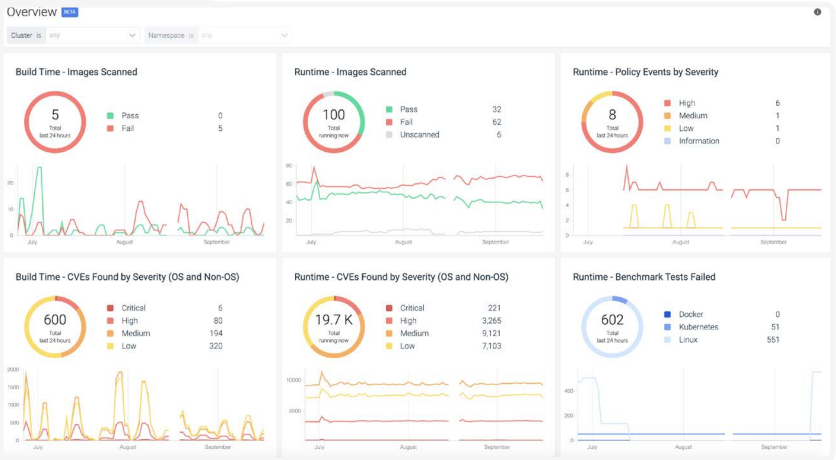
Sysdig Secure DevOps Platform

sysdig.com/platform

The Sysdig Secure DevOps Platform provides security to confidently run containers, Kubernetes and cloud services. With Sysdig you can secure the build pipeline, detect and respond to runtime threats, continuously validate compliance, and monitor and troubleshoot cloud infrastructure and services. Sysdig is a SaaS platform, built on open source software.



Sysdig Benefits

Security Built on an Open Source

- Scan images for vulnerabilities using open-source Anchore Engine.
- Accurately detect runtime threats using Falco, the open standard for runtime detection, across containers, hosts, Kubernetes and AWS cloud services.
- Accelerate incident response and troubleshooting with a detailed record of all activity using sysdig OSS.
- Continuously validate NIST, PCI, and SOC2 compliance against using Anchore Engine, Falco and sysdig OSS.

Deep Visibility to Run Apps Confidently

- Unified view spanning on-premise, hybrid, and multi cloud environments.
- Visibility into security threats, operational alerts and compliance risks with fewer false positives across container, kubernetes and cloud services.
- Use rich context to understand impact by user, app and service for resolving vulnerabilities, threats and performance issues.

Scale Simply with SaaS and DevOps Integrations

- Leverage a SaaS-first option for efficiency and faster innovation.
- Plug security into your DevOps and SIEM tool sets with automation and out of the box integrations.
- Easily meet security, availability, and compliance requirements with curated workflows.

Key Use Cases

Image Scanning

Scan container images for vulnerabilities and misconfigurations and validate best practices directly within CI/CD pipelines and registries.

Runtime Security for Containers, Cloud and Kubernetes

Protect containers, Kubernetes, hosts and AWS infrastructure (using CloudTrail) using open-source Falco, with out of the box policies. Visualize, auto-create and modify Kubernetes network policies. Automatically trigger response actions and notify the right teams immediately.

Continuous Compliance

Ensure ongoing compliance across container lifecycle for standards like NIST, PCI, SOC2 and more with compliance dashboards. Ensure configuration meets security best practices based on CIS Benchmarks or your own guidelines.

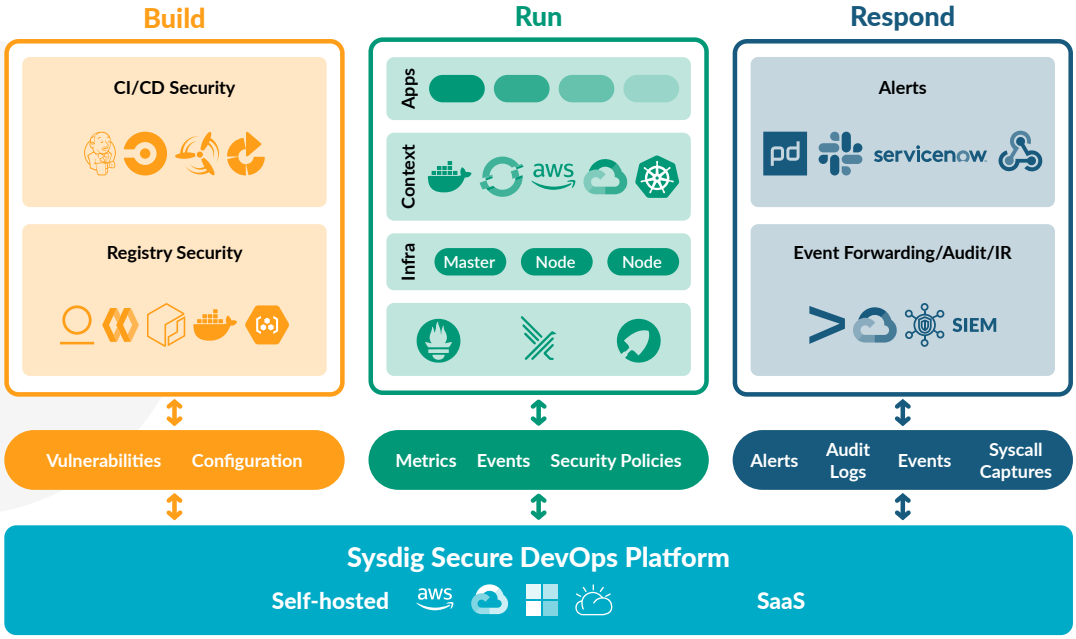
Monitor & Troubleshoot Containers, Cloud Services & Kubernetes

Gain deep visibility with rich Kubernetes context to maximize performance and availability of your cloud applications and infrastructure using Prometheus native exporters, visualizations, dashboards, and alerts.

Troubleshooting and Incident Response with Syscall Data- A Single Source of Truth

Resolve issues inside pods and conduct forensics by reconstructing system activities with Kubernetes application context. Perform root cause analysis and contain the impact of security breaches. Correlate system, user, and container activity over time with a forensics workflow and streamline audit support.

Unified Workflow Across the Cloud-Native Lifecycle



With the Sysdig Secure DevOps Platform, cloud teams secure the build pipeline, detect and respond to runtime threats, continuously validate compliance, and monitor and troubleshoot cloud infrastructure and services. Sysdig is a SaaS platform, built on an open source stack that includes Falco and sysdig OSS, the open standards for runtime threat detection and response. Hundreds of companies rely on Sysdig for container and Kubernetes security and visibility.

Get the confidence you need to run containers, Kubernetes, and cloud services.
Start your 30-day free trial now:
https://sysdig.com/company/free-trial/

Copyright © 2020 Sysdig, Inc. All rights reserved. PB-010 Rev.D 12/20