

HELLO FROM THE OTHER SIDE

Dispatches From a Kubernetes Attacker

[Twitter](#) @ianColdwater





My name is Ian Coldwater.

I'm a Lead Platform Security Engineer at Heroku, a Salesforce company.

I specialize in hacking and hardening Kubernetes, containers and cloud infrastructure.

HI COMMUNITY!



Twitter @ianColdwater



DIVERSITY
BUILDS
STRONGER
SYSTEMS

[Twitter](#) @ianColdwater

WHO DO YOU DESIGN FOR?



[Twitter](#) @ianColdwater

ATTACKERS HAVE USER STORIES TOO



Twitter @ianColdwater

WHO ARE ATTACKERS?



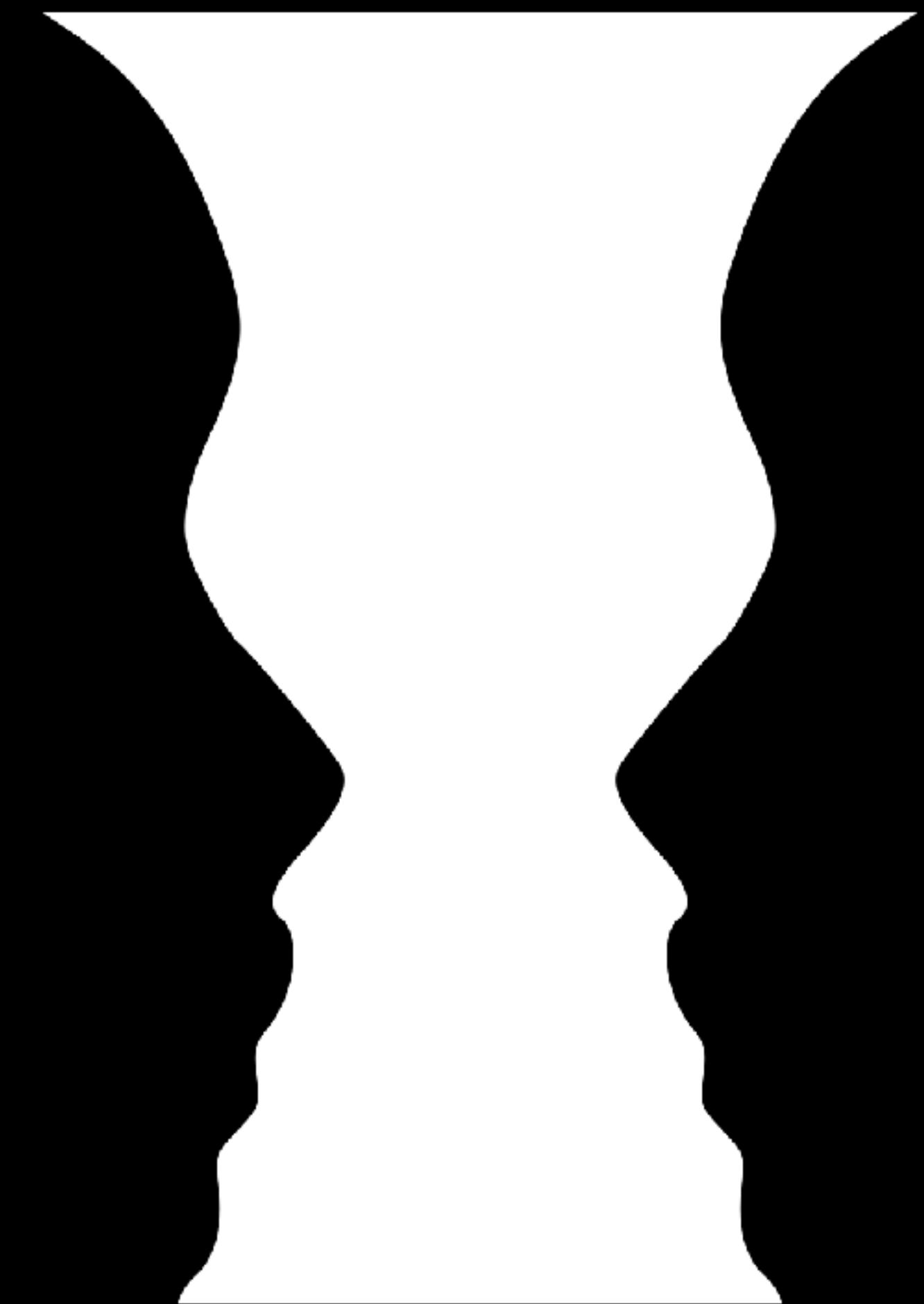
[Twitter](#) @ianColdwater

HOW DO ATTACKERS THINK?



[Twitter](#) @ianColdwater

WHAT DO YOU SEE?





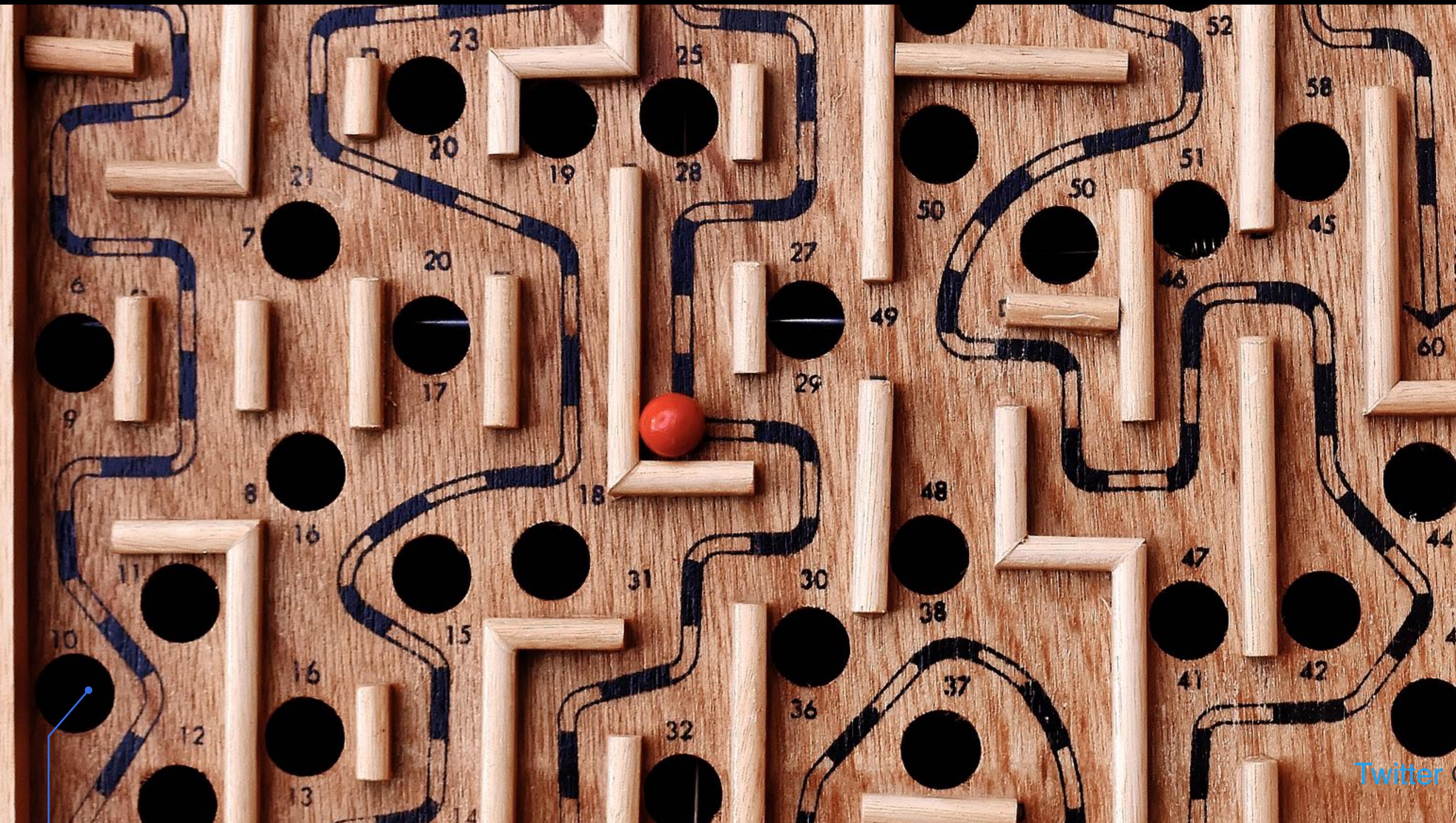
WHAT DO YOU SEE?

```
kubectl auth can-i --list  
--namespace=kube-system
```

WHAT DO ATTACKERS LOOK FOR?



ATTACKER METHODOLOGY



DESIGNING FOR DEFENSE



[Twitter](#) @ianColdwater



WHAT IS YOUR THREAT MODEL?

- What are you trying to protect?
 - Who are you trying to protect it from?
- 

WHAT'S IN YOUR GRAPH?

- Know what you're running, and understand it well.
- What connects? What crosses? Where are the rough edges?
- What would an attacker see?

CHECK YOUR ASSUMPTIONS



THINGS YOU CAN DO



MAKE FRIENDS!



[Twitter](#) @lan_Coldwater

GET PRACTICE

- Capture the Flag:
overthewire.org, picoctf.com,
hackthebox.eu



goose.game

- Play with your own systems!



Twitter @lanColdwater

BETTER TOGETHER

A wide-angle photograph of a double rainbow arching across a sky filled with scattered clouds. The rainbow is vibrant, with distinct bands of color. It appears to originate from a line of trees in the foreground, which separates a grassy field from a dense forest. The overall scene is bright and suggests a post-rain environment.

Twitter @ianColdwater



WE CAN DO IT!

[Twitter](#) @ianColdwater

RESOURCES

- K8s security audit
- attack trees
- attackers think in graphs
- bug bounties and black swans
- CIS benchmarks
- <https://k8s.io/security>
- github.com/kelseyhightower/nocode - the best way to write secure and reliable applications!