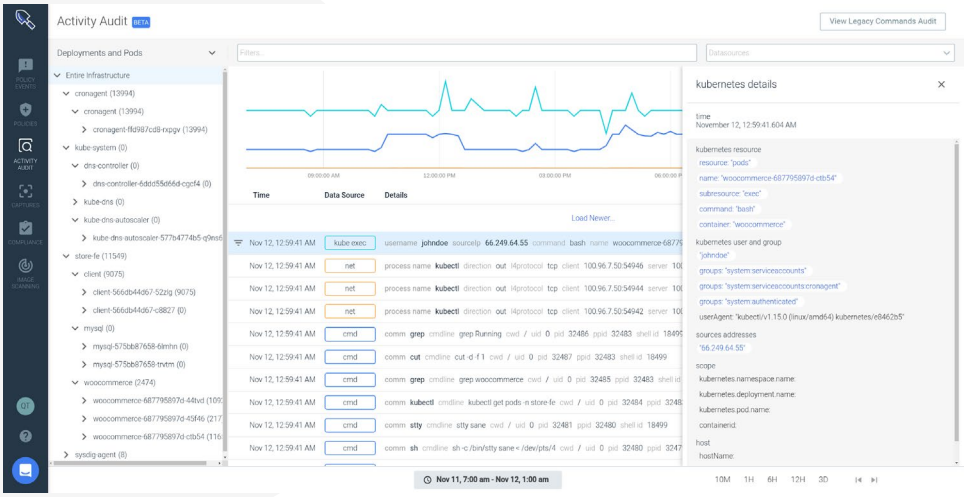
Sysdig Secure

www.sysdig.com/secure

Sysdig Secure embeds security and compliance into the build, run and respond stages of the Kubernetes lifecycle. Manage cloud security risk by integrating image scanning, compliance, runtime security, and incident response into your secure DevOps workflow.



Sysdig Secure Benefits

Deploy Securely

- Use a single workflow for detecting vulnerabilities and misconfigurations in containers.
- Flag vulnerabilities across the Kubernetes infrastructure and quickly identify owners.
- Continuous compliance for standards (PCI, NIST) with out of the box policies.
- Verify Kubernetes and container configurations meet CIS benchmarks with pre-built checks to make your teams more efficient.

Block threats at runtime

- Prevent threats without impacting performance using Kubernetes native controls.
- Save time creating policies by using MIL based profiling to baseline a healthy image.
- Make Falco easier to use with built-in runtime policies and remediation actions.

Respond Quickly

- Implement File Integrity Monitoring for hosts and containers.
- Automatically remediate by triggering response actions and notifications.
- Conduct forensics after the container is gone.
- Enable audit by correlating Kubernetes activity.

Key Use Cases

Image Scanning
Detect vulnerabilities within the CI/CD pipeline. Scan locally in the pipeline and prevent risky images from going into the registry or from being deployed (via Kubernetes admission controller).

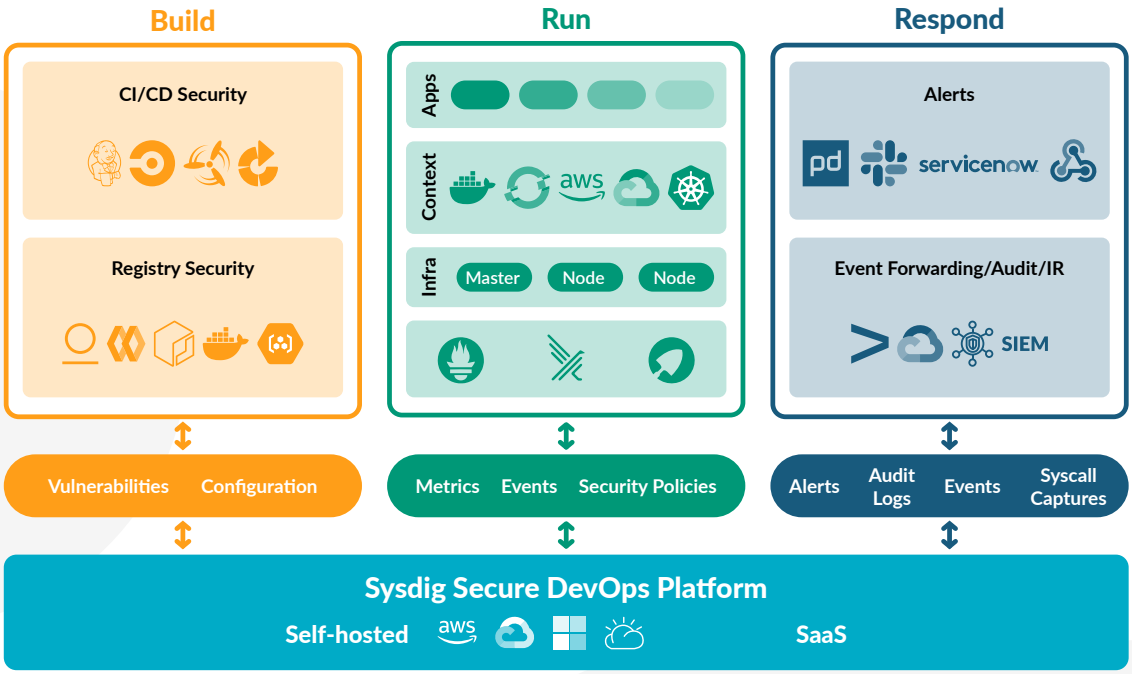
Forensics and Audit
Speed up forensics and incident response for containers and Kubernetes with a single source of truth. Record a snapshot of pre- and post-attack activity via system calls that are enriched with cloud/Kubernetes metadata.

Compliance Validation
Validate compliance and ensure file integrity monitoring across the lifecycle of containers, Kubernetes and cloud-native workloads based on regulatory standards (NIST, PCI).

Runtime Security
Detect and block attacks, combining deep visibility through system calls with Kubernetes metadata, labels and audit events. Powered by the open-source cloud native runtime security project called Falco.

Configuration Validation
Ensure configuration meets security best practices based on CIS Benchmarks or your own guidelines.

Unified Workflow Across the Cloud-Native Lifecycle



Sysdig Secure DevOps Platform enriches open-source data sources with cloud and Kubernetes application context. Now you can have a unified workflow to run cloud-native workloads confidently at scale.

Start your 30 day free trial now:
https://sysdig.com/company/free-trial/