Automatisierung für Sicherheit und Compliance

Einhaltung, Aktualisierung und Verifizierung von Compliance für Rüstungskonzerne

Lösungen von Red Hat für die Automatisierung von Sicherheit und Compliance:

- Red Hat Enterprise Linux
- Red Hat Ansible Automation Platform
- Red Hat Insights
- Red Hat Smart Management
- Red Hat OpenShift
- Red Hat Advanced Cluster Management for Kubernetes
- Red Hat Quay

Sicherheitsherausforderungen für Rüstungskonzerne

Auftragnehmer des Verteidigungsministeriums sehen sich dringenden Herausforderungen ausgesetzt, denn sie müssen unter anderem:

- **Den Zustand ihrer Cybersicherheit verbessern**. Organisationen müssen ein besseres Verständnis ihrer allgemeinen Risikoprofile gewinnen, um mit den sich rasant entwickelnden Bedrohungen Schritt halten zu können.
- **Die Implementierung von Cybersicherheits-Kontrollen und -Prozessen verifizieren**. Diese Standards sind notwendig, um durchgehend Konfigurationsdrift entdecken und beheben zu können sowie menschliche Fehler zu reduzieren.
- **Ausgaben reduzieren und gleichzeitig Funktionen hinzufügen**. Es ist eine Herausforderung, Compliance stets einzuhalten, zu aktualisieren und zu verifizieren, ohne dafür hohe Ausgaben zu tätigen.
- **Einen ganzheitlichen Sicherheitsansatz einführen**. Organisationen müssen sich vom linearen Wasserfall-Projektmanagement und manuellen Sicherheitsüberprüfungen hin zu agilen DevSecOps sowie automatisierter Diagnostik und Fehlerbehebung wandeln.

Mit technischen Anforderungen Compliance verifizieren und Informationen schützen

Der Schutz sensibler Informationen ist weiterhin die wichtigste Priorität für das Verteidigungsministerium und den öffentlichen Sektor. Neue Cybersicherheitsmodelle meistern diese Herausforderung, indem sie:

- **Cybersicherheitsrisiken messen**. Manche Daten sind sensibler als andere und erfordern schärfere Sicherheitskontrollen.
- **Einen ganzheitlichen Sicherheitsansatz verfolgen**. Netzwerksicherheit reicht nicht aus, um das wachsende Perimeter vor Angreifern zu schützen. Standardisierte Prozesse und sicherheitsorientierte Verhaltensweise sind für den Schutz von Informationen unerlässlich.
- **Durchgehende Compliance mithilfe von Drittanbieter-Bewertungen verifizieren**. Organisationen können Unternehmen in ihrer Lieferkette dazu verpflichten, ihre Compliance durch eine unabhängige Drittanbieter-Verifizierung nachzuweisen.

Warum Red Hat?

- **Verbesserte Sicherheit**. Unsere Lösungen erfüllen strenge Anforderungen für Bundessicherheit.
- **Niedrigere Kosten**. Unsere Subskriptionen sind oft günstiger als proprietäre Softwarelizenzen und Support-Regierungsverträge.
- **Partnernetzwerk**. Red Hat verfügt über ein Partnernetzwerk mit Tausenden von Produkten und Services, die für die Nutzung mit Technologien von Red Hat® getestet, unterstützt und zertifiziert wurden.
- **Führend in Open Source**. Wir sind ein führender Befürworter und Entwickler von Open Source-Software und arbeiten eng mit der Open Source Community zusammen, um Lösungen bereitzustellen, die Ihrer Organisation zum Erfolg verhelfen.
- **Erfahrung.** Wir haben umfangreiche Expertise in der Arbeit mit Behörden in den Vereinigten Staaten, für die wir Prozesse in der Anwendungsentwicklung modernisiert haben.

Eine effektive Strategie für automatisierte Sicherheit und Compliance

Die Technologien von Red Hat bieten Sichtbarkeit und Kontrolle und helfen Ihnen dabei, die Kosten für Compliance zu senken.[1] Red Hat bietet bewährte, zertifizierte, zuverlässige und unterstützte Open Source-Software für Unternehmen und arbeitet mit Cloud-, Netzwerk- und Storage-Anbietern in einem Partnernetzwerk zusammen, um Integrationen zu vereinfachen. Das Portfolio von Red Hat enthält Tools, mit denen Sie die technischen Sicherheitsanforderungen erfüllen und Compliance einhalten können, sowie Produkte auf Open Source-Basis mit einem bekannten Lifecycle.

Die wandelnde Dynamik in der Cybersicherheit erfordert einen ganzheitlichen Sicherheitsansatz, bei dem Automatisierung den Kern der Sicherheits- und Compliance-Strategie bildet.

Mit den Technologien von Red Hat können Sie dabei unterstützen, stets die aktuellen Sicherheitsanforderungen einzuhalten.

Software für die Infrastruktur

Red Hat Enterprise Linux® bietet ein sicherheitsorientiertes Betriebssystem mit integrierten Tools zum Schutz Ihrer Umgebung, inklusive SCAP (Security Content Automation Protocol). Seit 2008 ist Red Hat führend in der Open Source Community, die Tools für SCAP definiert und erstellt.[2] Bei SCAP handelt es sich um eine Sicherheits-Härtungslösung für die Betriebsumgebung, die vom NIST (National Institute of Standards and Technology) zertifiziert wurde. SCAP enthält **vorgefertigte** Sicherheitsprofile, die Ihnen die Einhaltung von Branchenstandards wie etwa PCI DSS, DISA STIG, und HIPAA,[3] erleichtern und ermöglicht auch die Erstellung benutzerdefinierter Profile.

Red Hat Enterprise Linux ist eine stabile, zuverlässige Basis für die Automatisierung und enthält SELinux (Security-Enhanced Linux), das Zugangskontrollen für die Systemnutzer, Anwendungen, Prozesse und Dateien definiert.

Konfiguration von Netzwerken und unterschiedlichen Sicherheits- und Netzwerk-Tools kann in einer gemeinsamen Sprache ausgeführt werden.

Automatisierung und Management

Red Hat Ansible® Automation Platform bietet eine einfache, flexible, agentenlose Automatisierungssprache für Ihre Umgebung, die von Systemen und Anwendungen bis hin zu Tools und Prozessen reicht. Sie können kontrollieren, wer Änderungen an der Konfiguration vornehmen darf und einsehen, wann diese Änderungen von wem durchgeführt wurden. Mit Ansible Automation Platform müssen Sie Ihre vorhandenen Sicherheitstools nicht ersetzen, sondern können sie zusammenführen. Ansible Automation Platform ermöglicht die Integration und Interoperabilität von Sicherheitstechnologien in Ihrer Hybrid Multicloud-Umgebung.

Red Hat Insights untersucht proaktiv die Umgebungen in Red Hat Enterprise Linux, um Risiken für die Abläufe und Sicherheit festzustellen. Es bietet außerdem Anweisungen dafür, wie Sie diese Risiken schnell beheben, bevor sie zu größeren Problemen werden können.

Red Hat Smart Management kombiniert die Vorteile von Red Hat Insights und Red Hat Satellite und bietet ein vollständiges Lifecycle-Management mit einer GUI (Graphic User Interface), mit der Sie Ihre von Red Hat Enterprise Linux unterstützten Umgebungen von physischen Maschinen bis hin zu hybriden Multiclouds sicherer verwalten können.

Container-Plattformen

Mit Red Hat OpenShift® und Red Hat Advanced Cluster Management for Kubernetes können Sie eine weltweit verteilte Anwendungsplattform mit einem standardisierten Workflow für Deployment, Upgrade, Patching und Sicherheitsüberprüfungen verwalten.

Red Hat® Quay Container Image Registry bietet Storage, mit der Sie kryptografisch signierte Container erstellen, verteilen und bereitstellen können. Erhalten Sie mehr Sicherheit für Ihre Image Repositories – mit Systemen zur Automatisierung, Authentifizierung und Autorisierung.

[1] Red Hat Überblick. „Compliance verbessern und automatisieren – mit Red Hat und OpenSCAP," Oktober 2019.

[2] Red Hat Blog. „Red Hat OpenSCAP ist im Verifizierungsprozess für SCAP 1.2 NIST Standard," 13. März 2013.

[3] PCI DSS (Payment Card Industry Data Security Standard), DISA (Defense Information Systems Agency) STIG (Security Technical Implementation Guides), HIPAA (Health Insurance Portability and Accountability Act).

Services und Support

Wir bieten außerdem Training, Support und Consulting-Services für unsere streng regulierten und sicherheitsbewussten Kunden an. Mit diesen Services können Sie Ihre Technologien optimal nutzen.

Mehr erfahren

Automatisierung, Containerisierung, Infrastruktur-Lifecycle-Management und proaktive Untersuchungen der Betriebsumgebung unterstützen Auftragnehmer des Verteidigungsministeriums dabei, den stetig wandelnden Herausforderungen der Compliance gerecht zu werden.

Besuchen Sie redhat.com/gov, um zu erfahren, wie Sie mit Red Hat die Sicherheit und Stabilität Ihrer Systeme schützen können.

Weitere Ressourcen:

Red Hat ATO Pathways

Offizielle Red Hat Ansible Rollen für Compliance as Code

Red Hat Knowledgebase für Common Criteria, FIPS 140-2, STIG, USGCB, USGV6 (DoD IPv6), Section 508 und mehr

Red Hat Sicherheitsdaten inklusive OVAL-Definitionen (Open Vulnerability and Assessment Language)

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

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

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

Über Red Hat

Red Hat, weltweit führender Anbieter von Open-Source-Software-Lösungen für Unternehmen, folgt einem community-basierten Ansatz, um zuverlässige und leistungsstarke Linux-, Hybrid Cloud-, Container- und Kubernetes-Technologien bereitzustellen. Red Hat unterstützt Kunden bei der Integration neuer und bestehender IT-Anwendungen, der Entwicklung cloudnativer Applikationen, der Standardisierung auf unserem branchenführenden Betriebssystem sowie der Automatisierung, Sicherung und Verwaltung komplexer Umgebungen. Dank der vielfach ausgezeichneten Support-, Trainings- und Consulting-Services ist Red Hat ein bewährter Partner der Fortune 500-Unternehmen. Als strategischer Partner von Cloud-Providern, Systemintegratoren, Applikationsanbietern, Kunden und Open Source Communities unterstützt Red Hat Unternehmen auf ihrem Weg in die digitale Zukunft.

O-F26829