Shift-left Can Effect Positive Outcomes in **Threat Detection**

ANNA BELAK
Director, Office of Cybersecurity Strategy, Sysdig

Agenda

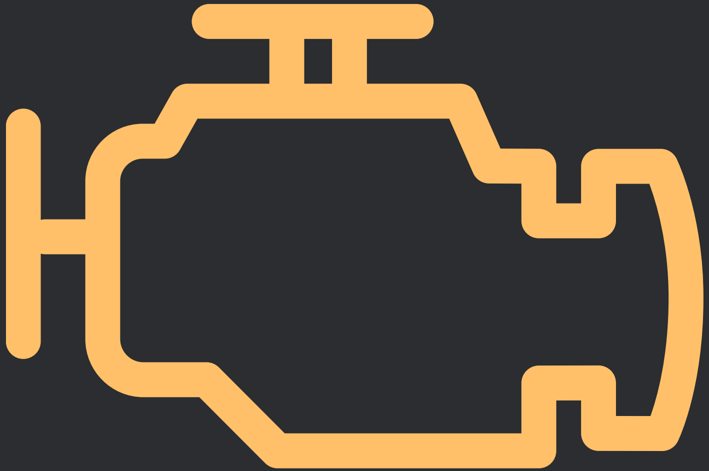
1 Car problems

2 Drift control in mutable and immutable systems

3 Aligning security controls to technical realities

4 Helping others for no personal gain

There are things developers can do to make security people less sad.



Tire Pressure Monitoring System (TPMS)

5% of car accidents

involve tire problems

Accident prevention

79 deaths

10,365 injuries

75% of roadside flats

were preceded by slow leaks or underinflation

Cost reduction

3% fuel efficiency improvement

reducing fuel costs by $2B

ALERT!: kubectl executed in container while not part of base image

How do you monitor custom applications for security?

You don’t.

DevOps

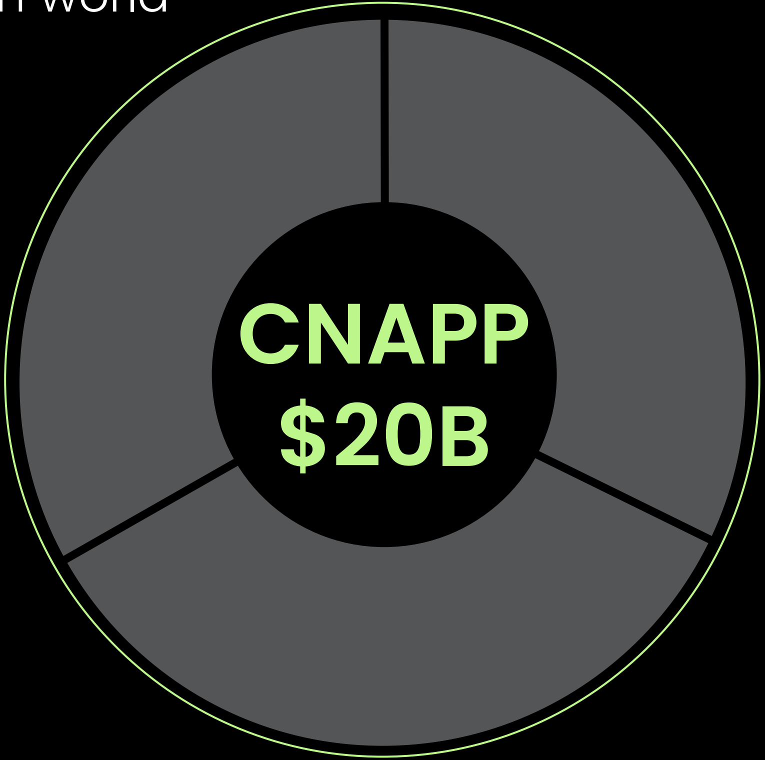
DevSecOps

SecDevOps

SecDevOpsSecOps

Cloud Security Monitoring

in a software-eaten world



legacy vendors

new vendors

cloud providers

adjacent markets

not-so-adjacent markets

New world,
new security

What is **Drift?**

Configuration drift is the divergence of a system's actual settings or state from a predefined **secure baseline.**

Drift in mutable environments

like legacy servers and workloads

Patches

Troubleshooting

External integrations

Human error

Upgrades

Ad-hoc configuration

Poor change control

Malicious activity

- Difficult to avoid
- Difficult to monitor
- Low fidelity source of security data

The immutable promise

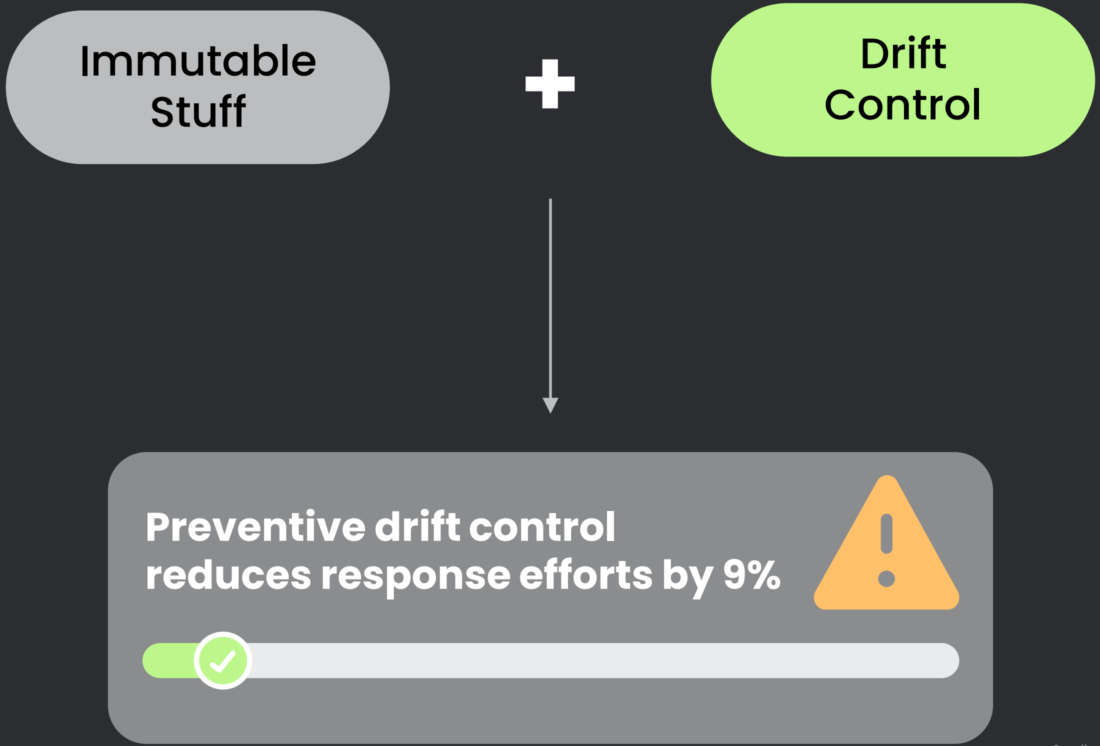
of containers

~~Patches~~ ~~Troubleshooting~~ External integrations Human error

~~Upgrades~~ ~~Ad-hoc configuration~~ ~~Poor change control~~ Malicious activity

- Everything-as-code, including secure baseline configuration
- Git-based workflows and change control
- Never interactively alter live workloads, always redeploy
- Loosely coupled architecture for resilience
- Short-lived workloads

The immutable promise



Immutable Stuff

+

Drift Control

Preventive drift control reduces response efforts by 9%

Real cyber attacks

can be mitigated with drift control

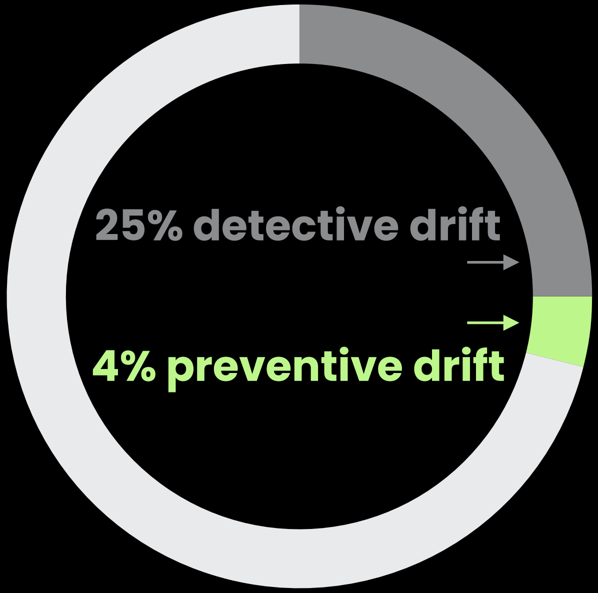
- Crypto malware !
- DDoS malware !
- Credential stealers !

Real cyber attacks

can be mitigated with drift control

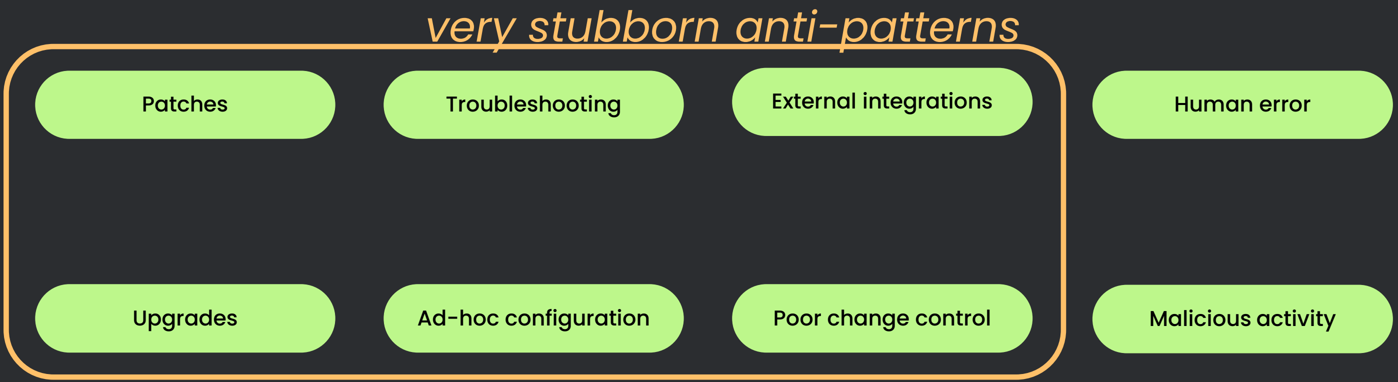
- Crypto malware
- DDoS malware
- Credential stealers
- Remote access
- Side channel

Drift Control



Drift in immutable systems

in reality



very stubborn anti-patterns

Patches

Troubleshooting

External integrations

Upgrades

Ad-hoc configuration

Poor change control

Human error

Malicious activity

- Most things are mutable
- Dev and test environments can look very different from production
- Old habits die hard
- There’s an exception for everything

drift detected: kubectl executed in container while not part of base image

SOC: ???
DevOps: lol this is fine

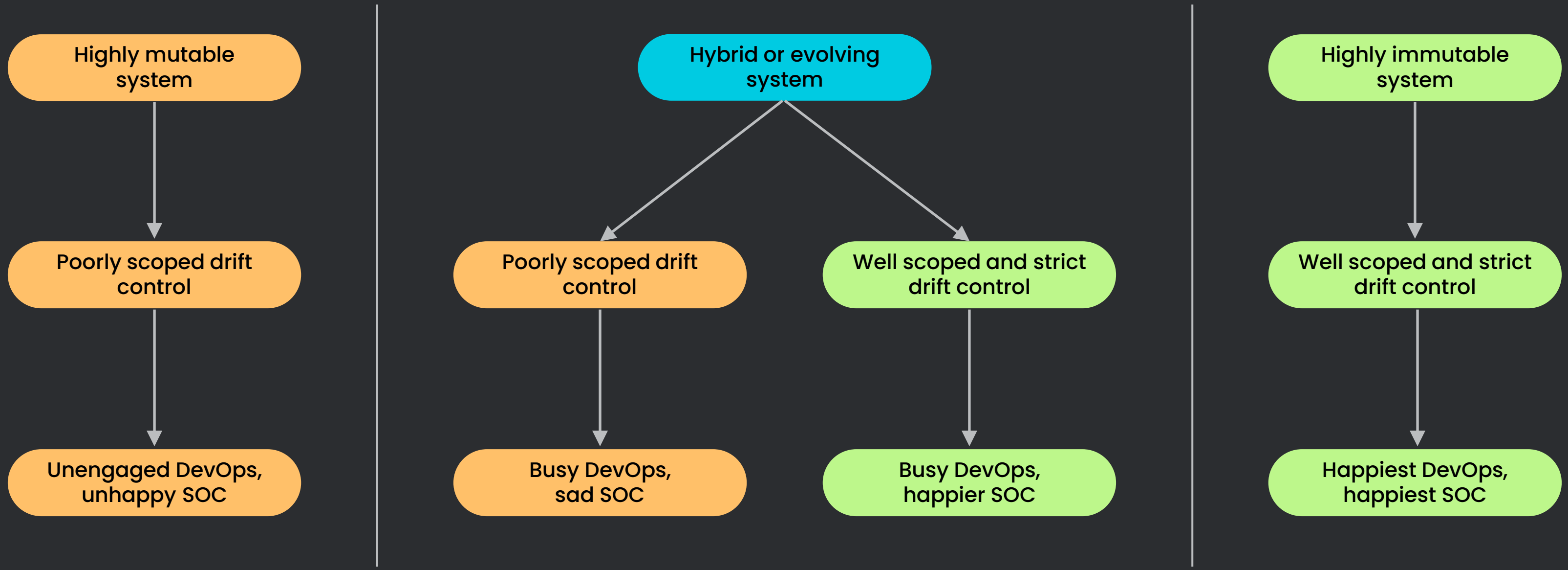
drift detected: curl/wget executed in container while not part of base image

SOC: seems very bad
DevOps: lol this is fine

drift detected: some binary, not part of the application, connects to malicious IP

SOC: seems very bad
DevOps: ??? not my problem

3 drift control scenarios



Highly mutable system

Poorly scoped drift control

Unengaged DevOps, unhappy SOC

Hybrid or evolving system

Poorly scoped drift control

Busy DevOps, sad SOC

Well scoped and strict drift control

Busy DevOps, happier SOC

Highly immutable system

Well scoped and strict drift control

Happiest DevOps, happiest SOC

Software should be **“secure-by-design.”**

Software security should be “designed for the software being secured.”

What can you do?

Recommendations for drift control and other cloud-native detections

- ~~Teach the application owners security operations~~
- ~~Teach the SOC cloud-native everything~~
- Create communication channels to share the most actionable information
  - Integrate SOC requirements into appdev workflows
  - Define and enforce secure and operational baselines
  - Select and tune security controls by environment scope
  - Close tuning and troubleshooting feedback loops

Correctly implemented drift control can reduce SOC sadness by 9%

sysdig

SECURE
EVERY
SECOND.

sysdig

SECURE
EVERY
SECOND.