

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!





**DIVERSITY
BUILDS
STRONGER
SYSTEMS**

WHO DO YOU DESIGN FOR?

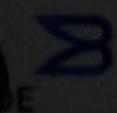


Twitter @IanColdwater

ATTACKERS HAVE USER STORIES TOO



Sch



EMC²



Twitter @IanColdwater

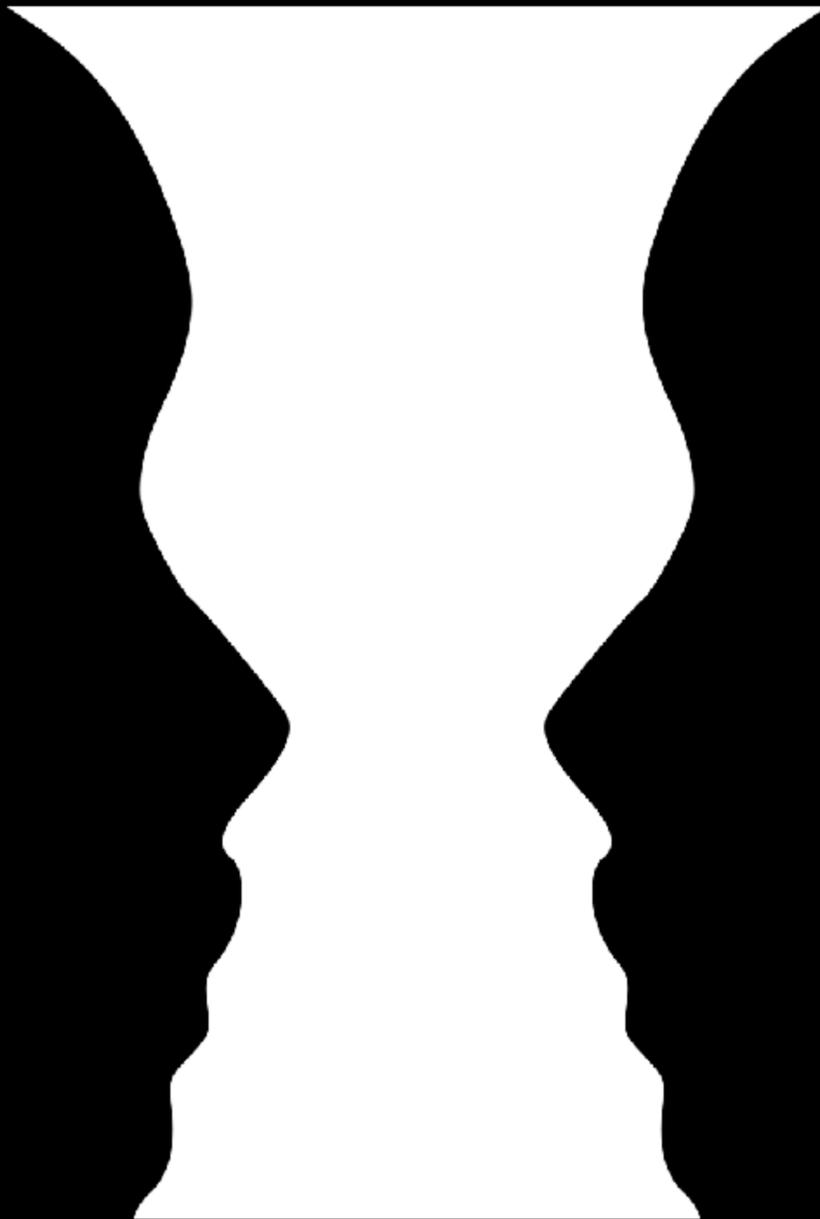
WHO ARE ATTACKERS?



HOW DO ATTACKERS THINK?



WHAT DO YOU SEE?



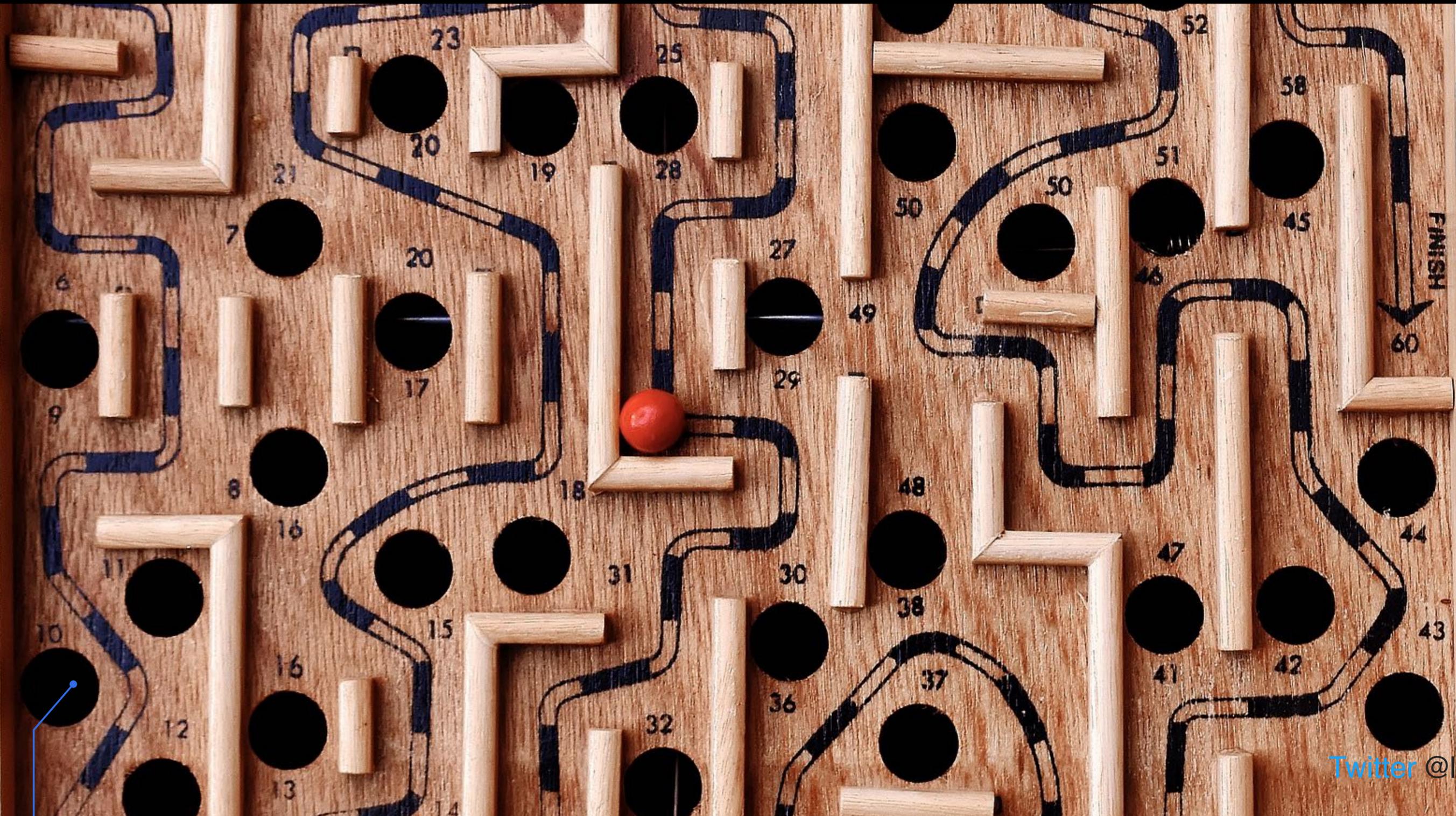
WHAT DO YOU SEE?

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

WHAT DO ATTACKERS LOOK FOR?



ATTACKER METHODOLOGY



DESIGNING FOR DEFENSE



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!



GET PRACTICE

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



goose.game

- Play with your own systems!



BETTER TOGETHER





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!