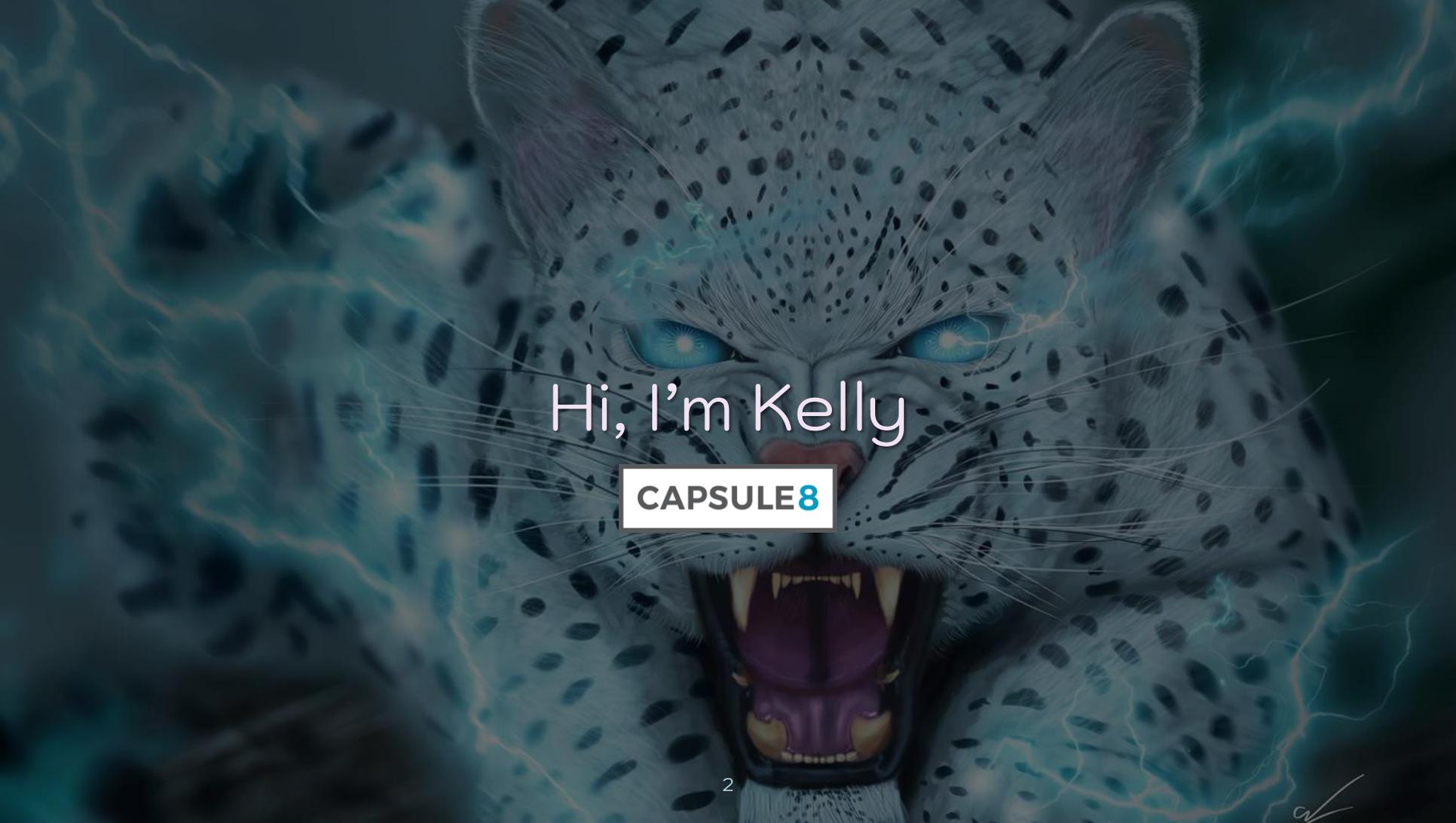


CONTROLLED CHAOS

The Inevitable Marriage of DevOps & Security

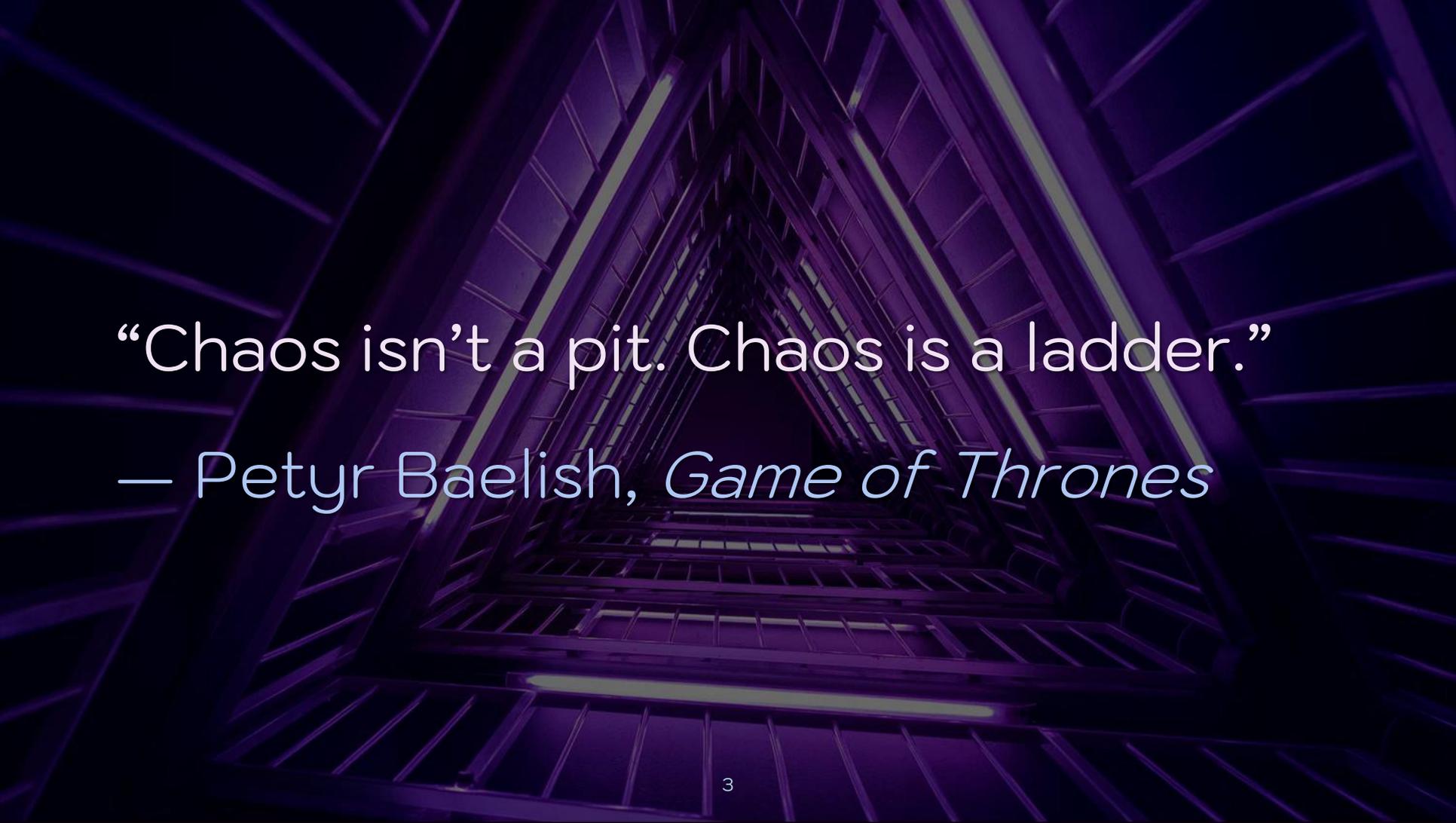
Kelly Shortridge (@swagitda_)

S4x20

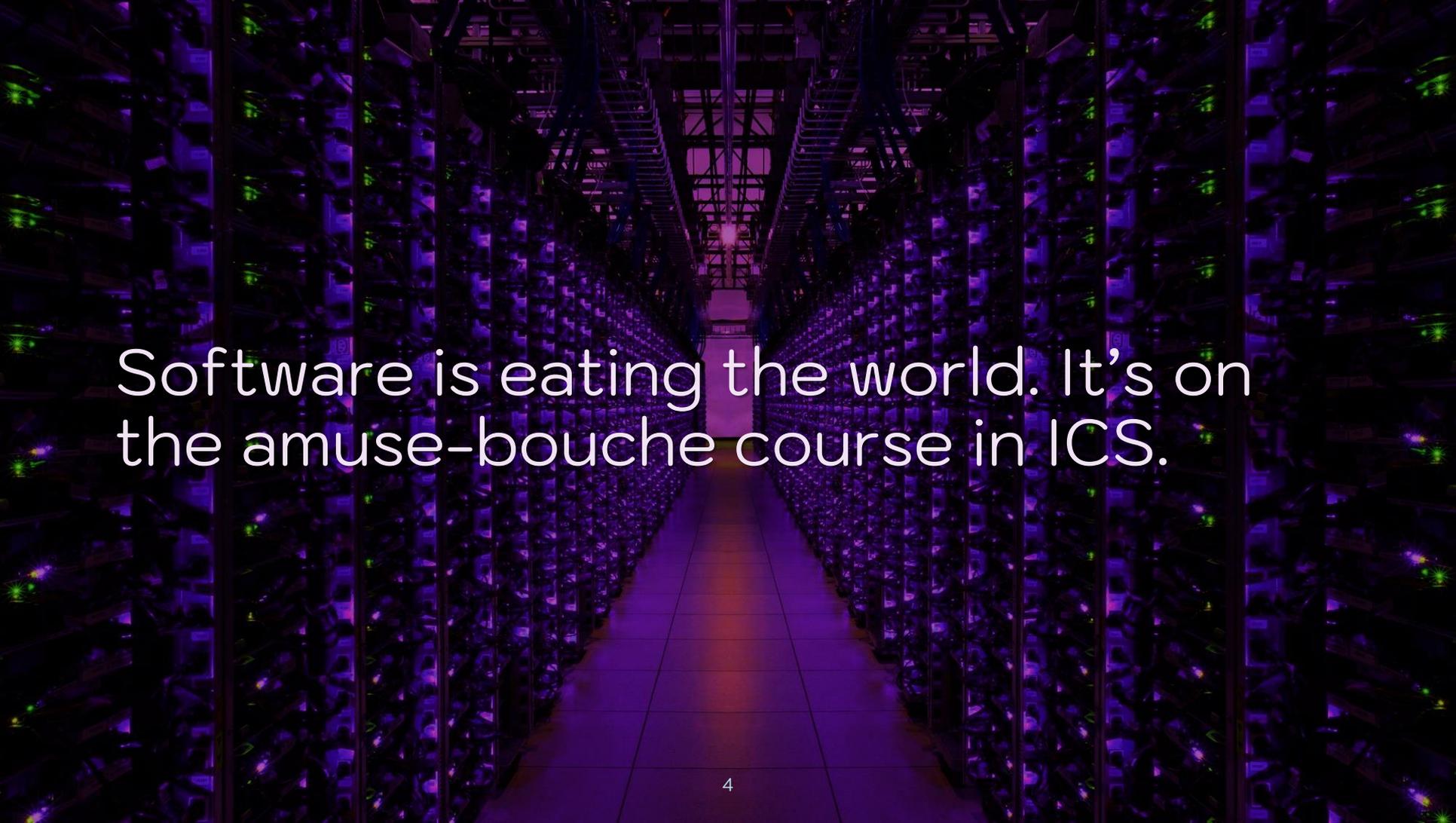


Hi, I'm Kelly

CAPSULE 8



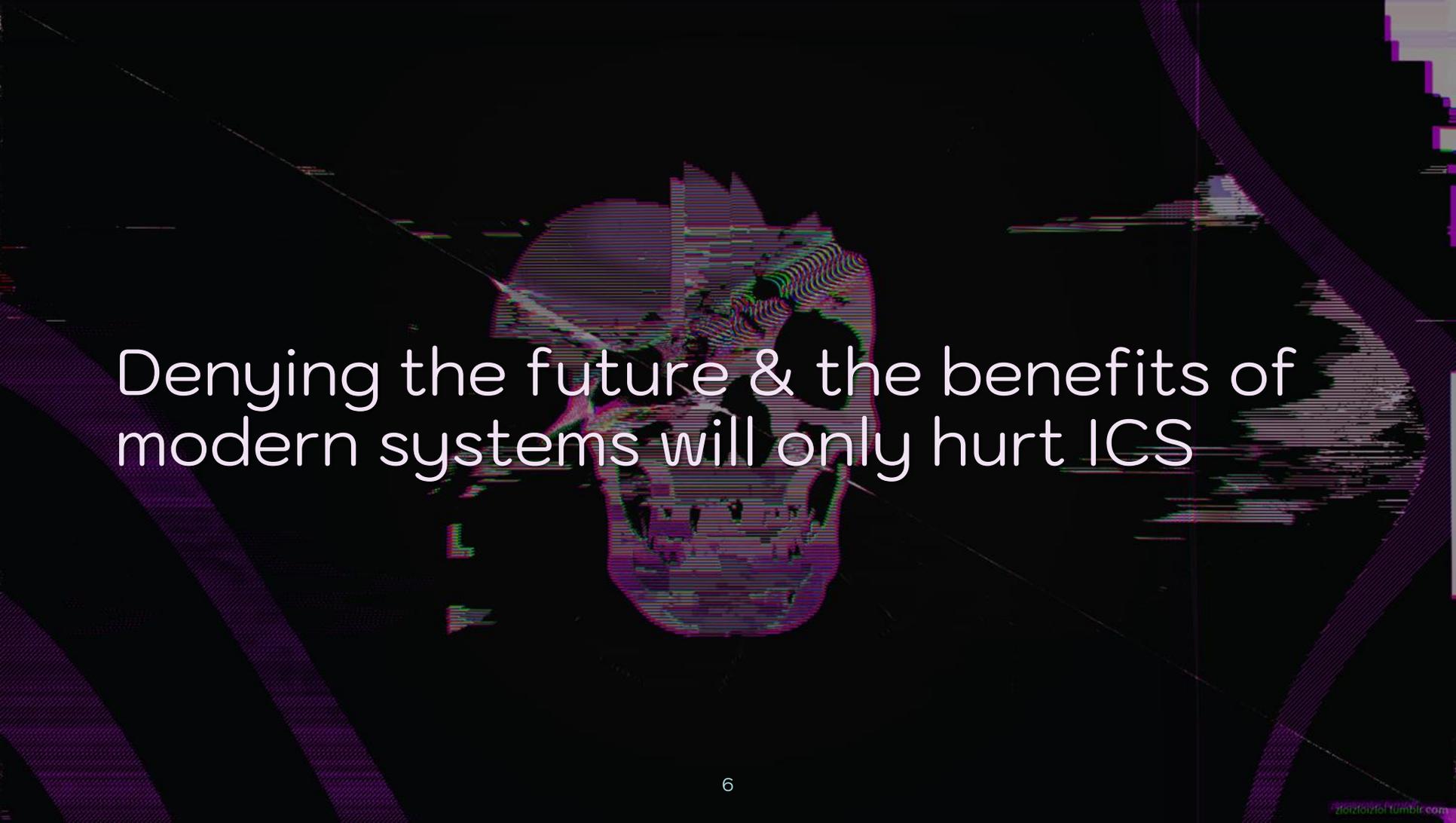
“Chaos isn’t a pit. Chaos is a ladder.”
— Petyr Baelish, *Game of Thrones*



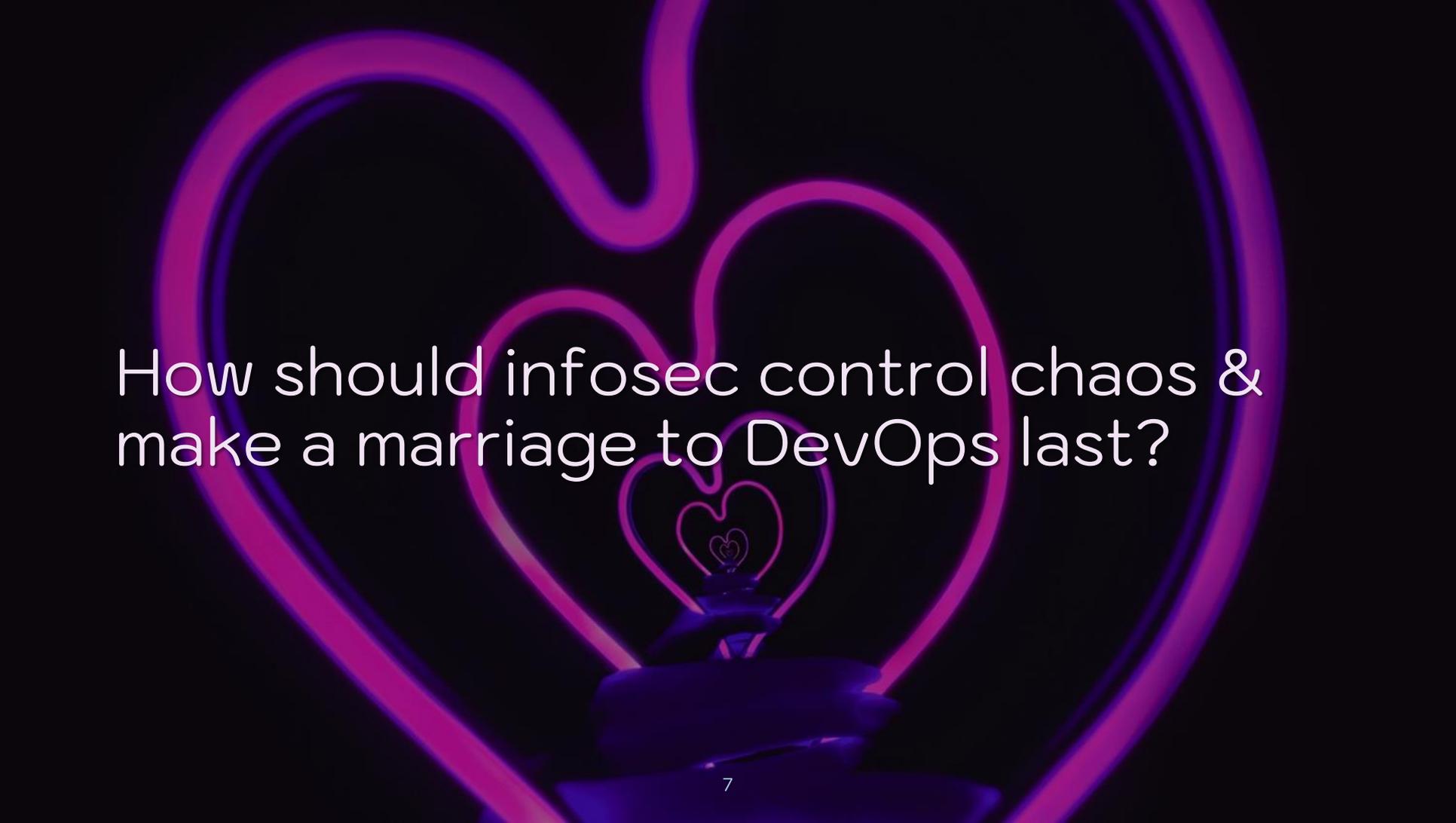
Software is eating the world. It's on the amuse-bouche course in ICS.

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





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

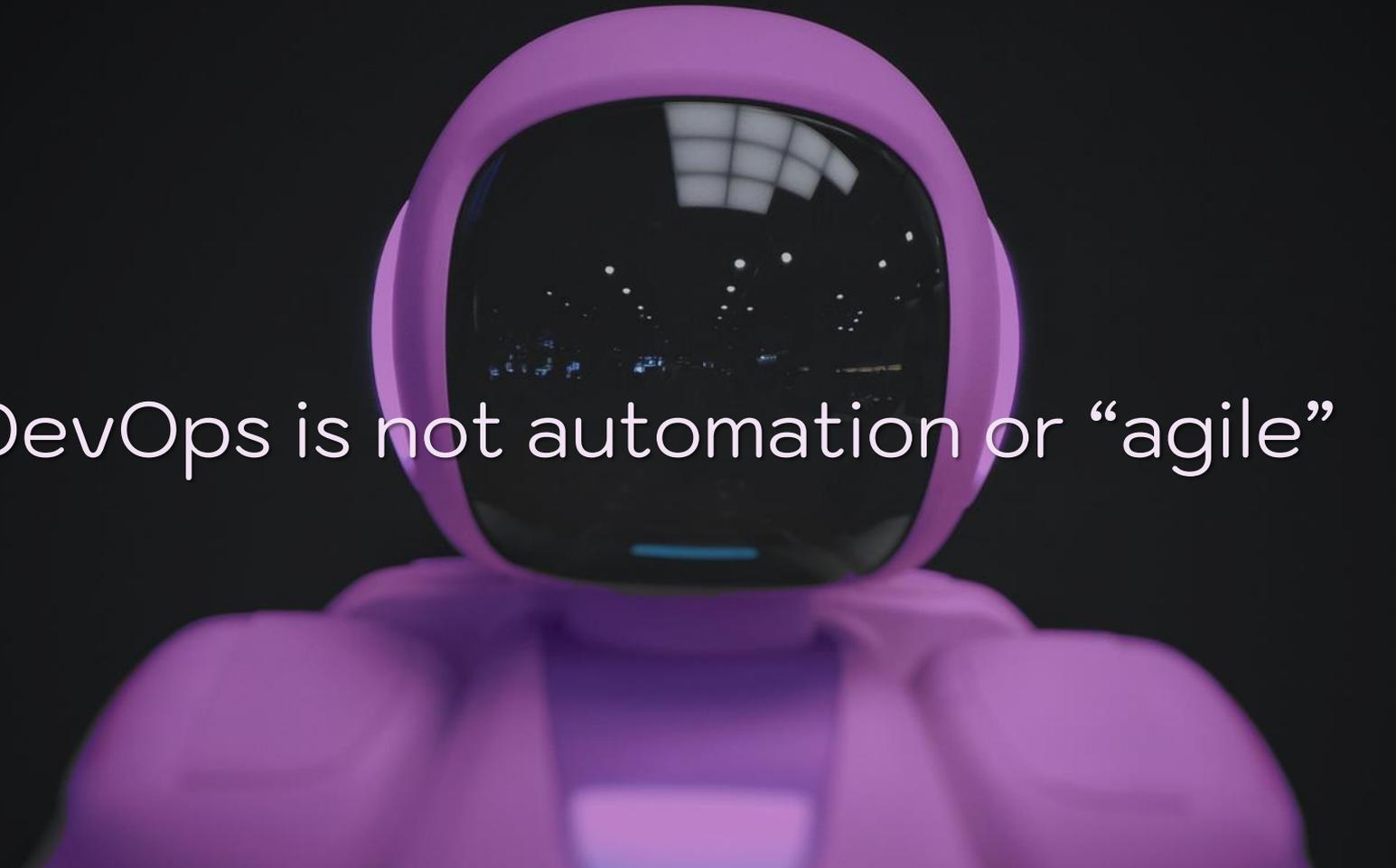
A hand holding a glowing purple heart-shaped lightbulb against a black background with a large purple heart outline.

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

A close-up photograph of a person's hand typing on a laptop keyboard. The scene is dimly lit with a strong blue and purple color cast, creating a futuristic or tech-oriented atmosphere. The background is blurred, showing what appears to be a computer monitor or another screen with some light patterns. The text 'DevOps Dominion' is overlaid in the center-left of the image in a white, sans-serif font.

DevOps Dominion

A purple, stylized robot head with a large, dark, reflective visor. The visor reflects a cityscape at night with lights and a grid pattern. The robot's body is also purple and appears to be wearing a hood or helmet.

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?

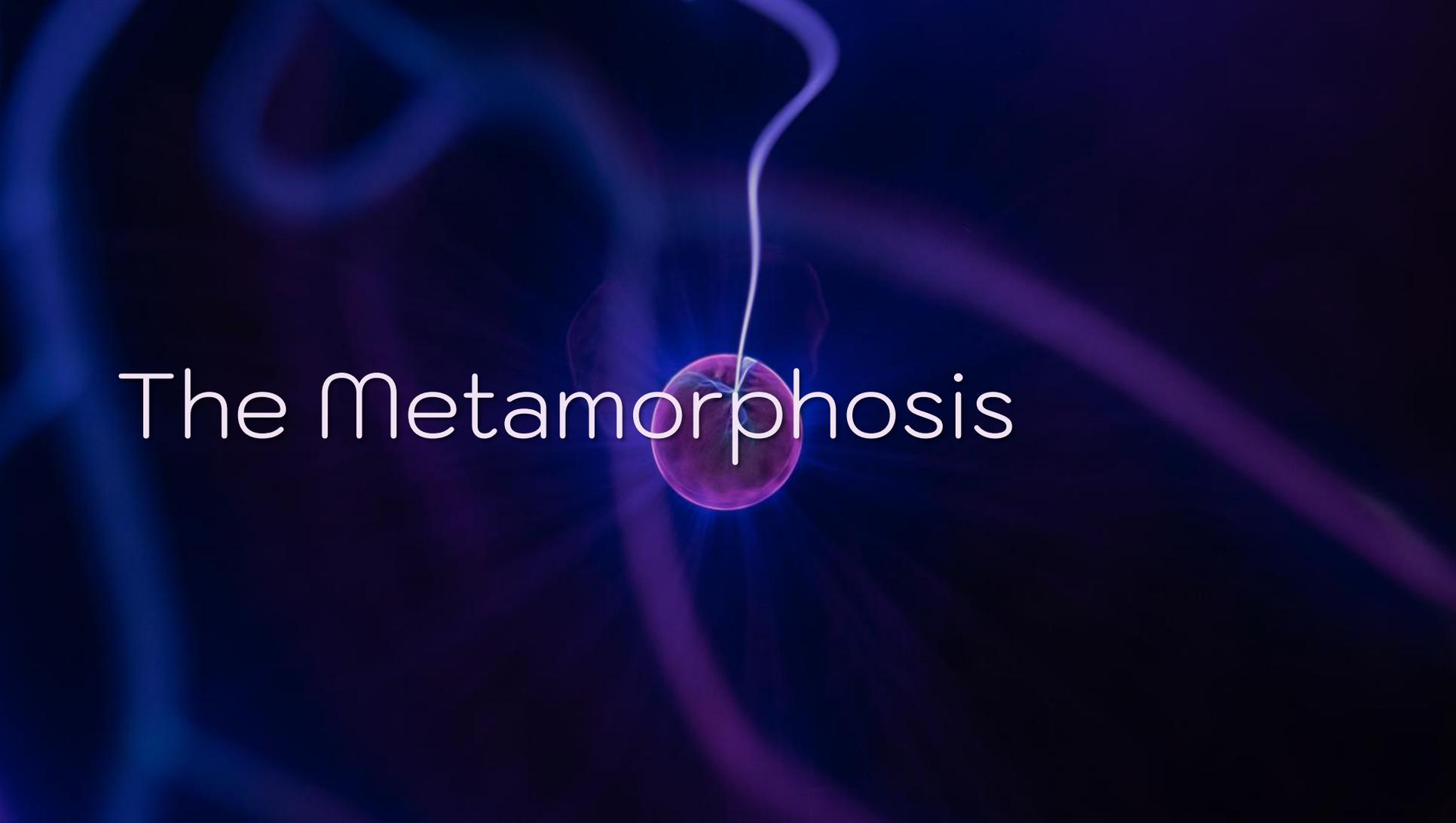
Optimization of software delivery
performance so tech delivers value

A long-exposure photograph of a city street at night. The image is dominated by vibrant light trails from moving vehicles, primarily in shades of red and white, streaking across the foreground. In the background, multi-story buildings with lit windows and streetlights are visible, creating a sense of urban activity. The overall color palette is dark with high-contrast highlights from the lights.

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

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

The Metamorphosis

The image features a central, glowing purple planet with a white line extending upwards from its top. The planet has a textured, slightly grainy surface and a bright white point at the top where the line originates. The background is a deep, dark blue with several large, abstract, glowing light patterns in shades of blue and purple, resembling nebulae or energy fields. The overall aesthetic is futuristic and ethereal.

Partitioning of responsibility &
accountability engenders conflict

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

A hand is shown reaching out from the left side of the frame, composed of numerous glowing purple particles. The background is a dark green to black gradient, also filled with a grid of glowing purple particles, creating a sense of depth and digital space.

What goals should infosec pursue in this evolution?

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

A glowing purple jellyfish is centered in the background. The jellyfish has a large, bright purple 'X' on its bell. The tentacles are also glowing purple and hang down from the bottom of the bell. The entire scene is set against a solid black background.

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

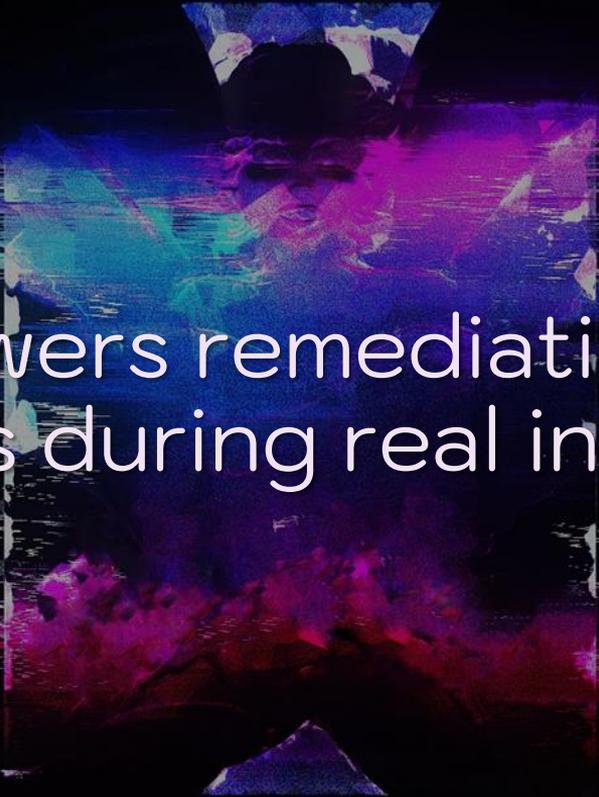
A dramatic night scene of a volcanic eruption. A volcano is shown with a bright red and orange lava flow cascading down its right side. A powerful lightning bolt strikes the peak of the volcano, illuminating the dark, billowing ash and smoke plume that rises into the starry night sky. The overall atmosphere is one of intense natural power and chaos.

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



Benefits: creates feedback loops to foster understanding of systemic risk

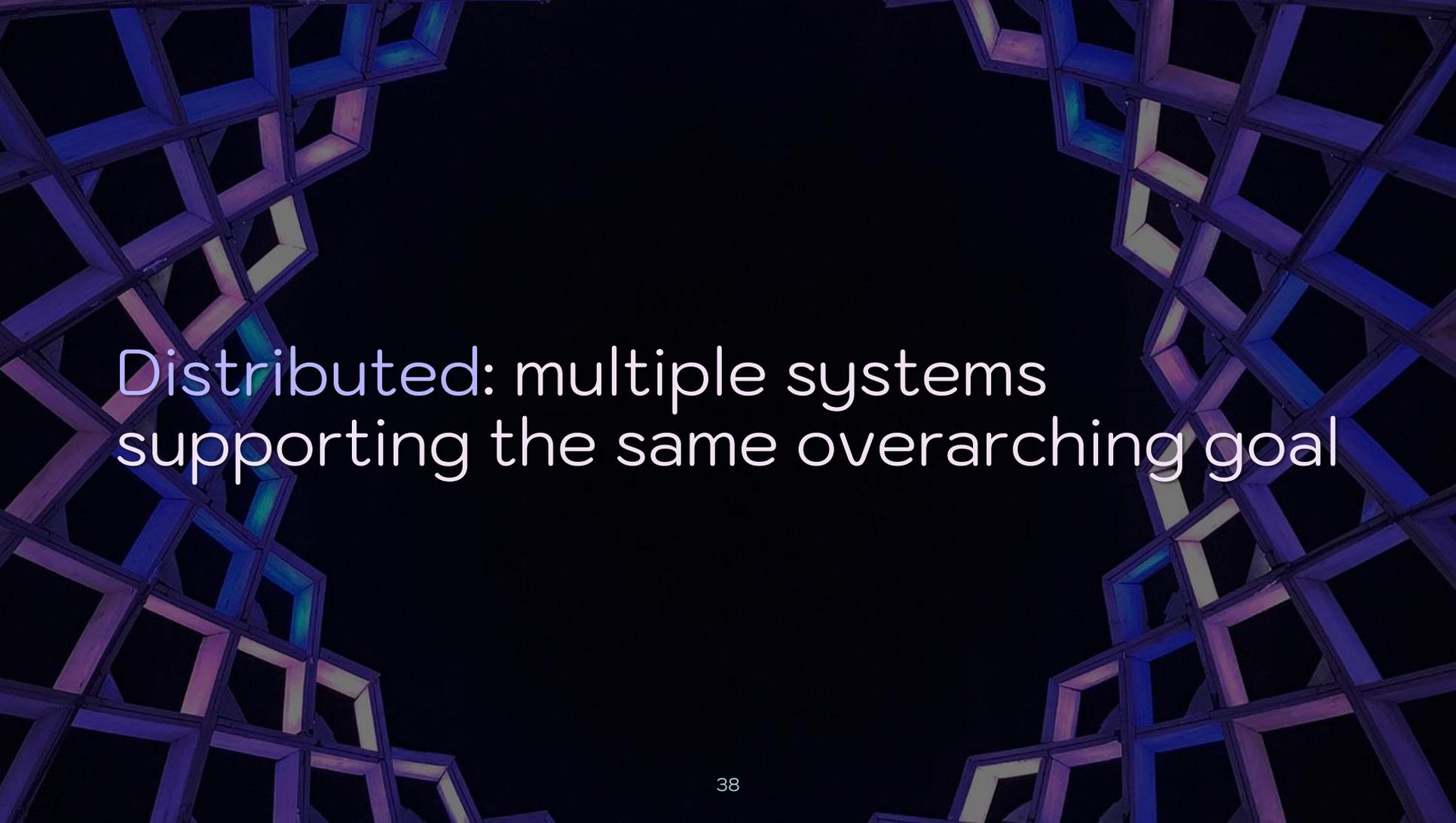
What other ways can infosec become more strategic?



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



Distributed: multiple systems
supporting the same overarching goal

Distributed infrastructure reduces risk of DoS attacks by design



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



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

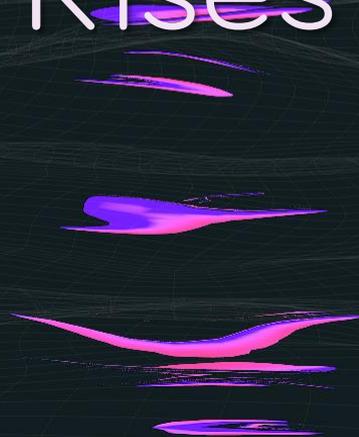


ICS attacks take months to plan;
ephemerality constantly disrupts it

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

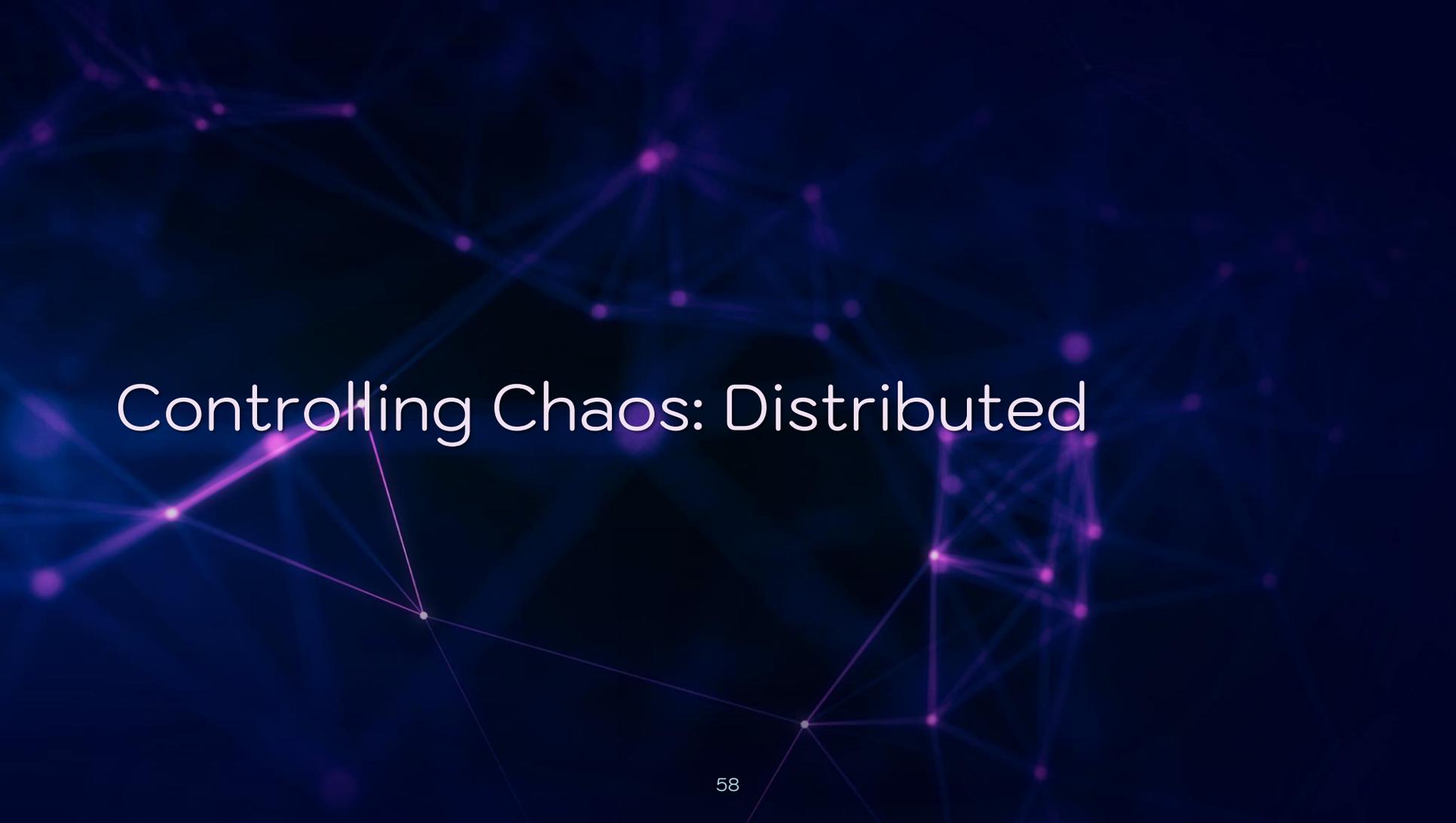
Determine the attacker's least-cost path (hint: it doesn't involve 0day)

Architecting chaos



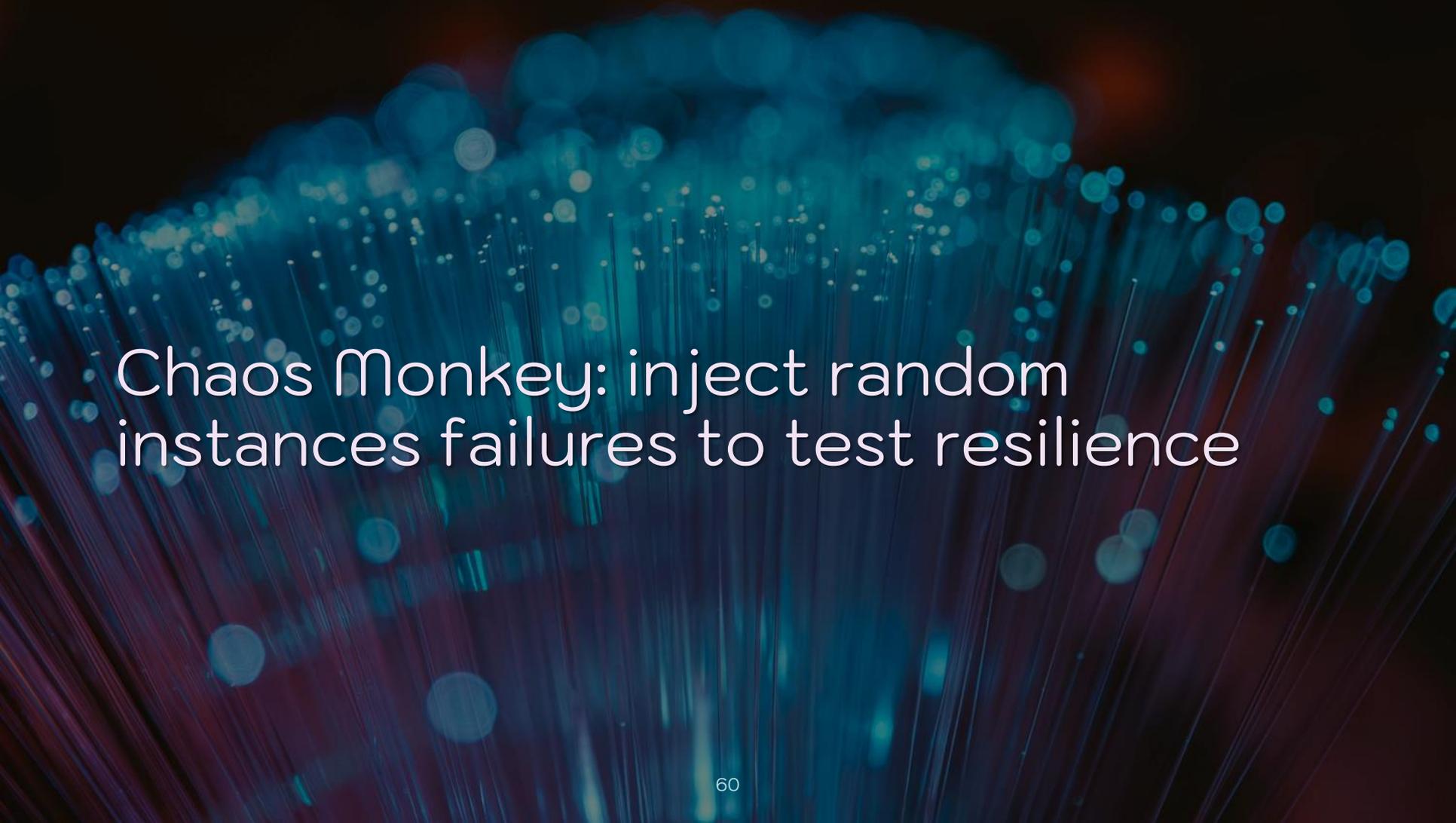
Begin with “dumb” testing before moving to “fancy” testing

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

The background features a complex network graph with numerous nodes and connecting lines, rendered in shades of purple and blue against a dark blue gradient. The nodes are small circles, and the lines are thin, creating a web-like structure that spans the entire frame.

Controlling Chaos: Distributed

Distributed mostly overlaps with
availability in modern infra contexts



Chaos Monkey: inject random
instances failures to test resilience

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

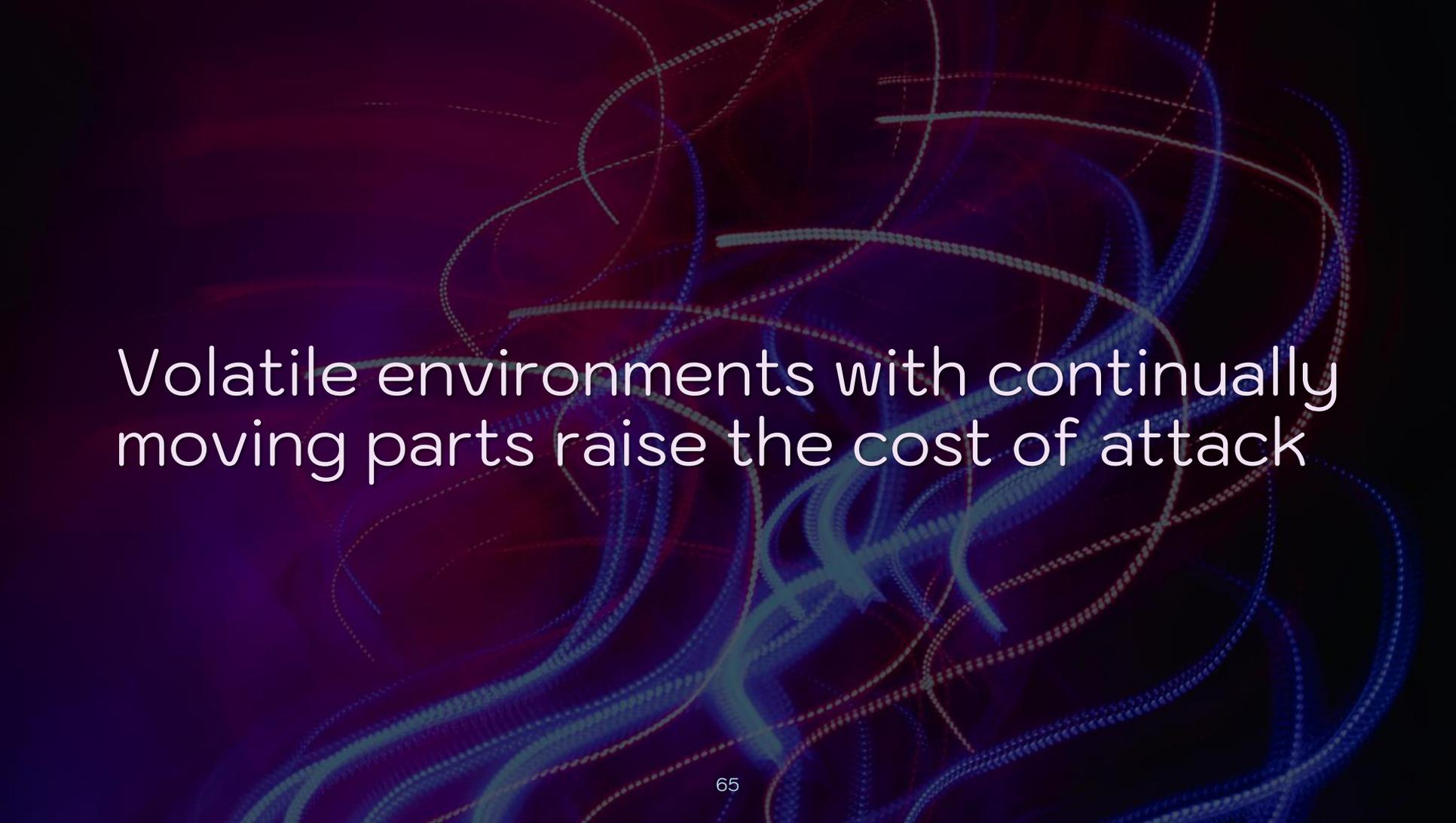
A futuristic, glowing tunnel with a person standing in the center. The tunnel is illuminated with vibrant purple and blue light, creating a sense of depth and mystery. The person is standing on a circular platform in the middle of the tunnel, looking towards the viewer. The overall atmosphere is high-tech and cybernetic.

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

Shuffle IP blocks regularly to change
attackers' lateral movement game

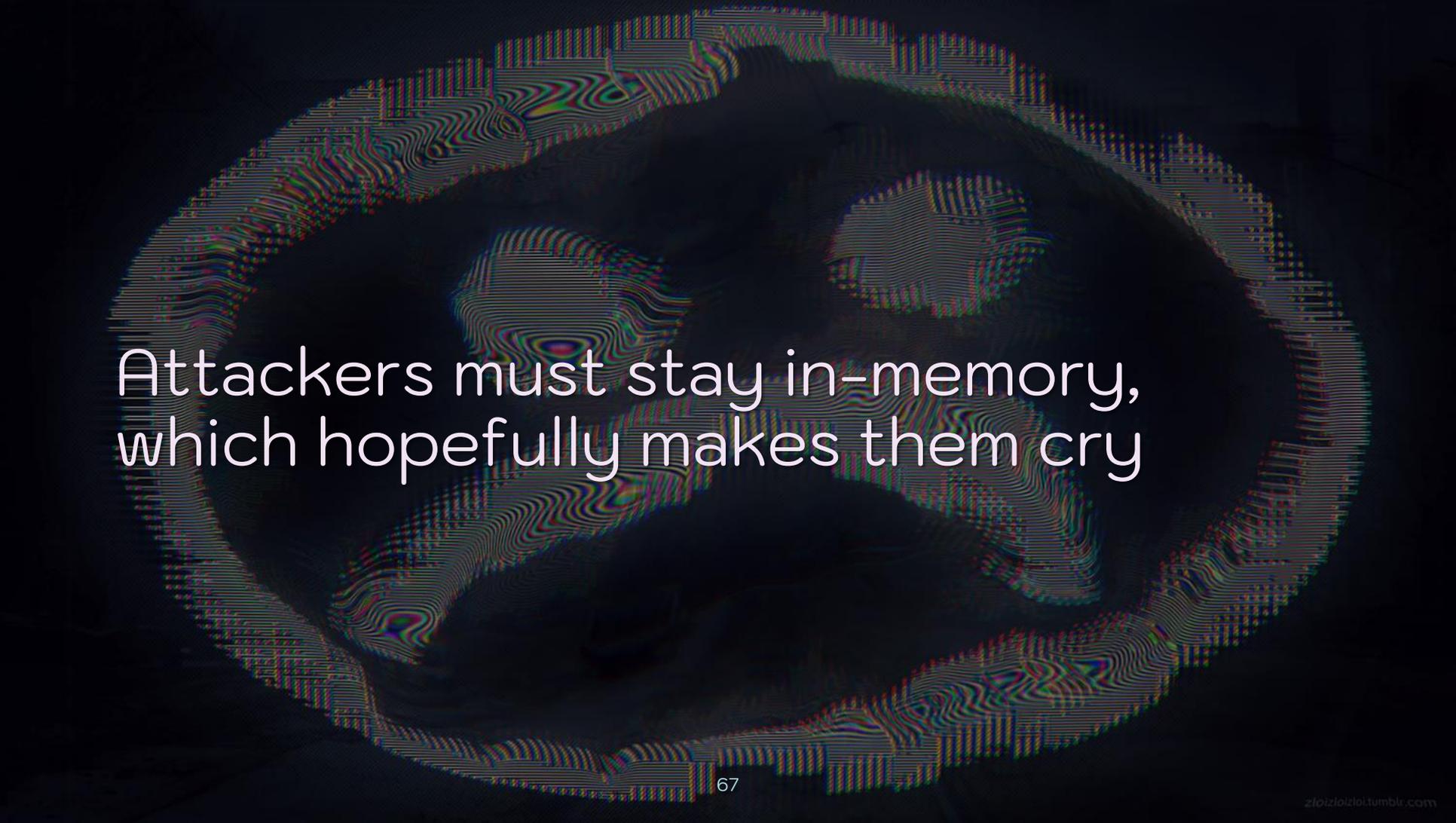
A glowing pink square frame is centered in a dark, snowy landscape at night. The frame is illuminated from within, casting a soft pink glow. The background shows silhouettes of trees and a dark sky. The text "Controlling Chaos: Immutable" is overlaid in white, sans-serif font across the middle of the image.

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”



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

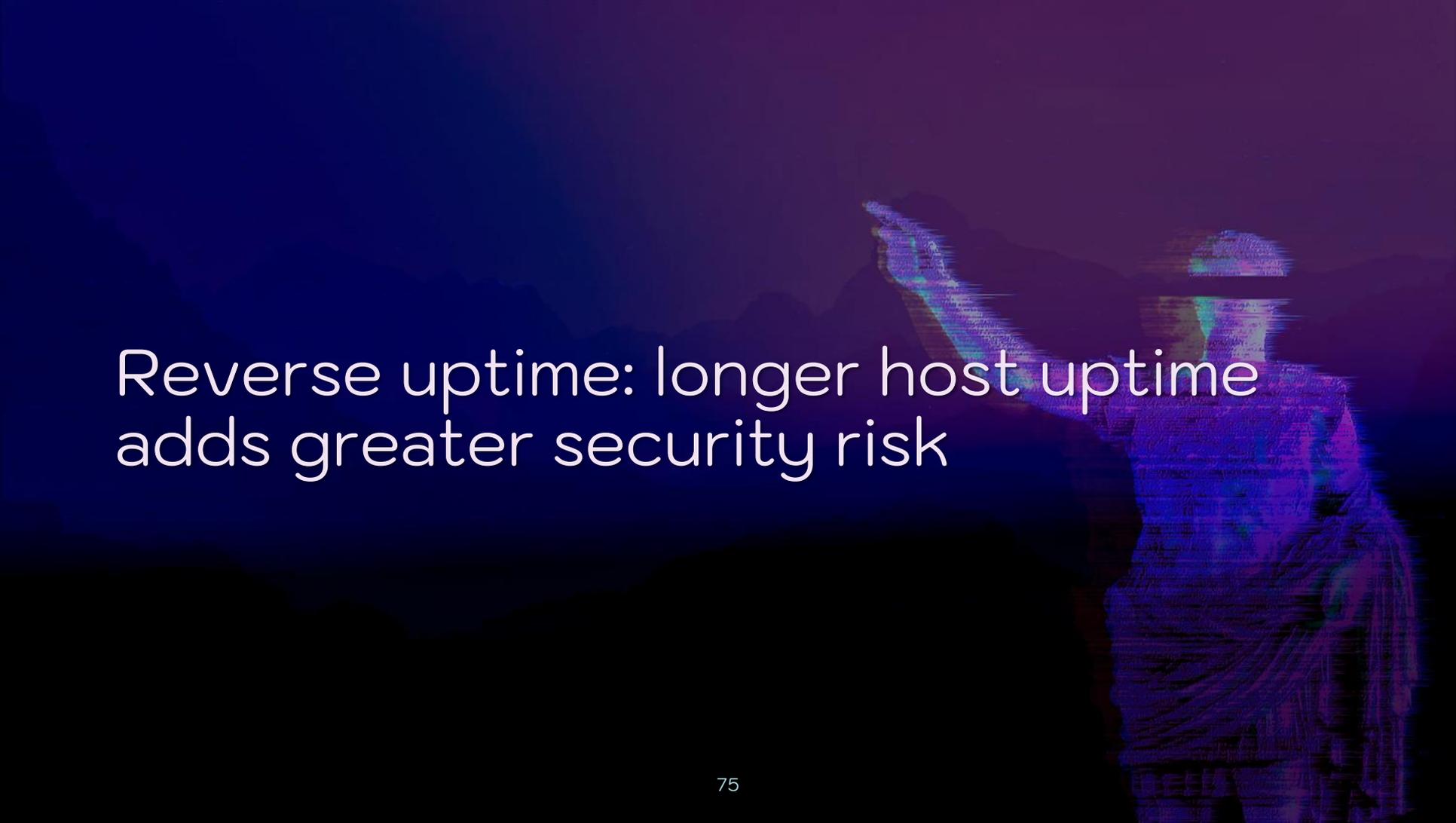


Test: inject attempts at writing to disk to ensure detection & reversion



Controlling Chaos: Ephemeral

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

A person is shown in profile, pointing towards a screen that displays a colorful, abstract pattern of blue and purple light. The background is dark, suggesting a dimly lit room or a stage setting. The overall mood is technical and focused.

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.



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.

A close-up photograph of a hand holding a glowing, multi-colored orb. The hand is positioned in the lower half of the frame, with the fingers gently cupping the orb. The orb emits a bright, multi-colored light, primarily in shades of blue, purple, and pink. The background is dark and out of focus, with some blurred light spots. The overall mood is one of hope and resilience.

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



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

— Friedrich Nietzsche



@swagitda_



/in/kellyshortridge



kelly@greywire.net