



CONTROLLED CHAOS

The Inevitable Marriage of DevOps & Security

Kelly Shortridge (@swagitda_)

S4x20



Hi, I'm Kelly

CAPSULE8



“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

The background of the slide features a hand holding a glowing heart-shaped lightbulb. The lightbulb is the central focus, with its glow illuminating the surrounding area. Behind the lightbulb, there are several concentric heart outlines, creating a sense of depth and focus on the central heart. The overall color scheme is dark, with the light from the bulb providing a warm, yellowish glow.

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 bathed in a cool, blue and purple light, creating a high-tech, digital atmosphere. The background is blurred, showing hints of other lights and possibly another person's hand. The text "DevOps Dominion" is overlaid in a clean, white, sans-serif font on the left side of the image.

DevOps Dominion

A purple robot head with a large, black, reflective visor. The visor shows a reflection of a city skyline at night, with a grid-like pattern of lights at the top. The robot's body is also purple and has a glowing blue light at the bottom of its chest.

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

A glowing purple sphere, resembling a planet or a celestial body, is the central focus. A thin, white, smoke-like trail rises from its top, curving upwards and to the right. The sphere has a bright, white, star-like glow emanating from its center. The background is a deep, dark blue, filled with abstract, swirling light patterns in shades of blue and purple, creating a sense of movement and depth. The overall composition is centered and balanced, with the sphere and its trail acting as the primary visual element.

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

A red neon sign with the words "HURT ME" in a stylized, blocky font. The sign is mounted on a wooden crate. The background is dark, and the sign is illuminated, casting a red glow. The sign is positioned in the lower right quadrant of the image, below the title text.

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 volcanic eruption at night. A large, dark plume of smoke and ash rises from a volcano, illuminated from within by a bright orange and yellow lightning bolt that strikes the lava flow. The lava flow is visible as a bright orange and yellow stream cascading down the side of the volcano. The background is a dark, starry night sky.

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

The background of the slide is a complex, abstract geometric pattern. It consists of numerous interconnected cubes or rectangular frames, creating a lattice-like structure. The colors are primarily deep blue and purple, with some lighter, almost white, highlights that give the structure a three-dimensional appearance. The pattern is dense and fills the entire frame, with the central area being slightly darker to make the white text stand out.

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”

The background is a dark, teal-colored abstract image. It features a grid of glowing blue lines that resemble a circuit board or a digital map. Scattered across this grid are numerous small, glowing red and pink dots, some of which are arranged in faint, larger patterns. The overall effect is a high-tech, digital aesthetic.

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)

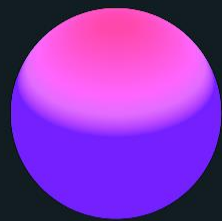


Installing a rootkit on a resource that
dies in minutes is a waste of effort

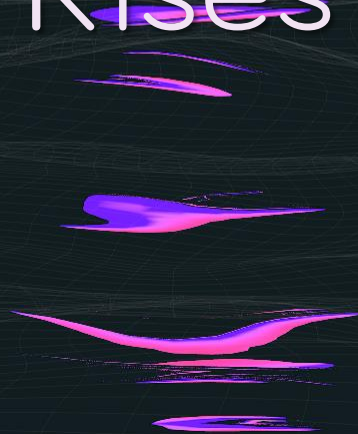


ICS attacks take months to plan;
ephemerality constantly disrupts it

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 of the slide is a dark blue field filled with a complex, interconnected network of thin, glowing purple lines. These lines connect numerous small, bright purple dots, creating a web-like structure that suggests a distributed system or a complex network. The lines and dots vary in brightness, with some appearing more prominent than others.

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



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 the image, set against a dark, snowy landscape at night. The frame's light reflects on a body of water in the foreground. The background shows silhouettes of trees and a dark sky.

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 wearing a dark, hooded garment is visible on the right side of the slide. They are pointing their right index finger towards the text. The background is dark and textured, possibly a wall or a large screen.

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 is a deep purple with a black geometric pattern of triangles meeting at the center. A glowing, slightly offset square frame is centered, with a bright red and orange light emanating from its center. The text is white and positioned within this central area.

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 cupping a small, glowing, translucent sphere. The hand is positioned in the lower half of the frame, with fingers slightly curled. The sphere emits a bright, warm light, creating a strong contrast with the dark background. The background is filled with soft, out-of-focus blue and purple bokeh lights, suggesting a night scene or a digital environment. The overall mood is one of hope, protection, 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