The Challenge of Securing Containers and Kubernetes

Diego Gagliardo
Technical Account Manager
Diego Gagliardo

V2

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

Me

Jon "maddog" Hall

V1

diego@sysdig.com

V2

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

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

>700
>500

~5k GitHub stars
40M downloads
Agenda

• Cloud-Native architecture security challenge
• K8s/containers general security workflow overview
• Runtime Threat Detection with Falco
From Monolithic to Microservices
Kubernetes, the cloud OS

The components of a Kubernetes cluster
Operational Challenges with Containers

- Containers disappear and leave no trail
- Cloud native leaves you blind
- Security and operations fail without context
Traditional Security Challenges Exist in Cloud

- Fix Software Vulnerabilities
- Manage Configs and Permissions
- Detect and Respond to Threats
- Meet Compliance
## Secure Containers, Kubernetes and Cloud Services

<table>
<thead>
<tr>
<th>CODE</th>
<th>BUILD</th>
<th>RUN</th>
<th>RESPOND</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure as Code Validation</strong></td>
<td><strong>Vulnerability Management</strong></td>
<td><strong>Configuration and Permission Management</strong></td>
<td><strong>Threat Detection</strong></td>
</tr>
</tbody>
</table>
| • Block risky configs  
• Auto-remEDIATE at the source | • Scan in CI/CD and registries  
• Block risky images  
• Prioritize vulns using security context | • Detect cloud misconfigurations  
• Enforce least privilege access | • Detect threats, drift, config changes, and runtime vulns  
• Implement K8s native microsegmentation | • Capture detailed record for forensics  
• Remediate config issues  
• Block malicious activity |

---

**Compliance (PCI, NIST, SOC 2 and others)**
Falco

Cloud native threat and anomaly detection

~5k GitHub stars  40M downloads
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
Falco High Level Architecture

Falco
- Rule Engine

Falco Sidekick
- Falco Sidekick UI

Falco Libs
- Kernel Module
- eBPF probe

Plugins

System Calls

Kubernetes Audit Logs

Slack, email, S3, Elastic, ...

Logs, Cloud Trails, APIs, ...

sysdig
Edge Computing to Scale!!

System Calls → Sensor → Collector

System Calls → Sensor → Collector

Audit Logs → Sensor → Collector

Cloudtrail → Sensor → Collector

Alerts

Rules → Sensor → Alerts

Events → Sensor → Alerts
Falco Demo