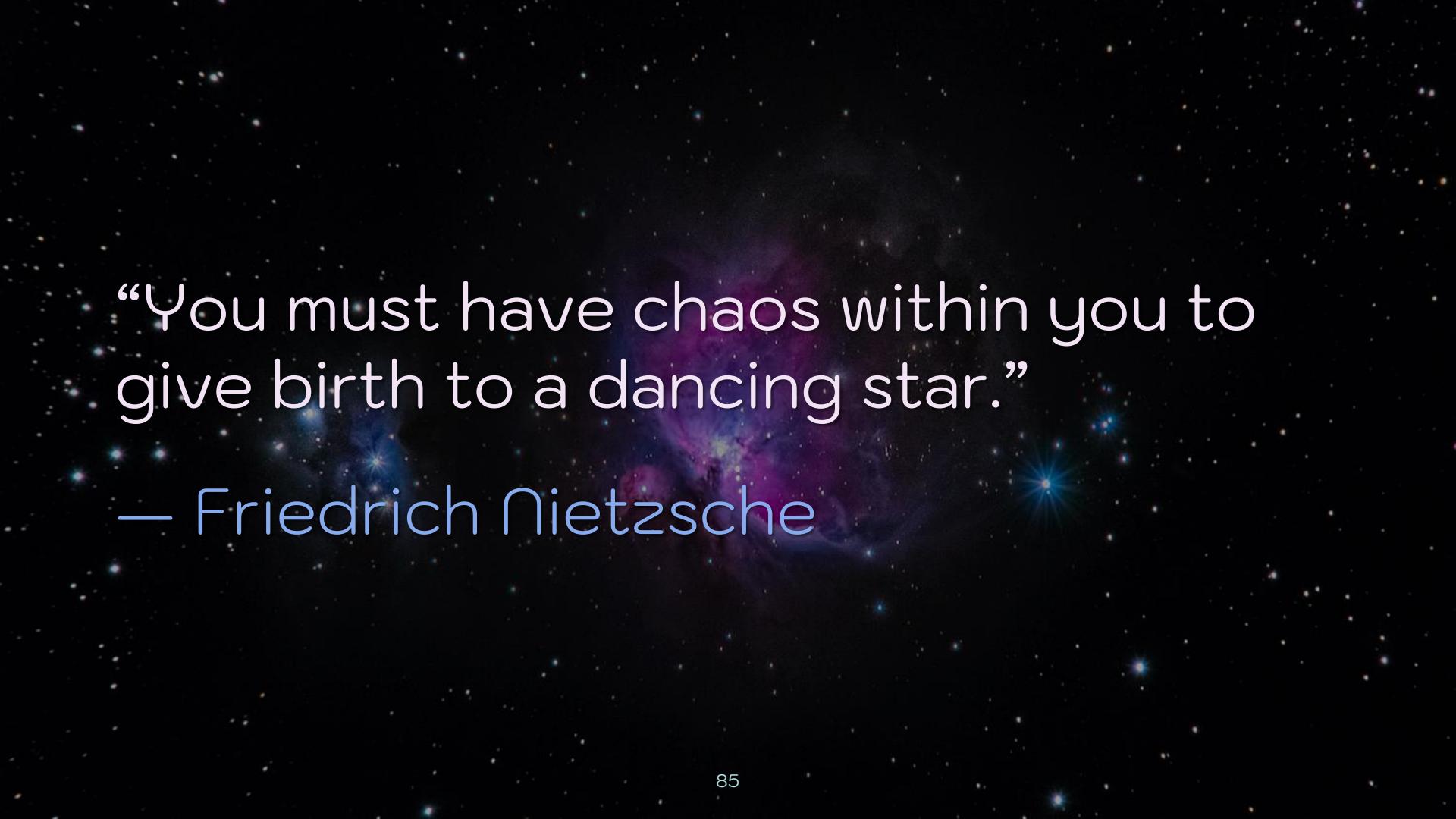
Infosec must now evolve to unify  
responsibility & accountability.



ICS is already cloudy – get ready now  
before OT migrates as well.



Giving up control isn't a harbinger of doom. Resilience is a beacon of hope.

The background of the slide is a dark, textured space filled with numerous small, glowing stars of varying colors. In the center, there is a more prominent, larger nebula or galaxy formation with a mix of purple, blue, and yellow hues, emitting a soft glow.

“You must have chaos within you to  
give birth to a dancing star.”

— Friedrich Nietzsche



@swagitda\_



/in/kellyshortridge



kelly@greywire.net