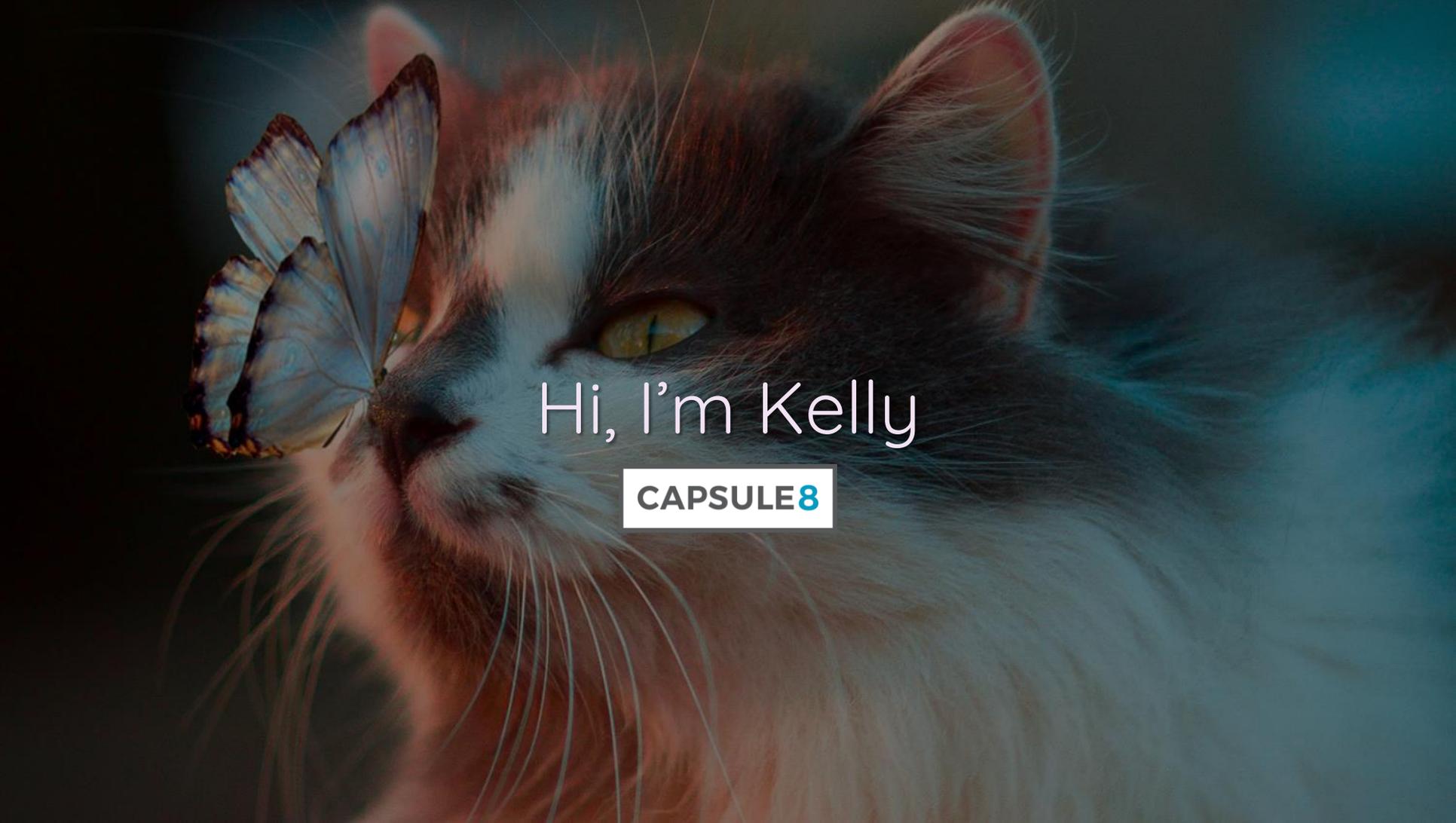




Security Delusions

Kelly Shortridge (@swagitda_)

QCon NYC 2019

A close-up photograph of a cat's face, primarily white with dark patches around its eyes and ears. A blue and white butterfly is perched on the cat's nose. The background is dark and out of focus. The text "Hi, I'm Kelly" is overlaid in white, and "CAPSULE 8" is in a white box with a blue number 8.

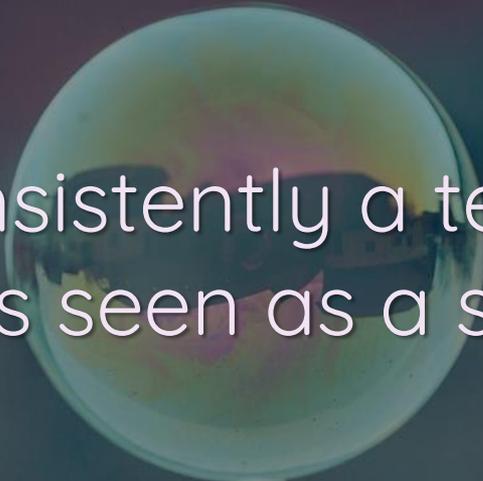
Hi, I'm Kelly

CAPSULE 8



“Ignorance is the parent of fear.”

— Herman Melville, *Moby Dick*



Infosec is consistently a tech laggard –
“skepticism” is seen as a strength

A landscape photograph featuring a green field with several sheep. In the foreground, two sheep are prominent: one with large, curved horns and another smaller one. In the background, there are more sheep grazing. A vibrant rainbow arches across the sky, which is filled with dramatic, dark clouds. The overall scene suggests a rural, pastoral setting.

How can you herd these frightened sheep to modern tech pastures?

1. A History of Cloud Compunction
2. APIs: Infosec's Anathema
3. The Curse of Containers
4. Cheat Codes for Dealing with This



A History of Cloud Compunction



“Cloud transformation” ruffled infosec feathers in the early 2010s

“Storing data online,” shared resources,
insider threat, DDoS, supply chain...

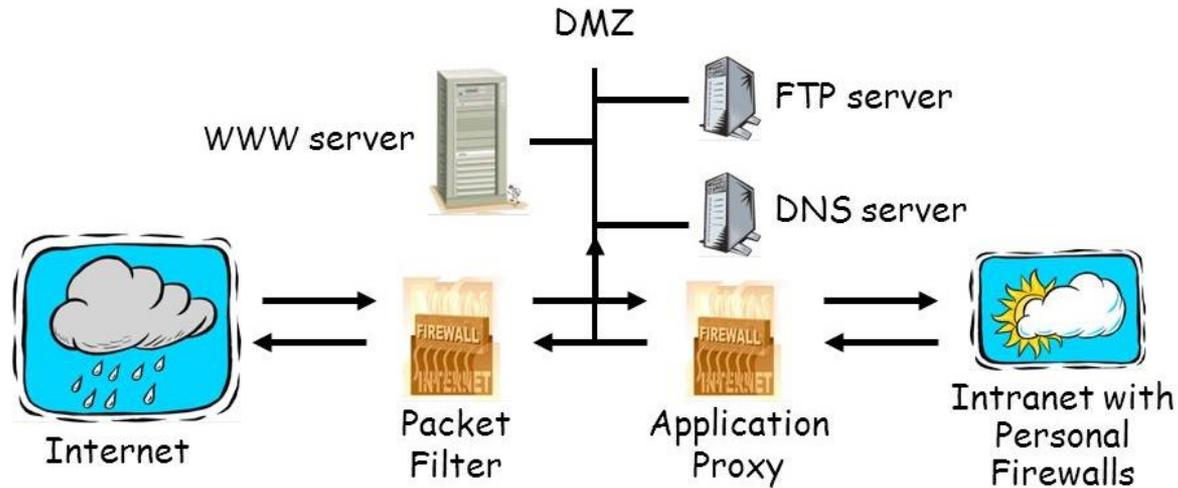


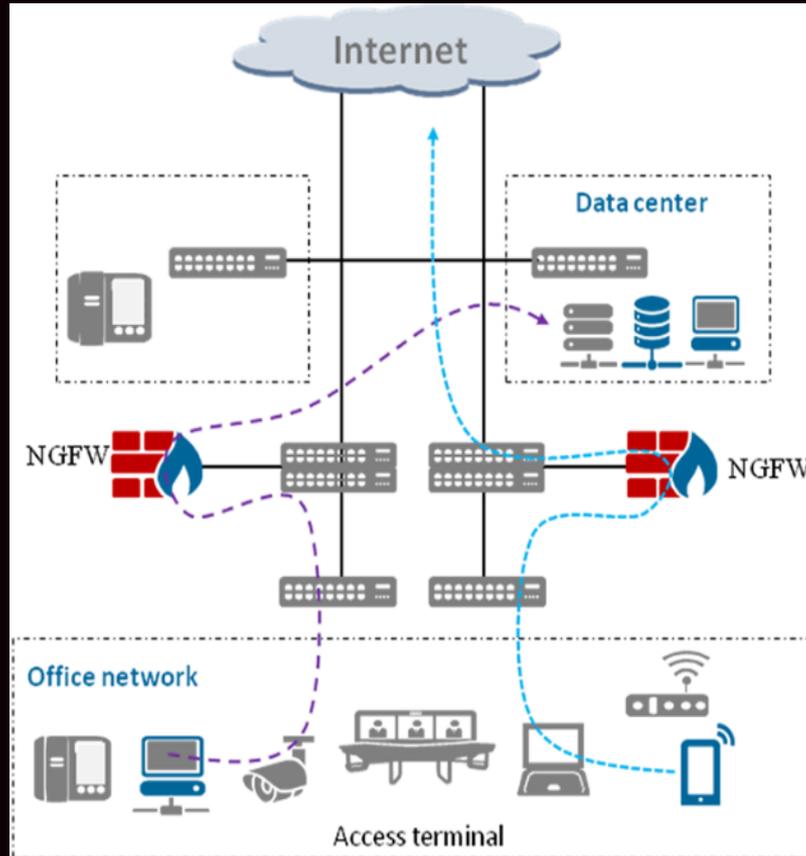
The crux of cloud fear was rooted in a
loss of control by the infosec team

The firewall was always the center of the enterprise infosec universe

Firewalls and Defense in Depth

- Example security architecture





Defense in Depth model: the firewall is the first line of defense

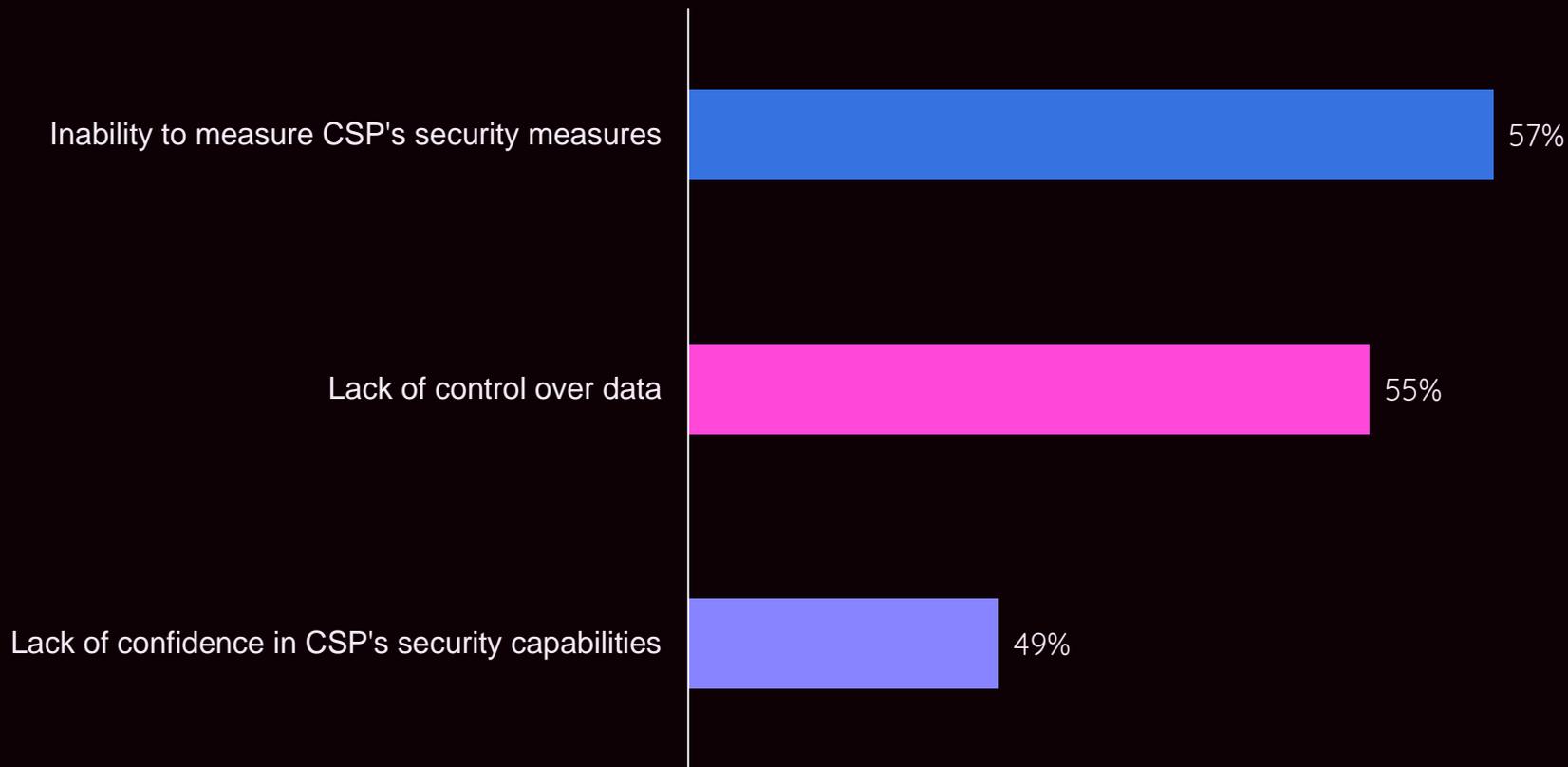


Cloud + microservices represents a
Copernican revolution for infosec

What do surveys from yesteryear reveal about infosec's fear of cloud tech?



2012: “What is holding back cloud?”

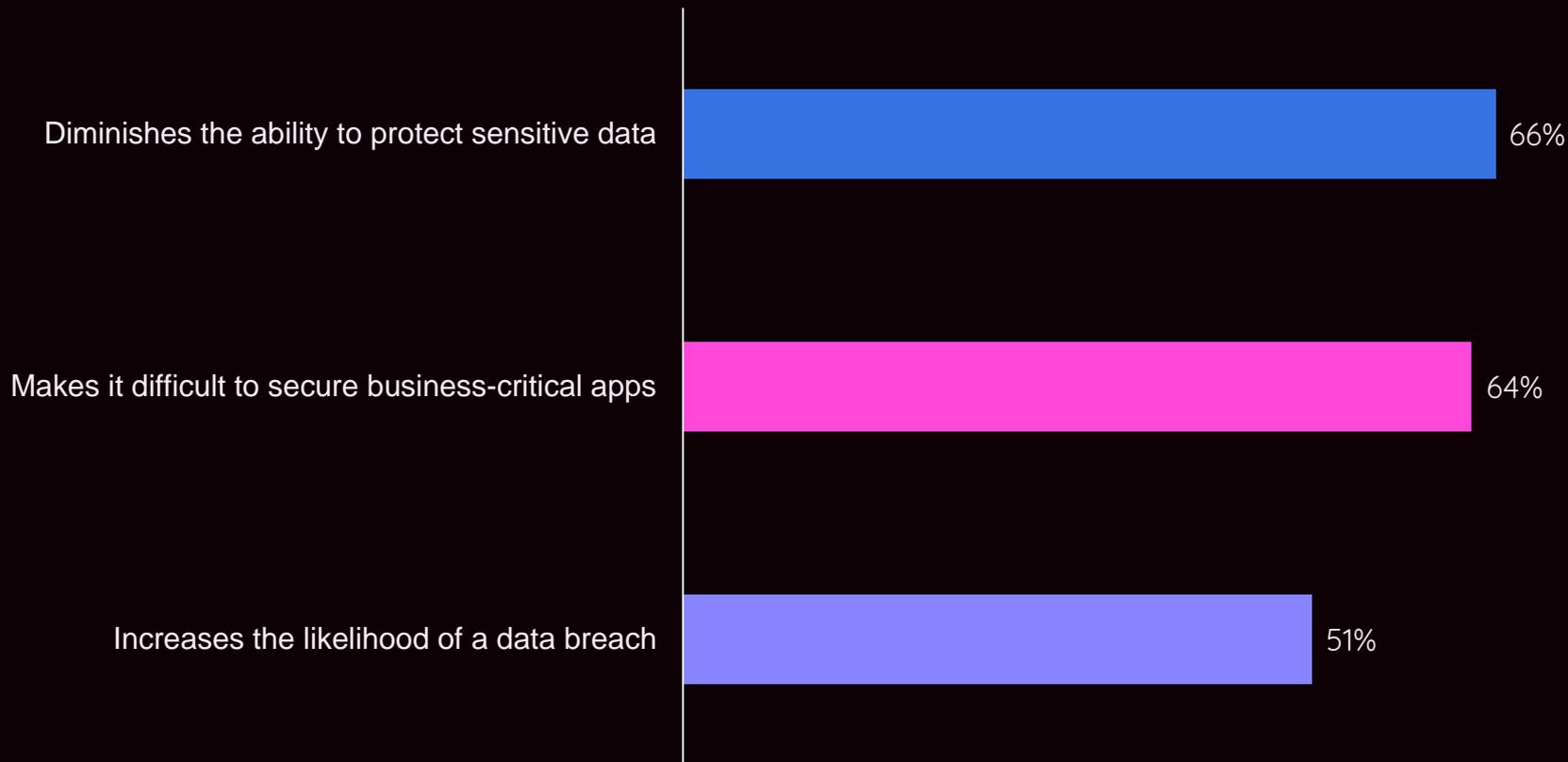


Source: Intel

“Uneasiness about adequate firewalling”
= the pre-Copernican mindset

A dramatic, low-angle photograph of a stormy sky. The sky is filled with dark, heavy clouds, and several bright, jagged lightning bolts are visible, striking downwards. The bottom of the frame shows the dark silhouettes of trees against the stormy background. The overall mood is intense and ominous.

2014: Cloud Multiplier effect on security

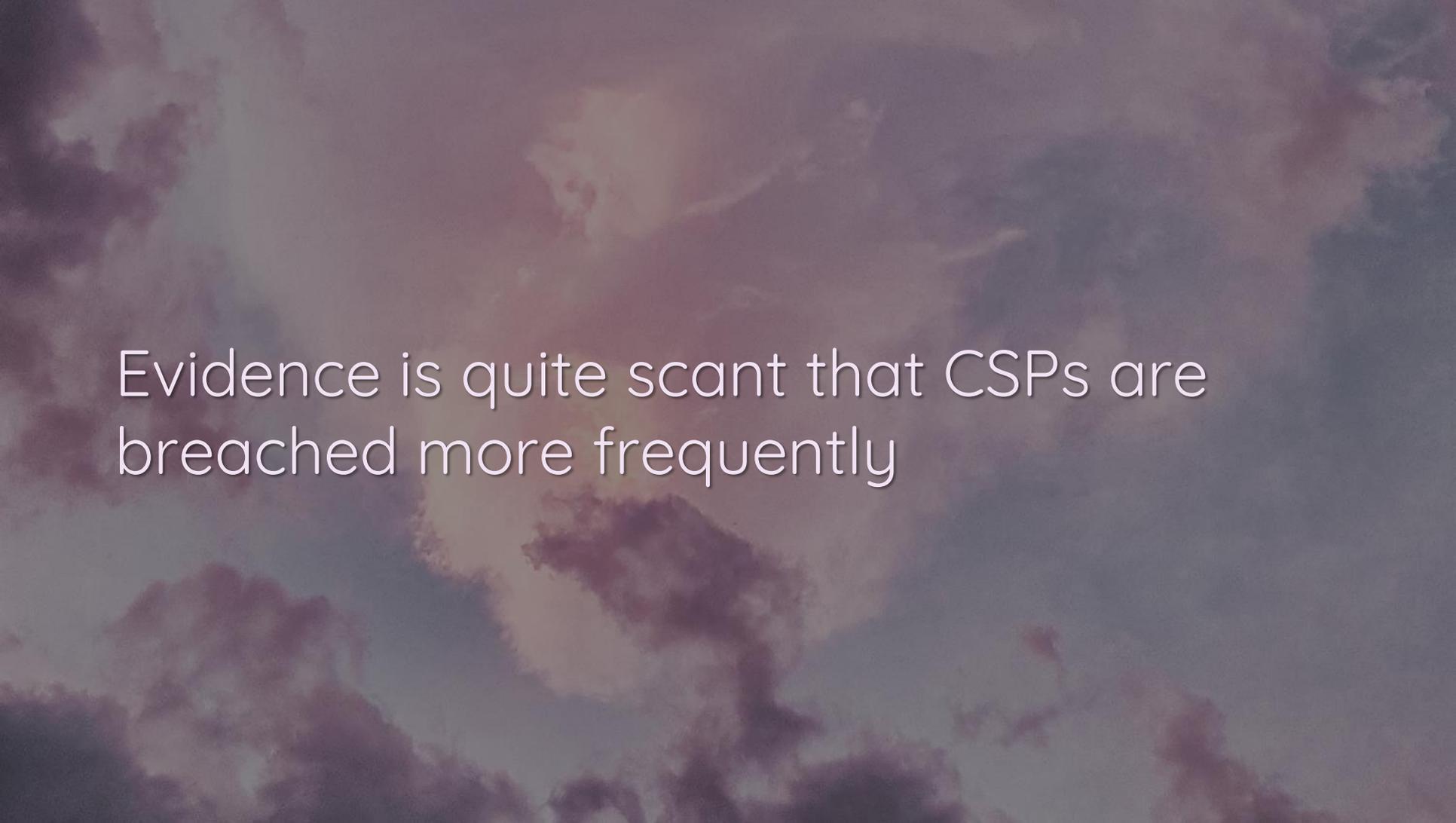


Source: Ponemon

2015: 71% view cloud data security as a big red flag & 38% feared loss of control

Source: Cloud Security Alliance

Endowment effect & sunk cost fallacy:
“Our security is better than CSPs!”



Evidence is quite scant that CSPs are breached more frequently

Acceptance that CSPs have better security is only in the past few years



Reality: misconfigurations are the biggest concern for cloud security

Gartner: “Through 2020, 80% of cloud breaches will be due to misconfiguration ... not cloud provider vulnerabilities”



Using cloud-native security controls can reduce security expense by 30%

Source: McKinsey

The background consists of several overlapping New Zealand dollar banknotes. Visible denominations include a \$10 note with a blue and orange bird, a \$20 note with a green frog, and a \$50 note with a blue fish. The notes are slightly out of focus and layered, creating a textured, financial backdrop.

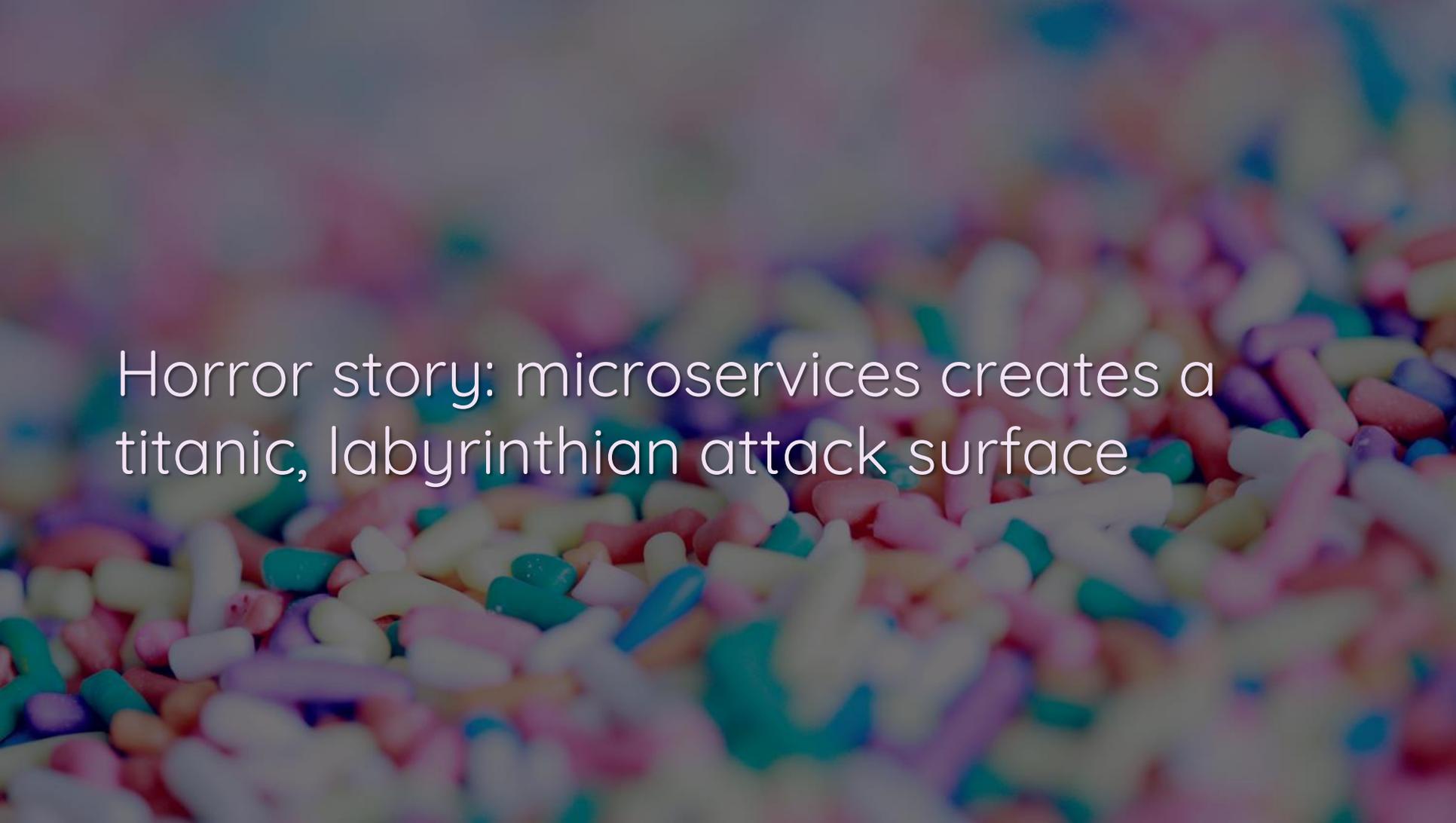
Network security blinky boxes often
carry price tags of \$100k - \$200k

So, how is infosec reacting to emerging tech today?

A grid of colorful lollipops on a pink background. The lollipops are arranged in a 6x10 grid. The colors of the lollipops, from top to bottom, are: red, yellow, orange, light green, blue, and purple. The text "APIs: Infosec's Anathema" is centered over the grid in a white, sans-serif font.

APIs: Infosec's Anathema

Microservices fears: APIs + containers



Horror story: microservices creates a titanic, labyrinthian attack surface

Basically monolithic app risk x 10,000 =
infosec's mental model of microservices



Revisionist history: as long as the perimeter is secure, the org is safe

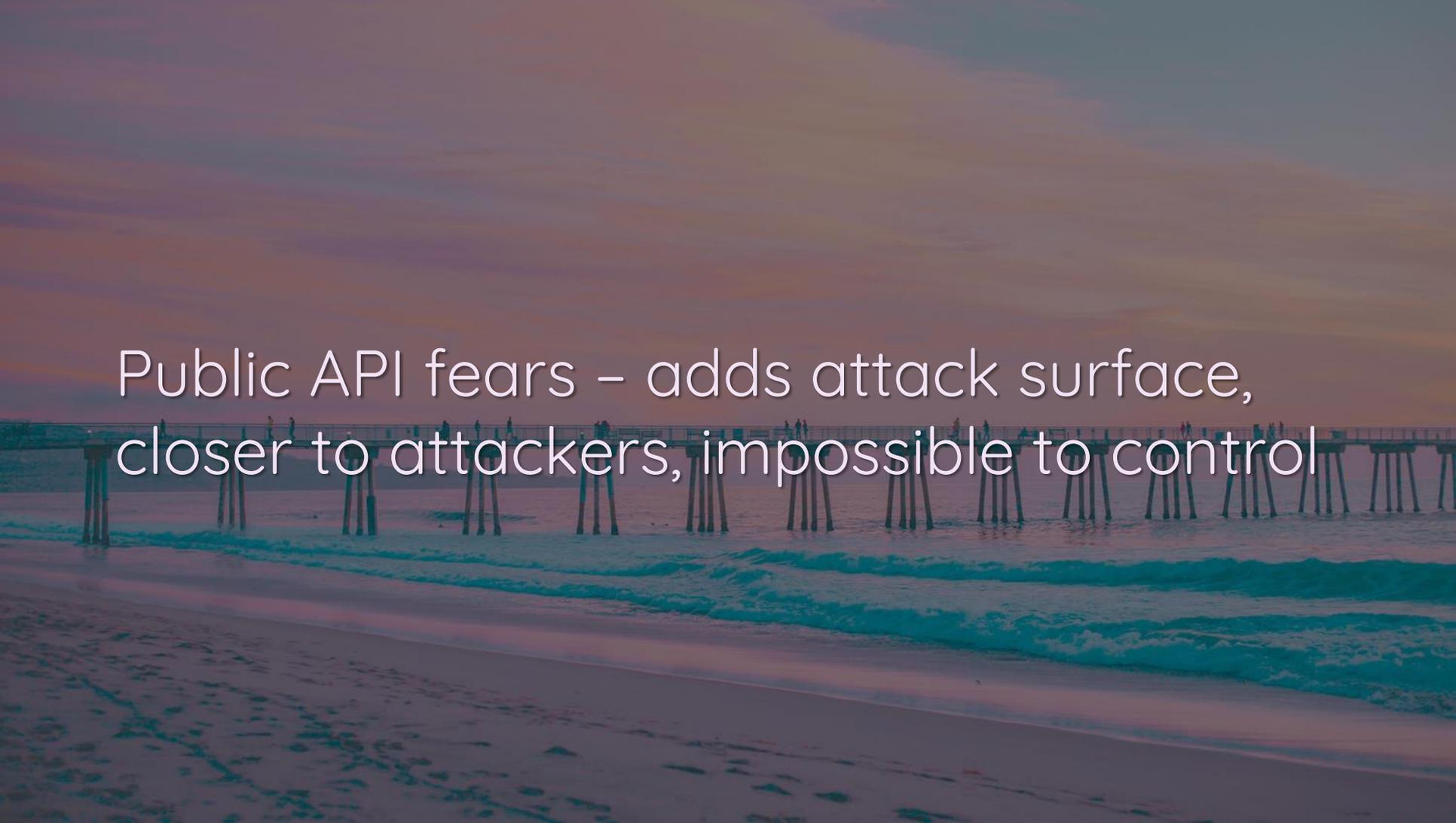
Real history: lateral movement was easy
because everything else was #yolosec

A wooden observation tower with a gabled roof, elevated on four wooden posts. It is situated on a pier with a metal railing, overlooking a body of water at dusk. The sky is a soft, hazy purple and blue. The tower has a small window and a door. The overall mood is quiet and contemplative.

Public-by-default begets embedded security vs. bolt-on security – a big win

2018: 51% aren't certain the infosec team knows all APIs within the organization

Source: Ping Identity

A photograph of a beach at sunset. The sky is a mix of orange, pink, and purple. The ocean is dark with white foam from waves breaking on the shore. A long pier with many wooden posts extends from the beach into the water. Several people are visible walking on the pier. The text "Public API fears - adds attack surface, closer to attackers, impossible to control" is overlaid in white on the image.

Public API fears - adds attack surface,
closer to attackers, impossible to control

A lie: “Formerly, local networks had only a few connections to the outside world, & securing those endpoints was sufficient.”

A background image featuring several strings of clear, round string lights hanging diagonally across a bright blue sky with soft, white clouds. The lights are out of focus, creating a bokeh effect.

Public API fears – provides a “roadmap”
for underlying functionality of the app

Reality: “Security through obscurity” is a
garbage cop-out



Security resilience: assume your added security controls will fail



API endpoints actually raise the cost of attack – attack tools don't work & entire vuln classes are removed

Standardization begets security benefits
– but isn't a common concept in infosec

A stack of four macarons in shades of pink, purple, and green, with a yellow macaron on the side. The macarons are arranged in a stack of four, with a yellow macaron on the right side. The background is a soft, out-of-focus light color.

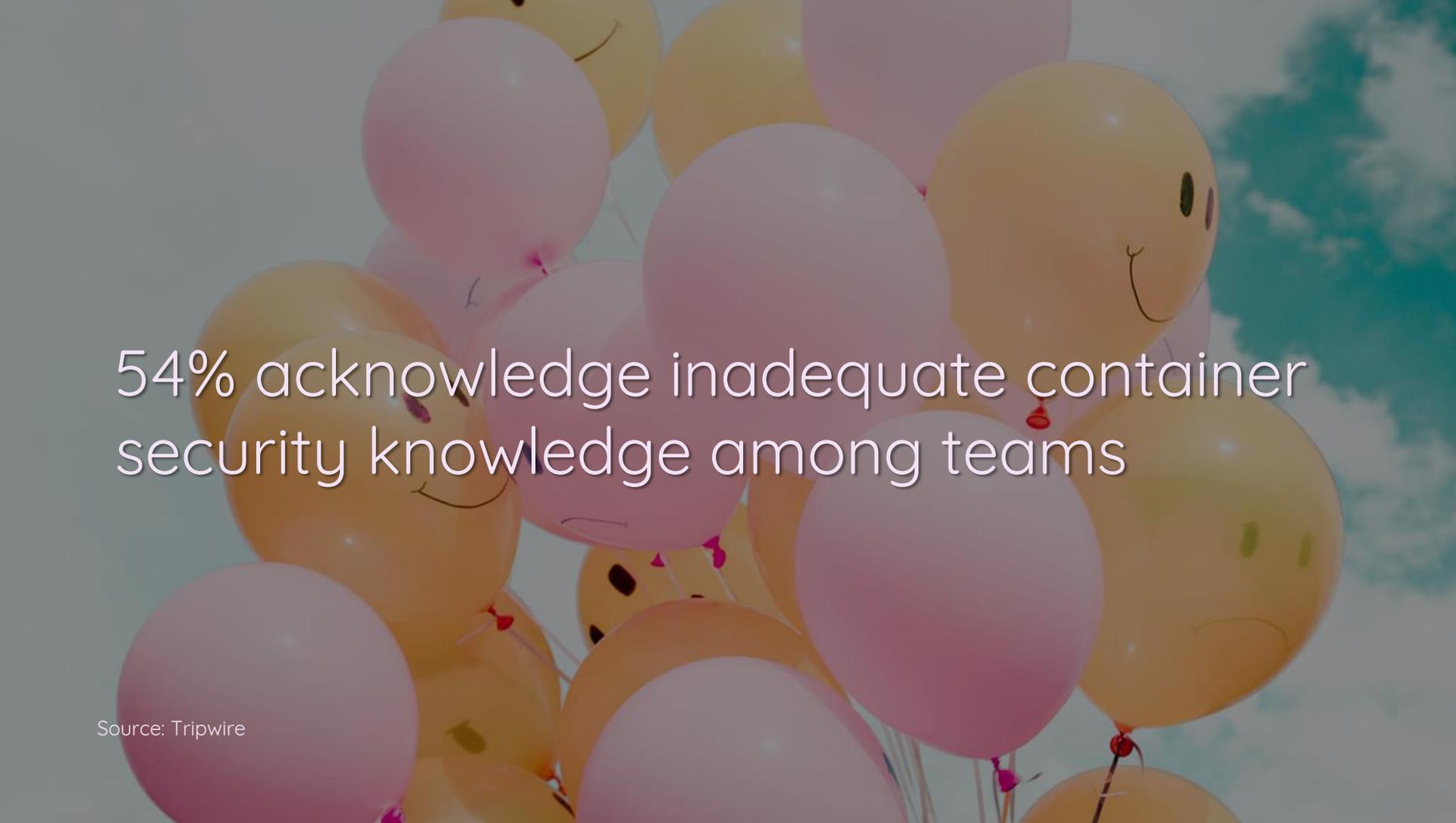
The Curse of Containers



Few in infosec realize containers aren't
just featherweight VMs

2019: 94% have concerns on container security – leading 42% to delay adoption

Source: Tripwire

A cluster of pink and yellow balloons with smiley faces against a blue sky background. The balloons are of various sizes and are tied together with strings. The background is a clear blue sky with some light clouds.

54% acknowledge inadequate container security knowledge among teams

Source: Tripwire



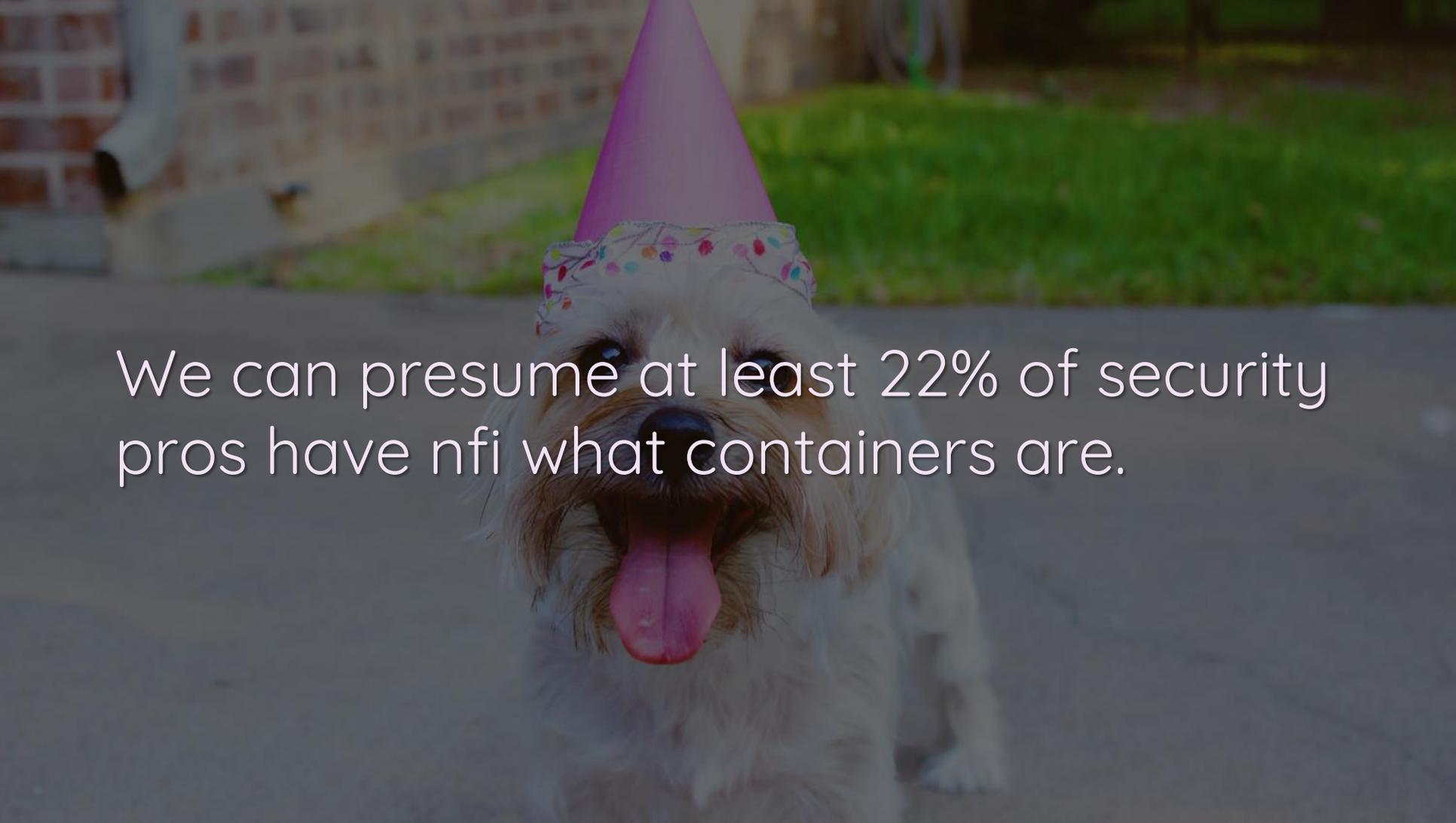
Source: Tripwire

52% want incident detection & response.
49% want isolation of pwned containers.

Source: Tripwire

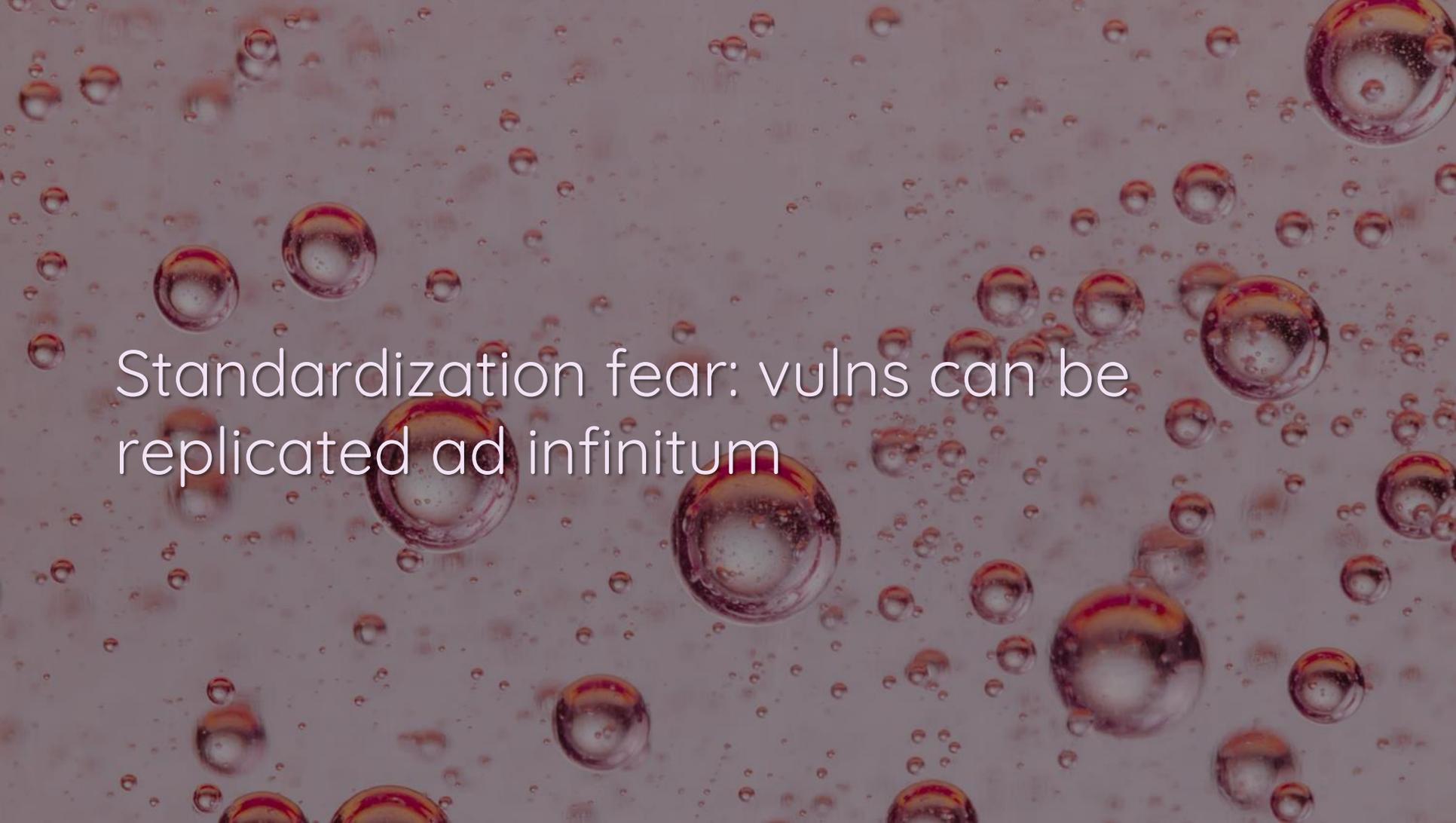
40% want “AI security analytics” & 22% want “blockchain” to secure containers.

Source: Tripwire



We can presume at least 22% of security pros have nfi what containers are.

Straw man: each container needs its own monitoring, management, & securing

The background of the image is a close-up, macro shot of numerous water droplets of various sizes scattered across a light-colored, slightly textured surface. The droplets are in sharp focus, showing their spherical shape and the way they reflect light, creating bright highlights and darker shadows. The overall color palette is soft and muted, with light pinks, greys, and whites. The text is centered horizontally and vertically over the image.

Standardization fear: vulns can be replicated ad infinitum

Because scanning for vulns in monolithic,
custom-built Java apps is easy???

Rose-tinted glasses: monolithic apps =
“You know exactly where the bad guys
are going to try to get in”

A photograph of a stack of green macarons and a glass bottle of milk. The macarons are stacked vertically, with one broken in the middle to show the filling. The bottle is filled with white milk and has a pink flower petal on the lid. The background is a plain, light color.

Microservices: easily mapped workflows
means easier threat models



Container fear: shared environments
(just like with cloud previously)

Should we go back to apps talking over FTP, telnet, SSH, random UDP ports, etc.?

A hand holding a scallop shell against a beach background. The background shows a sandy beach, the ocean, and a clear blue sky. The text is overlaid on the image.

Past: get in via a running FTP service

Containers: exploit the web server

Container fear: too easy for devs to use
vulnerable versions of software

As opposed to what – versions of Windows Server 2008 with Metasploit backdoors ready to go?



Separating complex functionality into
separate services is better for security

Now that we've explored the tinfoil universe, how do we return to reality?

A hand holding a lit sparkler in the water. The background is a dark, rippling body of water. The sparkler is lit, creating a bright burst of light and sparks that scatter across the upper half of the frame. The hand is positioned in the center, with the arm extending upwards from the water. The overall mood is one of hope or celebration amidst a dark, turbulent environment.

Cheat Codes for Dealing with This Mess

How can we evangelize real threat models & solutions in this new world?

A person wearing a white mask with the words "KISS ME" written in red on the forehead. The mask has a grotesque, bloody appearance with sharp teeth. The person is holding a spray can and is in a dark, industrial setting. The background is dark and blurry, suggesting an indoor environment with some structural elements.

Warning: Infosec largely views DevOps as a frenemy (at best)

“DevOps is like a black hole to security teams because they have no idea what DevOps is doing and have no way of ensuring security policy is enforced.”



Telling someone gripped by fear to
“calm down” will backfire

Acknowledge there are relevant concerns for using this tech – just not the ones they believe

The image features two glowing incandescent light bulbs, each housed within a large, clear glass sphere. The spheres are positioned in the foreground and background, creating a sense of depth. The background is a soft, out-of-focus purple. The text is centered in the upper half of the image, overlaid on the purple background.

Which concerns should you highlight?
There are three critical basics:

1. Don't expose cloud storage publicly
2. Don't use unauthenticated APIs
3. Don't use “god mode” in containers



Infosec's job becomes validating adherence to established best practices

Analogize “new security” to pre-Copernican methods to facilitate comms



Example: security groups & network
isolation by CSPs = firewall equivalent

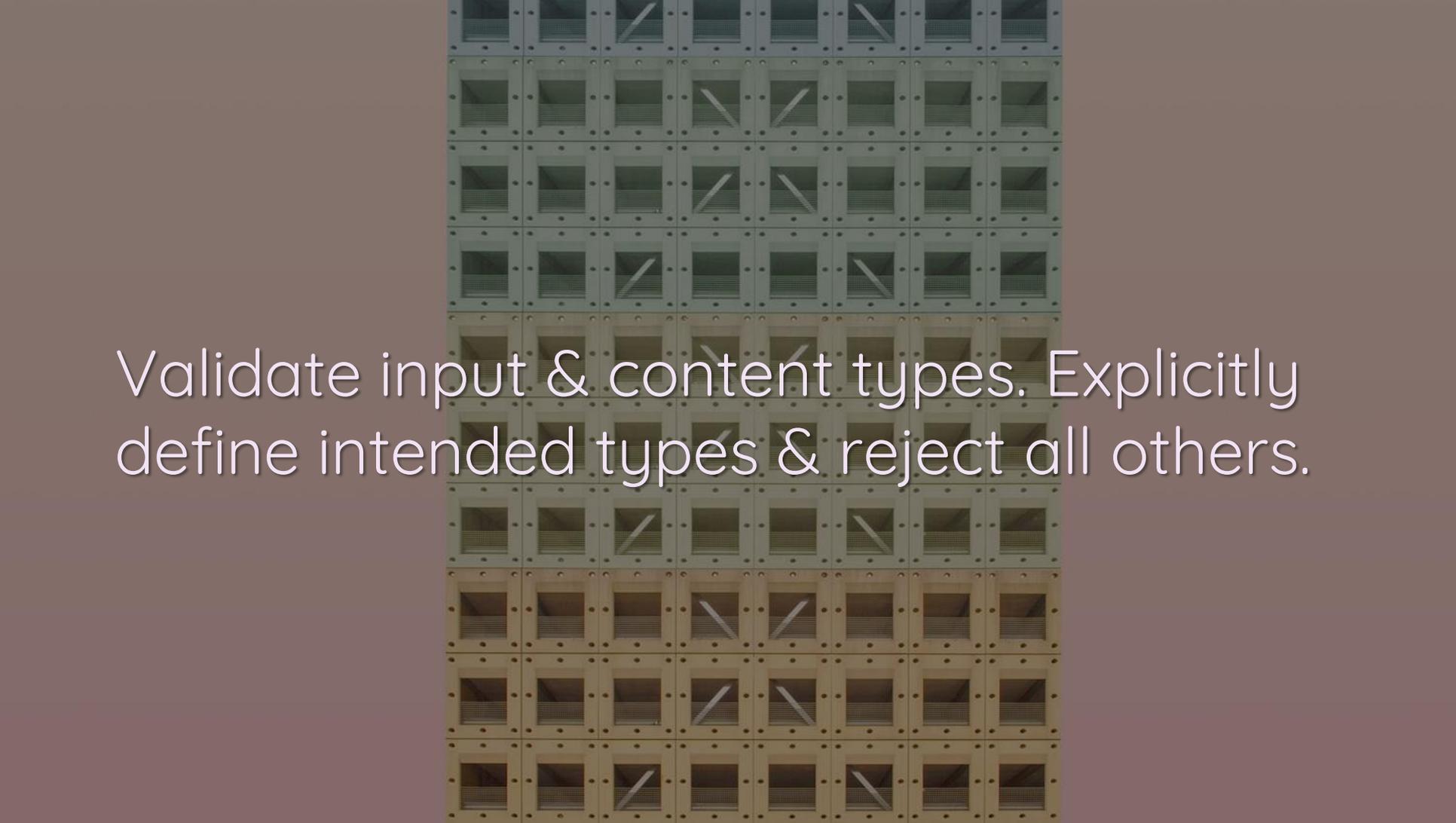
Amazon Inspector + AWS Trusted Advisor are great tools to start

Use IAM roles for least priv or segment
prod + dev through different accounts



Basic API hygiene will suffice – auth, validation, & not trusting external data

Example: Don't expose API keys in the URL, only use HTTPS endpoints, etc.



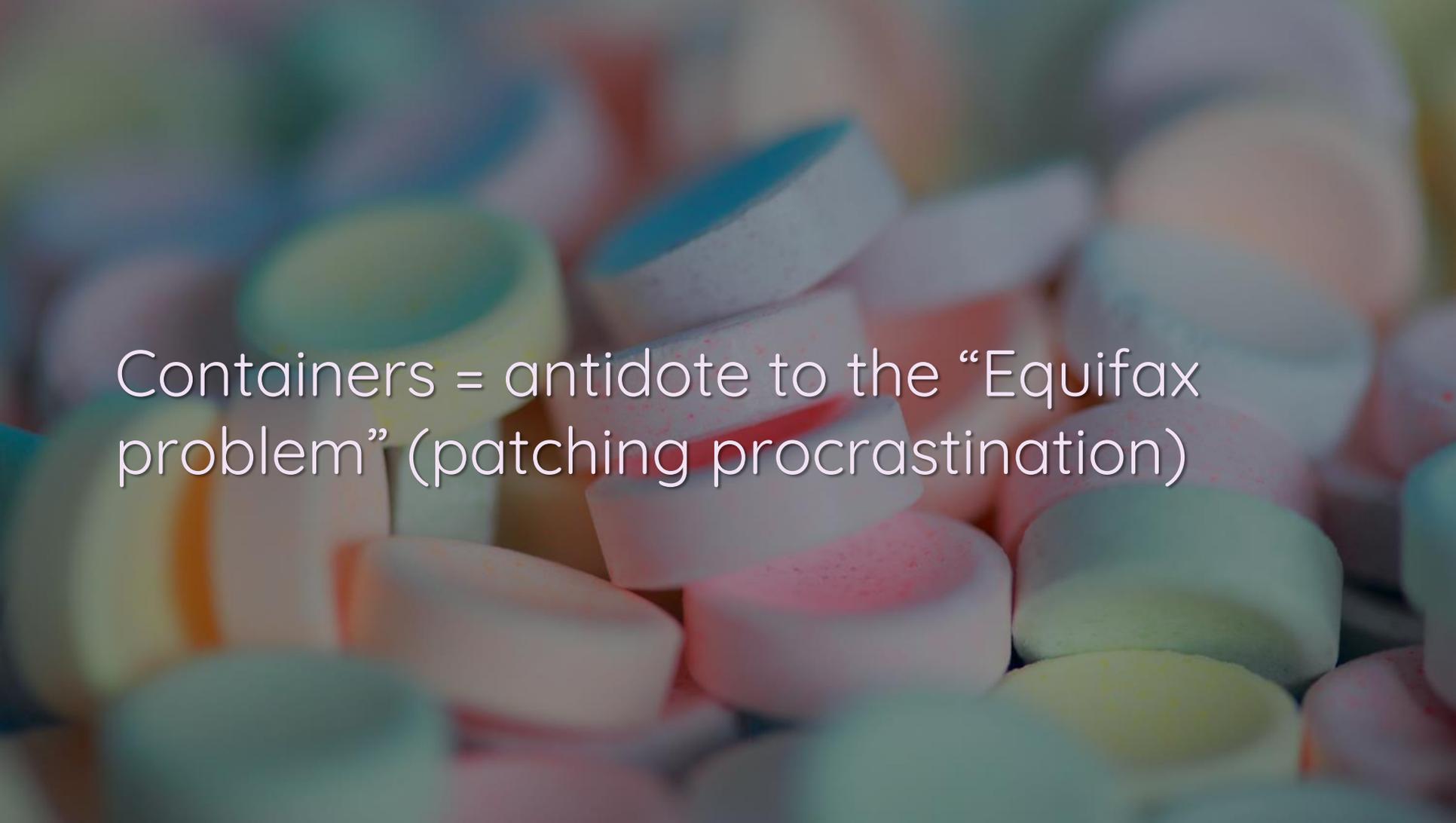
Validate input & content types. Explicitly define intended types & reject all others.

Analogize this as a form of granular whitelisting only possible with APIs

A photograph of a white box filled with macarons, tied with a white ribbon. The macarons are in various colors including pink, green, and brown. The image is slightly blurred and has a dark overlay.

For containers, restrict access – no “god mode”, no anon access, don’t expose management dashboards, etc.

Any CISO will already be familiar with the concept of “Least Privilege”



Containers = antidote to the “Equifax problem” (patching procrastination)

Container registries make security scanning easier & add sense of control

The background is a solid light pink color with a pattern of numerous water droplets of various sizes. Some droplets are large and clear, while others are smaller and more numerous, creating a textured, bubbly effect.

Live migration means security can patch
without impacting end users

Analogy: Windows updates if Word & PPT docs were migrated to a healthy OS

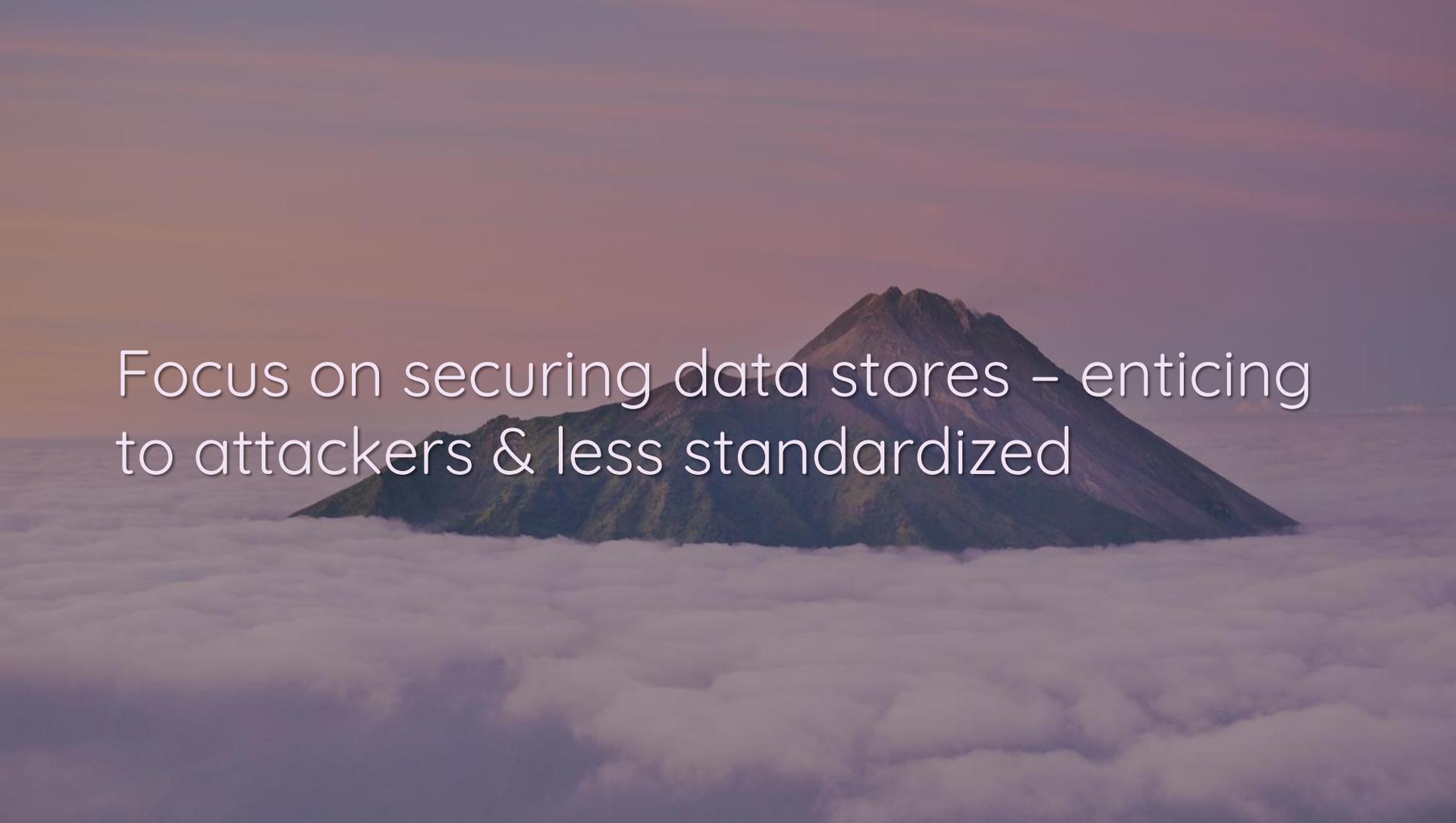
The background is a solid light pink color. Scattered around the edges are several macarons. In the top left, there is a light green macaron. In the top center, there is a pink macaron that is broken in half, showing a dark red filling. In the top right, there is a pale yellow macaron. In the bottom left, there is a pink macaron. In the bottom right, there is a light green macaron.

If misconfigs are covered, what remains
for infosec teams to tackle?

Codifying secure configs – modern
equivalent of security policy templates

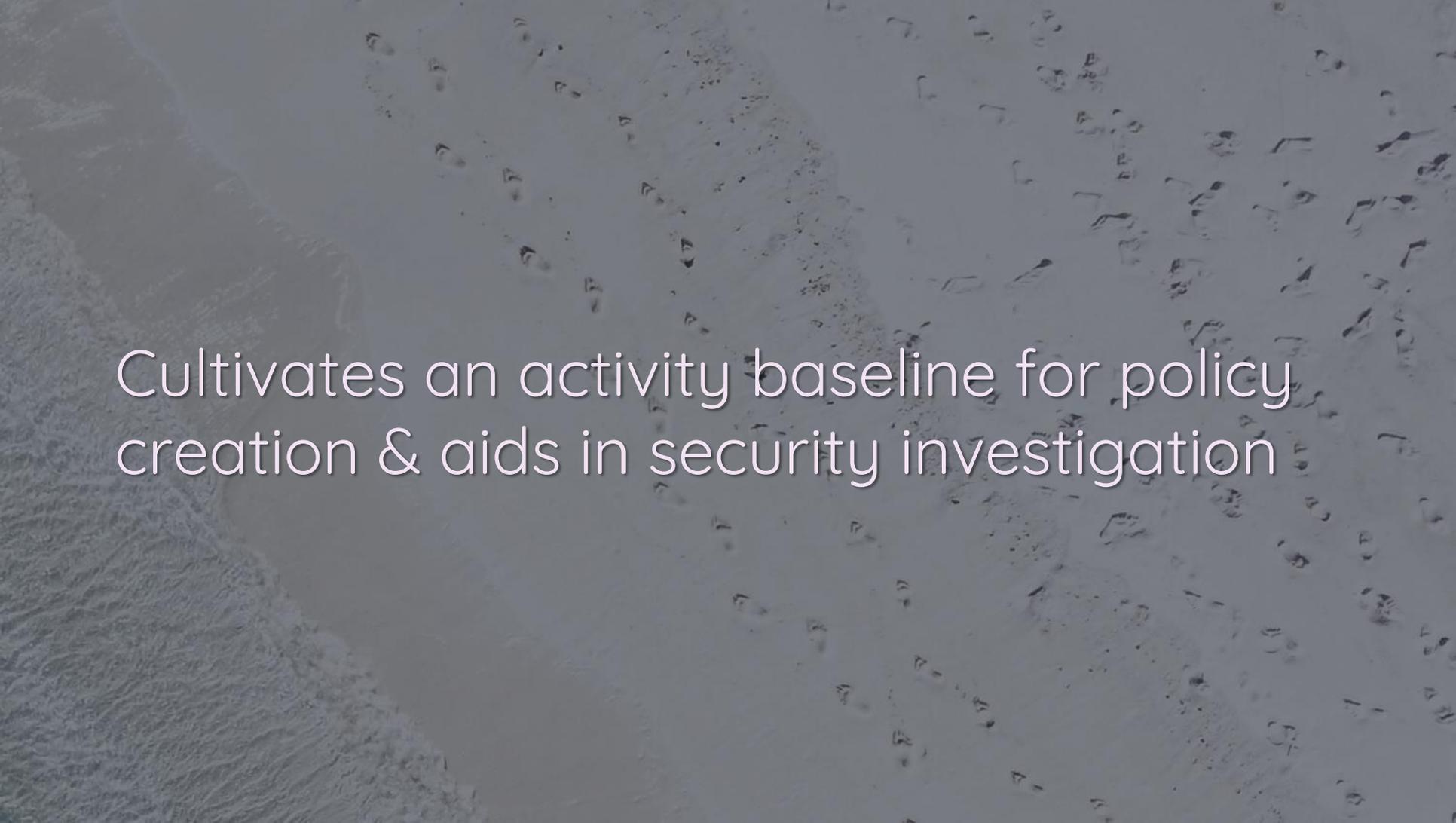


Documenting threat models, starting with scenarios most damaging to the org & working back to likely vectors

A photograph of a volcano, likely Mount Fuji, rising above a thick layer of white clouds. The sky is a mix of soft purple, pink, and blue, suggesting a sunset or sunrise. The volcano's peak is dark and jagged, contrasting with the smooth, billowy clouds below.

Focus on securing data stores – enticing
to attackers & less standardized

Help infosec finds database visibility & monitoring tools (e.g. Vivid Cortex)

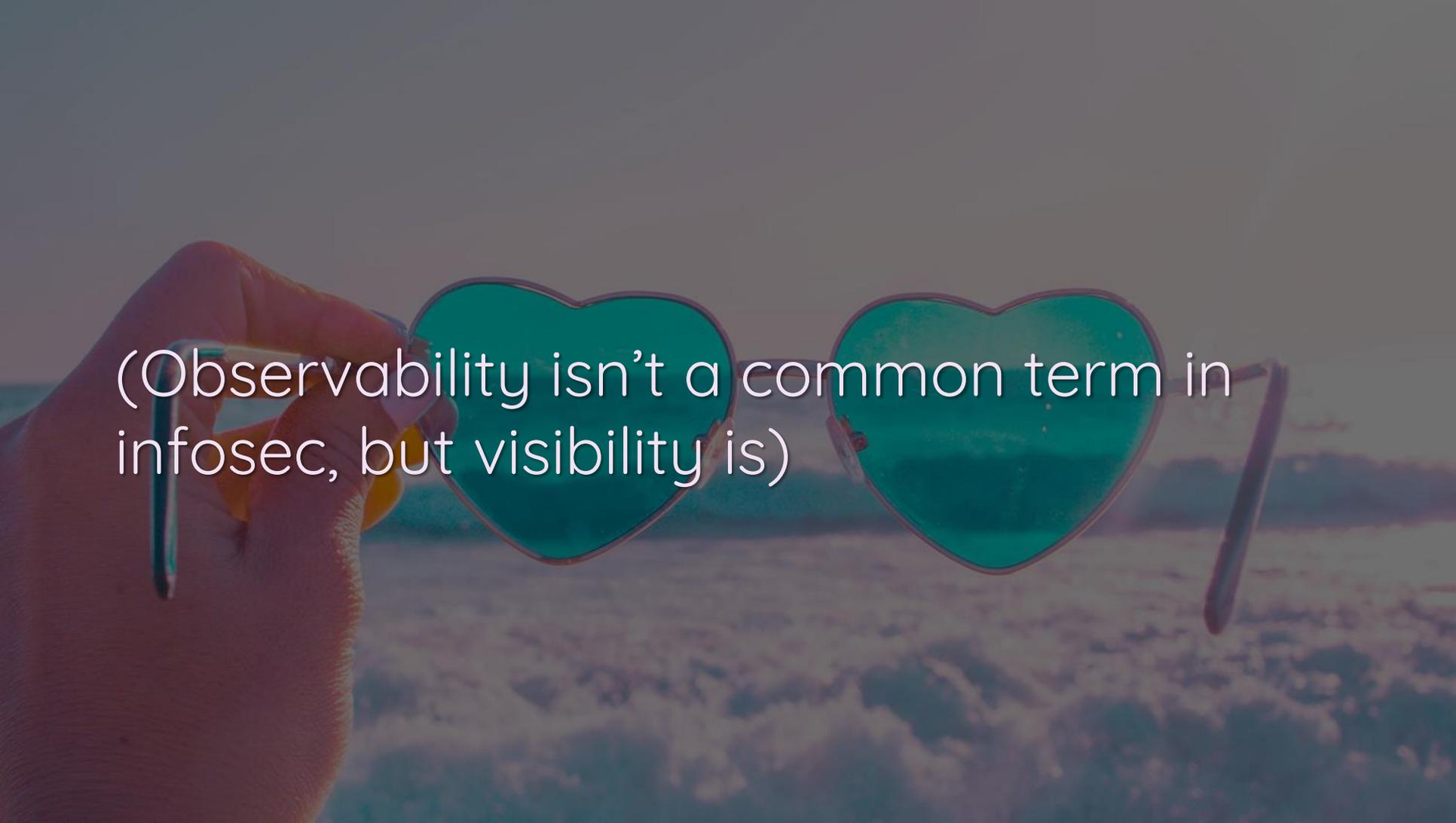
An aerial photograph of a sandy beach with numerous footprints scattered across the surface. The text is overlaid on the image.

Cultivates an activity baseline for policy creation & aids in security investigation

The background consists of a dense, overlapping pile of small, rectangular paper scraps in various colors including light green, pink, purple, and yellow. Each scrap has faint, illegible text printed on it, suggesting they are fragments of a larger document. The overall effect is one of a chaotic but organized collection of information.

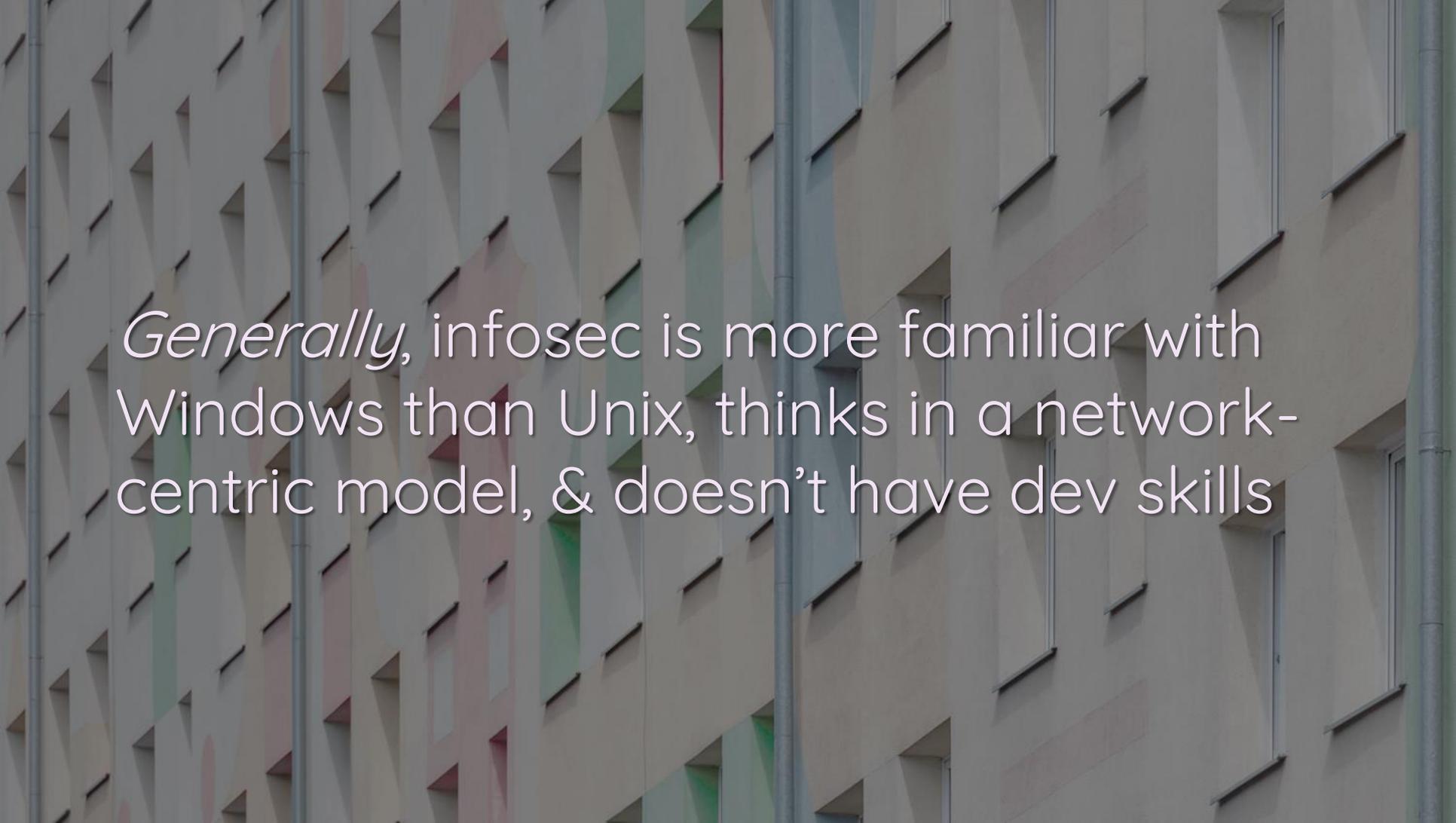
Highlight compliance – file integrity
monitoring underpins most standards

FIM is easier given the improved inspectability of containers

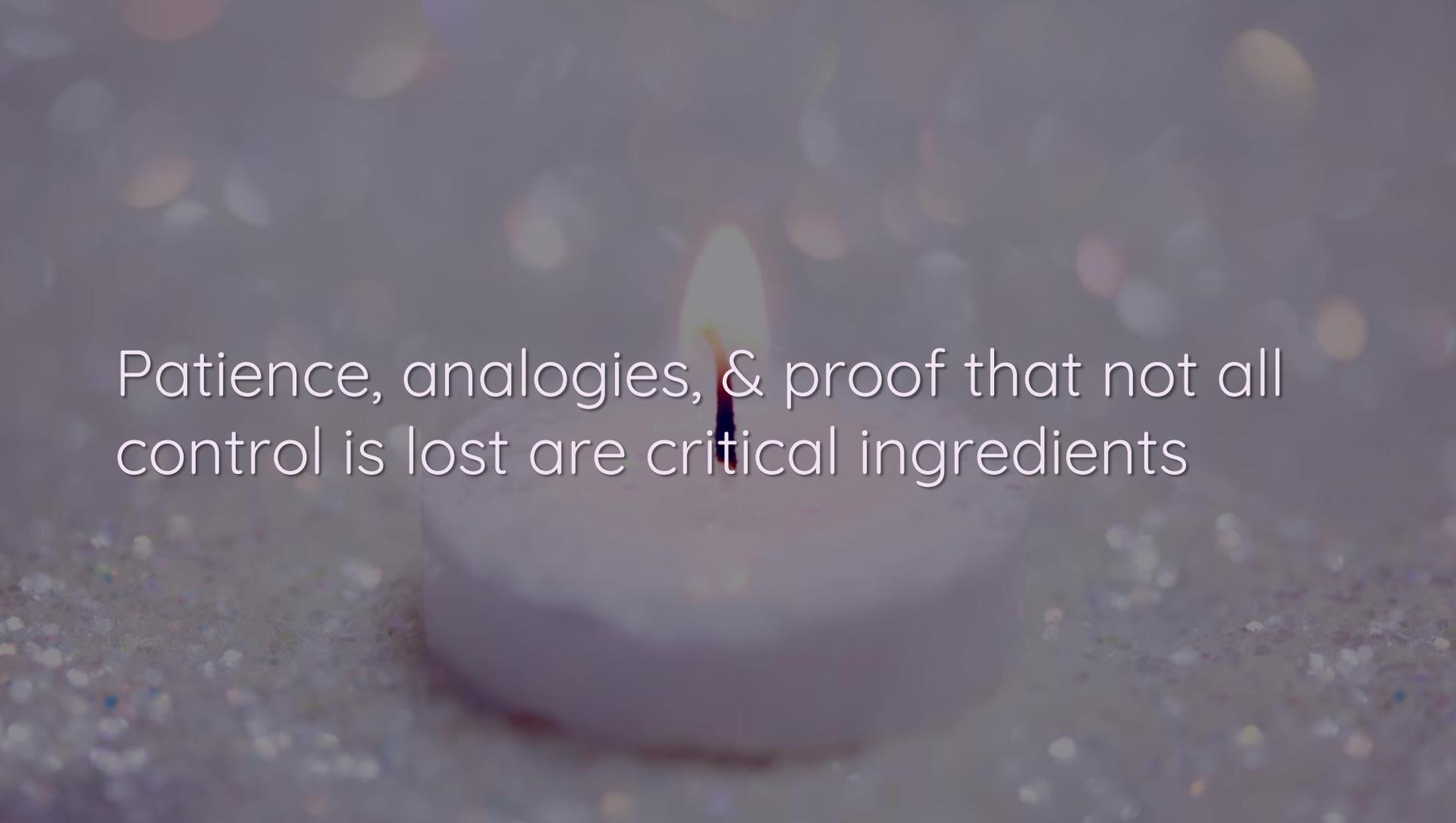
A hand is holding a pair of heart-shaped sunglasses with teal lenses. The sunglasses are positioned horizontally across the middle of the frame. The background is a blurred beach scene with waves and a clear sky. The text is overlaid on the sunglasses.

(Observability isn't a common term in infosec, but visibility is)

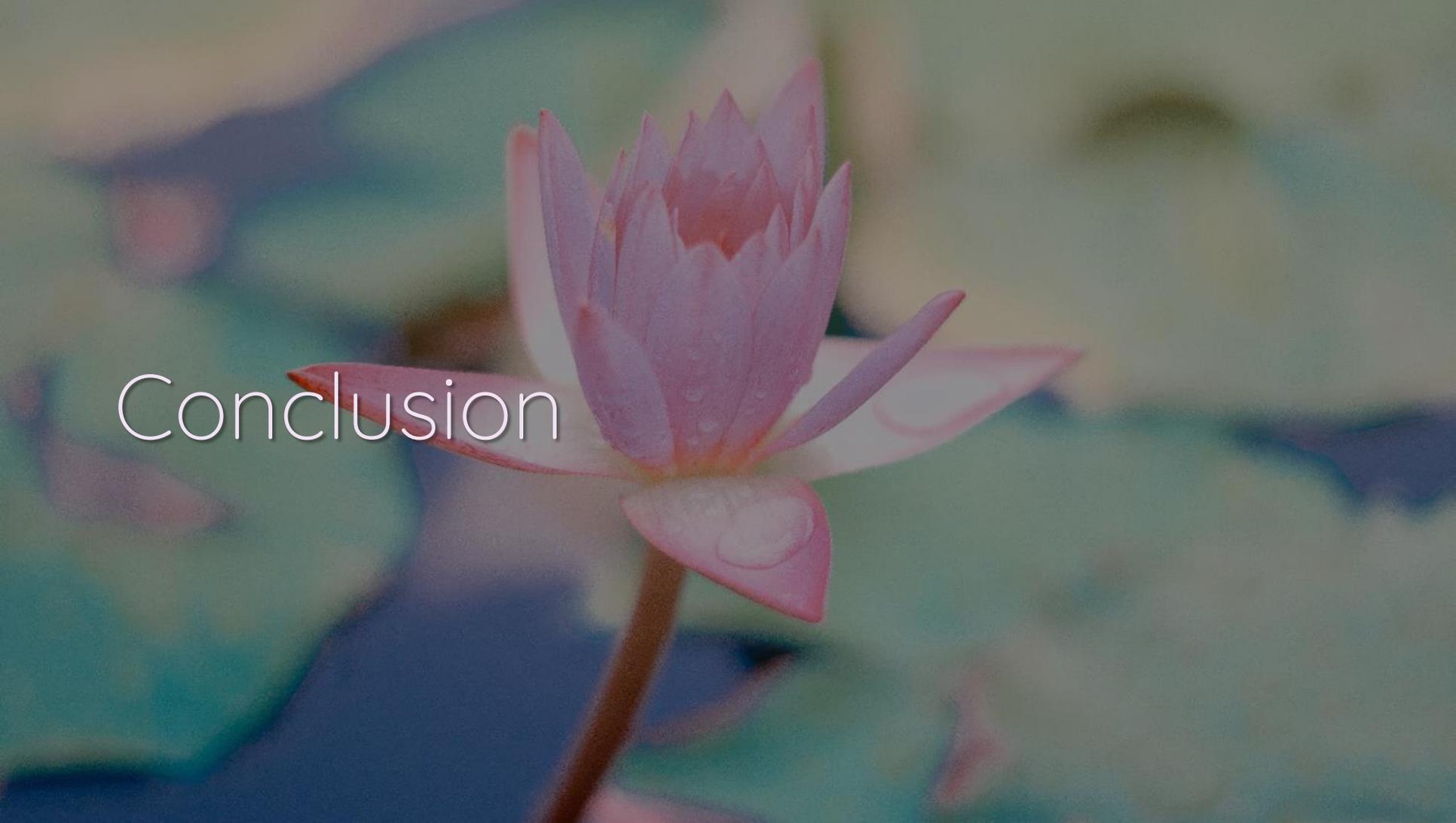
Infosec ppl aren't all the same – different tactics will work to build understanding



Generally, infosec is more familiar with Windows than Unix, thinks in a network-centric model, & doesn't have dev skills

A lit candle sits on a sandy surface, its flame glowing. The background is filled with soft, out-of-focus bokeh lights in various colors, creating a dreamy atmosphere. The text is overlaid in the center of the image.

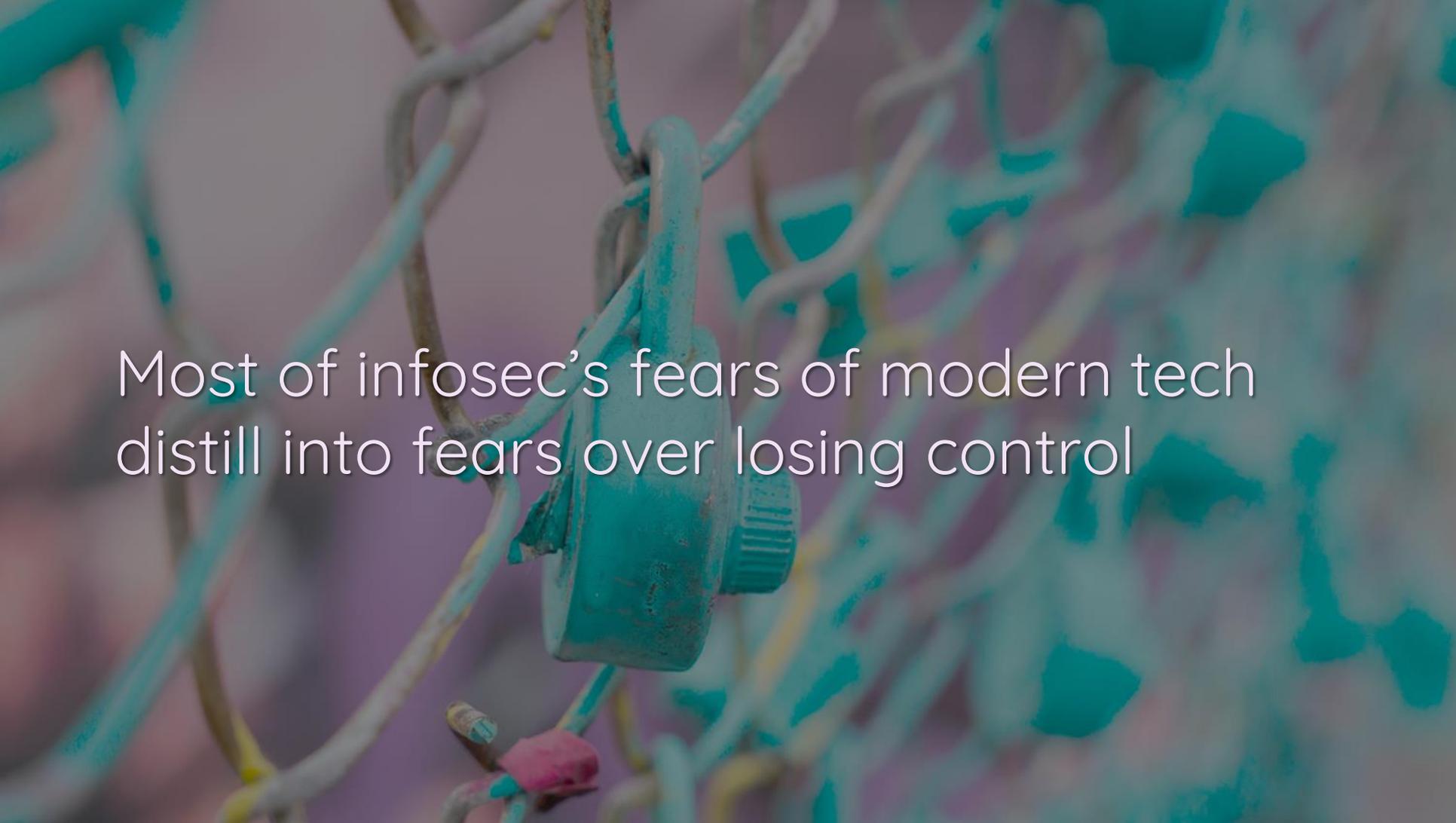
Patience, analogies, & proof that not all control is lost are critical ingredients



Conclusion

A hand with yellow nail polish holds a clear funnel. Gold glitter is falling from the narrow neck of the funnel, forming a curved trail in the air. The background is a soft, light pinkish-red gradient.

Letting go of core, long-held beliefs is difficult for anyone



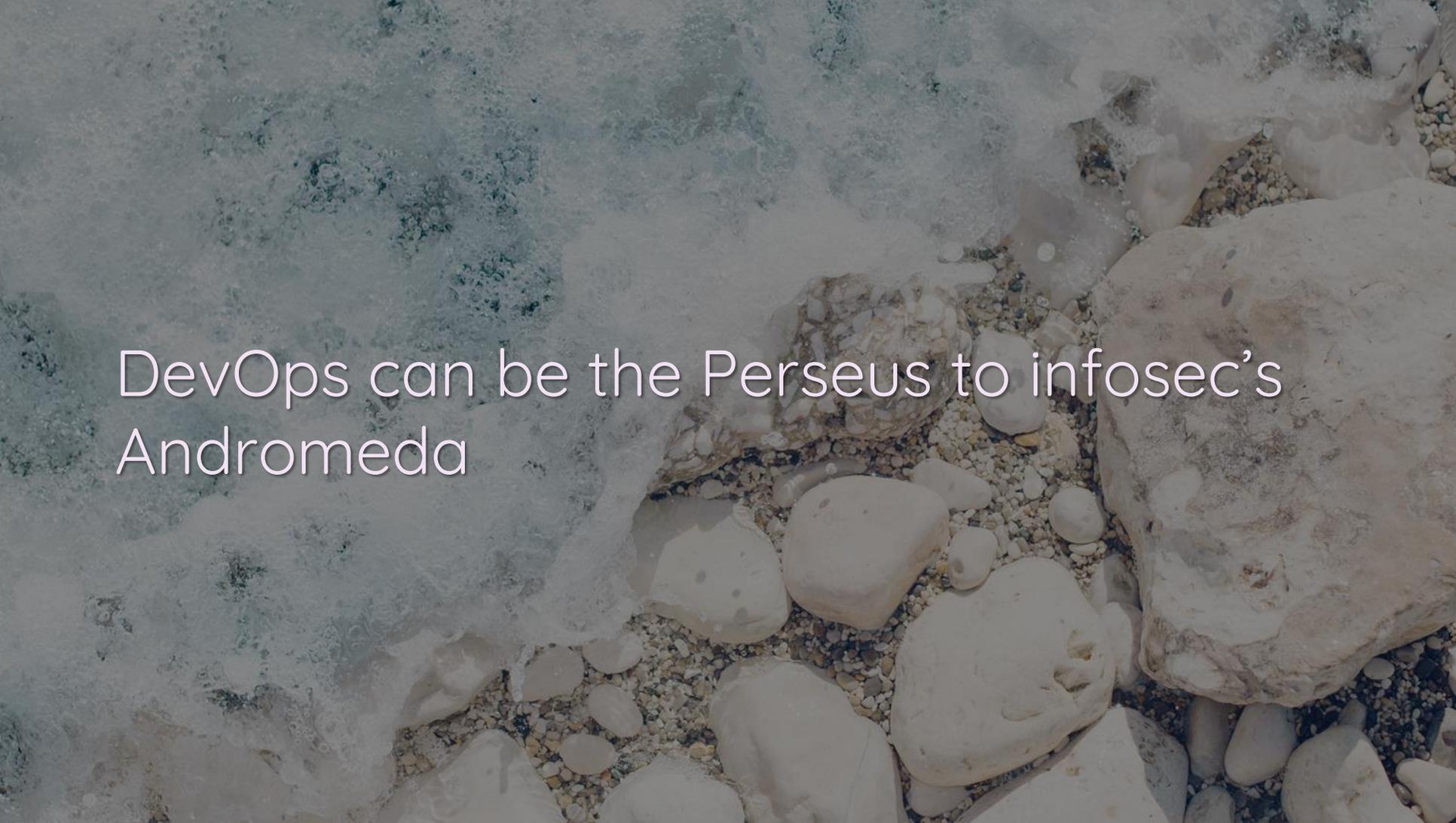
Most of infosec's fears of modern tech
distill into fears over losing control



Redirect grasping at phantasms towards
control of meaningful threat mitigation

A close-up photograph of a white kitten with blue eyes and a pink tongue sticking out, sitting on a white surface. The kitten is looking directly at the camera. The background is a soft, out-of-focus white surface.

Work together to codify standards so
infosec can focus on securing “pets”



DevOps can be the Perseus to infosec's
Andromeda

A dramatic sky scene featuring a sunburst breaking through a gap in dark, heavy clouds. The sunburst is positioned centrally, with rays of light emanating from it. The sky above the clouds is a lighter, hazy blue, while the clouds below are dark and textured. The overall mood is one of hope and breakthrough.

Unchain infosec from their fears & bring
forth a new dawn of secure & resilient
software delivery performance



@swagitda_



/in/kellyshortridge



kelly@greywire.net