



Secure DevOps for OpenShift

Enhancing Security, Compliance and Performance

Chris Kranz
Principal Sales Engineer, EMEA

Sysdig Secure DevOps Platform



Secure DevOps converges security and observability functions

Use the Same Data to Monitor and Secure



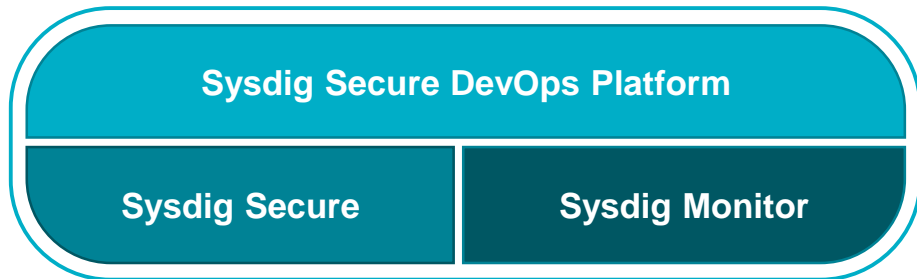
Embed security



Maximize availability

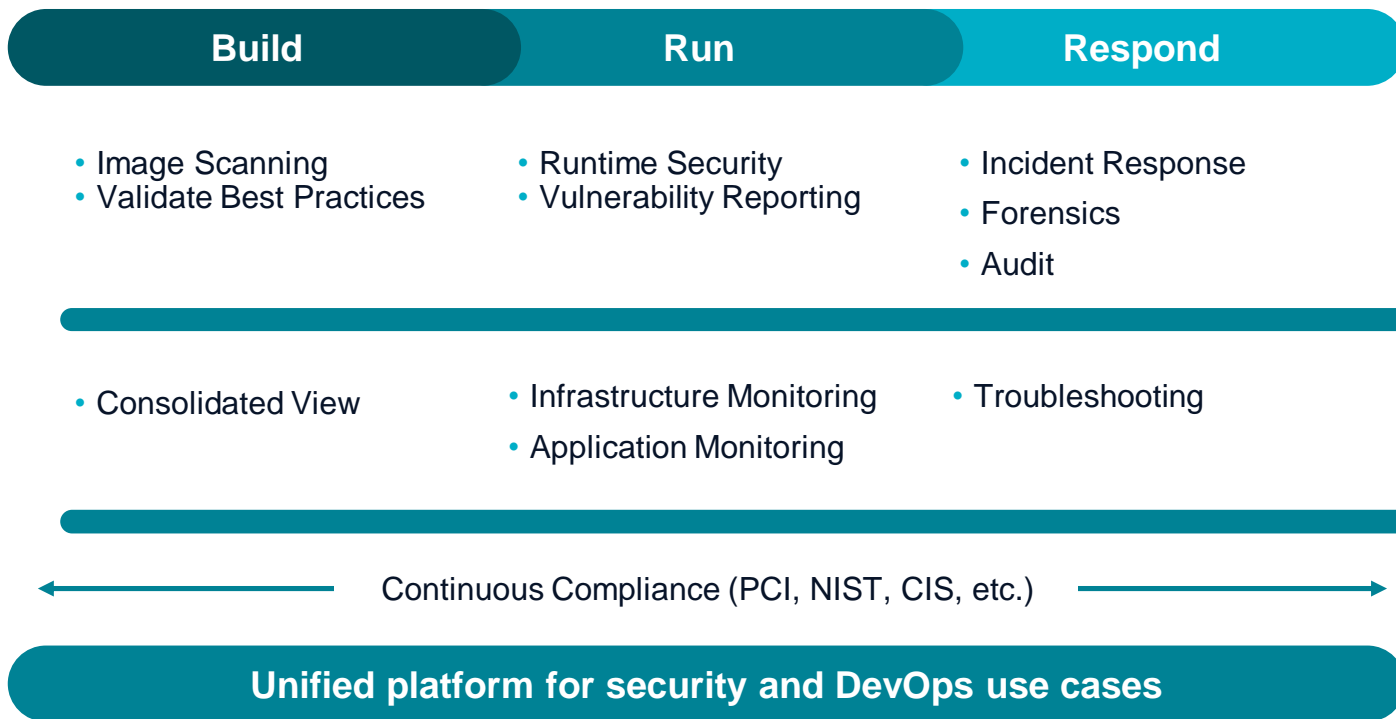


Validate compliance

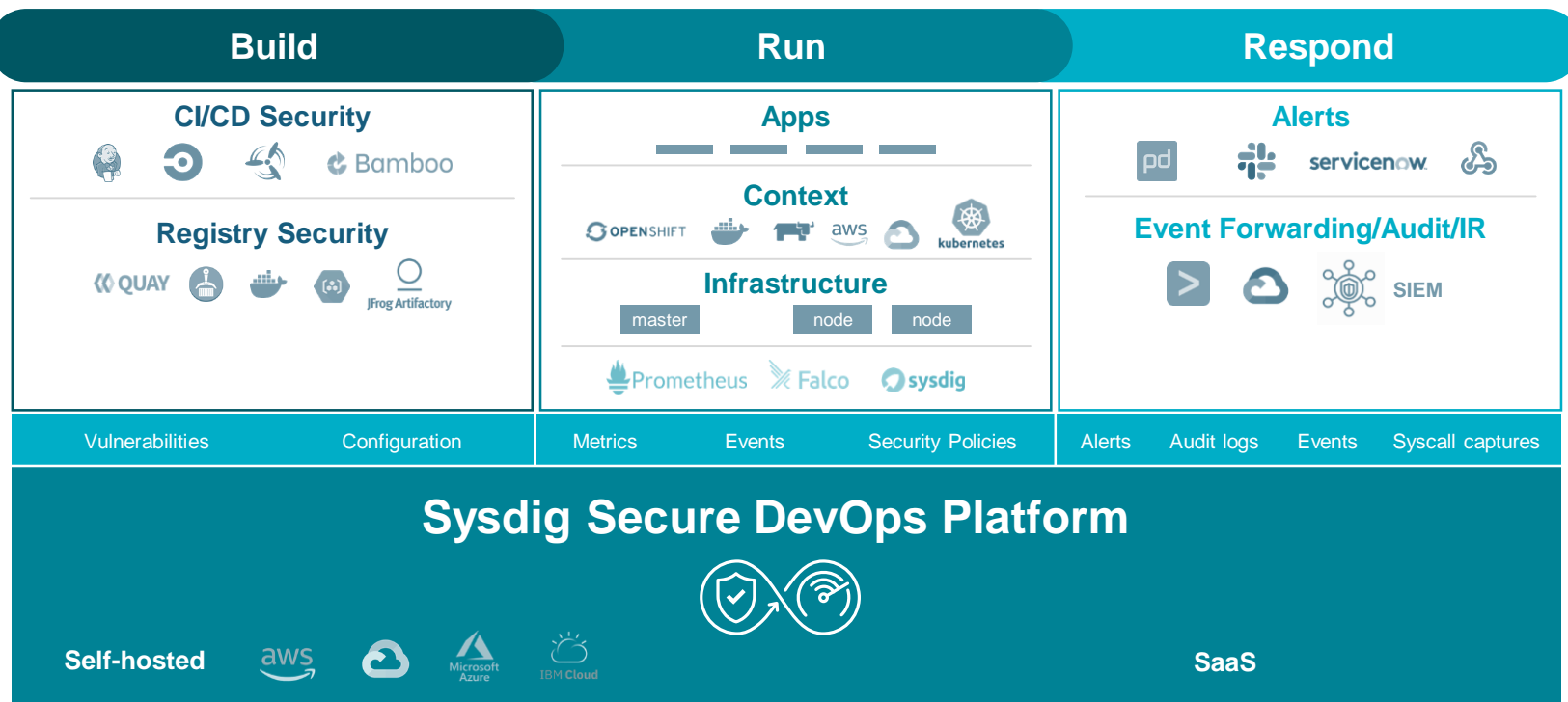


Converging visibility and security for production deployments

Secure DevOps Across Cloud-Native Lifecycle



Unified Workflow Across the Cloud-Native Lifecycle



Sysdig Platform Complementary Benefits

Red Hat OpenShift Component	Coverage	Sysdig Complement
RH Quay Container Registry	<ul style="list-style-type: none"> Image repository, versioning, roll-back 	<ul style="list-style-type: none"> Auto detection and analysis of new images Extend visibility into external repositories
Clair	<ul style="list-style-type: none"> Static analysis and image vulnerability scanning (OS,NIST NVD) 	<ul style="list-style-type: none"> Application vulnerability scanning Security best practices Container image best practices
OpenSCAP	<ul style="list-style-type: none"> Configuration compliance, vulnerabilities assessment, scanning & remediation 	<ul style="list-style-type: none"> Container based compliance and best practices Fine grained runtime security detection & prevention (selinux / seccomp ++)
Insights	<ul style="list-style-type: none"> Proactive configuration management advise & remediation 	
Prometheus	<ul style="list-style-type: none"> Telemetry monitoring & alerting 	<ul style="list-style-type: none"> Centralised telemetry data across multiple clusters & orchestrators Help migration events across environments / platforms Analytics across multiple environments concurrently
RHCOS	<ul style="list-style-type: none"> Immutable, secure by default container optimised OS 	<ul style="list-style-type: none"> Runtime security and auditing Zero day detection & prevention
OpenShift Enterprise Container Application Platform	<ul style="list-style-type: none"> Secure by default container orchestrator 	<ul style="list-style-type: none"> Centralised view across platforms Capacity planning & chargeback guidance Combined security & application monitoring
RH bundled EFK	<ul style="list-style-type: none"> Log aggregation 	<ul style="list-style-type: none"> Event integration and correlation across security & telemetry
RHEL	<ul style="list-style-type: none"> Enterprise Linux Operating System, system hardening 	<ul style="list-style-type: none"> Runtime security and auditing Zero day detection & prevention



sysdig

Dig deeper