Wie Sie eine umfassende DevSecOps-Lösung bereitstellen

Das DevSecOps-Framework von Red Hat schafft eine solide Basis für eine hochgradig skalierbare, umfassende DevSecOps-Lösung.

Die DevOps-Sicherung ist eine komplizierte Angelegenheit

Das Sichern von DevOps ist ein komplexes Unterfangen, da DevOps-Tools sich schnell entwickeln und ändern. Container und Kubernetes erhöhen die Komplexität, bieten mehr Angriffsflächen und stellen damit ein erhöhtes Sicherheitsrisiko dar. Um betriebswichtige IT-Infrastrukturen und vertrauliche Daten zu schützen, müssen Entwicklungs- und Operations-Teams mit Veränderungen Schritt halten und die Sicherheit im gesamten Lifecycle von Anwendungen großschreiben.

Red Hat und sein Sicherheitspartnernetzwerk haben ein Framework geschaffen, das eine solide Basis und Vorlage für die Bereitstellung von DevSecOps-Lösungen bietet und so effizientere Deployments und Skalierungen ermöglicht. Im Rahmen seiner umfassenden Defense-in-Depth-Strategie erfüllt das DevSecOps-Framework von Red Hat® die wichtigen Sicherheitsanforderungen des gesamten DevOps-Lifecycles. Red Hat und seine Sicherheitspartner unterstützen Sie dabei, Risiken zu reduzieren, indem sie die DevOps-Sicherheit vereinfachen und die DevSecOps-Einführung beschleunigen.

Sicherheitspartner wie Anchore, Aqua, CyberArk, Lacework, NeuVector, Palo Alto Networks, Portshift, Snyk, StackRox, Synopsys, Sysdig, Thales, Tigera, Trend Micro und Tufin ergänzen die nativen Sicherheitsfunktionen von Red Hat. Zusammen können wir Ihnen so umfassende DevSecOps-Lösungen bereitstellen, mit denen Sie Ihre Sicherheitsaufstellung verbessern und Ihre Red Hat Investitionen voll ausschöpfen können.

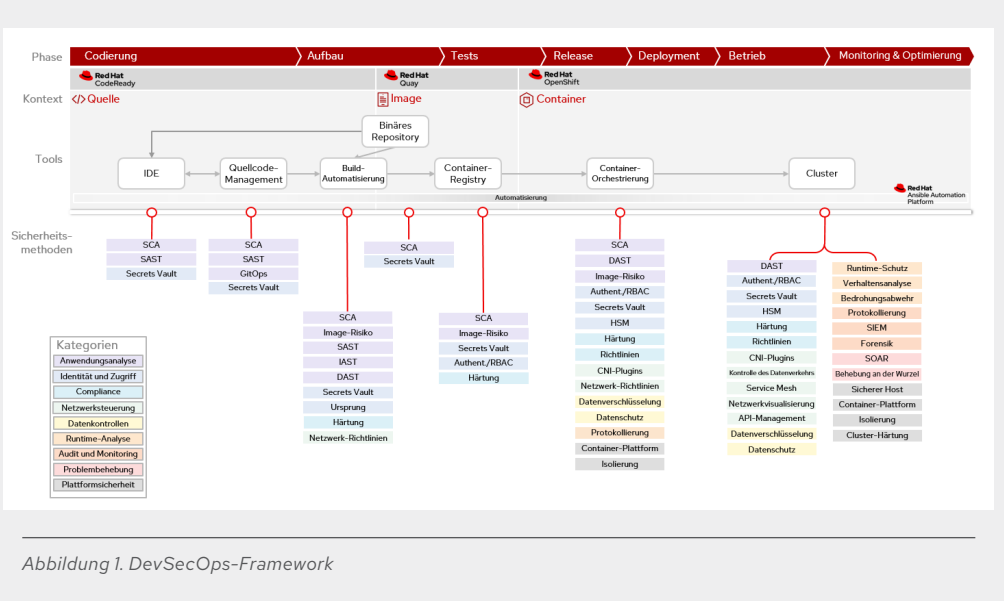

Abbildung 1. DevSecOps-Framework

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

Ein umfassendes Framework mit verschiedenen Sicherheitsmethoden

Das DevSecOps-Framework von Red Hat besteht aus neun Sicherheitskategorien sowie 32 Methoden und Technologien, die den gesamten Anwendungs-Lifecycle abdecken. Das Framework platziert integrierte Red Hat Funktionen, DevOps-Toolchains und Sicherheitspartnerlösungen an wichtigen Integrationspunkten in der Pipeline. Je nach dem Umfang Ihrer DevOps-Umgebung und Ihren spezifischen Anforderungen können Sie alle oder nur bestimmte Methoden und Technologien innerhalb einer Kategorie implementieren.

Plattformsicherheit

Die Sicherung Ihrer Kubernetes-Plattform ist unabdingbar. Sie auf die sichere, zuverlässige und skalierbare Unterstützung betriebswichtiger Anwendungen vorzubereiten, kann dabei zur Herausforderung werden. Tatsächlich stellen das Deployment und das Management von Kubernetes weiterhin die beiden größten Herausforderungen für Unternehmen dar.[1] Die unternehmensgerechte Kubernetes-Container-Plattform Red Hat OpenShift® beseitigt Komplexität und Einführungshindernisse und bietet Ihnen eine Vielzahl an integrierten Sicherheits-Features.

Das DevSecOps-Framework von Red Hat bietet grundlegende Funktionen zur Sicherung der zugrunde liegenden Container-Hosts (Red Hat Enterprise Linux® und Red Hat CoreOS) sowie der Container-Plattform. Die meisten Sicherheitsfunktionen von Red Hat sind standardmäßig darauf ausgerichtet, das Deployment zu vereinfachen und Risiken zu minimieren. Mit diesen Funktionen können Sie die Container-Sicherheit an den Grenzen gewährleisten und den Host vor Container-Ausbrüchen schützen.

Methoden der Plattformsicherung

- Host-Sicherheit: Bietet MAC (Mandatory Access Controls) mit SELinux und Kernel-Funktionen zur Kontrolle von Systemaufrufen mit seccomp (Secure Computing Mode) sowie zur Isolierung von CPU-, Speicher- und anderer Ressourcen mit CGroups.
- Container-Plattform-Sicherheit: Enthält die schlanke Container-Runtime CRI-O sowie Quay, eine sichere Registry für Container-Images.
- Linux-Namespaces: Isolieren Anwendungen für ganze Teams, Gruppen und Abteilungen.
- Kubernetes- und Container-Härtung: Wenden Standards wie NIST 800-190 und CIS-Benchmarks an.

Anwendungsanalyse

Anwendungsanalysefunktionen helfen Ihnen dabei, Schwachstellen und andere Sicherheitsprobleme in Anwendungen möglichst früh im Lifecycle zu erkennen. Indem Sie die Sicherheit des DevOps-Lifecycles vorverlegen, können Sie Sicherheitsrisiken frühzeitig identifizieren und beheben. So ersparen Sie sich spätere repetitive Aufgaben zur Problembehebung.

Methoden der Anwendungsanalyse

- SAST (Static Application Security Testing): Analysiert Code in der Entwicklungsphase auf Schwachstellen und Qualitätsprobleme.
- SCA (Software Composition Analysis): Untersucht abhängige, in Anwendungen enthaltene Pakete auf bekannte Schwachstellen und Lizenzierungsprobleme.
- IAST-Tools (Interactive Application Security Testing) und DAST-Tools (Dynamic Application Security Testing): Analysieren aktive Anwendungen auf Schwachstellen bei der Ausführung.

---

1 *Vizard, Mike: „Survey Sees Kubernetes Enterprise Adoption Gains". Container Journal, März 2020.*

Teil der Anwendungsanalyse sind außerdem Sicherheitsmethoden wie das GitOps-Konfigurationsmanagement sowie Risikomanagementfunktionen für Container-Images, etwa zur Erkennung von Malware, eingebetteten Secrets und fehlerhaften Konfigurationen.

Identitäts- und Zugriffsmanagement

IAM-Methoden (Identitäts- und Zugriffsmanagement) steuern sowohl lokal als auch in der Cloud den Zugriff auf Assets, Anwendungen und Daten basierend auf der Nutzer- oder Anwendungsidentität sowie auf administrativ festgelegte Richtlinien. Sie sind in allen Phasen des DevOps-Lifecycles zu finden und können unautorisierte Systemzugriffe und Lateral Movements verhindern.

IAM-Methoden

- Authentifizierungs- und Autorisierungskontrollen: Verifizieren die Identität von Nutzern und Anwendungen und gewähren Zugriff auf spezifische Ressourcen und Funktionen.
- RBACs (Role-based Access Controls): Gewähren Nutzergruppen basierend auf deren Verantwortlichkeiten Zugriff auf Ressourcen oder Funktionen, vereinfachen die Administration und das Onboarding und reduzieren die schleichende Ausweitung von Berechtigungen.
- Identity Providers, Secrets Vaults und HSMs (Hardware Security Modules): Verwalten und schützen Zugangsdaten, Sicherheitsschlüssel und -zertifikate sowie Secrets sowohl bei Inaktivität als auch während der Übertragung.

Mit zusätzlichen IAM-Methoden wie Funktionen zum Ursprung und zur Signierung von Images kann die Authentizität von Container-Images validiert und Vertrauen geschaffen werden.

Compliance

Compliance-Methoden und -Technologien unterstützen Sie bei der Einhaltung von Branchen- und Verwaltungsvorschriften und Unternehmensrichtlinien. Sie automatisieren die Erstellung von Compliance-Nachweisen und -Berichten in der gesamten DevOps-Pipeline und helfen Ihnen so dabei, Audits zu vereinfachen und teure Bußgelder und Prozesse zu verhindern.

Mit diesen Methoden erreichen Sie eine bessere Compliance mit Datenschutz- und Datensicherheitsanforderungen, darunter:

- PCI-DSS (Payment Card Industry Data Security Standard)
- ISO 27001 (Informationssicherheits-Management-Standard)
- HIPAA (Health Insurance Portability and Accountability Act)
- DSGVO (EU-Datenschutz-Grundverordnung)

Netzwerksteuerung und -segmentierung

Mithilfe von Methoden der Netzwerksteuerung und -segmentierung lässt sich der Datenverkehr in Kubernetes besser steuern, trennen und visualisieren. So können Sie Mandanten isolieren und die Kommunikation zwischen containerisierten Anwendungen und Microservices sichern.

Methoden der Netzwerksteuerung und -segmentierung

- Netzwerksicherheitsrichtlinien in Kubernetes: Steuern den Datenverkehr auf IP-Adressen- oder Port-Ebene und lassen sich durch verschiedene Optionen wie Kontrolle von Cluster-Ingress- und -Egress-Datenverkehr, Protokollierung und Netzwerkvisualisierung erweitern.
- SDN (Software-Defined Networking): Stellt eine programmierbare, anpassbare Netzwerkstruktur in Echtzeit bereit und unterstützt so dynamische Sicherheitsanforderungen und sich weiterentwickelnde Geschäftsanforderungen.
- Service Mesh: Bietet Netzwerksegmentierung und -visualisierung sowie Authentifizierungs- und Autorisierungsfunktionen für containerisierte Anwendungen und Microservices.

Datenkontrollen

Datenkontrollmethoden und -technologien helfen Ihnen dabei, die Integrität von Daten zu schützen und nicht autorisiertes Offenlegen von Daten zu verhindern. Sie schützen Daten sowohl bei Inaktivität als auch bei der Übertragung und unterstützen Sie so beim Schutz von geistigem Eigentum und vertraulichen Kundendaten.

Datenkontrollmethoden

- Datenverschlüsselung: Bietet Datenkryptografie, Tokenisierung, Datenmaskierung und wichtige Management-Funktionen, mit denen das nicht autorisierte Offenlegen von Daten in Datenbanken, Dateien und Containern verhindert werden kann.
- Datenschutz: Erkennt und klassifiziert Daten und überwacht und prüft deren Aktivität, um vertrauliche Daten zu schützen und die Compliance zu verbessern.

Runtime-Analyse und -Schutz

Runtime-Methoden in der Produktion helfen Ihnen dabei, für eine gute Cluster-Hygiene zu sorgen, da verdächtige und bösartige Aktivitäten in Echtzeit erkannt und behoben werden.

Analyse- und -Schutzmethoden für Runtimes

- Zugangskontrolle: Sorgt als eine Art Gatekeeper in Kubernetes für die Regelung und Durchsetzung von erlaubten Ausführungen im Cluster.
- Verhaltensanalyse für Runtime-Anwendungen: Untersucht die Systemaktivität und erkennt dabei verdächtige und bösartige Aktivitäten in Echtzeit.
- RASP (Runtime Application Self Protection): Erkennt und blockiert Cyberangriffe in Echtzeit.
- API-Management: Steuert den Zugriff auf APIs und sichert den API-Datenverkehr.

Audit und Monitoring

Audit- und Monitoring-Methoden informieren Sie über Sicherheitsvorfälle in Ihrer Produktivumgebung. Sie erfahren, wann das jeweilige Ereignis aufgetreten ist, und erhalten Informationen zu möglichen Ursachen und Auswirkungen. So erhalten Sie einen besseren Überblick und können schneller auf Vorfälle reagieren.

Audit- und Monitoring-Methoden

- SIEM (Security Information and Event Management): Bietet zentrale Berichte zu Ereignissen durch konsolidierte Protokolle und Netzwerkdaten verschiedener Geräte, Endpunkte und Anwendungen.
- Forensik: Bietet Insights zu Sicherheitsverletzungen, stellt Nachweise für Compliance-Audits zur Verfügung und beschleunigt Wiederherstellungsmaßnahmen.

Problembehebung

Behebungsprozesse greifen automatisch korrigierend ein, wenn es in der Produktion zu Sicherheitsvorfällen kommt. Damit können Sie die Verfügbarkeit von Systemen verbessern und Datenverluste verhindern.

Problembehebungsmethoden

- SOAR-Plattformen (Security Orchestration, Automation and Response): Automatisierung von Maßnahmen und Integration in andere Sicherheitstools als Reaktion auf Sicherheitsvorfälle.
- Problembehebung an der Wurzel: Löst automatisch Probleme, die auf Konfigurationsfehlern und Richtlinienverletzungen in Kubernetes basieren.

Fazit

Das DevSecOps-Framework von Red Hat schafft eine zuverlässige und skalierbare Basis, mit der Sie die DevOps-Sicherheit erhöhen und Risiken reduzieren können. Red Hat und seine Sicherheitspartner bieten Ihnen die notwendige Technologie, mit der Sie DevSecOps einfacher und schneller implementieren können. Kontaktieren Sie uns, um mehr zu erfahren.

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

EUROPA, NAHOST, UND AFRIKA (EMEA)
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

de.redhat.com
#F26043_1220