The Challenge of Securing Containers and Kubernetes

Diego Gagliardo
Technical Account Manager

Me

Jon "maddog" Hall

- Network Security
- Endian co-founder (Endian Firewall)
- Industrial/Healthcare IoT Security

Diego Gagliardo
V1

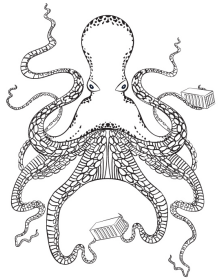
diego@sysdig.com

- K8s and SecDevOps world
- Cloud Native Security
- Sysdig + Falco

Diego Gagliardo
V2

sysdig

Sysdig - Open Source Foundation



Founded by the creator of

WIRESHARK

Protocol analysis and network security

Sysdig | *Open Source*

Deep container forensics and troubleshooting

Falco

Cloud native threat and anomaly detection

aws · GitLab · Google · HUAWEI · IBM · mercari · Postmates · T-Mobile · SAMSUNG · VOLVO · Walmart

~5k GitHub stars · 40M downloads

HQ in	Operations in	Employees:	Customers:	VC Funding:
San Francisco	**20+ Countries**	**>500**	**>700**	**$750M**

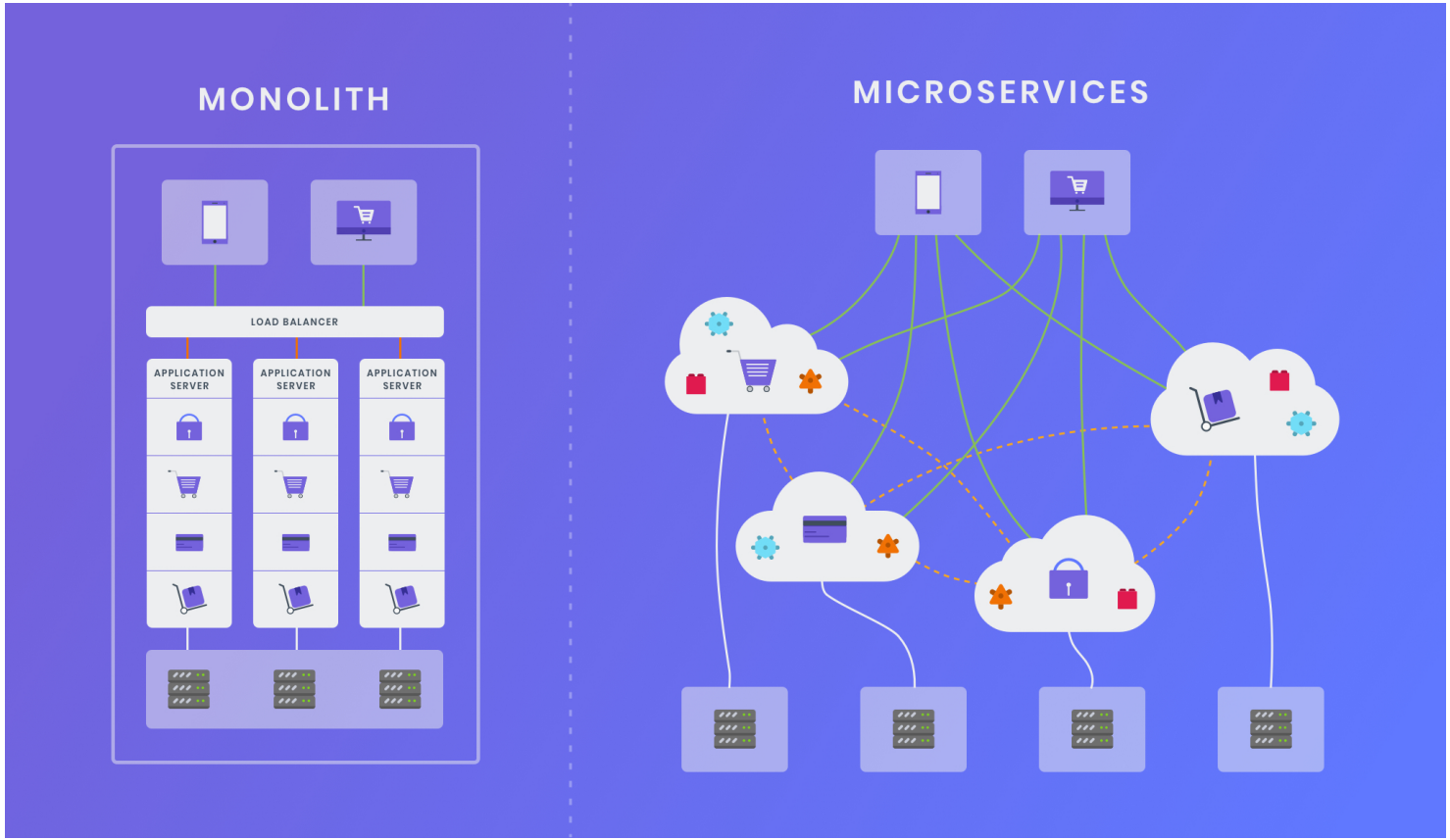
sysdig

Agenda

- Cloud-Native architecture security challenge
- K8s/containers general security workflow overview
- Runtime Threat Detection with Falco

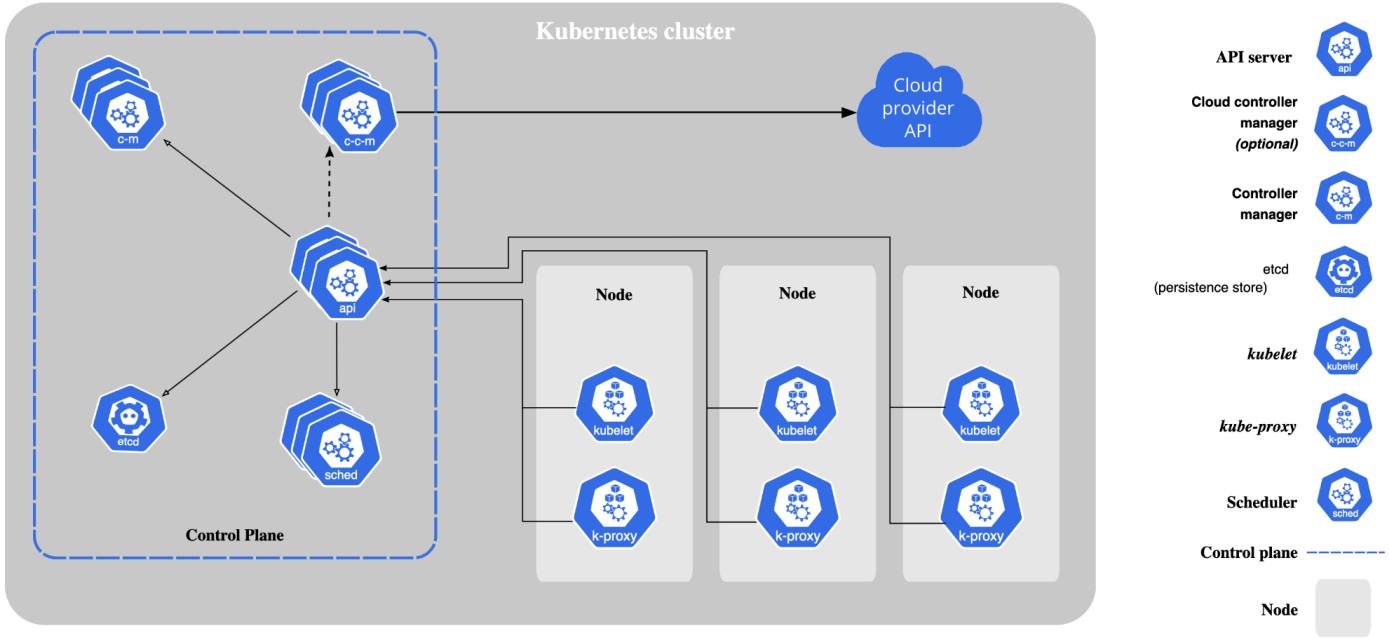
sysdig

From Monolithic to Microservices



sysdig

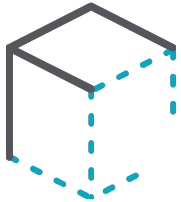
Kubernetes, the cloud OS



The components of a Kubernetes cluster

sysdig

Operational Challenges with Containers



Containers disappear and leave no trail

Cloud native leaves you blind

Security and operations fail without context

sysdig

Traditional Security Challenges Exist in Cloud

Fix Software Vulnerabilities

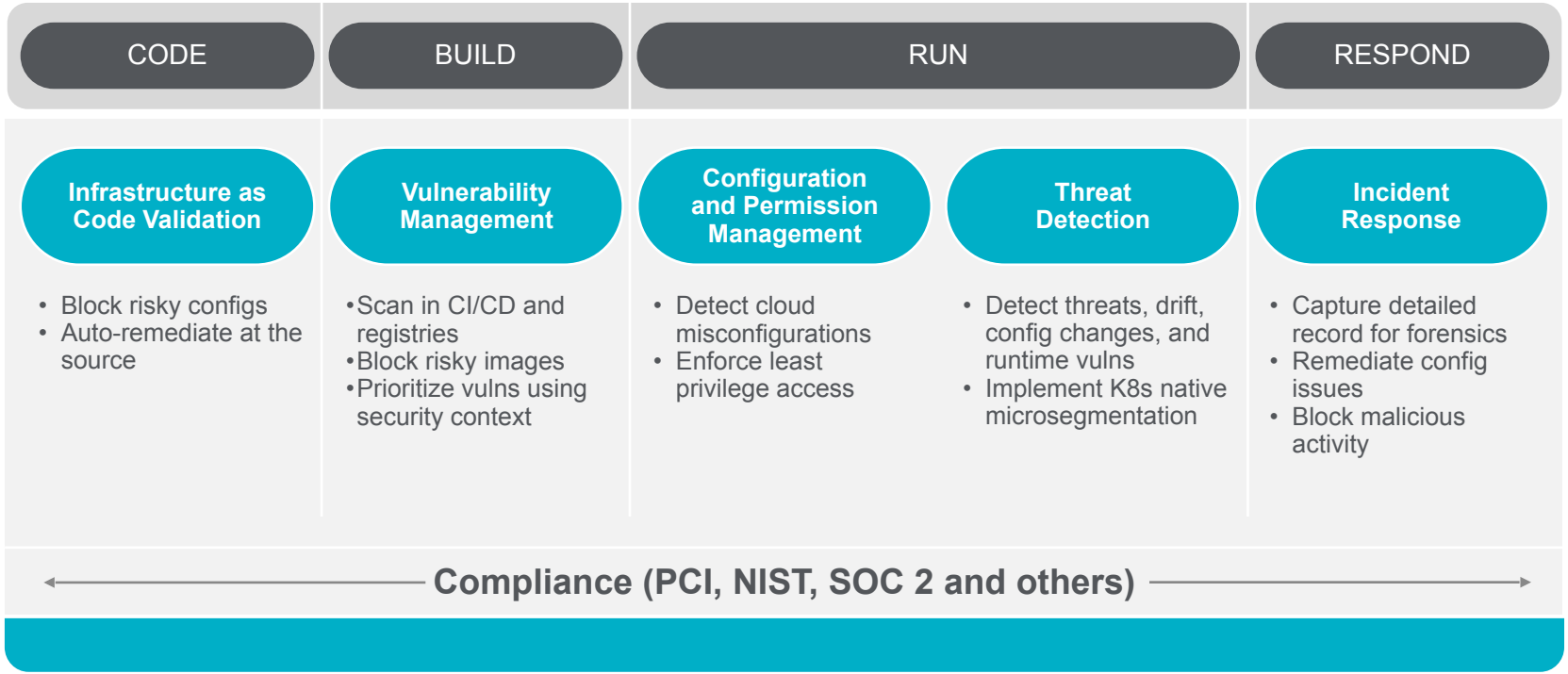
Manage Configs and Permissions

Detect and Respond to Threats

Meet Compliance

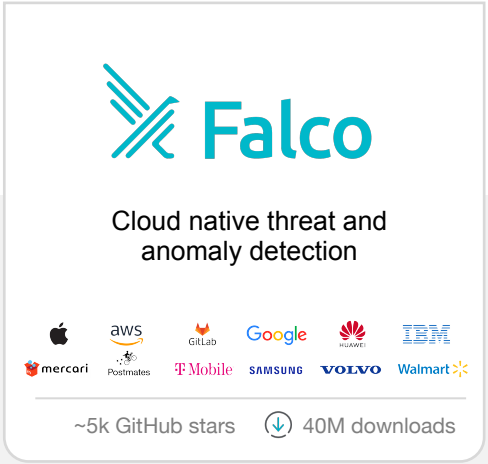
sysdig

Secure Containers, Kubernetes and Cloud Services



sysdig

Falco



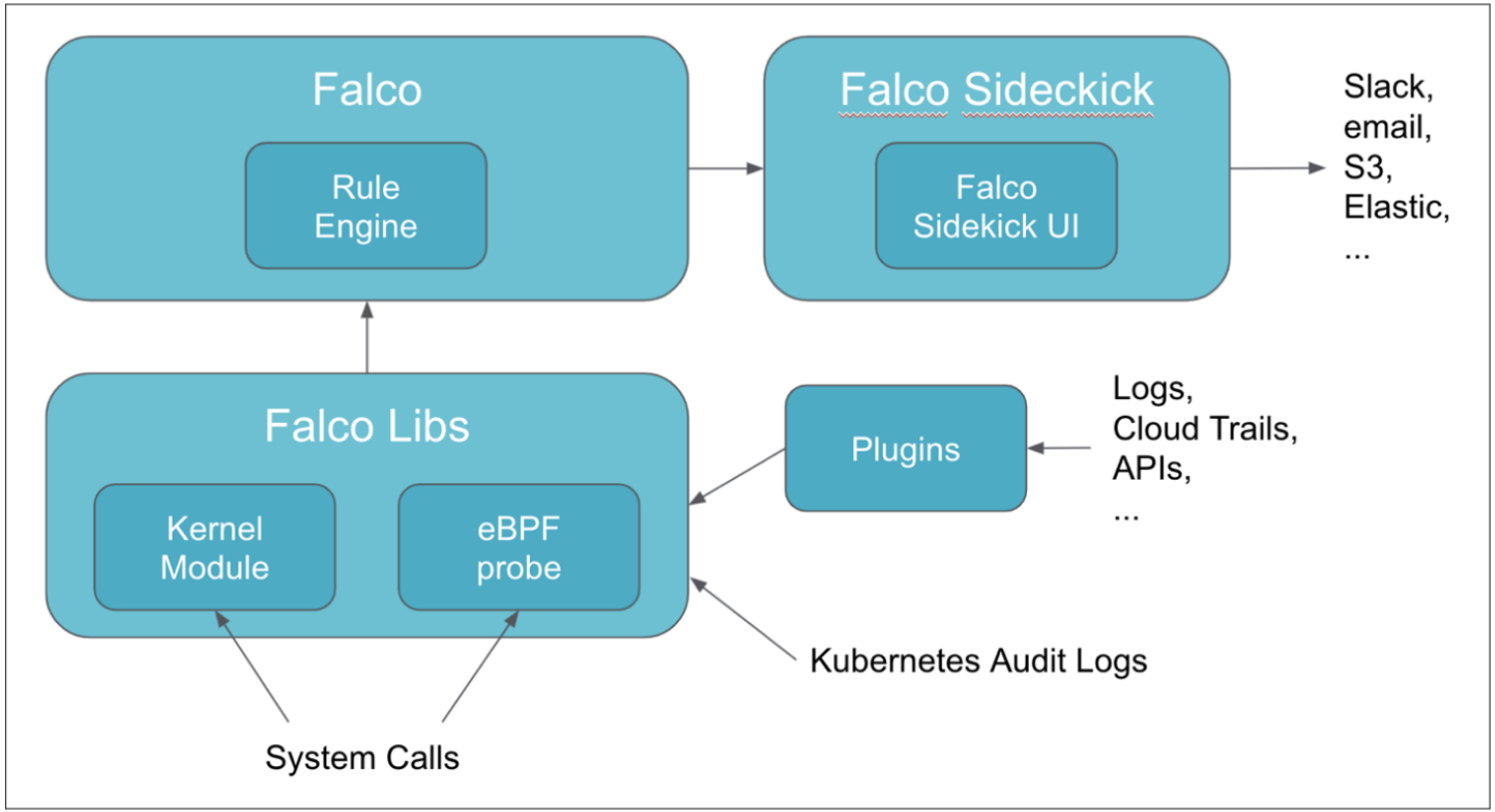
sysdig

What Falco is used for?

- **Runtime container security:** Detect intrusions and anomalous file, user, and network activity using community-driven policies
- **Kubernetes security monitoring:** Detect suspicious activities on Kubernetes' control plane APIs
- **Cloud security monitoring:** Detect unexpected behaviors and changes to configurations, intrusions, and data theft

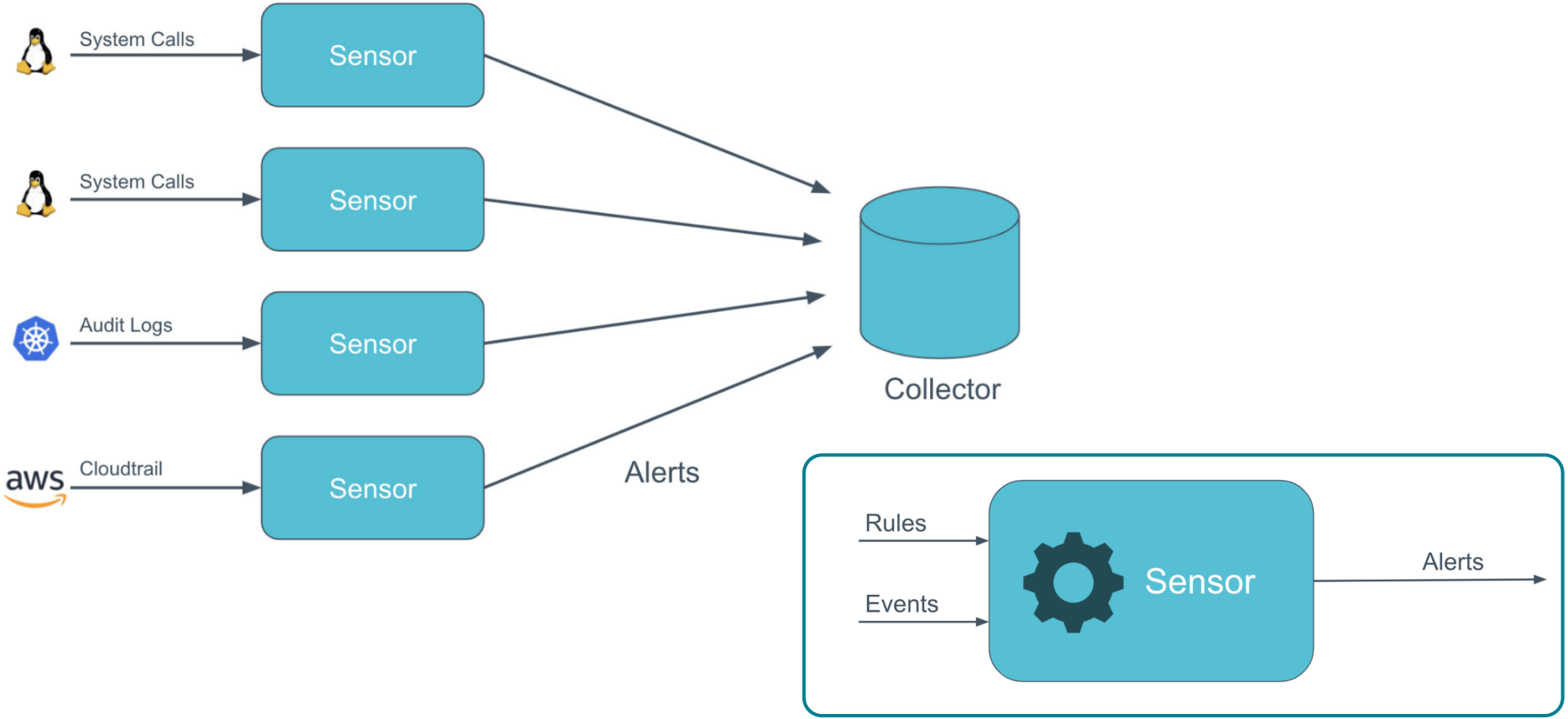
sysdig

Falco High Level Architecture



sysdig

Edge Computing to Scale!!



Falco Demo

sysdig

sysdig

Seeing is Securing