Red Hat

Verbesserte Sicherheit durch Automatisierung

Eine Red Hat
Customer Success Serie

Einleitung 03

Success Stories 05-13

1

Emory University mindert sudo-Bedrohung mit Red Hat Ansible Automation Platform

05

2

Die Schwarz Gruppe automatisiert die IT mit Red Hat Ansible Automation Platform

07

3

Agile Defense verbessert Sicherheitscompliance mit Red Hat Ansible Automation Platform

09

4

Cepsa steigert die Effizienz mit Red Hat Ansible Automation Platform

12

5

Siemens verbessert Kommunikationssicherheit mit Red Hat Ansible Automation Platform

14

Fazit 16

Einlei-tung

Automatisierung verändert Sicherheit

Viele Unternehmen stehen vor der Herausforderung, IT-Sicherheitsteams und -lösungen in eine schnelllebige Umgebung integrieren zu müssen. Und obwohl die Sicherheitsansätze unterschiedlich sind, gibt es Strategien, die gelernt und angepasst werden können, um Ihre wertvollen Daten, Anwendungen, IT-Systeme, Netzwerke und Geräte vor schädlichen oder unbeabsichtigten Aktivitäten zu schützen.

Um diese Strategien bekannter zu machen, stellt dieses E-Book 5 Success Stories von Kunden von Red Hat® Ansible® Automation Platform vor, die ihre Sicherheitslösungen mithilfe von Automatisierung so integrieren und skalieren, dass diese auf eine koordinierte und einheitliche Art und Weise auf Bedrohungen in ihrer Organisation reagieren können.

Wie verbessert Automatisierung die Sicherheit?

Die meisten Unternehmen haben ein Sicherheitsteam, das weiß, was zu tun ist. Aber die manuelle Konfiguration von oftmals Tausenden von Systemen und Anwendungen, mit dem Ziel, diese vor Angreifern zu schützen, erfordert viel Zeit und qualifizierte Ressourcen.

Automatisierung kann diese Kompetenz- und Ressourcenlücke schließen, indem es and interne und externe Sicherheitsrichtlinien angepasste Sicherheitsstandards anwendet und durchsetzt. Das Ergebnis ist eine drastisch reduzierte Reaktionszeit und weniger Schwachstellen.

> ***Organisationen mit vollständig bereitgestellter Sicherheits-KI und -Automatisierung konnten eine Sicherheitsverletzung sehr viel schneller entdecken und beseitigen als Organisationen, die keine Sicherheits-KI und -Automatisierung bereitgestellt hatten.***
>
> IBM. „Cost of a Data Breach Report 2022“, Juli 2022.

Mit Ansible Automation Platform können Teams Sicherheitslösungen automatisieren und integrieren, die Bedrohungen im gesamten Unternehmen auf koordinierte und einheitliche Art und Weise untersuchen und auf diese reagieren. Dabei werden sie durch eine kuratierte Sammlung von Modulen, Rollen und Playbooks unterstützt.

Was gehört zu einem einheitlichen Sicherheitsansatz?

Sicherheitslösungen unterliegen ständigem Wandel, um Bedrohungen immer einen Schritt voraus zu sein. Die wichtigsten Aspekte sind:

Datenangereicherte Untersuchung

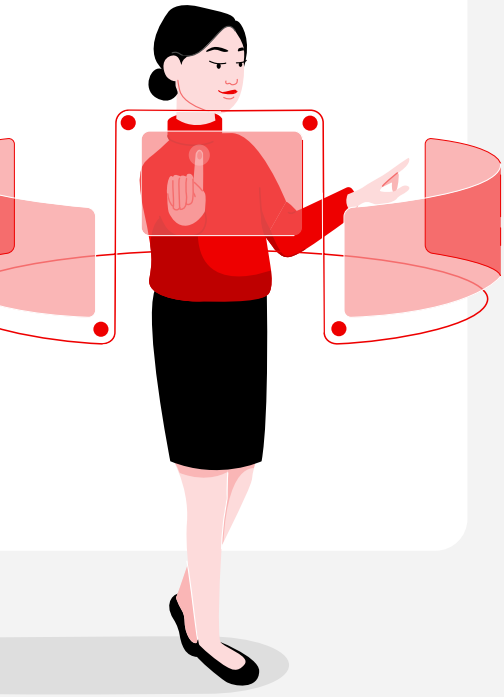
Das Sammeln von Logs in Firewalls, IDS (Intrusion Detection Systems) und anderen Sicherheitssystemen ermöglicht programmatisch die On-Demand-Anreicherung von Daten durch Kategorisierungsprozesse, die von SIEMs (Security Information and Event Management Systems) durchgeführt werden.

Bedrohungssuche

Passen Sie das Level der Protokollierung automatisch an und erstellen Sie neue IDS-Regeln und Firewall-Richtlinien, um in kürzerer Zeit mehr Bedrohungen aufdecken zu können.

Reaktion auf Sicherheitsvorfälle

Sorgen Sie für eine schnellere Automatisierung, indem Sie bedrohliche IP-Adressen oder Domains einer Sperrliste und nicht-bedrohlichen Verkehr einer Zulassungsliste hinzufügen oder verdächtige Workloads für weitere Untersuchungen isolieren.



Warum Ansible für Sicherheitsautomatisierung?

Die Verantwortung für Sicherheit ruht auf vielen Schultern. Ansible ist ein leistungsfähiges, agentenloses Tool, das Automatisierung in einer von Menschen lesbaren Sprache präsentiert. Dadurch wird Automatisierung für Teams im gesamten Unternehmen zugänglich, etwa in den Abteilungen IT-Operations und -Development, Network Engineering und Sicherheit. Unternehmen können dadurch mit Automatisierung mehr erreichen, darunter:

- Erhöhte Produktivität. Ansible verwendet eine einfache, von Menschen lesbare Sprache, weshalb keine speziellen Management- oder Programmierfähigkeiten benötigt werden, um Aufgaben in der korrekten Reihenfolge auszuführen.
- Verwaltung der gesamten IT-Infrastruktur. Nutzen Sie die Funktionen, um Informationen zu sammeln und zu untersuchen sowie bei Konfigurationsmanagement und Workflow-Orchestrierung auf dem neuesten Stand zu bleiben.
- Verbesserte Effizienz und Sicherheit. Mit einer agentenlosen Architektur stellen Sie Lösungen schneller bereit und verzichten auf Agenten, die aktualisiert werden müssen oder als Schwachstelle ausgenutzt werden könnten.

Die folgenden Success Stories zeigen die Leistung und Skalierbarkeit von Sicherheitsautomatisierung und wie Organisationen mit einer einheitlichen Automatisierungsplattform wie Ansible Automation Platform ihre Sicherheitslage verbessern können.

1

EMORY UNIVERSITY

Emory University mindert sudo-Bedrohung mit Red Hat Ansible Automation Platform

> *Niemand hätte geglaubt, dass wir Linux-Server alle 30 Tage patchen können, aber mit Red Hat Ansible Automation Platform ist es möglich und nötig.*
>
> Steve Siegelman, Manager of Systems Engineering, Office of Information Technology, Emory University

Die Emory University in Atlanta, Georgia, hat mehr als 15.000 Studierende. Da sie Forschungsbeziehungen mit Institutionen auf der ganzen Welt unterhält und das größte Gesundheitssystem von Georgia betreibt, ist es nicht verwunderlich, dass die Institution ein Ziel für Cyberangreifer ist, die über ihren digitalen Footprint Zugriff auf vertrauliche Information erhalten wollen.

Sind sie erst einmal durch eine Schwachstelle in das Netzwerk eingedrungen, können sich Angreifer dort heimlich bewegen, geistiges Eigentum stehlen und dann unentdeckt verschwinden. Das OIT (Office of Information Technology) der Universität hat die Aufgabe, die Systeme für Studierende, Angestellte, Fakultät, Forschende und andere Stakeholder zu verwalten und sicherzustellen, dass Netzwerke und Daten vor unautorisierten Zugriffen und möglichen Datenpannen geschützt sind. Deshalb gab es einen großen Alarm im Januar 2021, als das Team von Red Hat das OIT der Universität über eine Systemschwachstelle innerhalb von Red Hat Enterprise Linux® informierte, die den sudo-Dienst des Betriebssystems betraf.

Ansible Automation beschleunigt das Beheben von Sicherheitsrisiken

Updates in Stunden, statt Wochen, gepatcht

Bei der Emory University verwenden mehr als 500 Server Red Hat Enterprise Linux. Das OIT war sich daher bewusst, dass eine manuelle Patch-Installation schwierig und langwierig sein und die Infrastruktur der Universität Bedrohungen aussetzen würde. Die Lösung: Mit einem Ansible Playbook ließen sich die Patches automatisch auf die einzelnen Server anwenden. Was normalerweise für die Gesamtheit der Server bis zu 2 Wochen gedauert hätte, hat dadurch insgesamt nur 4 Stunden gedauert.

Wertvolle Ressourcen freigesetzt: mehr Zeit für wichtige Projekte

Ansible Automation Platform wurde zuerst für die Finanzsysteme von Emory verwendet, bevor die Nutzung auf die Studierenden- und HR-Systeme ausgeweitet wurde. „Wie viele andere Organisationen auch, müssen wir trotz gleichbleibender Personalanzahl mehr erreichen. Dadurch, dass Ansible Automation Platform uns repetitive Aufgaben abgenommen hat, kann sich das Personal nun um wichtigere Projekte kümmern," sagt Steve Siegelman.

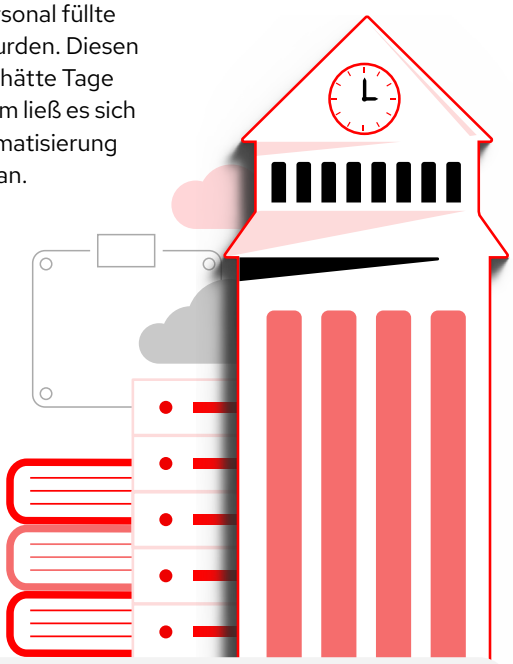
IT-Team hat mehr Zeit für die Anpassung an COVID-19-Herausforderungen

Ein weiteres Beispiel für die Flexibilität von Ansible Automation Platform zeigte sich im März 2020, als Emory, ebenso wie die große Mehrheit der Schulen und Organisationen, schließen und seine Studierenden und Angestellten zum Arbeiten ins Homeoffice schicken musste.

Das OIT musste schnell Datenbankserver bereitstellen, um die Campus-Berechtigungen von wichtigen Angestellten protokollieren zu können. Das ausgewählte Personal füllte Fragebögen aus, die ins System eingespeist wurden. Diesen Prozess manuell auf den Servern einzurichten, hätte Tage gedauert, aber mit Ansible Automation Platform ließ es sich in Minuten erledigen. „Es zeigte uns, was Automatisierung im Backend erreichen kann," so Steve Siegelman.

Sicherheitsinnovation über den Campus hinaus durch Automatisierung

Automatisierung ist für die Zukunftspläne von Emory äußerst wichtig, insbesondere, da eine Migration zur Cloud ansteht. „Wir haben Altsysteme mit einer Mischung aus alten und neuen Builds und investieren viel Aufwand in unsere AWS-Plattform," erklärt Siegelman. „Ansible Automation Platform ermöglicht es uns, mit diesen verschiedenen Systemen standardisierte Prozesse zu haben, die sich wiederholen. Alles ist an Ort und Stelle, unabhängig davon, ob die Plattform in der Cloud oder On-Premise ist."



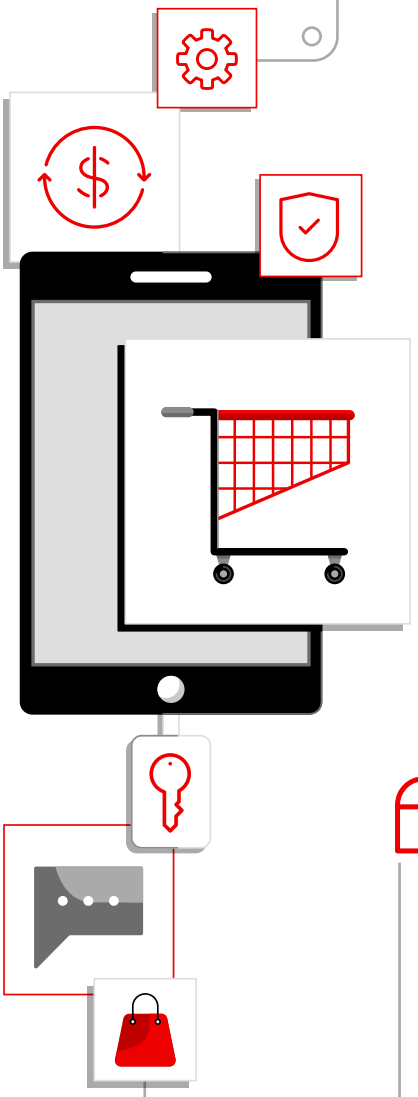
Jetzt die Success Story der Emory University herunterladen

2

Die Schwarz Gruppe automatisiert die IT mit Red Hat Ansible Automation Platform

Die Schwarz Gruppe ist der viertgrößte Einzelhändler der Welt. Die deutsche Einzelhandelsgruppe betreibt mehr als 12.500 Filialen in 33 Ländern. Schwarz baut schnell die internationale Präsenz aus. Um erfolgreich zu sein, muss die Gruppe ein Gleichgewicht finden zwischen einem konsistenten Filialmanagement und der notwendigen Flexibilität und Agilität, sich an lokale Anforderungen anpassen und neue Filialen schnell eröffnen zu können. Dies gilt besonders in neuen Märkten. Dabei muss sie aber auch die Risikenminderung im Auge behalten.

Um die neuen Filialen konsistent zu managen und sie gleichzeitig an die jeweiligen Anforderungen vor Ort anpassen zu können, migrierte die Gruppe von der bestehenden Managementlösung Puppet zur Red Hat Ansible Automation Platform. Durch die konsistente zentrale Betriebsbasis kann die Gruppe innovative digitale Services mithilfe von Self-Service-Funktionen schnell bereitstellen und so wettbewerbsfähig bleiben und gleichzeitig eine stabile Sicherheitslage beibehalten.



Konsistenz ist der Schlüssel für die Sicherheit in Tausenden von Einzelhandelsfilialen weltweit

Schwarz IT beschäftigt mehr als 3.500 Ingenieure, die über 1.000 SAP-Systeme und 28 PB von in Rechenzentrum-gehostetem Storage unterstützen. Jede Schwarz-Filiale betreibt einen Storeserver. Dabei handelt es sich um eine zentrale Betriebsbasis, die vom lokalen IT-Team des Unternehmens installiert wird. Sie dient der Steuerung verschiedener Filialfunktionen, von den Systemen für Selbstbedienungskassen und Videoüberwachungsanlagen (CCTV) bis hin zu Recycling- und Prämienprogrammen.

Für eine bessere Verwaltung und Autorisierung der Nutzer entschied sich die Schwarz IT, gesteuerte, effiziente Self-Service-Funktionen einzuführen, um so Deployment-Prozesse zu beschleunigen. Um dies zu erreichen, führte Schwarz IT Ansible Automation Platform ein.

> *Wegen ihrer komplexen und zeitintensiven Prozesse hat die Community-Version unsere Anforderungen nicht erfüllt. Automatisierung ist ein wichtiger Bestandteil unserer geschäftlichen Abläufe. Der Support für Unternehmen war dann einer der Hauptgründe, warum wir uns für die Lösung von Red Hat entschieden haben.*
>
> Felix Kuehner, Head of Storeserver, Core Infrastructure Services, Schwarz IT.

Im Rahmen eines zweitägigen Workshops haben die IT-Teams des Unternehmens zusammen mit den technischen Experten von Red Hat die Architektur überprüft und Best Practices für die neue Automatisierungslösung aufgestellt.

Die Gruppe führt jetzt täglich mehr als 5.000 Jobs auf Ansible Automation Platform aus, um die Storeserver der Filialen zu managen.

Besseres Risikomanagement durch rollenbasierten Systemzugriff

Mithilfe von Ansible Automation Platform erreicht die Schwarz IT ein effektiveres Gleichgewicht zwischen der Kontrolle des Systemzugriffs durch autorisierte Anwendungen und der Entwicklung von gewünschten Self-Service-Funktionen. RBAC (Role-based Access Control) bedeutet, dass Anwendungsteams automatische Deployments als gewöhnliche Nutzende ausführen können – ohne Root-Zugriff auf wichtige Geschäftssysteme zu benötigen. „Diese Funktion sorgt für ein hohes Maß an Konsistenz, lässt die einzelnen Mitarbeiter aber gleichzeitig proaktiv an neuen oder bestehenden Projekten arbeiten", erklärt Kuehner.

Nach den ersten Erfolgen mit Ansible Automation Platform will Schwarz IT jetzt weitere Möglichkeiten erkunden, wie die Schwarz Gruppe mit der Plattform konsistente, aber flexible Filialabläufe erreichen kann.

> ***Die enge Zusammenarbeit mit Red Hat war für uns sehr wertvoll, und wir hoffen, mit Ansible weiterhin neue Wege zu finden, unser Geschäft moderner und effizienter zu machen.***
>
> Felix Kühner, Head of Storeserver, Core Infrastructure Services, Schwarz IT

Jetzt die Schwarz Success Story herunterladen

Agile Defense verbessert Sicherheitscompliance mit Red Hat Ansible Automation Platform

3

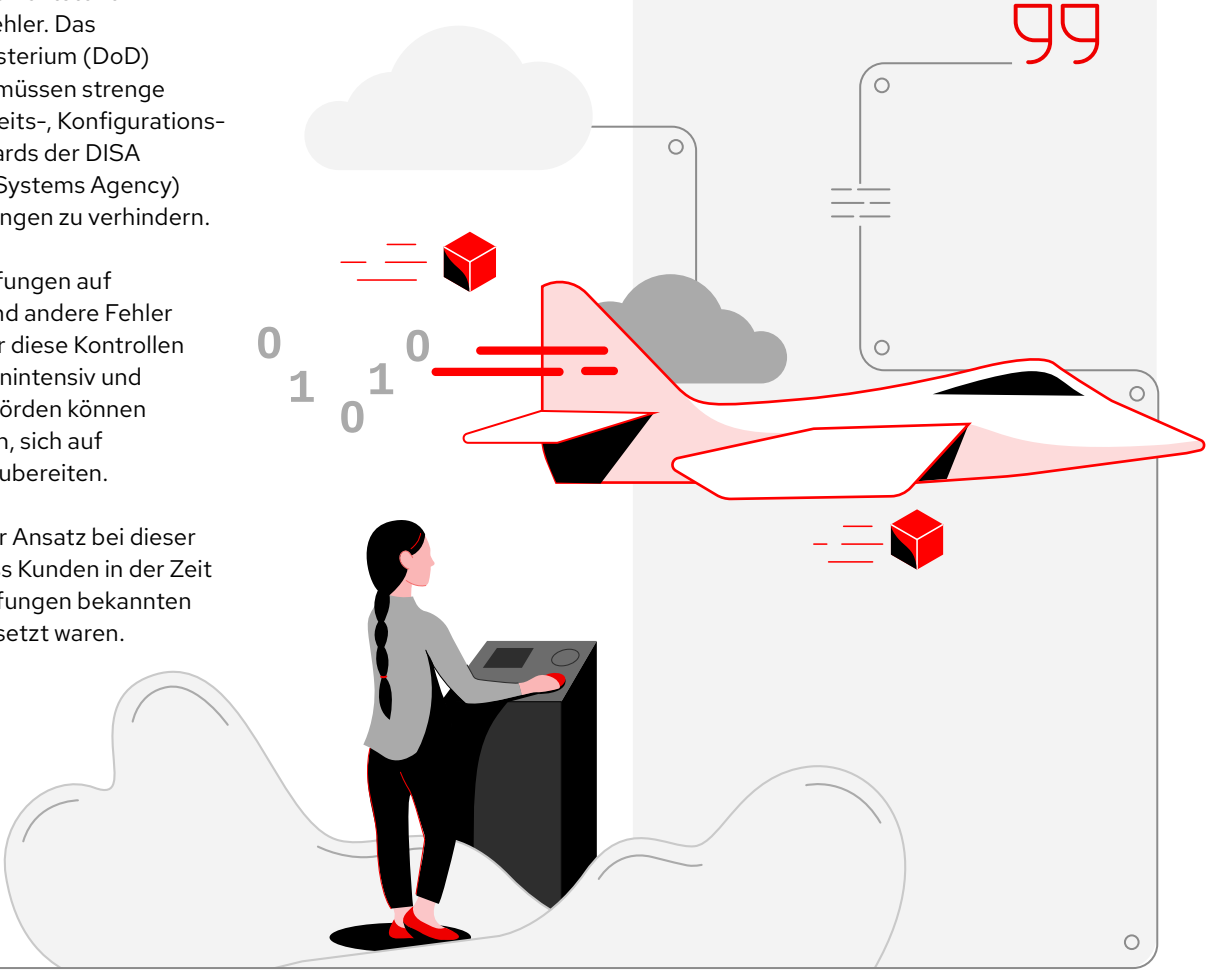
Agile Defense ist ein führendes IT-Serviceunternehmen aus Reston, Virginia. Es hat viele US-Regierungskunden, darunter mehrere US-Bürgerbehörden und verschiedene Abteilungen innerhalb des US-Verteidigungsministeriums, weshalb IT-Sicherheit oberste Priorität hat.

Cyberkriminelle davon abzuhalten, unberechtigten Zugang zu ihren Systemen und Infrastrukturen zu erhalten, ist wichtiger als je zuvor. Viele Sicherheitsverletzungen entstehen durch Konfigurationsfehler. Das US-Verteidigungsministerium (DoD) und Bundesbehörden müssen strenge Informations-, Sicherheits-, Konfigurations- und Compliancestandards der DISA (Defense Information Systems Agency) einhalten, um Bedrohungen zu verhindern.

Regelmäßige Überprüfungen auf Fehlkonfigurationen und andere Fehler sind Teil des Jobs, aber diese Kontrollen waren teuer, ressourcenintensiv und wiederholten sich. Behörden können Monate dafür brauchen, sich auf eine Überprüfung vorzubereiten.

Ein manueller, reaktiver Ansatz bei dieser Arbeit führte dazu, dass Kunden in der Zeit zwischen den Überprüfungen bekannten Schwachstellen ausgesetzt waren.

> ***Die Produktionsaufgaben unserer Kunden stoppten vor einer Inspektion, da sie ihre Dokumentation vorbereiten mussten.***
>
> Shawn Draper, Solutions Engineer bei Agile Defense



Mit Automatisierung die Auswirkungen von Überprüfungen mindern

Fehlkonfigurationen und Überprüfungen sind stetige Problembereiche für viele Regierungskunden von Agile Defense. Das führende IT-Serviceunternehmen, das sich der Innovation mithilfe von IT verschrieben hat, erstellte zusammen mit Red Hat ein Tool für ein STIG-Konfigurations, -Reporting und -Problembehebungs-Tool (Security Technical Implementation Guide). Diese STIG-Automatisierungslösung führt ad hoc Systemüberprüfungen durch, behebt bei Bedarf Fehlkonfigurationen und erstellt Berichte über den aktuellen Zustand der Geräte. Die Lösung verwendet Red Hat Ansible Automation Platform aufgrund seiner flexiblen und skalierbaren Automatisierungsfähigkeiten und ist bei Agile Defense auch als CPaaS (Compliance as a Service) bekannt.

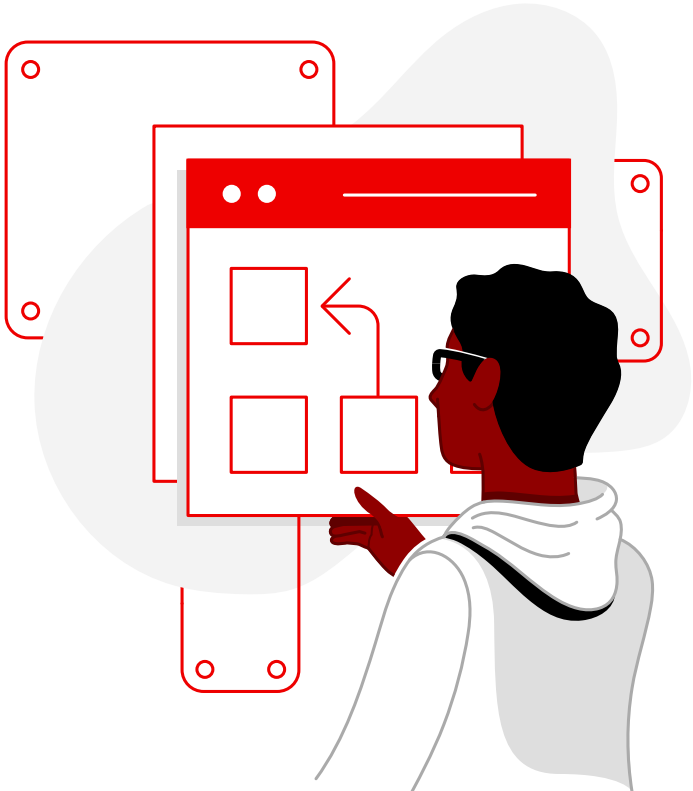
Zusätzlich arbeitete Red Hat mit DISA an einer STIG für Red Hat Enterprise Linux und versteht, wie wichtig es ist, Standards für Geräte, Betriebssysteme und Softwareversionen zu erstellen.

> ***Wir haben uns für Red Hat Ansible Automation Platform entschieden, um dieses Problem zu lösen, da es mit nahezu allem kommunizieren kann.***
>
> Shawn Draper, Solutions Engineer bei Agile Defense

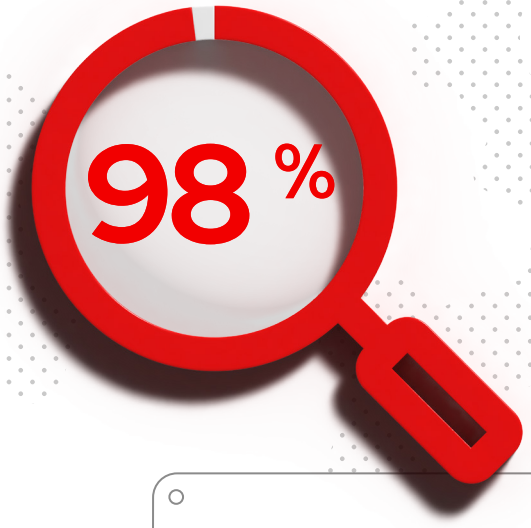
Der Sicherheitsvorteil von Ansible Playbooks

CPaaS verwendet die in Red Hat Ansible Automation Platform enthaltenen Automatisierungsfähigkeiten zum Konfigurationsmanagement, um nach offenen Schwachstellen zu suchen. „Red Hat Ansible Automation Platform verbindet sich mit Geräten und führt die in einem Ansible Playbook festgelegten Befehle aus," erklärt Draper.

Wenn es Fehlkonfigurationen automatisch identifiziert hat, kann CPaaS diese auch automatisch beheben, indem es die Befehle aus einem maßgeschneiderten Ansible Playbook ausführt. Agile Defense hat eine Vielzahl an Playbooks für Tests unterschiedlicher Gerätearten testet. Darunter sind Playbooks für Plattformen von Red Hat, Windows-Geräte, VMware-Hypervisoren, Cisco-Router und -Switches sowie Firewalls.



Zeitaufwand der Kunden für Überprüfungen reduzierte sich um



CPaaS kümmert sich um die Formalitäten, indem es automatisch die benötigte Dokumentation erstellt. Genauer gesagt nutzt CPaaS Ansible Automation Platform, um eine XML-Checkfile (sichtbar im STIG-Viewer von DISA) für die Geräte im Netzwerk und identifizierten Schwachstellen zu schreiben, um sie dem Auditor zu präsentieren. Diese Artefakte können aktuelle Informationen zeigen und nachweisen, dass bestimmte Sicherheitskonfigurationen implementiert wurden. Ansible Automation Platform ermöglicht es Kunden zusätzlich, die Funktionen von CPaaS zu erweitern und Workflows sowie Inventory zu verwalten, Überprüfungen zu planen und Role-based Access Control einzuführen. CPaaS stellt außerdem Konsistenz auf verschiedenen Geräten sicher.

> ***Einer der besten Aspekte von Automatisierung ist, dass sie jedes Mal dasselbe macht.***
>
> Shawn Draper

CPaaS ermöglicht die wichtige und proaktive Überwachung der Sicherheitslage einer Behörde, um stets auf Cyberbedrohungen vorbereitet zu sein. In der Vergangenheit war diese Überwachung ressourcenintensiv und benötigte zusätzliche Software auf Endgeräten. Indem es Ansible Automation Platform zum Scannen offener Schwachstellen verwendet, kann das CPaaS von Agile Defense seinen Regierungskunden 98 % des Zeitaufwands für Überprüfungen einsparen.

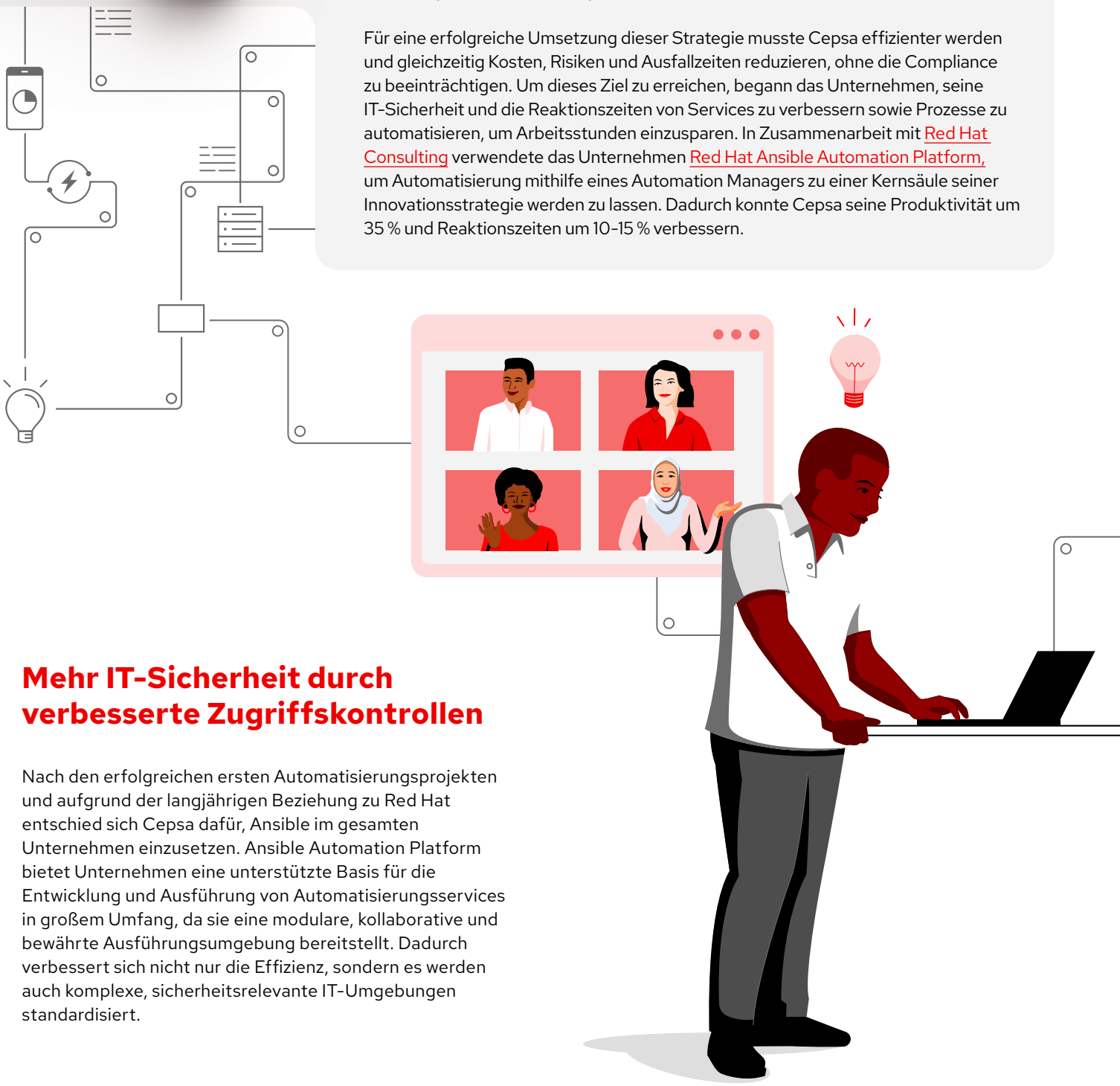
Jetzt die Agile Defense Success Story herunterladen

4

Cepsa steigert die Effizienz mit Red Hat Ansible Automation Platform

Das globale Energie- und Chemieunternehmen Cepsa möchte weltweit CO2-Emissionen reduzieren. Das Unternehmen präsentierte 2022 seine Strategie, in den Bereichen nachhaltige Mobilität, Biokraftstoffen und grünen Wasserstoffen zum Anführer zu werden. Dabei legte es seinen Fokus auf Spanien und Portugal sowie auf den Energiewandel als wichtigste Benchmark.

Für eine erfolgreiche Umsetzung dieser Strategie musste Cepsa effizienter werden und gleichzeitig Kosten, Risiken und Ausfallzeiten reduzieren, ohne die Compliance zu beeinträchtigen. Um dieses Ziel zu erreichen, begann das Unternehmen, seine IT-Sicherheit und die Reaktionszeiten von Services zu verbessern sowie Prozesse zu automatisieren, um Arbeitsstunden einzusparen. In Zusammenarbeit mit Red Hat Consulting verwendete das Unternehmen Red Hat Ansible Automation Platform, um Automatisierung mithilfe eines Automation Managers zu einer Kernsäule seiner Innovationsstrategie werden zu lassen. Dadurch konnte Cepsa seine Produktivität um 35 % und Reaktionszeiten um 10-15 % verbessern.



Mehr IT-Sicherheit durch verbesserte Zugriffskontrollen

Nach den erfolgreichen ersten Automatisierungsprojekten und aufgrund der langjährigen Beziehung zu Red Hat entschied sich Cepsa dafür, Ansible im gesamten Unternehmen einzusetzen. Ansible Automation Platform bietet Unternehmen eine unterstützte Basis für die Entwicklung und Ausführung von Automatisierungsservices in großem Umfang, da sie eine modulare, kollaborative und bewährte Ausführungsumgebung bereitstellt. Dadurch verbessert sich nicht nur die Effizienz, sondern es werden auch komplexe, sicherheitsrelevante IT-Umgebungen standardisiert.

Die leicht verständliche Playbook-Syntax von Ansible erlaubt es Cepsa, Sicherheitsparameter für beliebige Teiles ihres Systems zu definieren. Dazu gehören das Erstellen von Firewall-Regeln, das Einschränken von Usern oder Gruppen sowie das Anwenden benutzerdefinierter Sicherheitsrichtlinien. Durch die Standardisierung seiner Prozesse konnte Cepsa die Zahl zusätzlicher Berechtigungen zur Sicherheitsadministration in seinen Systemen reduzieren und so Sicherheitsrisiken mindern. User werden jetzt nach Jobrolle und Abteilung gruppiert, damit ihnen die richtige Berechtigungsstufe gewährt wird, ohne dass Zugriffsrechte zu weit ausgedehnt werden.

Dadurch konnte Cepsa seine Produktivität um 35 % und Reaktionszeiten um 10-15 % verbessern.

Eine Technikfachkraft kann nun auf Ansible Automation Platform zugreifen und den Service ohne Zugangsdaten neustarten. Dabei kann diese sich sicher sein, dass Prozesse genau so ausgeführt werden, wie es im vordefinierten Code dargestellt wird.

Produktivität
erhöhte sich um
35 %

Reaktionszeiten
erhöhten sich um
10-15 %

Mithilfe von Automatisierung haben wir einen positiven kulturellen Wandel herbeigeführt, der die Zusammenarbeit zwischen den Teams verbessert hat. Red Hat arbeitet mit uns zusammen daran, in unserer gesamten Organisation Best Practices zu implementieren und von ihrer Expertise zu lernen.

Francisco José Martín, Automation Manager,
Department of Exploitation and Operation, Cepsa

Mit Automatisierungsfachleuten zu einer sicherheitsorientierten Kultur

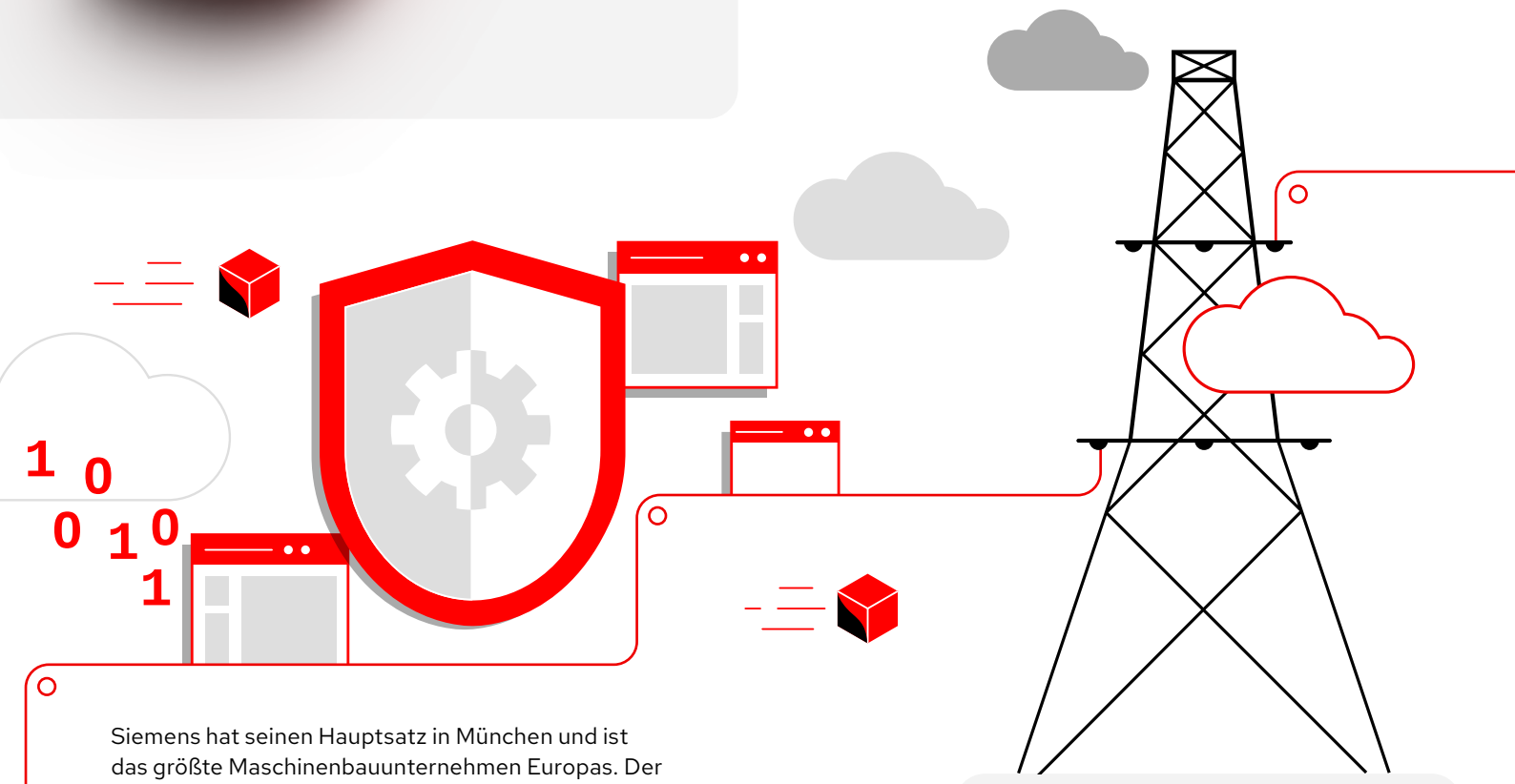
Red Hat Consulting unterstützte Cepsa dabei, die erforderlichen Änderungen zu implementieren und ihre neue Automatisierungstechnologie so vollständig zu nutzen. Die Fachkräfte von Red Hat machten dem Team von Cepsa im Rahmen der Zusammenarbeit deutlich, wie wertvoll ein agiler Arbeitsansatz und kontinuierliche Qualitätsverbesserungen durch einen CI/CD-Ansatz (Continuous Integration/Continuous Delivery) für Unternehmen sind.

Jetzt die Cepsa Success Story herunterladen

5

SIEMENS

Siemens verbessert Kommunikationssicherheit mit Red Hat Ansible Automation Platform



Siemens hat seinen Hauptsatz in München und ist das größte Maschinenbauunternehmen Europas. Der Fokus der internationalen Technologiegruppe liegt auf der Elektrifizierung. Dazu zählen unter anderem die Energieerzeugung, -übertragung und -verteilung, intelligente Netze sowie die effiziente Verwendung elektrischer Energie.

Aufgrund der sensiblen Natur seines Geschäfts möchte Siemens seine Vorreiterrolle im Bereich Sicherheitstechnologie beibehalten. Um den Zugriff auf vertrauliche Informationen zuverlässig zu schützen, verwenden die 295.000 Mitarbeitenden von Siemens und die 100.000 Mitarbeitenden seiner Geschäftspartner PKIs (Public Key Infrastructures), um die Zertifikate und Identität von öffentlichen Schlüsseln zu überprüfen. Diese Technologie wird vermehrt dafür genutzt, IoT-Kommunikation (Internet of Things) zu sichern. Siemens unterhält aktuell zwei PKI-Umgebungen für verschiedene Use Cases für Anwendungen.

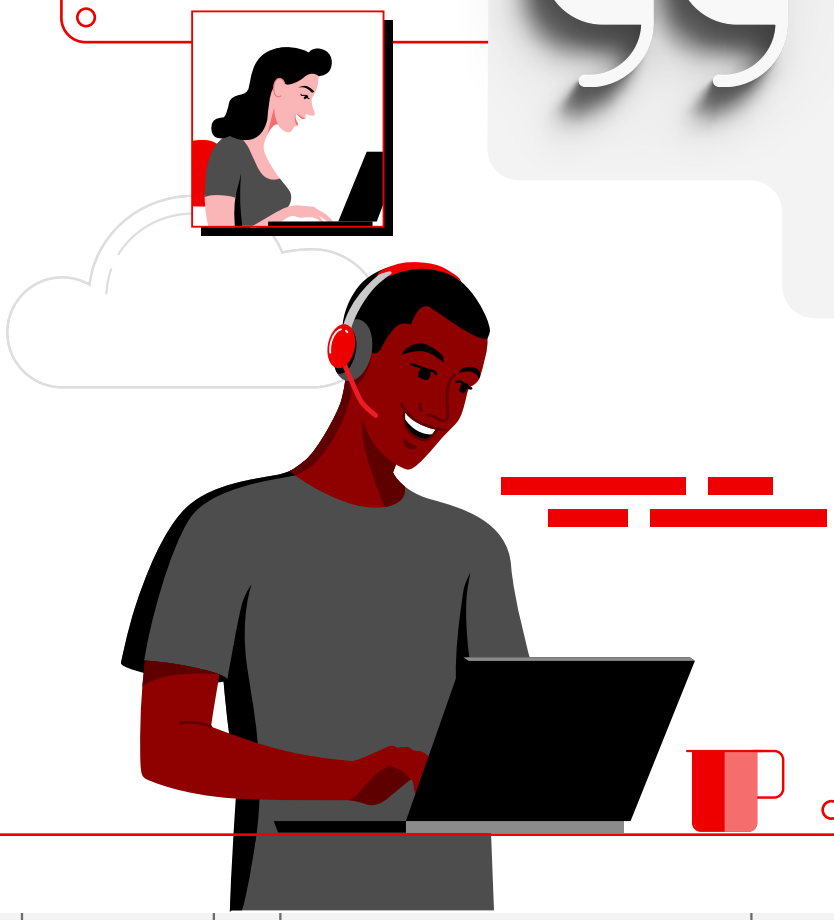
> ***Dies ist besonders wichtig, da Infrastructure-as-Code mit Red Hat Ansible Automation Platform nicht nur die Einführung eines neuen Tools bedeutet, sondern auch ein fundamentales Umdenken der Systemadministratoren erfordert.***
>
> Rufus Buschart, Head of PKI (Public Key Infrastructure), Siemens

Wenn wir Red Hat brauchen, sind sie immer für uns da. Unsere Vision ist es, gemeinsam eine Best-Practice-Automatisierungsplattform zu entwickeln und mit dieser die Effizienz und Innovation unserer Organisation zu optimieren.

Rufus Buschart

Mit der zunehmenden Kommunikation zwischen Serviceteams im gesamten Unternehmen steigt auch die Konfigurationskomplexität für das PKI-Team von Siemens. Um dieser Nachfrage gerecht zu werden, ersetzte Siemens seine Legacy-Automatisierungslösung durch Ansible Automation Platform.

Mit Ansible Automation Platform kann Siemens nun administrative Aufgaben automatisieren, Konfigurationsqualität steigern und die Kommunikationssicherheit im Unternehmen verbessern. Weiterhin profitierte Siemens von der Expertise von Red Hat und plant, mithilfe von Red Hat automatisierte Testprozesse auszuprobieren, mit dem Ziel, einen gemeinsamen Blueprint für CD (Continuous Deployment) zu erschaffen.



Jetzt die Siemens Success Story herunterladen

Fazit

Mit Ansible Automation Platform können Organisationen automatisierte Sicherheitssysteme verwalten, um schädlichen Attacken einen Schritt voraus zu sein. Sicherheitsteams haben Zugriff auf Hunderte von Modulen, mit denen sie ihre IT-Umgebung sowie -Prozesse automatisieren können. Weiterhin kann Ansible viele Teams integrieren, um komplexe Sicherheitsbereiche zu schützen, Ihren Sicherheitsansatz zu vereinheitlichen und Ihre Sicherheitslage zu stärken.

Wie Ansible Automation Sicherheitsteams unterstützt:

Verkettung von Workflows und Playbooks zur modularen Wiederverwendung

Sicherheitsteams können eine Abfolge von Jobs konfigurieren, die Inventories, Playbooks und Berechtigungen teilen, und so die Prüfung oder Behebung von Problemen vollständig automatisieren.

Unterstützung von lokalen Verzeichnisdiensten und Zugriffskontrollen.

Die Vernetzung von User Directory Services mit Infrastruktur ermöglicht es Sicherheitsteams, den Zugriff auf und die Ausführung von Aufgaben zu zentralisieren, Teile von Vorgängen bestimmten Rollen zuzuweisen und Aufgaben mit anderen Gruppen zu teilen.

Konsolidierung und Zentralisierung von Protokollen.

Integration mit Log Aggregation Services von Drittanbietern, was Sicherheitsteams dabei hilft, Trends zu erkennen, Infrastruktur-Events zu analysieren, Abweichungen zu überwachen und separate Events zu korrelieren.

Integration externer Anwendungen über RESTful APIs.

Sicherheitsteams können Red Hat Ansible Automation Platform dafür nutzen, andere Unternehmensanwendungen zu managen – zum Beispiel SOAR-Lösungen (Security Orchestration and Automated Response).

Verbessern Sie Ihre Sicherheitslage mit Automatisierung.

Mehr erfahren über Red Hat Ansible Automation Platform.

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

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549