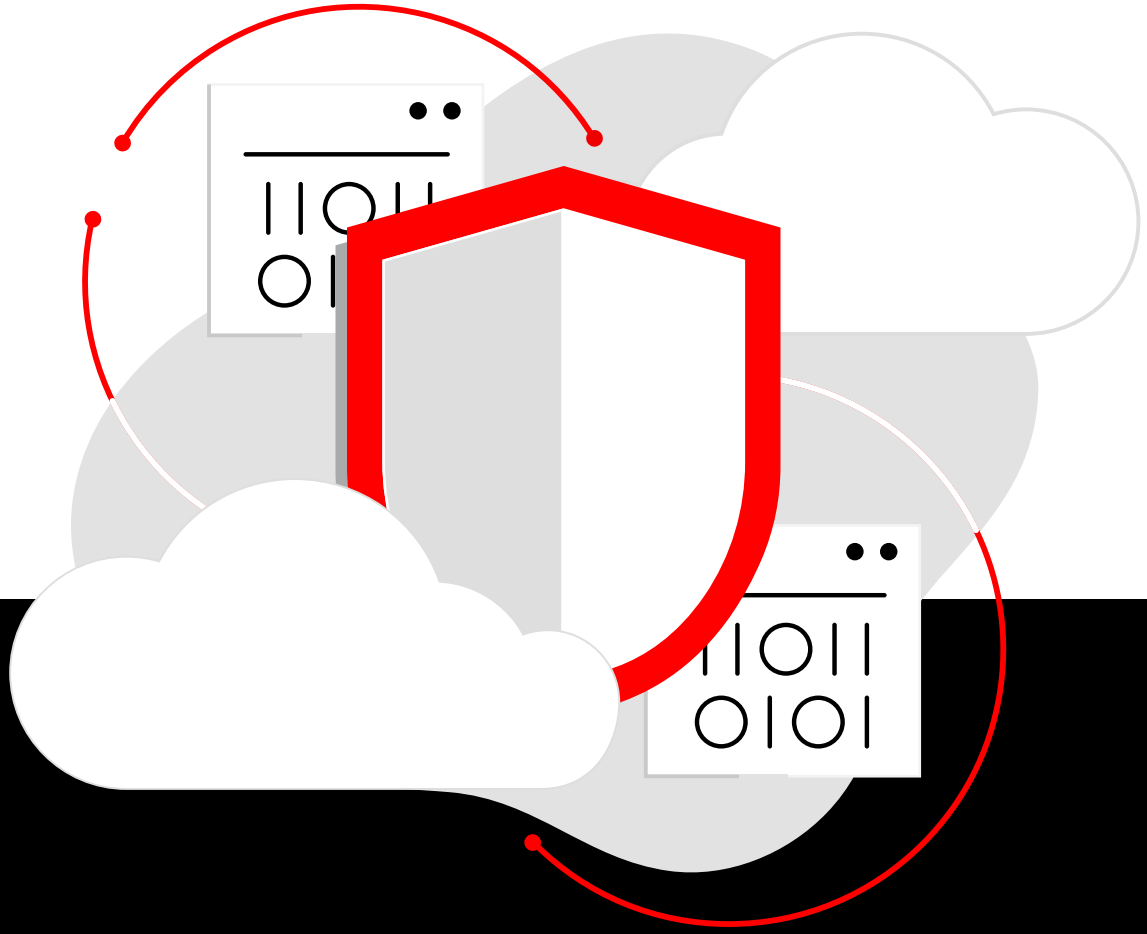
Red Hat



Anwendungs-Lifecycles mit DevSecOps modernisieren und sichern

Inhalt

Einleitung

Anwendungssicherheit ist in einer digitalen Welt entscheidend

Immer mehr Unternehmen führen Cloud-, Container- und Microservice-Technologien ein, um in einer digitalen Welt wettbewerbsfähig zu sein. In diesem Zusammenhang bleibt die Sicherheit ein wichtiger Aspekt. Tatsächlich nennen 50 % der leitenden IT-Führungskräfte in Unternehmen die Cybersicherheit als eine der 3 wichtigsten Prioritäten für Technologieinitiativen.[1] Gleichzeitig erwarten 86 %, dass sich das Tempo der digitalen Transformation in ihrem Unternehmen bis 2021 erhöhen wird.[1]

Diese neuen Technologien erfordern ein anderes Sicherheitskonzept, da traditionelle, perimeterbasierte Ansätze in verteilten Umgebungen nicht effektiv sind. Zudem steigen mit DevOps und cloudnativen Methoden die Entwicklungsgeschwindigkeit und die Bereitstellungsflexibilität. Daher ist es wichtig, das Thema Sicherheit früher im Prozess zu berücksichtigen. Das Anwenden von Sicherheitsmaßnahmen gegen Ende des Entwicklungszyklus führt oft zu Bereitstellungsverzögerungen und weniger Schutz.

Mit der Einführung von **DevSecOps**-Ansätzen und -Praktiken können Sie Ihre Anwendungsumgebung und Ihr Unternehmen besser schützen.

Was ist DevSecOps?

DevSecOps erweitert die auf Zusammenarbeit basierende Kultur von DevOps um den Faktor Sicherheit und integriert diese in den gesamten Anwendungs-Lifecycle. Der Ansatz bezieht Menschen, Prozesse und Technologie mit ein und sorgt so auch in verteilten Umgebungen für mehr Sicherheit.

Ohne DevSecOps besteht Sicherheit aus einer Reihe von Aufgaben, für die ein einziges Team zuständig ist und die am Ende des Entwicklungs- und Bereitstellungsprozesses angewandt werden. Mit DevSecOps sind mehrere Teams gemeinsam für die Sicherheit verantwortlich. Sicherheits-, Entwicklungs- und Operations-Teams arbeiten zusammen und tauschen dabei Informationen, Feedback, Erfahrungen und Insights aus. Mit diesem Ansatz kann die Sicherheit von Anfang an bei der Anwendungsentwicklung und Infrastrukturbereitstellung integriert werden, was den Schutz erhöht und Risiken senkt.

Vorteile von DevSecOps

Mehr Sicherheit und weniger Risiko

Beheben Sie Sicherheitsprobleme in der Entwicklung statt in der Produktion, um Ihre Anwendungen besser zu schützen und weniger Deployments wegen Fehlern bei den Richtlinienprüfungen zu verzögern oder zu stoppen.

Schnellere Behebung von Sicherheitsproblemen

Wenden Sie moderne Sicherheitspraktiken und -tools an, die die Zusammenarbeit fördern und Automatisierung ermöglichen. So können Sie Release-Zyklen beschleunigen, den Zeitaufwand für das Beheben von Sicherheitsproblemen in der Produktion verkürzen und Zeit und Geld sparen.

Erhöhte Compliance und Transparenz

Führen Sie automatisierte Prozesse und Tools ein, die das Risiko manueller Fehler verringern und die Vorhersehbarkeit und Wiederholbarkeit erhöhen. Dadurch können Sie die Compliance verbessern und Auditprozesse vereinfachen.

*1 Flexera: „**2021 Flexera State of Tech Spend Report**“, Januar 2021.*

Herausforderungen bei der DevSecOps-Implementierung

Obwohl DevSecOps-Ansätze viele Vorteile bieten, können verschiedene Faktoren die Implementierung von DevSecOps erschweren.

- **Weiterentwicklung der Sicherheitslandschaft:** Sicherheitsbedrohungen und -vorschriften – einschließlich geschäftlicher, technischer und geografischer Anforderungen – verändern sich in einem rasanten Tempo. Das erschwert es Unternehmen, auf dem Laufenden zu bleiben.
- **Komplexe Anwendungsumgebungen:** Umfangreiche, komplizierte Anwendungsumgebungen können aus vielen Containern, Microservices und Cloud Services bestehen. Die Verbindungen und Sicherheitsauswirkungen dieser verschiedenen Technologien zu verstehen, kann daher zur Herausforderung werden.
- **Ineffiziente bestehende Tools und Prozesse:** Viele Teams beginnen damit, ihre bestehenden Tools und Prozesse auf DevSecOps-Initiativen anzuwenden, stellen aber fest, dass dieser Ansatz langfristig nicht zielführend ist.
- **Mehrere Sicherheitstools:** Das Auswählen, Testen, Integrieren und Warten der richtigen Auswahl an Sicherheitstools für Ihr Unternehmen erfordert Zeit, Recherche und kontinuierlichen Einsatz.

Ein erfolgreicher DevSecOps-Ansatz bezieht Kultur, Prozesse und Technologie mit ein

Das Sichern von Anwendungs-Lifecycles mit DevSecOps erfordert Veränderungen und Anpassungen in 3 Bereichen: Kultur, Prozesse und Technologie.

Kultur

Fördern Sie Zusammenarbeit und gemeinsame Ziele zwischen Ihren Entwicklungs-, Operations- und Sicherheitsteams. Unterstützen Sie die Team dabei, die Gründe und Methoden für die Integration von Sicherheitsfunktionen in die Anwendungs-Lifecycles zu verstehen.

Prozesse

Standardisieren, dokumentieren und automatisieren Sie Ihre Prozesse und Workflows, um die Effizienz und Sicherheit im gesamten Anwendungs-Lifecycle zu verbessern.

Technologie

Integrieren Sie Ihre Plattformen, Tools und Prozesse für Anwendungsentwicklung, -bereitstellung und -betrieb in ein einheitliches, zusammenhängendes System.

Mehr über die Grundlagen von DevSecOps erfahren

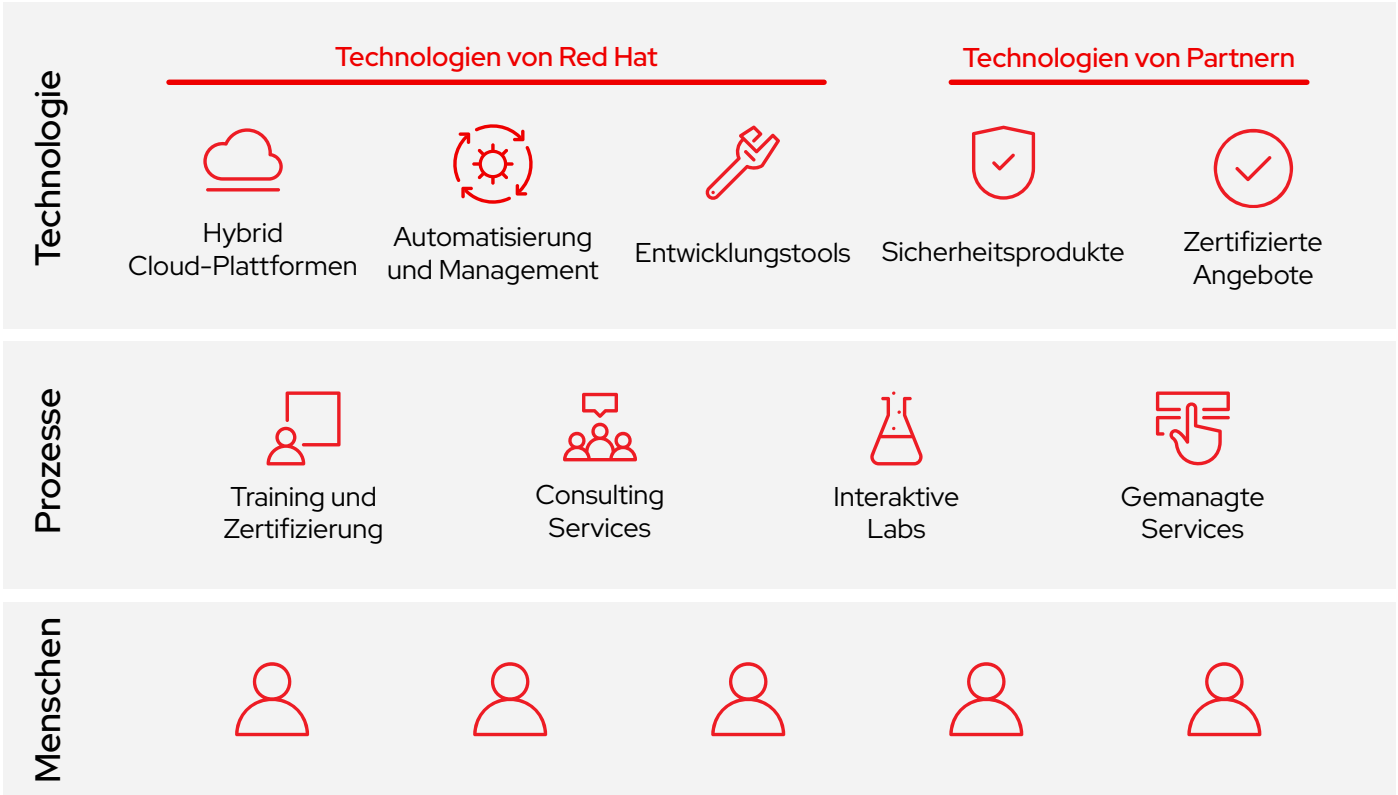
Im Blog-Beitrag „**Why your DevSecOps practice may be falling short**“ erfahren Sie mehr über die Änderungen, die für das erfolgreiche Implementieren von DevSecOps erforderlich sind. Im E-Book „**Mehr Sicherheit in der Hybrid Cloud**“ erfahren Sie, wie Sie Ihr Unternehmen mit cloudnativen Sicherheitsansätzen schützen können.

DevSecOps-Strategie von Red Hat

Red Hat bietet ein zertifiziertes Partnernetzwerk, umfangreiches Fachwissen und innovative Plattformen für die Entwicklung, Sicherung und Bereitstellung von Anwendungen in Hybrid Cloud-Umgebungen. Mit dieser Kombination können Sie umfassende DevSecOps-Lösungen implementieren, um die Anwendungssicherheit zu verbessern, Risiken zu minimieren, die Performance zu steigern und den Wert Ihrer Investitionen zu maximieren.

Dank einer vertrauenswürdigen Lieferkette für Inhalte, Support durch ein dediziertes Sicherheitsteam und der Rückportierung wichtiger Sicherheitsfunktionen stellen die Plattformen von Red Hat® eine ideale Basis für DevSecOps-Lösungen dar. Diese Basis wird durch unsere Partner mit innovativen, integrierten Produkten für Sicherheit und Automatisierung im gesamten Anwendungs-Lifecycle erweitert und verbessert. Wir bieten außerdem **Trainings- und Zertifizierungskurse**, **interaktive Labs**, **Consulting-Services** und **gemanagte Angebote**, mit denen Sie DevSecOps erfolgreich implementieren können.

Gemeinsam können wir eine geeignete Strategie entwickeln, unabhängig davon, in welcher Phase der DevSecOps-Einführung Sie sich befinden. Mit unseren modularen, erweiterbaren Lösungen und fachkundigen Services können Sie die Anwendungen bereitstellen, die Sie heute benötigen, diese an zukünftige Veränderungen anpassen und die Methoden und Ansätze erlernen, die Sie für eine effiziente und wirksame DevSecOps-Einführung brauchen.



Aufbau einer offenen DevSecOps-Basis mit Produkten von Red Hat

Red Hat OpenShift

Red Hat OpenShift® ist eine unternehmensgerechte, sicherheitsorientierte Hybrid Cloud-Plattform mit integrierten DevOps-Tools und standardmäßig aktivierten Sicherheitsfunktionen. Diese Plattform unterstützt Sicherheitstools und -technologien von Partnern und Drittanbietern, um die Sicherheit zu verbessern und solide DevSecOps zu implementieren. Im **Red Hat OpenShift Sicherheits-Guide** erfahren Sie mehr über die Sicherheit im gesamten Technologie-Stack.

Kostenlos testen

Wichtige Sicherheitsfunktionen

- SELinux (Security-Enhanced Linux)
- SCC (Security Context Constraint)
- Identitäts- und Zugriffsmanagement
- Datenverschlüsselung
- FIPS-Modus (Federal Information Processing Standards)

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform ist eine flexible, leistungsstarke Plattform, die Sicherheitslösungen automatisieren und integrieren kann und eine gemeinsame Sprache für Ihre Sicherheitstools bietet. Erfahren Sie mehr über **Use Cases zur Automatisierung**.

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux® CoreOS ist ein schlankes, unveränderliches, für Container optimiertes Betriebssystem, das auf der sicherheitsorientierten Basis von Red Hat Enterprise Linux aufbaut und in Red Hat OpenShift verwendet wird.

Red Hat Quay

Red Hat® Quay ist eine verteilte und hochverfügbare Container Image Registry, mit der Sie Container erstellen, verteilen und bereitstellen können.

Red Hat CodeReady Workspaces

Red Hat CodeReady Workspaces ist ein Tool, mit dem Entwicklungsteams in Containern, die auf Red Hat OpenShift ausgeführt werden, programmieren, entwickeln und testen können.

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes bietet eine cloudnative Architektur für Container-Sicherheit, die Anwendungen vom Build bis zur Runtime schützt.

Red Hat Advanced Cluster Management for Kubernetes

Mit **Red Hat Advanced Cluster Management for Kubernetes** können Sie Cluster und Anwendungen über eine zentrale Konsole mit integrierten Sicherheitsrichtlinien verwalten.

Flexibilität und Zuverlässigkeit mit einem Netzwerk aus zertifizierten Sicherheitspartnern

Kein einzelner Anbieter bietet sämtliche Funktionen, die für eine effektive DevSecOps-Implementierung erforderlich sind. Außerdem ist jedes Unternehmen anders und benötigt eine bestimmte Kombination aus Produkten und Technologien, um die jeweiligen Anforderungen zu erfüllen.

Red Hat bietet in Zusammenarbeit mit **innovativen, branchenführenden Sicherheitspartnern** Komplettlösungen an, die auf zertifizierten Integrationen, Container Images und **Red Hat OpenShift Operatoren** basieren. Sie können jederzeit vertrauensvoll die Partner, Produkte und Technologien auswählen, die Ihren Anforderungen am besten entsprechen, in der Gewissheit, dass sie zuverlässig und konsistent zusammenarbeiten. Diese Lösungen werden außerdem durch fachkundige Services, Support und Trainings unterstützt, damit Sie erfolgreich die DevSecOps-Kultur, -Prozesse und -Tools implementieren können.

Vorteile des Netzwerks aus Sicherheitspartnern von Red Hat

Auswahlmöglichkeiten

Wählen Sie die Produkte und Anbieter aus, die die Anforderungen Ihres Unternehmens am besten erfüllen.

Zertifizierung

Entwickeln Sie Ihre Lösung in der Gewissheit, dass die verschiedenen Komponenten zertifiziert sind, um zuverlässig zusammenzuarbeiten.

Fachwissen

Profitieren Sie von der kombinierten DevSecOps-Expertise und -Erfahrung von Red Hat und Partnern.

Services

Erhalten Sie Unterstützung bei der Implementierung von DevSecOps-Kultur, -Prozessen und -Tools in Ihrem Unternehmen.

Training

Lernen Sie Best Practices kennen, und erwerben Sie die erforderlichen Kompetenzen für die Einführung von DevSecOps-Ansätzen.

Red Hat Vulnerability Scanner-Zertifizierung

Die Red Hat Vulnerability Scanner-Zertifizierung minimiert Unstimmigkeiten zwischen den Ergebnissen von Schwachstellen-Scannern.
Red Hat arbeitet mit zertifizierten Sicherheitspartnern zusammen, um genauere und zuverlässigere Ergebnisse von Container-Schwachstellen-Scans für von Red Hat veröffentlichte Images und Pakete zu liefern.

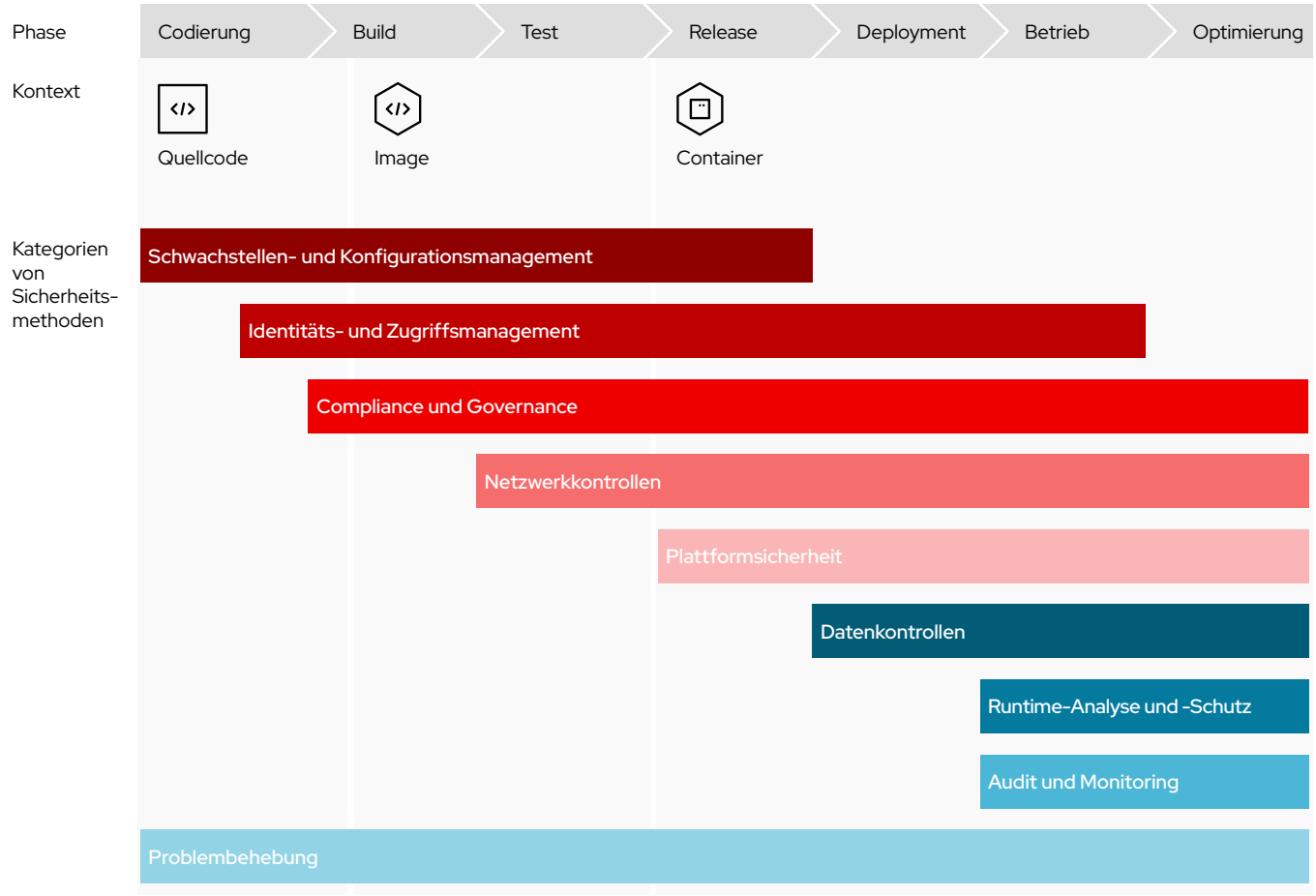
- Weniger falsch positive Ergebnisse und andere Unstimmigkeiten
- Mehr Zeit und Geld für strategische Projekte und Initiativen
- Höheres Sicherheitsniveau
- Verbesserte Genauigkeit durch zentralisierte Daten für von Red Hat veröffentlichte Images
- Vereinfachtes Schwachstellenmanagement

Zertifizierte Produkte anzeigen

Erstellung von DevSecOps-Komplettlösungen

Red Hat bietet ein Framework für die Entwicklung von hoch skalierbaren, umfassenden DevSecOps-Lösungen, die die Sicherheitsanforderungen während des gesamten Anwendungs-Lifecycles berücksichtigen. Das Framework wurde in Zusammenarbeit mit unseren Sicherheitspartnern entwickelt und kann Sie bei der Implementierung von DevSecOps in Ihrem Unternehmen entsprechend Ihren aktuellen und erwarteten Anforderungen unterstützen.

Das DevSecOps-Framework von Red Hat umfasst ein komplettes Set von Sicherheitstools und -methoden, die nach Funktionen kategorisiert sind und sich auf den Lifecycle der Anwendungsentwicklung beziehen.



Überblick lesen

Wahl der Sicherheitsmethoden und -produkte entsprechend Ihren Anforderungen

Das DevSecOps-Framework von Red Hat umfasst 34 primäre Sicherheitsmethoden, die in 9 Kategorien unterteilt sind. Die Technologien von Red Hat und zertifizierten Partnern sind auf eine oder mehrere dieser Methoden abgestimmt und unterstützen Sie beim Erstellen einer DevSecOps-Komplettlösung, die den Anforderungen Ihres Unternehmens entspricht und sich an zukünftige Veränderungen anpassen lässt.

Schwachstellen- und Konfigurationsmanagement

- Sicherheitstests für statische Anwendungen (Static Application Security Testing, SAST)
- Statische Codeanalysen (Static Code Analysis, SCA)
- Sicherheitstests für interaktive Anwendungen (Interactive Application Security Testing, IAST)
- Sicherheitstests für dynamische Anwendungen (Dynamic Application Security Testing, DAST)
- Konfigurationsmanagement
- Image-Risiko

Identitäts- und Zugriffsmanagement

- Authentifizierung
- Autorisierung
- Secrets Vault
- Hardware-Sicherheitsmodule (HSM)
- Datenherkunft

Compliance und Governance

- Regulatory Compliance Auditing
- Compliance-Kontrollen und Problembehebung

Netzwerkkontrollen

- CNI-Plugins (Container Network Interface)
- Netzwerkrichtlinien
- Kontrolle des Datenverkehrs
- Service Mesh
- Visualisierung
- Paketanalyse
- API-Management

Plattformsicherheit

- Sicherer Host
- Container-Plattform
- Namespace
- Isolation
- Kubernetes- und Container-Härtung

Datenkontrollen

- Datenschutz und -verschlüsselung

Runtime-Analyse und -Schutz

- Admission Controller
- Analyse von Anwendungsverhalten
- Bedrohungsabwehr

Audit und Monitoring

- Cluster-Überwachung
- Security Information and Event Management (SIEM)
- Forensik

Problembehebung

- SOAR-Plattformen (Sicherheit, Orchestrierung, Automatisierung und Reaktion)
- Automatische Problemlösung

Zertifizierte Partner anzeigen

Partner-Highlight

Sysdig

Sysdig unterstützt Unternehmen bei der sicheren Ausführung von Workloads in der Cloud mit sicherheitsorientierten DevOps-Technologien. Die Produkte von Sysdig für die Überwachung und die Sicherung von Anwendungen, Workloads und Containern helfen Hunderten von Unternehmen, cloudnative Anwendungen schneller bereitzustellen.

Red Hat und Sysdig unterstützen Unternehmen gemeinsam bei der schnellen Einführung cloudnativer Konzepte. **Sysdig Secure DevOps Platform**, **Sysdig Secure** und **Sysdig Monitor** stellen zusammen mit Red Hat OpenShift und **Red Hat Advanced Cluster Management for Kubernetes** einheitliche Sicherheits-, Compliance- und Monitoring-Funktionen für Private Cloud-, Hybrid Cloud- und Multi-Cloud-Umgebungen bereit. Mit diesen Lösungen können Sie Build-Pipelines sichern, Bedrohungen erkennen und darauf reagieren, kontinuierlich den Status und die Compliance der Cloud validieren und die Performance überwachen. Die cloudnativen Monitoring-, Sicherheits- und Forensik-Funktionen von Sysdig basieren auf einem Open Source-Stack und geben Ihnen die erforderlichen Insights und die Kontrolle, um mit weniger Risiko zur Cloud zu wechseln.

2020

„Red Hat Rising Star Partner of the Year" für den öffentlichen Sektor[2]

Mit den Lösungen von Red Hat und Sysdig können Sie:

- Images direkt in Ihren CI/CD-Pipelines (Continuous Integration/Continuous Deployment) scannen
- Performance und Verfügbarkeit auf Cloud-Ebene überwachen
- Kontinuierliche Compliance und Runtime-Sicherheit implementieren
- Infrastrukturkonfigurationen von Red Hat OpenShift validieren
- Probleme leichter beheben und darauf reagieren

Verwaltung von Sicherheitsrisiken

Identifizieren und beheben Sie Schwachstellen in Ihren Pipelines. Erkennen und blockieren Sie Bedrohungen zur Runtime mit automatisierten Richtlinien und Kontrollen. Reagieren Sie auf Zwischenfälle und untersuchen Sie diese, auch wenn die Container bereits stillgelegt sind.

Verbesserte Performance und Verfügbarkeit

Erfassen und speichern Sie Millionen von Metriken. Überwachen Sie den Zustand und die Performance Ihrer gesamten Umgebung, um Probleme proaktiv zu erkennen und zu beheben. Beheben Sie Probleme in Clustern, Pods und Containern auf unkomplizierte Weise.

Validierte Cloud Compliance

Validieren Sie die Compliance der Red Hat OpenShift Umgebung mit herkömmlichen Standards. Überprüfen Sie Cluster, Knoten und Container anhand detaillierter Aktivitätsberichte. Implementieren Sie das Monitoring der Dateiintegrität über den gesamten Container Lifecycle.

Zu den Integrationen

2 Red Hat Blog: „**Red Hat awards North American partners for commitment to open source innovation**", 23. April 2020.

Partner-Highlight

Synopsys

Synopsys bietet Lösungen für statische, dynamische und Software-Kompositionsanalysen für die schnelle Entwicklung sicherer Software. Mit einer Kombination aus branchenführenden Tools, Services und Know-how unterstützt Synopsys Unternehmen bei der Anwendung von DevSecOps, um die Sicherheit und Qualität im gesamten Lifecycle der Softwareentwicklung zu optimieren.

Mit Red Hat und Synopsys können Sie hochwertigen, sicherheitsorientierten Code erstellen, um Risiken zu minimieren und gleichzeitig sowohl Geschwindigkeit als auch Produktivität zu maximieren. Mit **Synopsys Black Duck Software Composition Analysis (SCA)** lassen sich Software-Kompositionsanalysen in Red Hat OpenShift integrieren, um die Transparenz und die Kontrolle über Sicherheitsschwachstellen und Richtlinienverstöße im Open Source-Code innerhalb Ihrer Container zu erhöhen.**Black Duck for OpenShift** erkennt, scannt, überwacht und untersucht automatisch die Container Images in Ihren Red Hat OpenShift Clustern, um Open Source-Sicherheits- und Compliance-Risiken in den verschiedenen Phasen der Container-Erstellung zu identifizieren. Mit der Software können Sie außerdem sicherstellen, dass Container mit Schwachstellen nicht in die Produktion gelangen, und schnell auf neue Sicherheitslücken reagieren, die ausgeführte Container betreffen.

Die Lösung Black Duck for OpenShift bietet folgende Vorteile:

- Sie bietet eine vollständige Liste der verschiedenen Open Source-Codes von Drittanbietern in den einzelnen Container Images und versieht Ihre Pods mit Metadaten zu Schwachstellen und Richtlinien.
- Sie werden sofort über neue Schwachstellen Ihrer Container benachrichtigt und erhalten Informationen darüber, welche Images und Container betroffen sind.
- Sie erkennt Open Source Forks und -Rückportierungen und markiert Schwachstellen gegebenenfalls als gepatcht, wodurch die Anzahl der zu untersuchenden Schwachstellen reduziert wird.
- Sie lässt sich mit Red Hat Advanced Cluster Management for Kubernetes **Integrieren**, um für ein konsistentes Deployment in den Clustern zu sorgen.

Automatisches Scannen von Container Images

Kontinuierliches Überwachen von Open Source-Code

Identifizieren von Sicherheitsschwachstellen

„Synopsys und Red Hat haben eine ähnliche Vision für die Zukunft der sicheren Anwendungsentwicklung und -bereitstellung. Zusammen möchten wir Unternehmen dabei unterstützen, Vertrauen in ihre containerisierten Anwendungen aufzubauen."

Vatsal Sonecha
VP of Business Development, Synopsys

Zu den Integrationen

Partner-Highlight

Palo Alto Networks

Palo Alto Networks liefert Innovationen, um die sichere digitale Transformation zu unterstützen – und das trotz des beschleunigten Wandels. Das Unternehmen bietet ein Portfolio von Sicherheitslösungen an, die weltweit mehr als 60.000 Kunden beim Schutz ihrer Unternehmen unterstützen.

Red Hat und Palo Alto Networks helfen Ihnen mit cloudnativen Sicherheits- und Compliance-Funktionen, Ihre Umgebung während des gesamten Lifecycles der Entwicklung zu schützen. Prisma Cloud by Palo Alto Networks bietet in Kombination mit Red Hat OpenShift ein umfassendes System mit Cloud Security Posture Management (CSPM) und Cloud Workload Protection (CWP) für Ihre Deployments. Diese Lösung bietet vollständige Lifecycle-Sicherheit für Hosts, Container und Serverless sowie Transparenz und Governance für Ihren Sicherheitsstatus.

Red Hat Partner seit

2017

Wichtige Funktionen und Vorteile

Schwachstellenmanagement

Integrieren Sie Sicherheit von der Entwicklung bis zur Produktion durch Erkennung, Verständnis und Vermeidung von Schwachstellen in den verschiedenen Phasen des Anwendungs-Lifecycles.

Compliance

Implementieren Sie mühelos die Compliance für CIS-Benchmarks (Center for Internet Security), externe Compliance-Systeme und benutzerdefinierte Anforderungen und halten Sie sie aufrecht.

CI/CD-Sicherheit

Integrieren Sie Sicherheitsfunktionen direkt in Ihre CI-Prozesse (Continuous Integration), um Probleme zu finden und zu beheben, bevor sie in der Produktion bereitgestellt werden.

Runtime-Verteidigung

Wenden Sie Sicherheit in großem Umfang mit maschinellem Lernen an, das automatisch zulassungslistenbasierte Runtime-Modelle nach dem Least Privilege-Prinzip für die verschiedenen Anwendungsversionen erstellt.

Sicherheit für Webanwendungen und Weboberflächen

Schützen Sie Ihre Public Cloud- und Private Cloud-Umgebungen vor Layer 7- und OWASP Top 10-Bedrohungen (Open Web Application Security Project).

Zugriffskontrollen

Erstellen und überwachen Sie Zugriffskontrollen für Workloads und Anwendungen, und integrieren Sie sie in vorhandene Managementtools für Identität, Zugriff und Secrets.

Zu den Integrationen

Partner-Highlight

CyberArk

CyberArk verfolgt einen speziellen sicherheitsorientierten Ansatz für identitätsbasierte privilegierte Zugriffskontrollen. Das Unternehmen bietet Komplettlösungen zum Schutz von Secrets und Zugangsdaten, die von Nutzenden, Anwendungen, Skripts und Maschinen in Unternehmen, Clouds und DevOps-Umgebungen verwendet werden.

Gemeinsam können Red Hat und CyberArk Sie bei der Verbesserung der Sicherheit Ihrer Container-Umgebungen und Automatisierungsskripts unterstützen. Unternehmensweite Sicherheitsrichtlinien für privilegierten Zugriff ermöglichen Transparenz-, Auditing-, Enforcement- und Secrets-Management und tragen so zur Minderung von Geschäftsrisiken bei. DevSecOps-Produkte von CyberArk – darunter **Conjur Secrets Manager** und **Credential Providers** – lassen sich in Red Hat OpenShift und Red Hat Ansible Automation Platform einbinden, um privilegierte Zugangsdaten für Nutzende, Anwendungen, Skripts und andere nicht menschliche Identitäten über eine zentralisierte Plattform zu schützen, zu rotieren, zu überwachen und zu managen. Mit einem einzigen Kontrollpunkt in Ihrem Unternehmen können Sie das Sicherheitsmanagement vereinheitlichen, Sicherheitsschwachstellen reduzieren, Angriffsflächen minimieren und die Abläufe optimieren.

Dank der modularen Architektur können Sie die Komponenten unabhängig voneinander einsetzen, um den Schutz für Hybrid Cloud-, Multi-Cloud-, containerisierte und DevOps-Umgebungen anzupassen. Eine starke Runtime-Authentifizierung und Role-based Access Control sorgen dafür, dass nur autorisierte Pods und Container Secrets erhalten. Durch die Integration mit Red Hat Ansible Automation Platform können Playbooks auf gemanagte Secrets zugreifen. So müssen Secrets nicht manuell eingegeben und rotiert werden. Mit dieser Integration können Sie auch Aufgaben zur Problembehebung als Reaktion auf erkannte Sicherheitsvorfälle automatisieren.

Einheitliche Sicherheit

Verwalten und sichern Sie Secrets und privilegierte Zugangsdaten in Ihrer gesamten Infrastruktur zentral und gemäß Ihrer Richtlinien.

Vereinfachte Abläufe

Ermöglichen Sie Entwicklungsteams und Automation Engineers das Sichern, Verwalten und Rotieren der verwendeten Secrets und Zugangsdaten gemäß Ihrer Richtlinien.

Verbesserte Konsistenz

Schützen Sie konsistent die Secrets und Zugangsdaten, die von Anwendungen, Skripts und Nutzenden verwendet werden, um auf Ihre Managementkonsolen zuzugreifen.

Webcast ansehen

Partner-Highlight

Tigera

Tigera revolutioniert die Sicherung, Überwachung und Fehlerbehebung von Kubernetes-Netzwerken und Microservice-Kommunikation in Unternehmen.

Red Hat und Tigera unterstützen Unternehmen bei der Integration von Sicherheit in ihre Kubernetes-Umgebungen durch Überwachen, Analysieren und Verwalten des Netzwerkverkehrs. **Tigera Calico Enterprise** ist für Red Hat OpenShift zertifiziert und unterstützt Sie beim erfolgreichen Ausführen, Optimieren und Schützen kritischer containerisierter Anwendungen in Cloud-Umgebungen. Dank der Kubernetes-nativen Architektur lässt sich die Lösung in Ihre Anwendungsumgebung einbinden, um detaillierte Sicherheitskontrollen und eine verbesserte Transparenz zwischen der Netzwerk- und der Microservice-Schicht bereitzustellen. Sie können diese Lösung auch in Ihre bestehenden Sicherheitstools, Umgebungen und SoCs (Security Operations Centers) integrieren, um zusätzliche Kontrollen und Funktionen für moderne Workloads zu liefern. Verbessern Sie die Anwendungssicherheit in Entwicklungs-, Test- und Produktivumgebungen mit Zero-Trust-Netzwerken, Egress-Zugriffskontrollen, Datenverkehrstransparenz, Bedrohungsschutz und -abwehr sowie automatischen Compliance-Auditberichten.

Erweiterte Sicherheitsfunktionen

Schützen Sie Anwendungen über vorhandene Firewalls, Sicherheit nach dem Least Privilege-Prinzip und Verschlüsselung des Datenverkehrs zwischen Pods.

Mehr Netzwerktransparenz

Greifen Sie auf Netzwerkflüsse zu, um die Konnektivität zu debuggen, Bedrohungen zu finden und Compliance-Berichte zu automatisieren.

Compliance

Überwachen Sie die Compliance von Anwendungen, und liefern Sie Warnmeldungen in Echtzeit für nicht konforme Workloads.

Zum Operator

Partner-Highlight

Aqua Security

Aqua Security unterstützt Kunden bei der Innovation und der reibungslosen Ausführung ihrer Geschäftsabläufe. Das Unternehmen bietet Automatisierung zur Vermeidung, Erkennung und Reaktion auf Bedrohungen im gesamten Lifecycle von Anwendungen, um die Sicherheit in den verschiedenen Aspekten Ihrer Umgebung zu verbessern.

Red Hat und Aqua Security unterstützen Sie beim sicheren Verwalten und Skalieren Ihrer cloudnativen Workloads in der Onsite-, Hybrid- und Cloud-Infrastruktur. **Aqua Cloud Native Security Platform** lässt sich in Red Hat OpenShift einbinden und ermöglicht risikobasiertes Schwachstellenmanagement, detaillierten Runtime-Schutz und umfassende Infrastruktursicherung und -Compliance. Mit der Lösung können Entwicklungs-, Sicherheits- und Operations-Teams Anwendungen sicher bereitstellen, zur Runtime vor Bedrohungen schützen sowie Infrastrukturkonfigurationen basierend auf Richtlinienprüfungen bewerten und eventuelle Fehler beheben.

Wichtige Funktionen und Vorteile

Unterstützung von DevSecOps-Ansätzen

- Analysieren Sie Code, Konfigurationen und Berechtigungen für Red Hat OpenShift Registry Images in großem Umfang.
- Priorisieren Sie die Schwachstellen nach Risiko.
- Automatisieren Sie Build-Prozesse durch Integration in CI/CD-Pipelines.

Anwendungsschutz zur Runtime

- Erkennen und minimieren Sie automatisch nicht autorisierte Container-Aktivitäten, ohne Anwendungen zu unterbrechen.
- Erzwingen Sie die Unveränderbarkeit von Containern, indem Sie nicht autorisierte Änderungen von Standard-Images identifizieren und verhindern.

Mehr Sicherheit in der Softwarelieferkette

- Führen Sie Images in geschützten Vorproduktiv-Testumgebungen aus, und validieren Sie sie.
- Identifizieren Sie komplexe Malware, die von statischen Scannern vor dem Deployment nicht erkannt werden kann.

Infrastruktur-Compliance

- Scannen und überprüfen Sie Hunderte von Konfigurations- und Kontrollrichtlinien auf Compliance mit Best Practices und CIS-Benchmarks (Center for Internet Security).
- Setzen Sie Role-based Access Controls (RBAC) über OPA-basierte (Open Policy Agent) deklarative Sicherheitsrichtlinien durch.

Zu den Integrationen

Bereit für den Einstieg in DevSecOps?

Anwendungssicherheit ist eine Voraussetzung für digitale Unternehmen. Mit der Einführung von DevSecOps-Ansätzen können Sie Ihre Anwendungsumgebung und Ihr Unternehmen besser schützen.

Red Hat kombiniert eine innovative technologische Basis mit einem umfassenden DevSecOps-IT-Ökosystem und umfangreichem Fachwissen, um Sie bei der erfolgreichen Implementierung von DevSecOps in Ihrem Unternehmen zu unterstützen.

- Wählen Sie aus einer Vielzahl von zertifizierten, branchenführenden Tools und Technologien, um Ihre Anforderungen jetzt und in Zukunft zu erfüllen.
- Lernen Sie Best Practices kennen, und erwerben Sie DevSecOps-Kompetenzen mit Trainingsressourcen von Fachleuten.
- Nutzen Sie die Vorteile eines schnellen Deployments mit spezialisierten Services und Consulting.

Weitere Informationen zur Implementierung von DevSecOps mit Red Hat:

redhat.com/de/partners/devsecops

F29623_0721_KVM

Red Hat