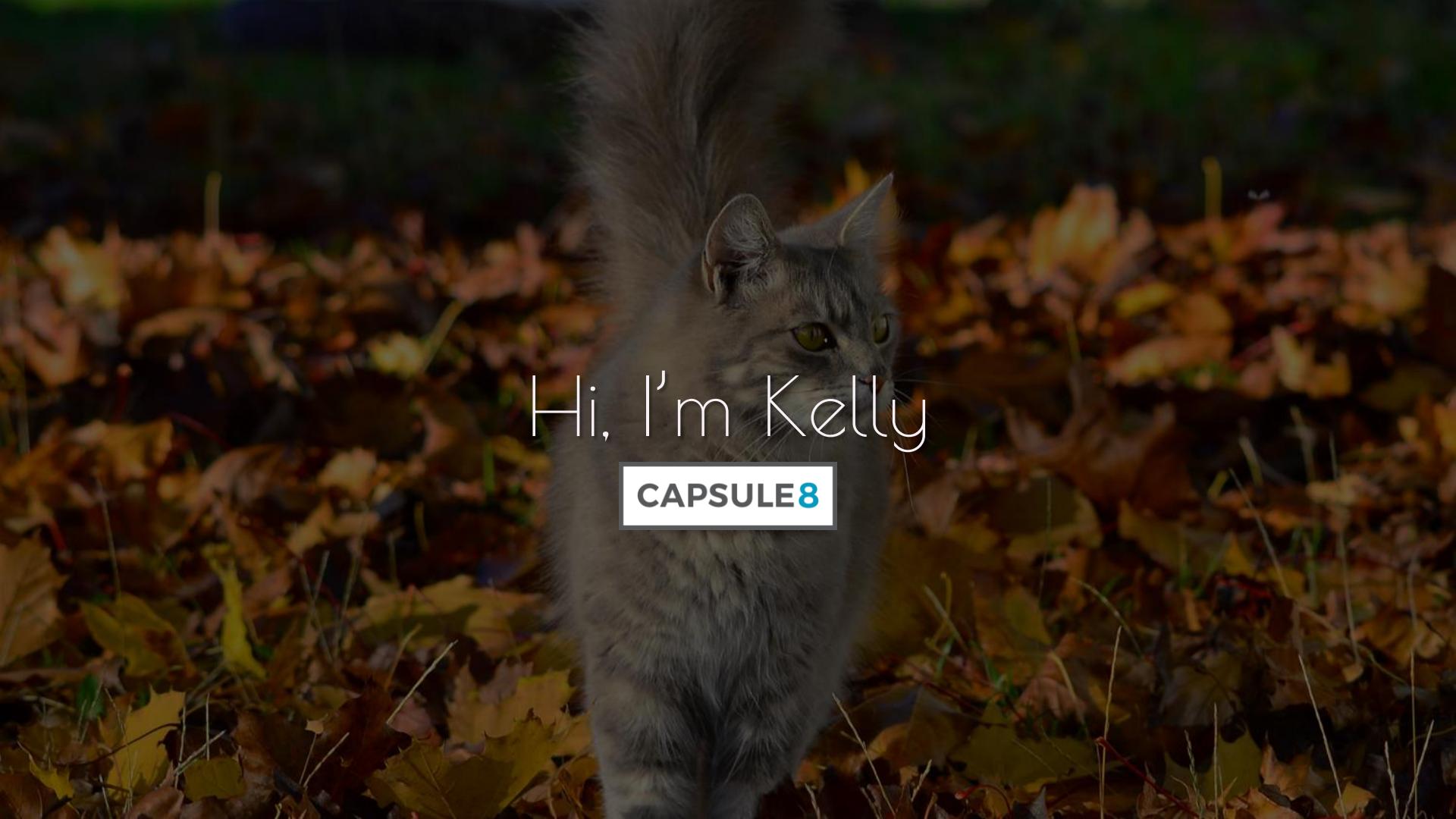


EXIT STAGE LEFT: Eradicating Security Theater

Kelly Shortridge (@swagitda_)

Snykcon 2020 Keynote

A fluffy gray cat with green eyes is sitting in a pile of fallen autumn leaves. The leaves are a mix of yellow, orange, and brown. The cat is looking directly at the camera. The background is dark and out of focus.

Hi, I'm Kelly

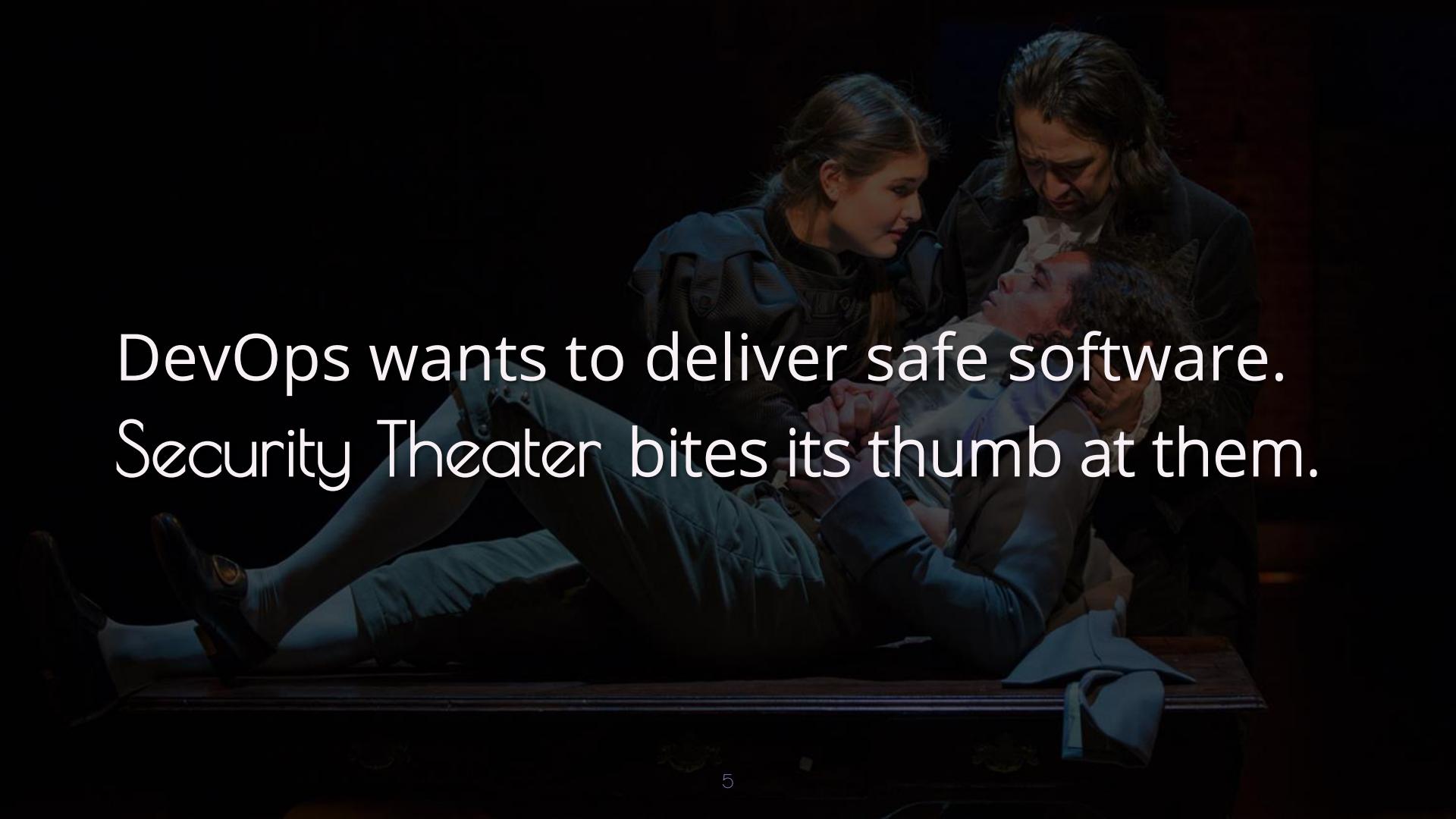
CAPSULE8



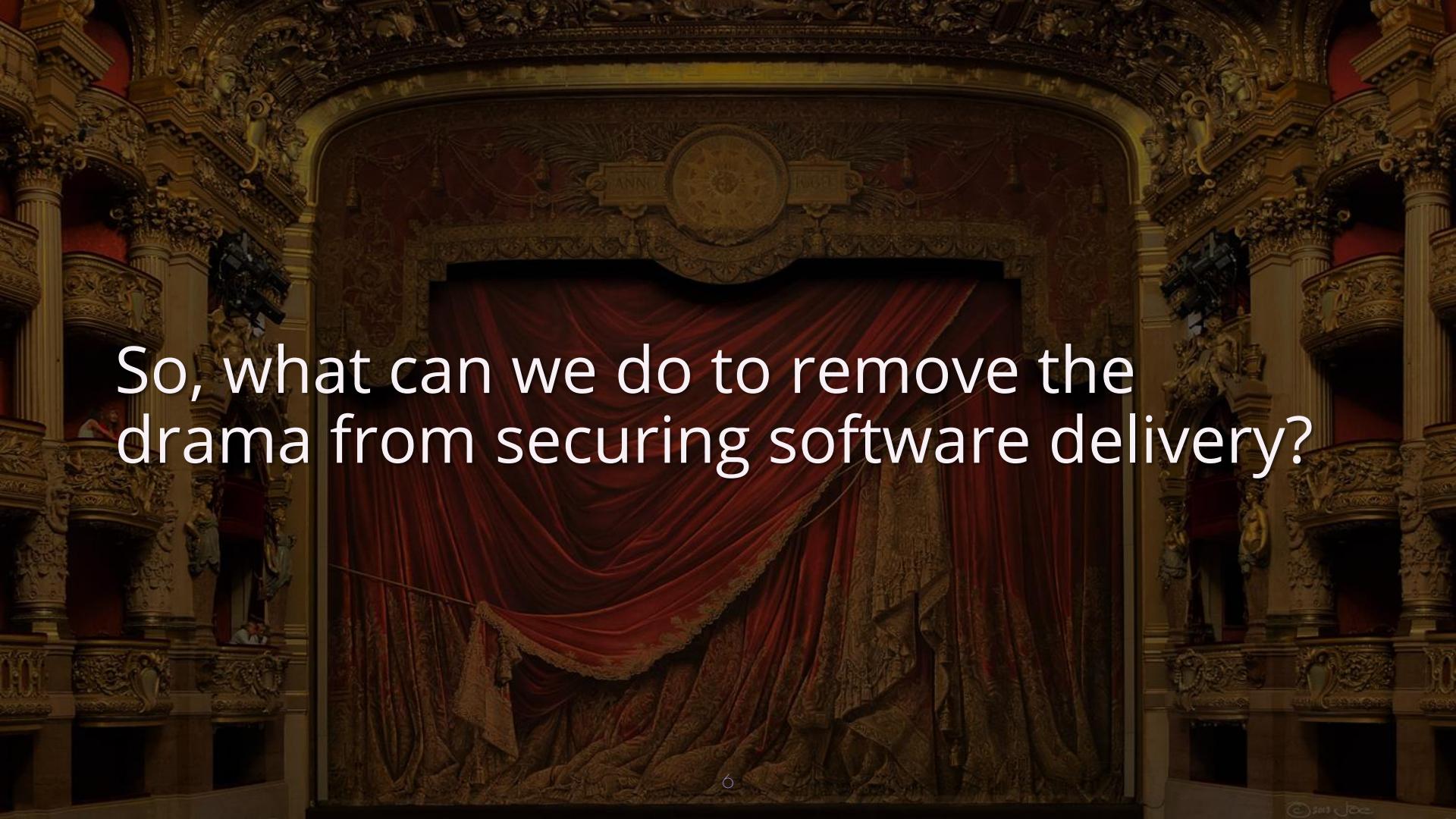
Information security sees itself as the underappreciated star on the I.T. stage

...infosec is certainly a **primadonna**

A photograph of a woman in a white dress dancing on a dark stage. She is in a crouched position, leaning forward with her hands near her face. The stage floor has some scratches and dust.



DevOps wants to deliver safe software.
Security Theater bites its thumb at them.

A photograph of a grand theater interior. The stage is framed by heavy, dark red velvet curtains with gold-colored fringe. Above the stage, a large, ornate gold-colored decorative element hangs, featuring a circular emblem and the word "ANNIS". The surrounding architecture is highly detailed with gold-colored moldings, columns, and statues. A small figure of a person is visible on the left side of the stage.

So, what can we do to remove the drama from securing software delivery?

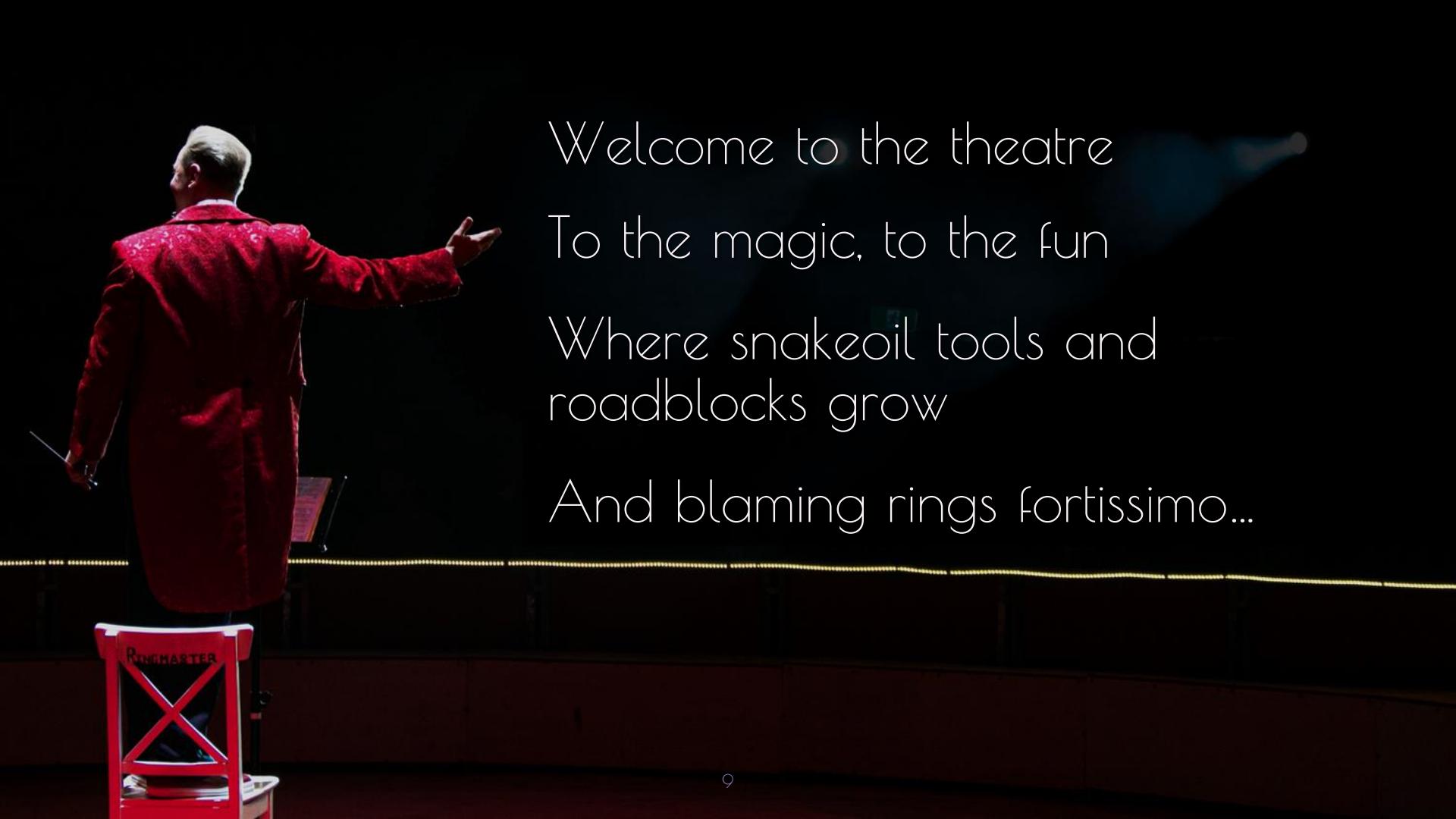
Act I: Welcome to Security Theater

Act II: Fisticuffs

Act III: Redemption

The background of the image shows a grand theater interior. A large, richly decorated red curtain hangs across the stage. Above the curtain, the ornate gold-colored proscenium arch is visible, featuring intricate carvings and gilded statues. A massive, multi-tiered chandelier hangs from the ceiling, its numerous lights reflecting off the dark surfaces. The overall atmosphere is one of luxury and historical grandeur.

Act I: Welcome to Security Theater

A man in a red sequined ringmaster's jacket and a top hat stands on a stage, facing away from the camera. He is gesturing with his right hand towards the audience. In front of him is a red chair with a large white 'X' on it, which has 'RINGMASTER' written on its backrest. The stage is dark, with a bright beam of light coming from the right side.

Welcome to the theatre
To the magic, to the fun
Where snakeoil tools and
roadblocks grow
And blaming rings fortissimo...

Security Theater: producing the
perception of improved security

Security Theater optimizes for **drama**



Processes apply to everyone just to
catch the extra rare “bad apples”

“The strategy seems to be preventative control on everybody instead of damage control on those few.”

- Bjarte Bogsnes



Hence: infosec as “Department of No”

This “makes life painful for the innocent
but can be circumvented by the guilty”

Are scanner results going into a pretty report, or actually being fixed?

The background of the slide is a dark, ornate interior of a cathedral or grand hall. The ceiling is high and decorated with intricate gold-colored moldings and several large, circular frescoes depicting figures. Numerous tall, thin chandeliers hang from the ceiling, each holding numerous lit candles that cast a warm glow. The overall atmosphere is one of grandeur and historical significance.

How long do your security tools take to run? Do they disrupt your pipelines?

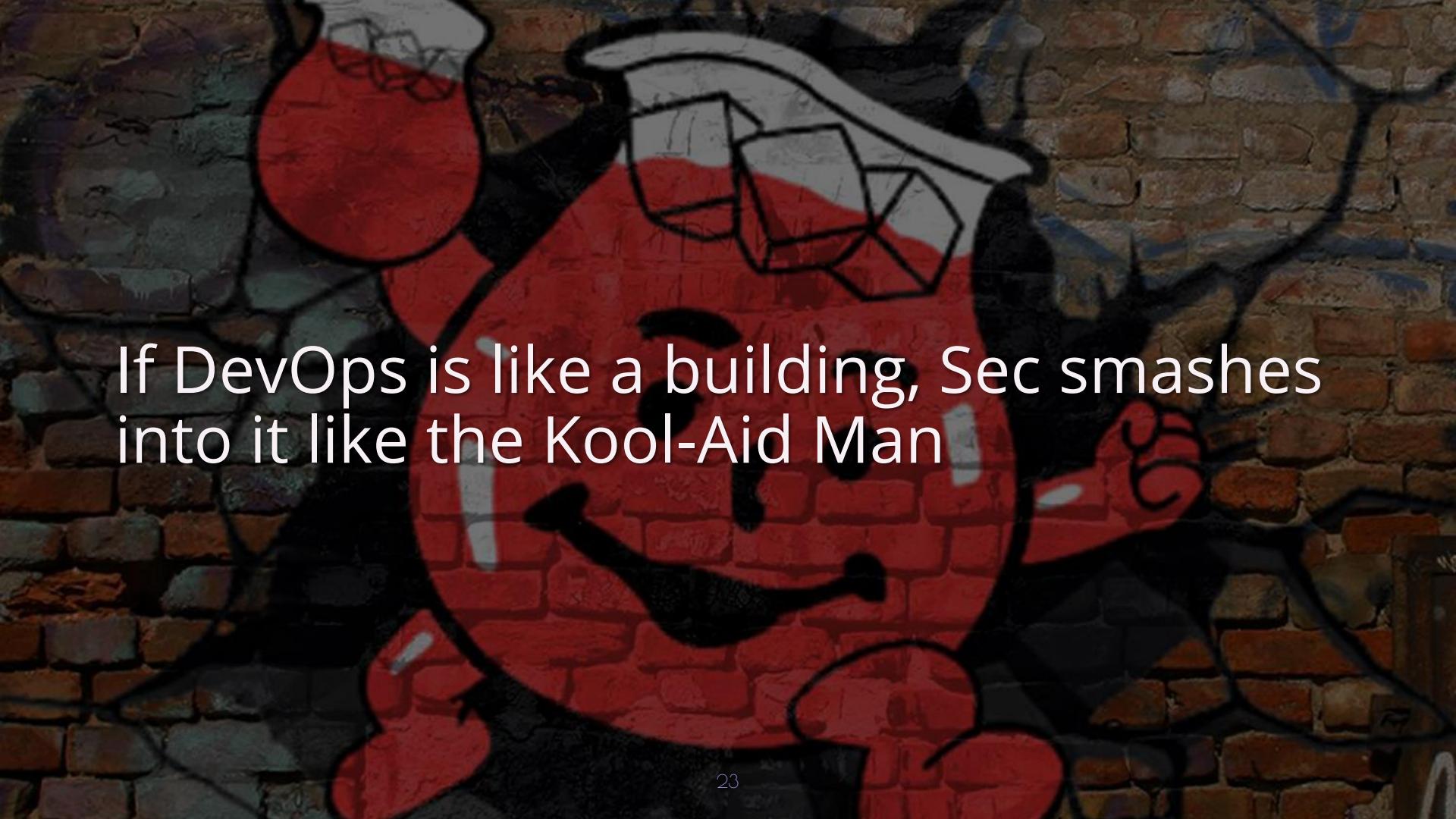
...and are the security tools' results
worthy of attention in the first place?

Too many security tools are “less than useless” from the SWE vantage point

Shifting Left is often more “shift friction earlier” than “build in security by design”

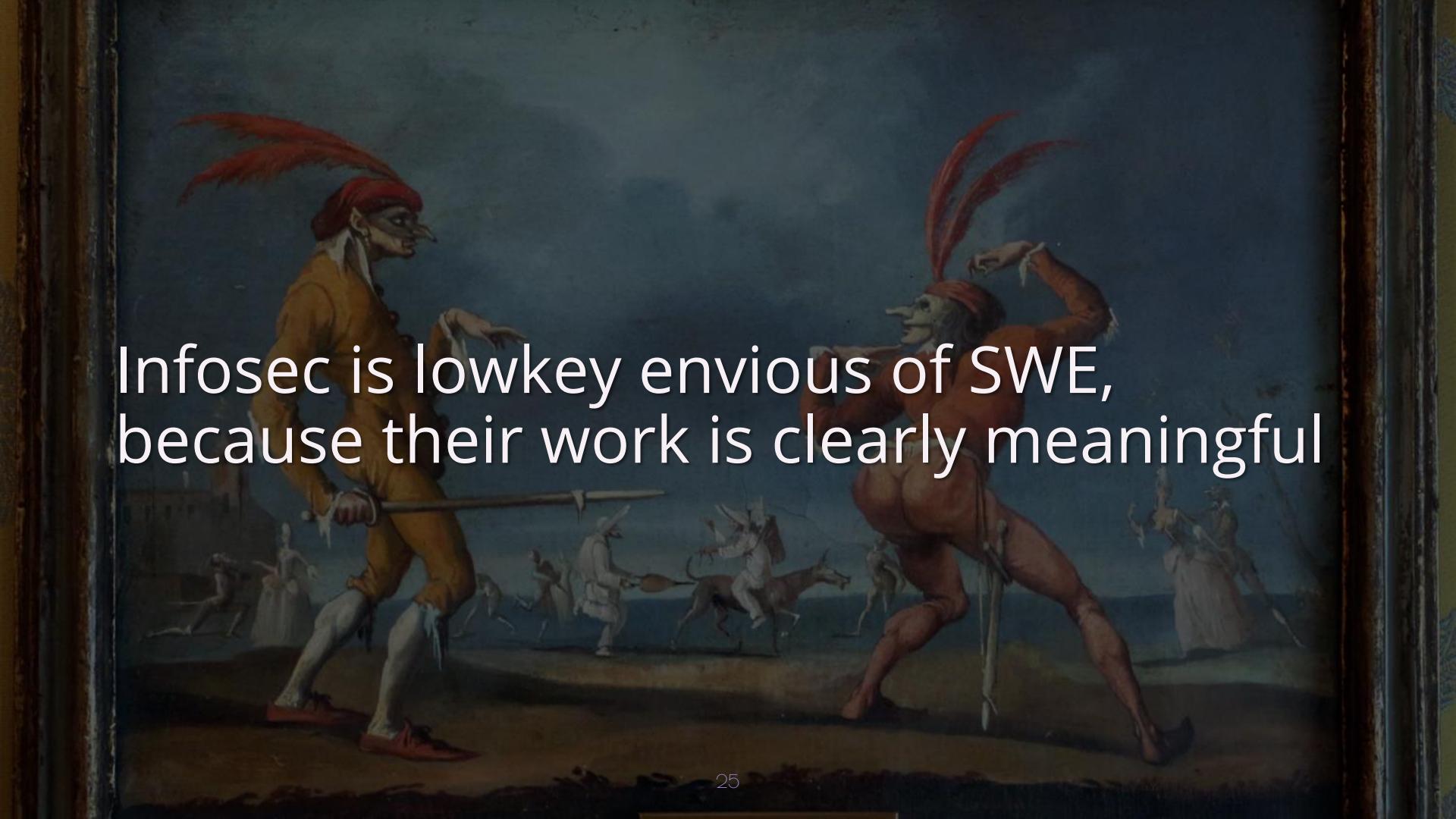
DevSecOps: “I’m not a regular Security Theater, I’m a cool Security Theater”

Jamming security in is different than aligning accountability & responsibility



If DevOps is like a building, Sec smashes
into it like the Kool-Aid Man

Driven by **FOMOsec**: wanting to *feel* like infosec is in control & not irrelevant



Infosec is lowkey envious of SWE,
because their work is clearly meaningful

FOMOsec's "Gotta Catch Em All" mindset
is a classic at the Security Theater

Infosec won't sit at the Big Kids' Business
Table if it stays a Security Theater kid

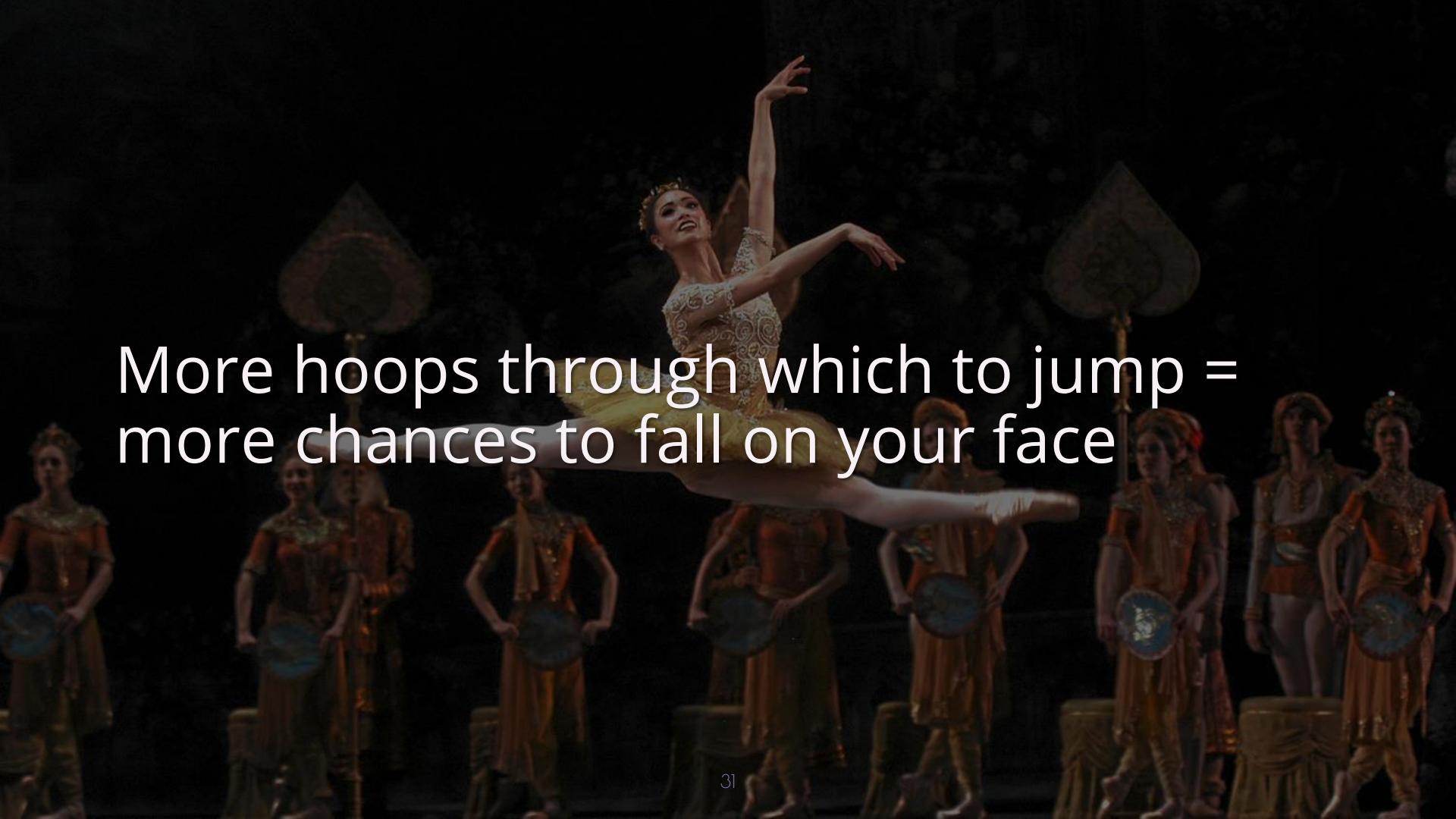
A dark, atmospheric photograph of an ornate theater interior. The ceiling is painted with a large, circular mural depicting a scene with figures and animals. The walls are lined with rows of dark theater seats. A curved balcony with a decorative railing runs along the side. The lighting is low, creating deep shadows and highlighting the intricate details of the architecture.

Frantically gripping a wheel to nowhere
results in stagnation, not stability

Stricter change management processes
do not lead to greater stability

46% - 60% of changes by “conservative” orgs lead to degraded service

– State of DevOps research by Dr. Forsgren

A ballerina in a white tutu and gold headpiece is captured mid-air, performing a high kick. She is positioned centrally against a dark background. In the foreground, a line of performers in traditional-style costumes, including men in tunics and women in orange dresses, stand holding large, ornate blue shields. The scene is dramatically lit from above, creating strong highlights and shadows.

More hoops through which to jump =
more chances to fall on your face

Cumbersome change management will hinder speedy patch deployments, too

The reality: security must be adaptive

The background of the slide shows a dark theater with rows of red velvet seats. A red curtain is visible at the top. The lighting is low, creating a dramatic atmosphere.

How do we spot Security Theater's red flags? And is there a better way ahead?

Act II: Fisticuffs



Fisticuffs emerges due to how to treat failure & where accountability rests

Security Chaos Engineering: Let's harness failure to build knowledge

Security Theater: Avoid failure at all costs
and punish any humans involved



Act II, Scene I: The Duel

SCE: Failure is a natural part of systems

ST: Bad humans cause failures

SCE: Adapt to minimize incident impact

ST: Prevent failure from happening

SCE: Security is collaborative & open

ST: Security teams operate in a silo

SCE: Rewards system-level improvement

ST: Rewards rigidity & saying “no”

SCE Culture: Learning & experimenting

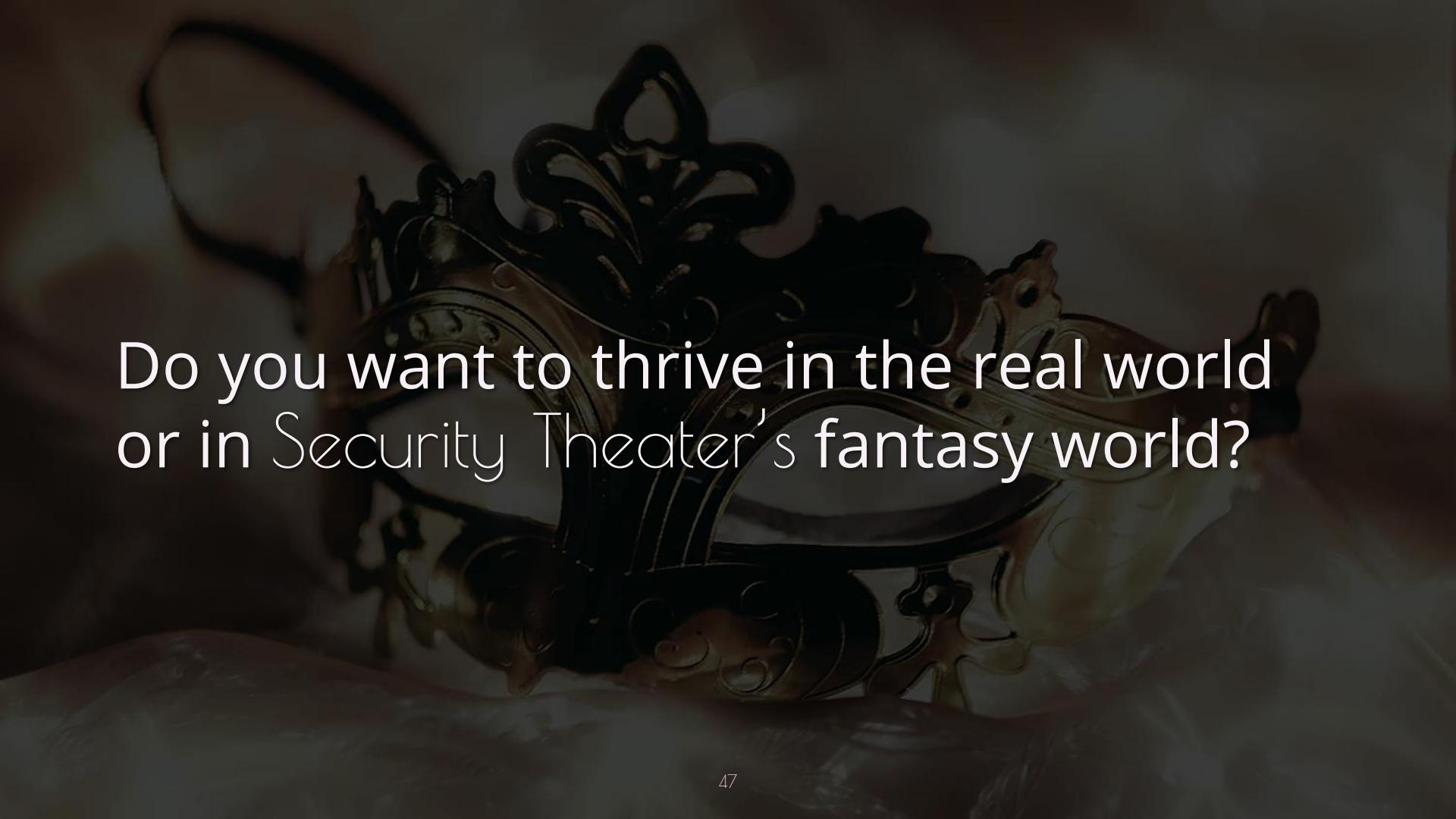
ST Culture: Fear and mistrust

SCE: Principles-based and adaptive

ST: Rule-based & prefers the status-quo

SCE Testing: Speedy and transparent

ST Testing: Manual, slow, and opaque

A close-up, low-angle shot of a hand gripping a highly ornate, gold-colored propeller or steering wheel. The object is intricately detailed with floral and geometric patterns. The background is dark and out of focus.

Do you want to thrive in the real world
or in Security Theater's **fantasy** world?

Security Chaos Engineering cares about meaningful outcomes (anti-FOMOSec)

A ballerina in a white tutu is captured mid-dance against a dark background. She is performing a high kick, with her right leg extended straight up and her foot in a pointe. Her arms are elegantly positioned to balance the pose. The tutu is full and white, contrasting with the dark stage.

SCE aligns with how dev and ops already
thinks and operates

Joining the Security Theater results in a dangerous, self-fulfilling prophecy...

A dramatic, low-key photograph of two figures, possibly actors or models, dressed in flowing white robes. They are positioned in a dark, hazy space, with one figure on the left reaching out with their right hand towards the other figure's face. The second figure is partially obscured by shadow, with only their head and shoulder visible. The lighting is moody and atmospheric, creating strong shadows and highlights on the robes and hands.

Strict control within a culture of fear
turns the innocent into bad apples

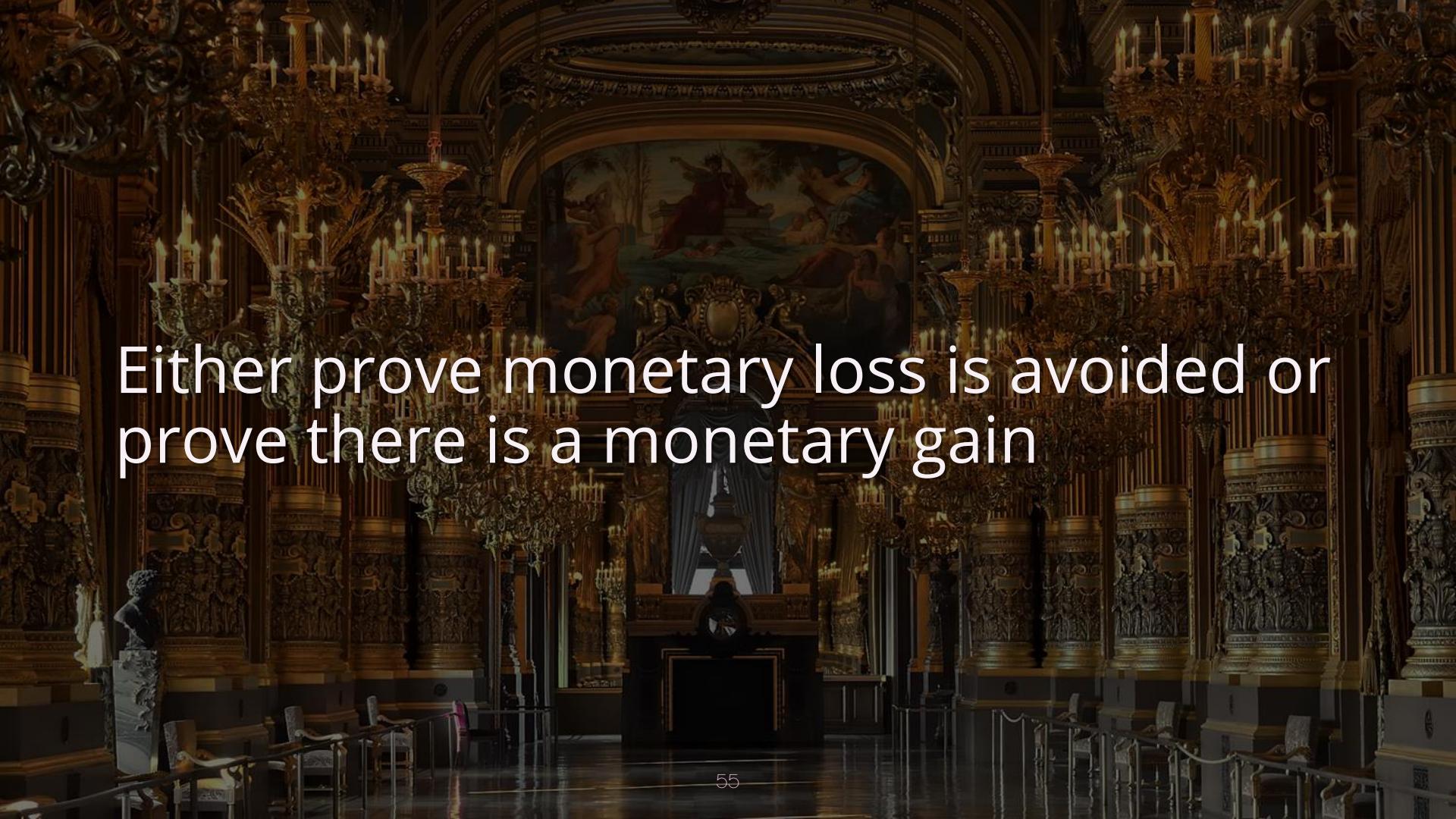
The background is a dark, atmospheric illustration of a theater interior. Red velvet curtains are drawn back, revealing a stage area with some equipment. The walls are decorated with intricate gold-colored patterns. In the foreground, the backs of many audience members' heads are visible, showing they are seated in rows of ornate green theater chairs.

Act II, Scene II: Judgment

A scene from a traditional Korean performance, likely a masked dance (Munmujeo). Several performers in elaborate costumes are shown in a dynamic, crouching pose. One central figure wears a large, ornate mask with long, sweeping eyebrows and a wide, toothy grin. He is surrounded by performers in red and blue tunics with yellow sashes and tall, decorative hats. The background features a dark, atmospheric setting with architectural elements and warm lighting.

Security Theatre shuns fair judgment

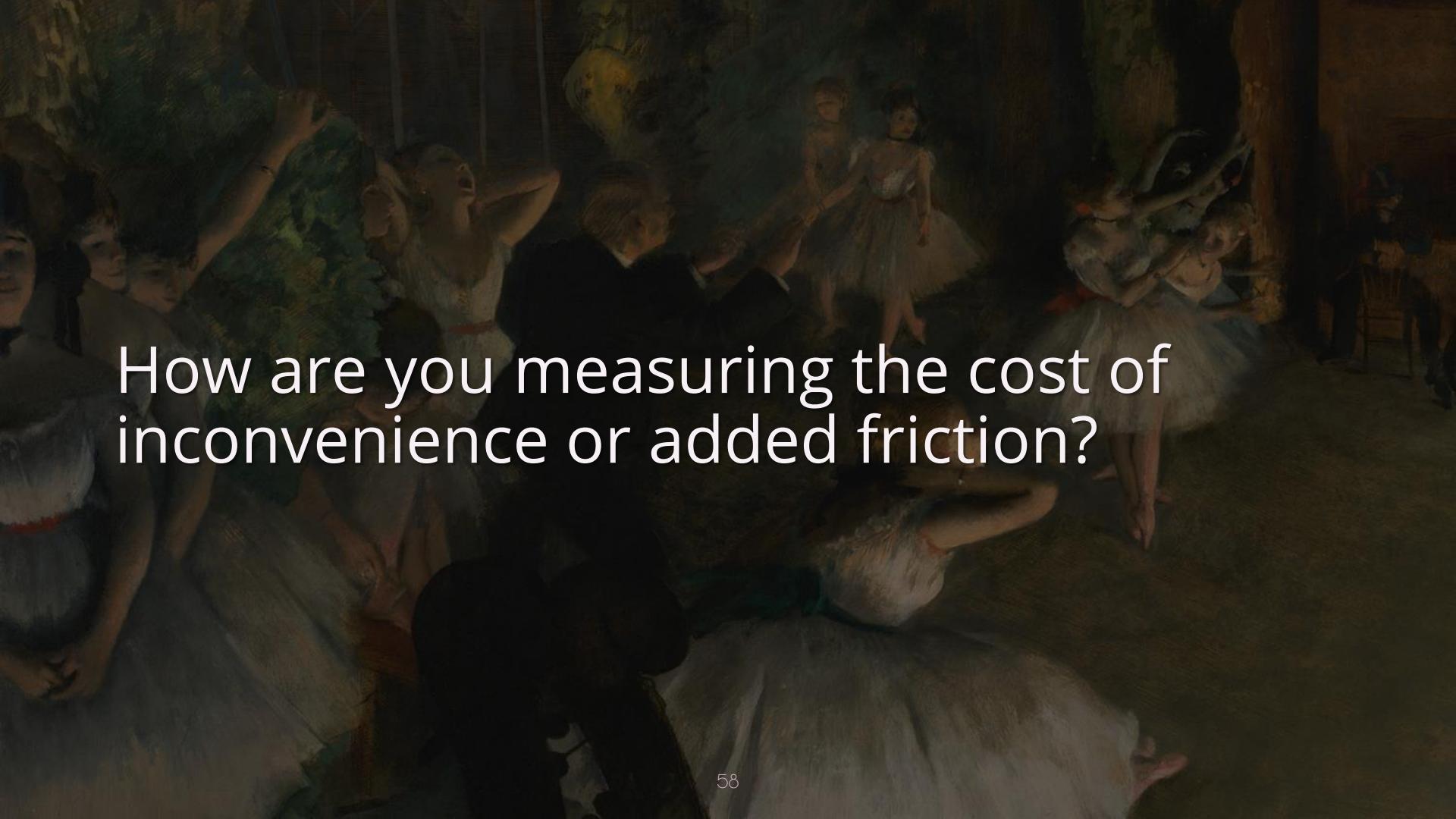
Moving away from ST towards SCE is a move towards success measurement

The background image depicts a highly ornate, neoclassical hall. The ceiling is dark with gold-colored moldings and features several large, multi-tiered chandeliers with numerous lit candles. A large, detailed painting on an arched wall depicts a scene with figures in a landscape. In the foreground, there is a dark, polished floor and some architectural details like columns and a bust statue on a pedestal.

Either prove monetary loss is avoided or
prove there is a monetary gain

What are the negative externalities of your security program?

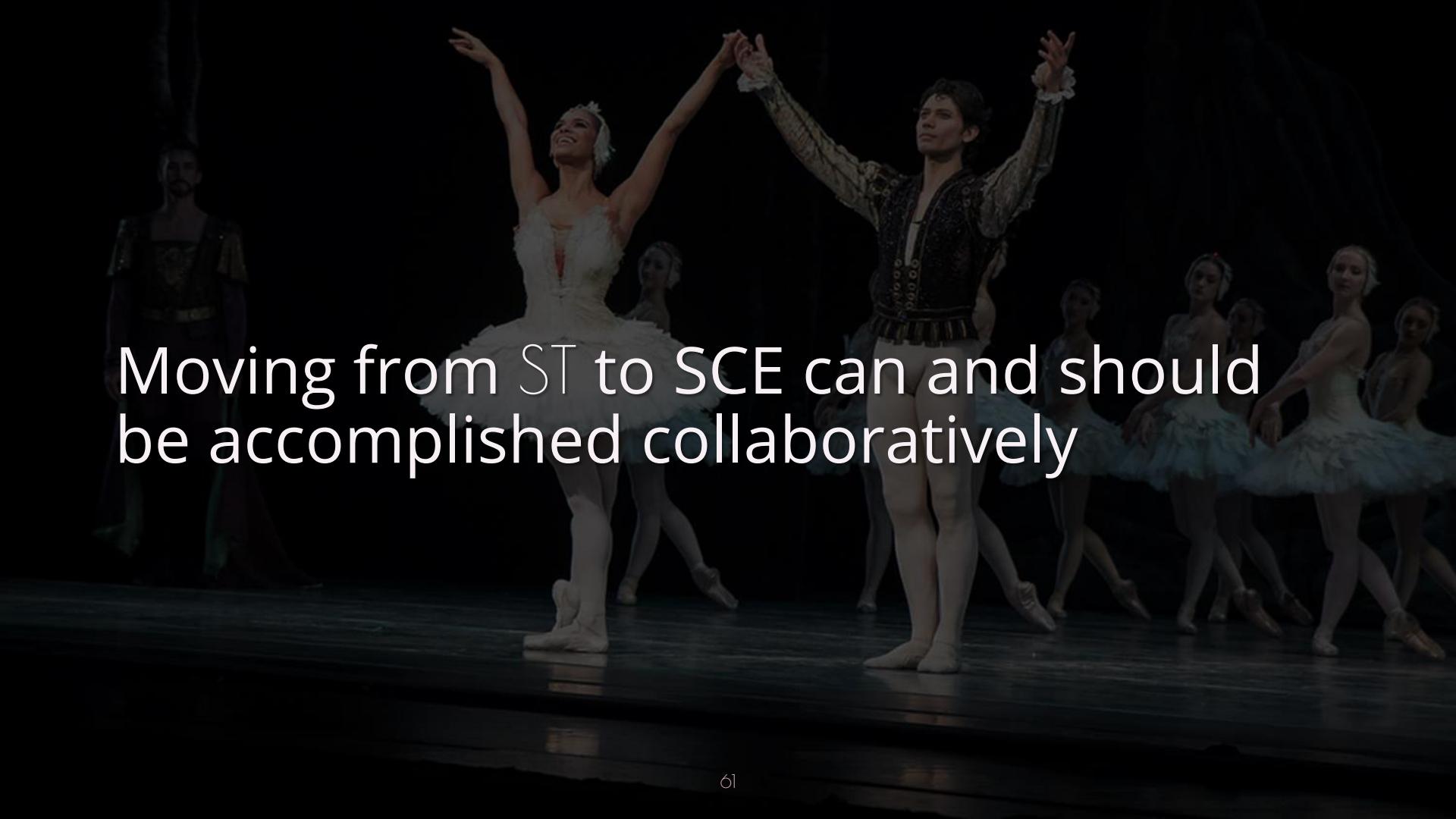
Security metrics are too often tone deaf
to what the rest of the org is doing

A dark, moody painting of ballerinas in tutus performing on stage. The scene is filled with motion and light, with figures blurred in the background.

How are you measuring the cost of
inconvenience or added friction?

Compare security code review coverage
vs. lead time or deploy frequency

Investigate any sources of friction and validate that it isn't due to security



Moving from ST to SCE can and should
be accomplished collaboratively

Act III: Redemption



A wide-angle shot of a stage during a grand opera performance. The stage is filled with a large ensemble of performers, mostly dressed in elaborate 19th-century-style costumes. In the center, a woman in a dark, ruffled dress lies on a bed or sofa, looking up at a man in a dark suit who stands beside her. To the left, another woman in a dark, patterned dress stands near a piano. The background features rich, dark curtains and a ceiling decorated with numerous small lights resembling stars. The overall atmosphere is dramatic and formal.

Security approvals don't have to suck

Optimize for “just enough” in security reviews and use evidence, not opinions

A wide-angle photograph of a theater interior during a performance. The seating consists of numerous rows of red upholstered theater seats. The auditorium is filled with spectators, though many seats are empty. The lighting is focused on the stage area, leaving the audience in relative darkness. The architecture features ornate gold-colored moldings and recessed lighting fixtures along the balconies.

Little's Law: $L = \lambda W$

Reducing the security review queue size
reduces the lead time to deploy

Treat high-impact changes differently
than low-impact changes



Act III, Scene I: High-risk, high-impact changes

High-risk, high impact changes are
worthy of security team scrutiny

High-risk, high-impact (HRHI) = affects the whole org or multiple products

Ensures the security team's efforts are prioritized more effectively

A wide-angle photograph of a grand concert hall. The ceiling is high and decorated with intricate gold-colored moldings and a large, multi-tiered crystal chandelier. The walls are made of light-colored wood paneling. In the foreground, a full orchestra is performing on a large stage. The musicians are dressed in dark formal attire and are playing various instruments, including violins, cellos, and brass instruments. The audience seating is visible in the background, arranged in several levels of balconies.

Who doesn't want to focus on higher-value work rather than battling noise?

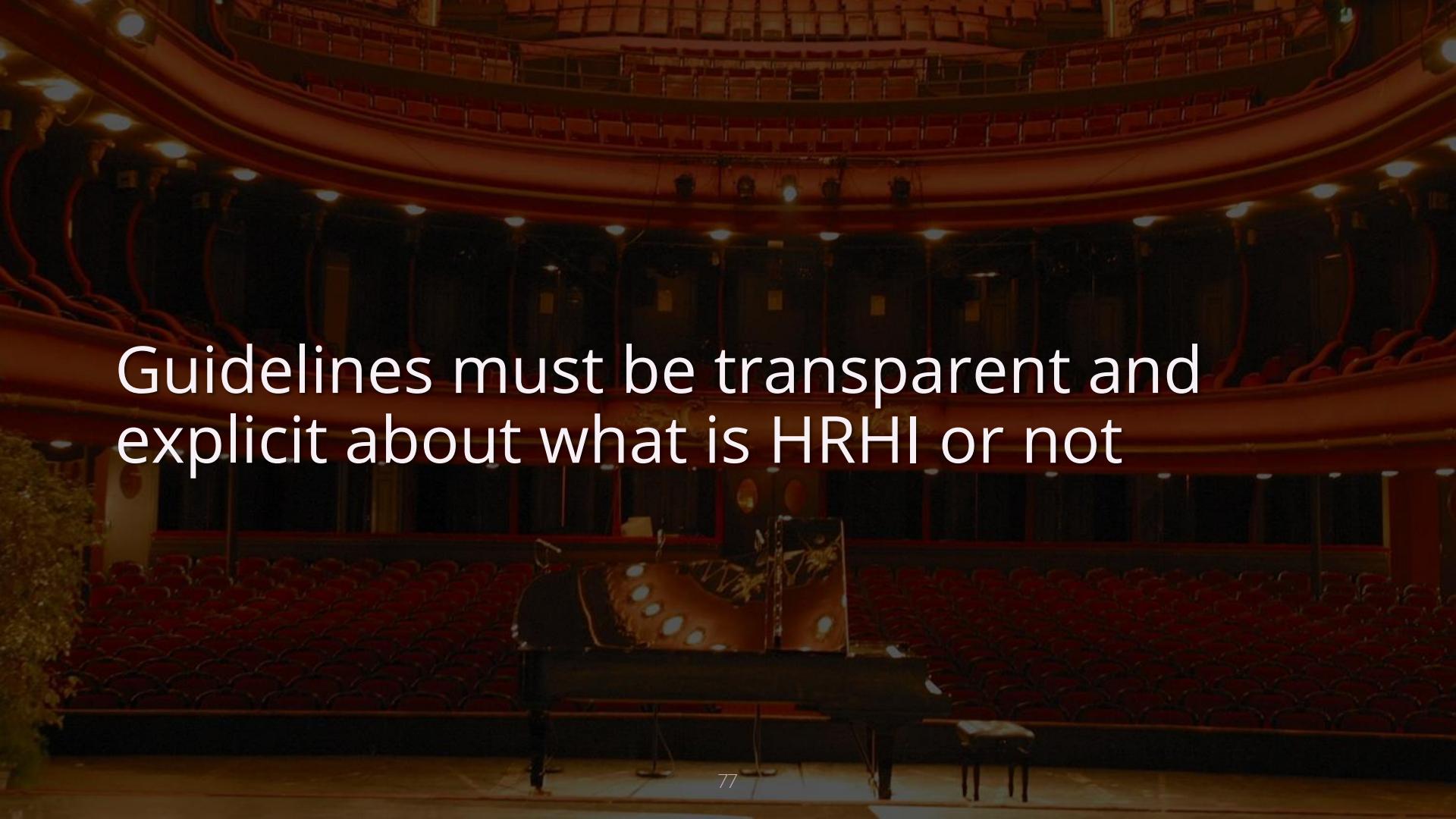
Product team is responsible for creating awareness & discussion of changes

A photograph of a ballet performance. Several dancers are on stage, some in the foreground and others slightly behind. They are wearing elaborate costumes, including a woman in a white tutu with a large red bow, a man in a blue and white outfit, and another man in a dark costume. The background is dark, making the performers stand out.

HRHI changes require sign-off by P&E leaders & acceptance of accountability

Security reviews are timeboxed &
limited in number to optimize attention

Build a redundancy plan for extra urgent HRHI changes (just in case)

A wide-angle photograph of a grand theater interior. The seating consists of numerous red upholstered chairs arranged in a semi-circular pattern. The ceiling is high and features multiple rows of recessed lighting. On the stage, there is a large, ornate set piece resembling a giant shell or conch. The overall atmosphere is formal and grand.

Guidelines must be transparent and explicit about what is HRHI or not

Retros on change impacts build
knowledge & should be shared widely

A dramatic scene from a production of "The Merry Widow". A woman in a white dress stands triumphantly in the center, her arms raised in victory. She is surrounded by a large group of men in blue military uniforms and green helmets, all looking up at her with admiration. The lighting is low, creating a moody atmosphere.

Act III, Scene II: Low-risk, low-impact changes

tl;dr straightforward classification and automated exemption process

The background image shows a dark, ornate interior of a grand hall, possibly a theater or a grand ballroom. A large, curved staircase leads upwards through the center. The walls are lined with gold-colored moldings and framed pictures. Several chandeliers hang from the ceiling, their light reflecting off the polished surfaces. In the distance, a few people can be seen walking up the stairs.

Incentivize appropriate security handling vs. incentivizing bypasses

Assessments & cross-team discussions
are unnecessary for LRLI changes

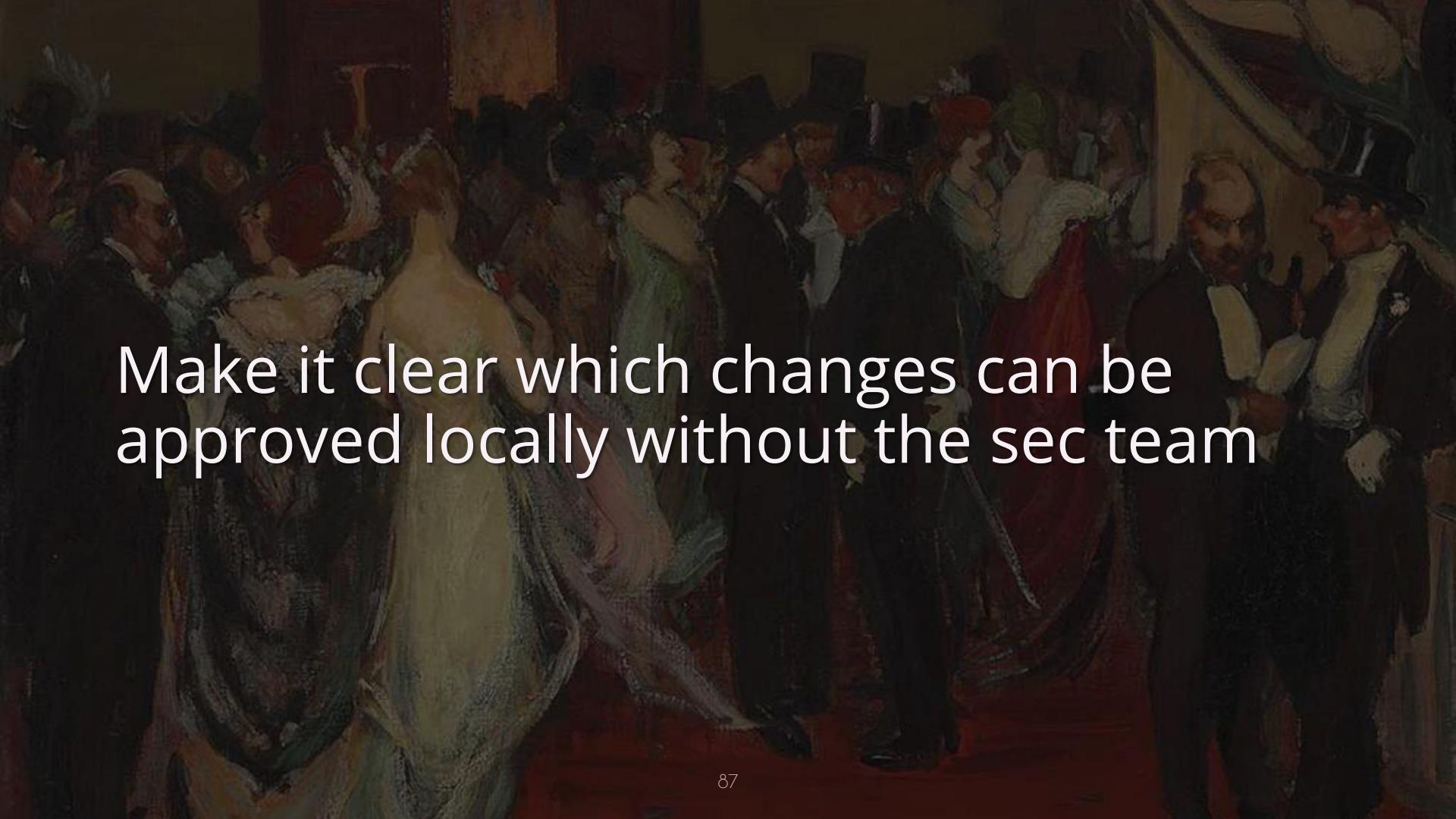
Classification with recommended steps for low, standard, critical, informational

A painting depicting a backstage scene, likely a rehearsal room for a ballet. Several figures are visible, including a woman in the foreground wearing a yellow top and a necklace, looking down at an open book or document. Other figures are seen in the background, some in tutus, suggesting they are ballerinas. The lighting is dramatic, with strong highlights and shadows.

Pipeline automation can facilitate exception handling (but also document!)

Encourage local approvals and peer reviews for LRLI changes

Track if LRLI changes are resulting in high impacts, then tweak the process



Make it clear which changes can be approved locally without the sec team

LRLI changes could include pricing updates, new cat gifs, tooltip copy...



The Grande Finale

The background image shows the interior of a grand theater. The walls and balconies are richly decorated with gold-colored, highly detailed carvings and moldings. The lighting is low, creating a dramatic and somewhat mysterious atmosphere. In the lower-middle section, a person is visible on a balcony, looking down towards the stage area.

Security Theater prioritizes gatekeeping
more than security outcomes



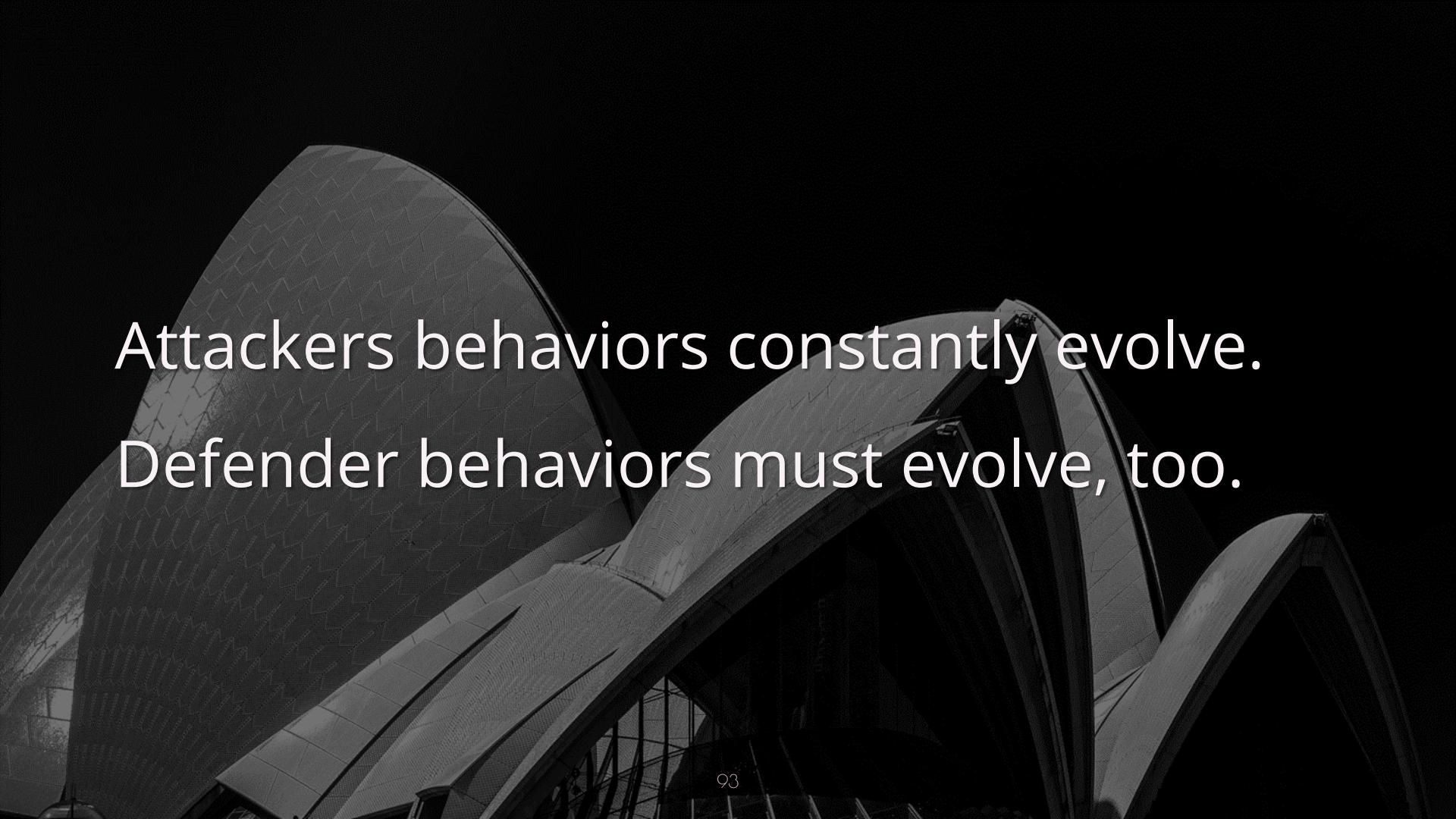
THE WORLD IS
TEMPORARILY CLOSED

WORLD

Heavy security approvals promote
friction and **bottlenecks**, not stability

A ballerina in a white tutu is performing a grand jete in the center of the stage. She is in mid-air, her arms extended elegantly. Behind her, a group of swans in white tutus are performing a synchronized pose. The background is dark, creating a dramatic effect.

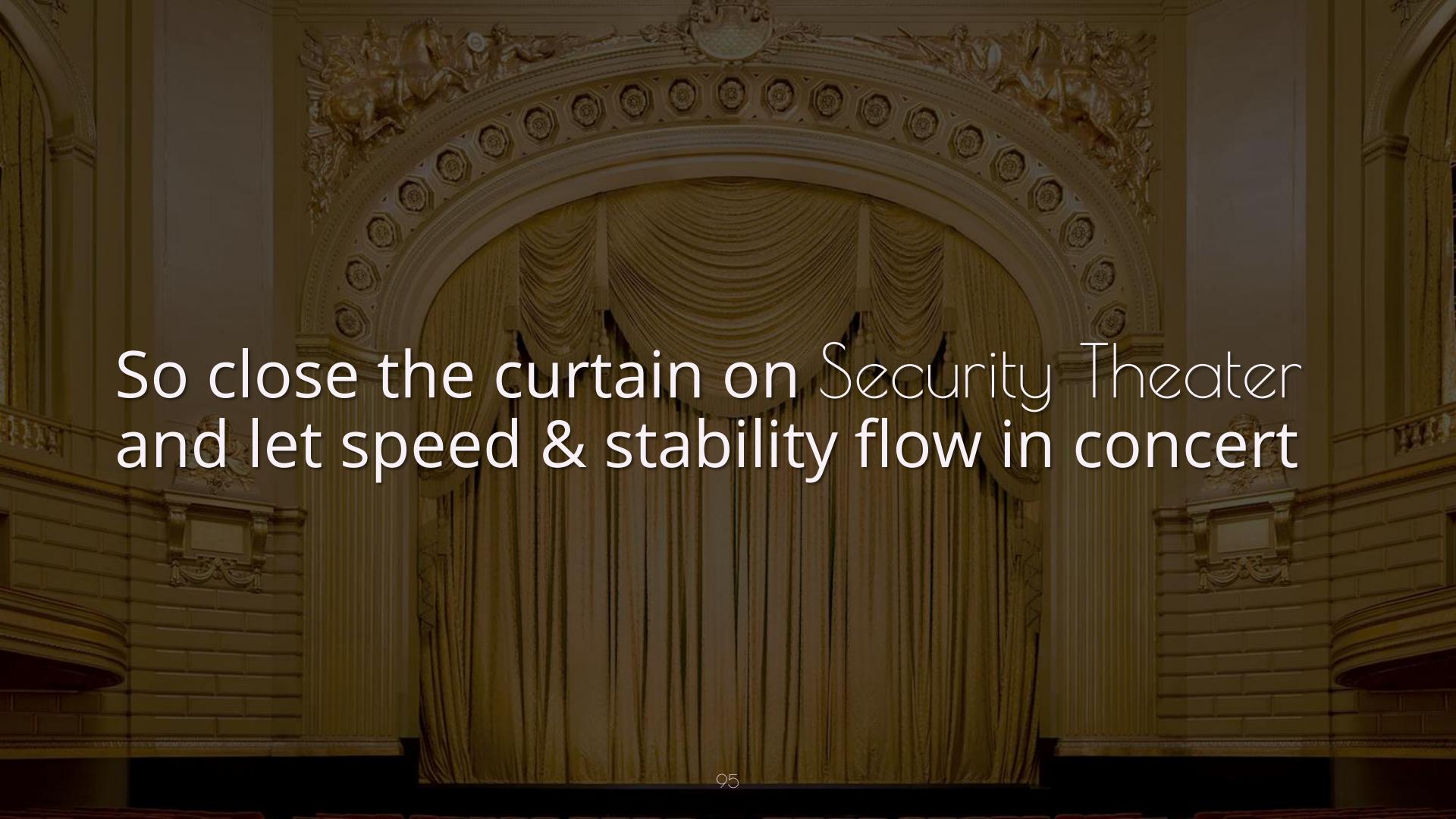
Strive for continuous improvement
through Security Chaos Engineering



Attackers behaviors constantly evolve.
Defender behaviors must evolve, too.

A scene from a production of 'The Merry Wives of Windsor'. In the center, Sir John Falstaff (John Lithgow) in his ornate green velvet doublet and hose, is being playfully poked in the nose by Mrs. Ford (Audra McDonald) in her voluminous yellow dress. Other characters in period clothing are visible in the background.

Treat security teams as **advisors** & hold
P&E teams **accountable** for changes

The background image shows a grand theater stage. A large, ornate arched proscenium is visible, featuring intricate gold-colored carvings and a decorative frieze. The stage itself is covered by a heavy, gold-colored curtain. The walls of the theater are also decorated with gold-colored moldings and architectural details. The overall atmosphere is one of luxury and tradition.

So close the curtain on Security Theater
and let speed & stability flow in concert

“People don't want their lives fixed.
Nobody wants their problems solved. Their
dramas. Their distractions. Their stories
resolved. Their messes cleaned up.
Because what would they have left? Just
the big scary unknown.”

- Chuck Palahniuk

Our forthcoming report
(early November):
<https://bit.ly/35fYxNR>

Security Chaos Engineering

Gaining Confidence in Resilience
and Safety at Speed and Scale

Aaron Rinehart & Kelly Shortridge

REPORT



@swagitda_



/in/kellyshortridge



https://get.oreilly.com/ind_security-chaos-engineering.html