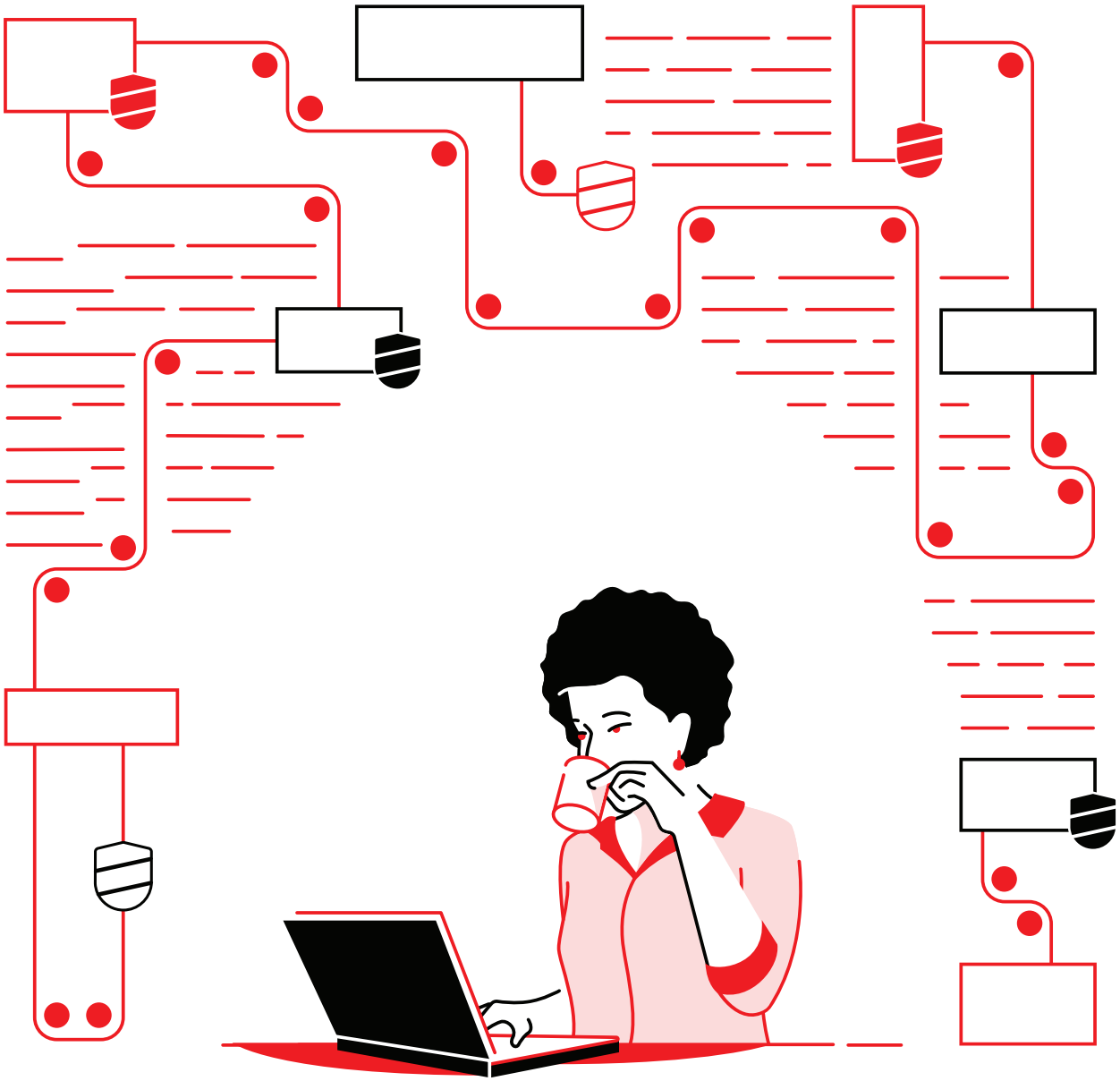
Vereinfachen Sie Ihr Security Operations Center

Mehr Geschwindigkeit, Zeit und Sicherheit durch eine einheitliche Automatisierungsplattform



Red Hat | IBM

Inhaltsverzeichnis

IT-Sicherheit hat oberste Priorität

Sicherheit ist für die meisten Organisationen ein Hauptanliegen. 33 % der CEOs sind angesichts von Cyberbedrohungen sogar sehr besorgt.[1] Diese Befürchtung ist nicht unbegründet: 32 % der Organisationen wurden in den letzten zwei Jahren Opfer eines großen Cyberangriffs.[2]

Der Schutz Ihrer Organisation ist wichtig – aber oft eine große Herausforderung. Sicherheitsteams müssen komplexe Umgebungen entwickeln, warten, verwalten und anpassen. Dabei nutzen sie eine Vielzahl an Tools und Services von verschiedenen, oft konkurrierenden Anbietern. Da die Anzahl an Angeboten jedes Jahr wächst und die Sicherheitslandschaft sich verändert, müssen die Teams kontinuierlich neue Produkte untersuchen, bewerten und integrieren.

Außerdem werden Sicherheitsverletzungen zunehmend häufiger, schwerwiegender und kostspieliger. Die Wahrscheinlichkeit, innerhalb von zwei Jahren Opfer einer Sicherheitsverletzung zu werden, liegt bei 29,6 % – im Vergleich zu 22,6 % im Jahr 2014.[3] Die durchschnittliche Anzahl der betroffenen Datensätze stieg 2019 um 3,9 % im Vergleich zum Vorjahr.[3] Die durchschnittlichen Kosten einer Datenschutzverletzung stiegen im Jahr 2019 auf 3,92 Millionen USD.[3]

Sicherheitsabläufe werden in den meisten Unternehmen manuell abgewickelt. Sicherheitsrelevante Aufgaben können zeitaufwändig, mühsam und fehleranfällig sein, wenn menschliches Eingreifen erforderlich ist. Sicherheitsteams sind daher überfordert. Sie müssen eine steigende Anzahl an Sicherheitswarnungen von zahlreichen Tools bewältigen. Tatsächlich erhalten 60 % der Sicherheitsteams täglich über 5.000 und 16 % täglich über 100.000 Warnmeldungen.[4]

Durch die an Größe und Komplexität zunehmende Infrastruktur wird es gleichzeitig schwieriger, Schwachstellen zu entdecken und Sicherheitsverletzungen zu überprüfen. Die meisten Sicherheitstools lassen sich nicht miteinander integrieren und sorgen so für zusätzlichen manuellen Arbeitsaufwand. Dementsprechend länger dauert es, Vorfälle zu untersuchen und auf diese zu reagieren. Im Jahr 2019 dauerte das Erkennen und Eindämmen einer Datenschutzverletzung im Durchschnitt 279 Tage – ein Anstieg von 4,9 % im Vergleich zu 2018.[3] Es ist zudem schwierig, Fachkräfte zur Erweiterung des Teams zu finden, um Schritt halten zu können: 39 % der Unternehmen berichteten 2019 von einem Fachkräftemangel im Bereich Cybersicherheit.[2] Hinzu kommt ein begrenztes Budget für Maßnahmen zur Cybersicherheit. Nur 33 % der Organisationen gaben an, über ausreichend finanzielle Mittel für ein hohes Maß an Cyberresilienz zu verfügen.[5]

Dementsprechend überprüfen und reagieren typische Sicherheitsteams nur auf 48 % der Warnmeldungen und nur 50 % der ernsthaften Bedrohungen werden behoben.[4] Viele Unternehmen werden damit anfällig für Angriffe.

77 % der Organisationen planen eine stärkere Automatisierung zur Vereinfachung und Beschleunigung der Reaktionszeiten in ihren Sicherheitsumgebungen.[4]

Auswirkungen ineffizienter Sicherheitsmaßnahmen

Sicherheitsverletzungen werden zunehmend häufiger, schwerwiegender und kostspieliger.

USD 3,92 Mio.
durchschnittliche Kosten für Datenschutzverletzungen im Jahr 2019[3]

279 Tage
durchschnittlicher Zeitraum zur Erkennung und Eindämmung einer Datenschutzverletzung im Jahr 2019[3]

USD 1,22 Mio.
Kosteneinsparungen, wenn die Erkennung und Eindämmung einer Verletzung innerhalb von **200 Tagen** oder schneller geschieht[3]

29,6 %
Wahrscheinlichkeit für eine Sicherheitsverletzung innerhalb von zwei Jahren[3]

50 %
Anteil der ernsthaften Bedrohungen, die behoben werden[4]

1 *PWC, „23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty", 2020.* pwc.com/ceosurvey.
2 *Harvey Nash and KPMG, „CIO Survey 2019: A Changing Perspective", 2019.* home.kpmg/xx/en/home/insights/2019/06/harvey-nash-kpmg-cio-survey-2019.html.
3 *IBM Security, „2019 Cost of a Data Breach Report", 2019.* ibm.com/security/data-breach.
4 *Cisco, „Cisco Benchmark Study: Securing What's Now and What's Next", Februar 2020.* cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html.
5 *Ponemon Institute, gesponsert von IBM Security, „The Cyber Resilient Organization", April 2019.* ibm.com/account/reg/us-en/signup?formid=urx-37792.

Was ist Sicherheitsautomatisierung?

Bei der Sicherheitsautomatisierung geht es um die Automatisierung manueller Aufgaben, die den Sicherheitszustand Ihres Unternehmens gewährleisten. Sie umfasst verschiedene Methoden, die wir in die folgenden vier allgemeinen Kategorien eingeteilt haben:

Reaktion und Problembehebung
Ereignisgesteuerte Aktivitäten, die das Mitwirken und/oder die Unterstützung durch einen Security Analyst erfordern

Sicherheitsabläufe
Tägliche prozess- und richtliniengesteuerte Aktivitäten, die technische Teams an Ihrer Sicherheitsinfrastruktur vornehmen

Sicherheits-Compliance
Aktivitäten, die für die Compliance der Infrastruktur mit Sicherheitsrichtlinien und -vorschriften sorgen

Härtung
Aktivitäten, die benutzerdefinierte Sicherheitsrichtlinien zielgerichtet auf die Infrastruktur anwenden

Mehr über Sicherheits-Compliance und Härtung erfahren

In diesen Ressourcen entdecken Sie, wie Automatisierung die Sicherheits-Compliance und Härtung verbessern kann:

- **Mehr Sicherheit in der Hybrid Cloud – E-Book**
- **Warum Sicherheit und Compliance automatisieren? – Überblick**
- **Red Hat Services: Automatisierte Sicherheit und zuverlässige Workflows – Datenblatt**

Dieses E-Book befasst sich mit der Automatisierung von Reaktion und Problembehebung sowie von Sicherheitsabläufen.

Vorteile der Automatisierung für Sicherheitsabläufe, Reaktion auf Vorfälle und Problembehebung

Geschwindigkeit und Effizienz steigern

Automatisierung optimiert Aufgaben und beseitigt die Notwendigkeit für manuelles Eingreifen. So werden Sicherheitsabläufe beschleunigt, und IT-Mitarbeiter können sich wieder auf wertsteigernde Initiativen konzentrieren. Sie kann zudem die Komplexität der IT-Infrastruktur reduzieren: 40 % der stark automatisierten Organisationen geben an, die richtige Anzahl an notwendigen Sicherheitslösungen und -technologien zu haben.[6]

Sicherheit in großem Umfang steigern

Durch die Anwendung von Automatisierung auf Ihre gesamte Sicherheitsinfrastruktur erreichen Sie eine höhere Konsistenz und ein ganzheitliches Sicherheitskonzept. Jeder Mitarbeiter kann so mehr Tools, Geräte und Systeme verwalten, was Ihnen einen Betrieb in großem Umfang ermöglicht. Automatisierung reduziert auch das Risiko von menschlichen Fehlern und verbessert so die Genauigkeit.

Risiko und Kosten von Sicherheitsverletzungen senken

Organisationen, die in großem Umfang automatisieren, können Sicherheitsvorfälle und Geschäftsunterbrechungen besser verhindern.[6] Die unternehmensweite Automatisierung von Sicherheitsprozessen kann die durchschnittlichen Kosten einer Sicherheitsverletzung um 95 % reduzieren.[7] 52 % der Organisationen haben daher bereits einen Teil ihrer Sicherheitsprozesse automatisiert und weitere 36 % planen dies für die nächsten 24 Monate.[7]

6 *Ponemon Institute, gesponsert von IBM Security, „The Cyber Resilient Organization", April 2019.* **ibm.com/account/reg/us-en/signup?formid=urx-37792**.

7 *IBM Security, „2019 Cost of a Data Breach Report", 2019.* **ibm.com/security/data-breach**.

Automatisierung integriert Ihre Sicherheitstools, -systeme und -prozesse

Mitarbeiter, Prozesse und Tools mit einer konsistenten, flexiblen Plattform vereinen

Eine Automatisierungsplattform kann als Integrationsschicht zwischen Sicherheitsteams, -tools und -prozessen dienen. Mit einer flexiblen, interoperablen Plattform können Sie:

- Ihre Sicherheitssysteme, -tools und -teams verbinden
- Informationen aus verschiedenen Systemen sammeln und diese schnell und ohne manuelles Eingreifen an vordefinierte Systeme und Speicherorte übermitteln
- Konfigurationen von zentralen Schnittstellen schnell ändern und propagieren
- Benutzerdefinierte Automatisierungsinhalte zu Ihren Sicherheitstools und -prozessen erstellen, warten und darauf zugreifen
- Beim Erkennen einer Bedrohung automatisierte Aktivitäten für mehrere Sicherheitstools auslösen

Der unternehmensweite Einsatz einer konsistenten Automatisierungsplattform und -sprache kann auch die Kommunikation und Zusammenarbeit verbessern. Wenn jede Sicherheitslösung in derselben Sprache automatisiert wird, können Analysten und Operatoren mehrere Maßnahmen für verschiedene Produkte in einem Bruchteil der Zeit ausführen und so die Effizienz des Sicherheitsteams steigern. Mit einem gemeinsamen Framework und einer gemeinsamen Sprache können Sicherheits- und IT-Teams außerdem Strategien, Prozesse und Ideen teamintern und unternehmensweit teilen.

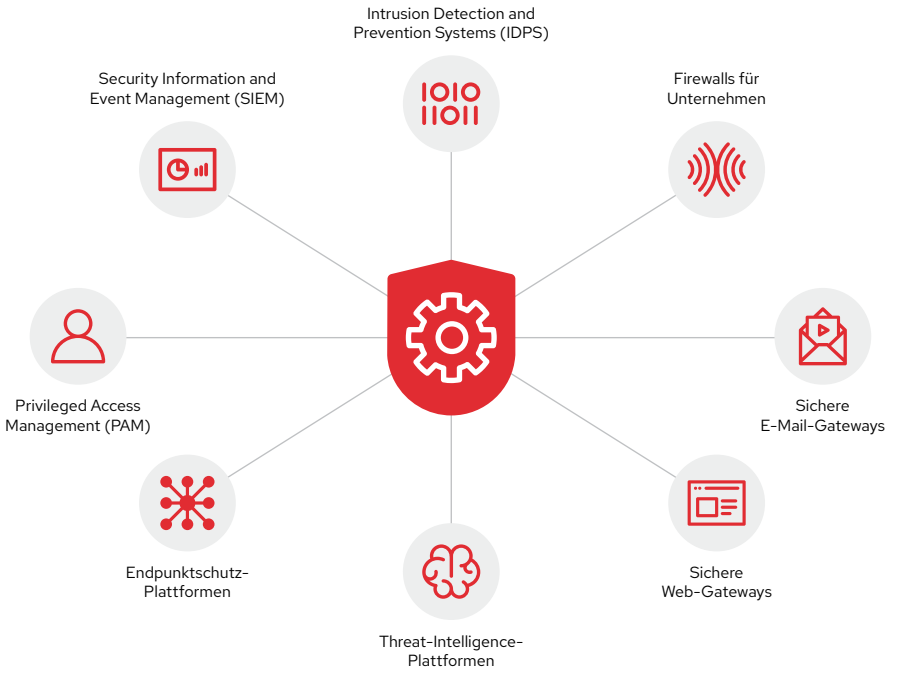


Abbildung 1. *Eine Automatisierungsplattform kann Ihre Sicherheitssysteme, -tools und -teams verbinden.*

Automatisierungserfolg = Personal + Prozesse + Plattform

Um Automatisierung optimal zu nutzen, benötigen Sie mehr als nur ein Tool – Sie müssen auch Ihr Personal, die Prozesse und die Plattform einbeziehen.

- **Das Personal** steht bei allen geschäftlichen Initiativen im Mittelpunkt. Durch die teaminterne und teamübergreifende Mitsprache können Mitarbeiter Ideen teilen und effektiver zusammenarbeiten.
- **Prozesse** sorgen dafür, dass Projekte innerhalb Ihres Unternehmens ordnungsgemäß abgewickelt werden. Klare, dokumentierte Prozesse sind für eine effektive Automatisierung entscheidend.
- Eine Automatisierungs **plattform** liefert die Funktionen zum Erstellen, Ausführen und Verwalten der Automatisierungs-Assets. Im Gegensatz zu einfachen Automatisierungstools bietet eine Automatisierungsplattform Ihrem Unternehmen eine einheitliche Basis, um konsistente Automatisierungsinhalte und -kenntnisse in großem Maßstab zu entwickeln, bereitzustellen und gemeinsam zu verwenden.

E-Book lesen

Sicherheitsautomatisierung ist ein Prozess

Automatisierung ist keine Alles-oder-Nichts-Lösung und lässt sich in keinem Unternehmensbereich mit einem Klick implementieren. Sicherheitsautomatisierung ist ein Prozess. Für jede Organisation beginnt – und endet – dieser Prozess ihren Anforderungen entsprechend an einem anderen Punkt. Diese Anforderungen bestimmen auch den Weg, den die Organisation geht. Aber unabhängig davon, in welcher Phase dieses Prozesses Sie sich befinden – selbst kleine Maßnahmen zur Sicherheitsautomatisierung können Vorteile bringen.

Bewerten Sie den Reifegrad Ihrer Sicherheitsautomatisierung

Die Sicherheitsautomatisierungsreife der meisten Organisationen fällt in eine von drei Hauptphasen. Wenn Sie wissen, in welcher Phase Ihre Organisation sich gerade befindet, können Sie die richtigen Tools und Prozesse zur richtigen Zeit einführen und so mit Erfolg automatisieren.

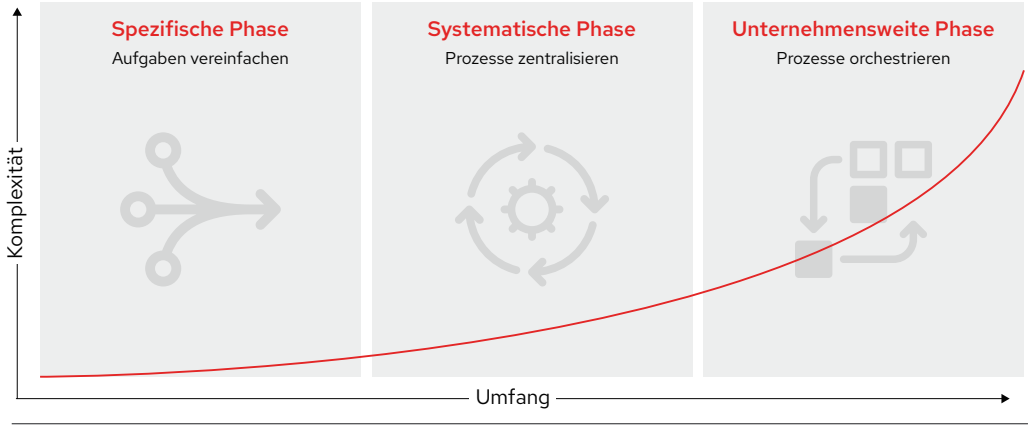


Abbildung 2. *Phasen der Sicherheitsautomatisierungsreife*

Phase 1: Spezifische Phase

In dieser Phase geht es darum, durch die Automatisierung von Sicherheitsabläufen Zeit zu sparen. Häufige Ziele sind die Standardisierung von Sicherheitsmaßnahmen für ähnliche Geräte und Technologien sowie die Optimierung von manuellen Aufgaben für die Produkte verschiedener Anbieter.

Phase 2: Systematische Phase

In dieser Phase geht es darum, die Prozesse und Effizienz durch die Einführung von einheitlichen Tools und Services für Sicherheitsabläufe zu verbessern. Häufige Ziele sind die Integration von Sicherheitsprozessen in übergeordnete Workflows sowie zentrale Reaktionen auf Sicherheitsvorfälle.

Phase 3: Unternehmensweite Phase

In dieser Phase geht es darum, die Zusammenarbeit zu fördern und Sicherheit zu integrieren – unternehmensweit. Häufige Ziele sind die Erstellung von automatisierten, programmatischen Workflows zu allen Sicherheitsaspekten sowie die Integration Ihrer Sicherheits- und IT-Technologien.

Definieren Sie Ihre Strategie zur Sicherheitsautomatisierung

Häufige, allgemeine Use Cases für die Sicherheitsautomatisierung

Jeder dieser Use Cases kann als Ausgangspunkt für Ihre Sicherheitsautomatisierung dienen. Entscheidend ist, dass Sie klein und einfach anfangen und die Automatisierung stetig ausweiten.

Datenangereicherte Untersuchung

Bei der Untersuchung von Sicherheitswarnungen und -vorfällen sollten Informationen aus mehreren Sicherheitssystemen erfasst werden, um einzuschätzen, ob ein ernsthaftes Sicherheitsereignis vorliegt. Die Daten werden dabei für gewöhnlich über verschiedene Benutzeroberflächen, E-Mails und Telefonanrufe erfasst. Dieser ineffiziente Prozess kann die Maßnahmen gegen Bedrohungen verzögern. Ihr Unternehmen wird so anfälliger, und die möglichen Kosten einer Sicherheitsverletzung steigen. Mit Automatisierung können Sie programmatisch Informationen aus allen Ihren Sicherheitssystemen erfassen. Zudem wird die On-Demand-Anreicherung von Daten durch die Kategorisierungsprozesse von SIEM-Systemen (Security Information and Event Management) unterstützt. So können Sie Warnmeldungen und Vorfälle schneller bewerten – und schneller darauf reagieren.

Threat Hunting

Beim Threat Hunting geht es um die proaktive Identifizierung und Untersuchung von möglichen Sicherheitsbedrohungen. Wie bei der Untersuchung von Vorfällen werden die Informationen manuell erfasst und zwischen mehreren Systemen verschickt. Mithilfe von Automatisierung können Sie Warnmeldungen, Korrelationssuchvorgänge und Signature Manipulation an Ihre Anforderungen anpassen und optimieren und mögliche Bedrohungen so schneller untersuchen. Außerdem können Sie SIEM-Korrelationsabfragen und IDS-Regeln (Intrusion Detection System) automatisch erstellen und aktualisieren, um die Bedrohungserkennung zu verbessern. Dadurch können Sie die Sicherheitsmaßnahmen Ihrer Organisation häufiger und effizienter aktualisieren und Ihr Unternehmen so besser schützen.

Reaktion auf Sicherheitsvorfälle

Bei der Reaktion auf Sicherheitsvorfälle geht es um schnelles Handeln, um die Ausweitung einer Verletzung zu verhindern. Wenn eine Verletzung entdeckt wird, muss das Sicherheitsteam schnell und in großem Umfang reagieren, um den Schaden einzudämmen. Die Reaktion auf Sicherheitsvorfälle umfasst aber oft verschiedene manuelle Aufgaben, wodurch die Problembehebung verlangsamt wird und Ihr Unternehmen den Sicherheitsrisiken länger ausgesetzt bleibt. Durch Automatisierung können Sie schneller reagieren, indem Sie Maßnahmen in wiederholbare, vorab genehmigte Playbooks codieren. Sie können Aufgaben wie das Blockieren von Angreifer-IP-Adressen oder -Domains beschleunigen und gleichzeitig sicheren Datenverkehr zulassen, gefährdete Zugangsdaten einfrieren und verdächtige Workloads zur weiteren Untersuchung isolieren, um den Schaden des Vorfalls zu minimieren.

Integration ist entscheidend

Eine einheitliche Automatisierung erfordert die Integration Ihrer Automatisierungsplattform mit Ihren Sicherheitstechnologien. Wesentliche Integrationen:

- **Firewalls** steuern den Datenverkehr zwischen Netzwerken und schützen mit dem Internet verbundene Anwendungen. Automatisierung kann Konfigurationsänderungen von Richtlinien und Protokollen beschleunigen.
- **IDPS-Systeme (Intrusion Detection and Prevention)** überwachen den Netzwerkverkehr auf verdächtige Aktivitäten, generieren Warnmeldungen und blockieren Angriffe. Automatisierung kann die Verwaltung von Regeln und Protokollen vereinfachen.
- **SIEM-Systeme (Security Information and Event Management)** erfassen und analysieren Sicherheitsereignisse, um Bedrohungen besser zu erkennen und auf sie zu reagieren. Automatisierung kann programmatischen Zugriff auf Datenquellen ermöglichen.
- **PAM-Tools (Privileged Access Management)** überwachen und verwalten privilegierte Konten und Zugriffe. Automatisierung optimiert die Verwaltung von Zugangsdaten.
- **Endpunktschutzsysteme** überwachen und verwalten Geräte, um diese besser zu schützen. Automatisierung kann allgemeine Aufgaben der Endpunktverwaltung vereinfachen.

Vereinfachen Sie Ihr Security Operations Center mit Red Hat Ansible Automation Platform

Auf dem Markt werden viele Automatisierungslösungen angeboten, aber nicht alle beinhalten die Funktionen, die für eine effektive Sicherheitsautomatisierung erforderlich sind. Eine Automatisierungsplattform sollte Folgendes bieten:

- **Eine universelle, zugängliche Automatisierungssprache.** Mit einer Sprache, die einfach zu verstehen und zu schreiben ist, können Sie Informationen dokumentieren und teilen, auch wenn die Mitglieder Ihres Sicherheitsteams über unterschiedliches Fachwissen verfügen.
- **Einen offenen, unvoreingenommenen Ansatz.** Eine für Sie effiziente Automatisierungsplattform muss mit Ihrer gesamten Sicherheitsinfrastruktur und mit allen Anbieterumgebungen interoperabel sein.
- **Ein modulares, erweiterbares Design.** Mit einer modularen Plattform können Sie Automatisierung schrittweise implementieren. Durch die Möglichkeit der Erweiterung können Sie bei Bedarf zusätzliche und zukünftige Tools anderer Anbieter aufnehmen.

Bringen Sie Ihre Sicherheit voran – mit Red Hat

Red Hat Ansible Automation Platform bietet eine Basis für die Entwicklung und Ausführung von Automatisierungs-Services in großem Umfang und enthält alle Tools, die Sie zur Implementierung von Sicherheitsautomatisierung brauchen. Sie vereint eine einfache, leicht verständliche Automatisierungssprache mit einer bewährten, modularen Ausführungsumgebung und sicherheitsorientierten Funktionen für die Zusammenarbeit. Mit einer offen angelegten Basis können Sie fast alles in Ihrer Sicherheits- und IT-Infrastruktur verbinden und automatisieren. So erstellen Sie eine allgemeine Plattform für die Einbindung und den Austausch innerhalb Ihrer gesamten Organisation. Red Hat Ansible Automation Platform hat auch in anderen Bereichen zu erwiesenen Ergebnissen geführt, darunter IT- und Netzwerkoperationen und DevOps.

Eine Reihe von unterstützten **sicherheitsbezogenen Ansible Collections** – einschließlich Modulen, Rollen und Playbooks – ist in der Plattform enthalten. Diese Assets koordinieren die Aktivität von verschiedenen Sicherheitslösungen und sorgen so für eine einheitliche Reaktion auf Cyberbedrohungen und einheitliche Sicherheitsabläufe:

- Verkettung von Workflows und Playbooks zur modularen Wiederverwendung
- Konsolidierung und Zentralisierung von Protokollen
- Unterstützung von lokalen Verzeichnisdiensten und Zugriffskontrollen
- Integration von externen Anwendungen mithilfe von RESTful APIs

Red Hat Ansible Automation Platform umfasst außerdem Tools und Funktionen, mit denen Sie Ihre Automatisierung noch weiter optimieren können. **Automation Analytics** bietet Insights, wie Ihre Organisation Automatisierung nutzt. Mit **Automation Hub** können Teams über ein zentralisiertes Repository auf zertifizierte Automatisierungsinhalte zugreifen. Und **Content Collections** optimieren das Management, die Verteilung und die Nutzung von Automatisierungs-Assets.

Unterstützung von Experten erhalten

Red Hat unterstützt Sie dabei, eine erfolgreiche Automatisierung schneller zu erreichen.

- **Red Hat Services Program: Automation Adoption** bietet ein Framework für das Management einer unternehmensweiten Automatisierung.
- **Red Hat Training and Certification** bietet praktisches Training und nützliche Zertifizierungen, damit Sie Automatisierung effektiver einsetzen können.
- **Red Hat Support** verhilft Ihnen zu erfolgreichen IT-Prozessen. Der vielfach ausgezeichnete Web-Support[8] gibt Ihnen Zugang zu Best Practices, Dokumentation, Updates sowie Sicherheitswarnungen und -patches. Sie können sich auch direkt an einen Support-Engineer oder Technical Account Manager wenden, um Probleme zu beheben oder fachkundige Beratung zu erhalten.
- **Content Collections von zertifizierten Partnern** ermöglichen Ihnen, Hardware und Software von einer großen Auswahl an Anbietern einfach zu automatisieren. Diese vertrauenswürdigen, vordefinierten Automatisierungsinhalte sind über Automation Hub verfügbar und werden vom jeweiligen Partner und von Red Hat unterstützt.

8 Red Hat Customer Portal, Awards & Recognition

Automatisierung in der Praxis

Red Hat Ansible Automation Platform sorgt für nachgewiesenen Geschäftswert

Red Hat Ansible Automation Platform bietet Ihnen einen effizienten, optimierten Weg, Ihr Security Operations Center zu automatisieren. Analystenberichte von Organisationen, die Red Hat Ansible Automation Platform nutzen, belegen einen messbaren geschäftlichen Wert. **IDC** befragte mehrere Entscheidungsträger zu ihren Erfahrungen mit Red Hat Ansible Automation Platform und fand heraus, dass jedes Unternehmen durch eine Automatisierung deutliche Vorteile in Bezug auf Produktivität, Agilität und Betriebsabläufe verzeichnen konnte.

mehr Effizienz und Produktivität für IT-Sicherheitsteams[9]

mehr Effizienz bei der Minimierung von Sicherheitsvorfällen[9]

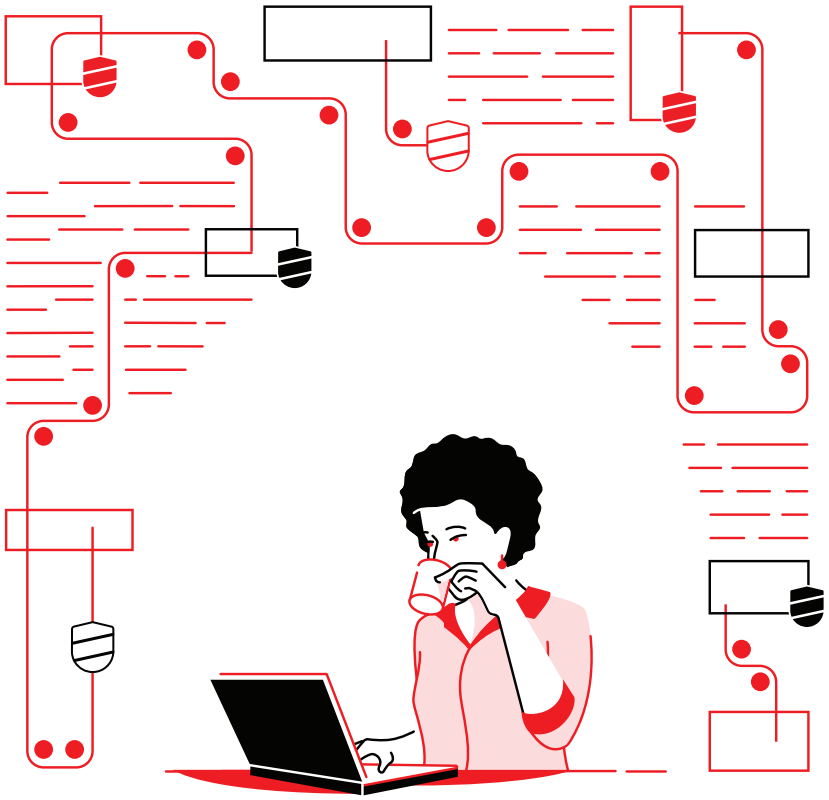
mehr Effizienz bei der Anwendung von Sicherheits-Patches[9]

„Red Hat Ansible [Automation Platform] schafft es hervorragend, unsere IT-Teams zusammenzubringen. Unsere Server-, Sicherheits-, Netzwerk- und Datenbankteams können alle auf ihren verschiedenen Ebenen arbeiten und anschließend mit Red Hat Ansible Automation ihre eigenen Playbooks erstellen.“[9]

9 IDC White Paper, gesponsert von Red Hat. „Red Hat Ansible Automation Improves IT Agility and Time to Market“, Juni 2019.

Sind Sie bereit für ein vereinfachtes Security Operations Center?

Mithilfe der Automatisierung können Sie wachsende Sicherheitsbedrohungen schneller und in größerem Umfang erkennen und darauf reagieren. Mit Red Hat können Sie Ihr Unternehmen schützen, indem Sie Ihre Sicherheitsteams, Tools und Prozesse mit einer konsistenten, kollaborativen Automatisierungsplattform verbinden.



Erfahren Sie, wie Sie die Sicherheit mit der Red Hat Ansible Automation Platform automatisieren

F24343_0720_KVM

Red Hat | IBM