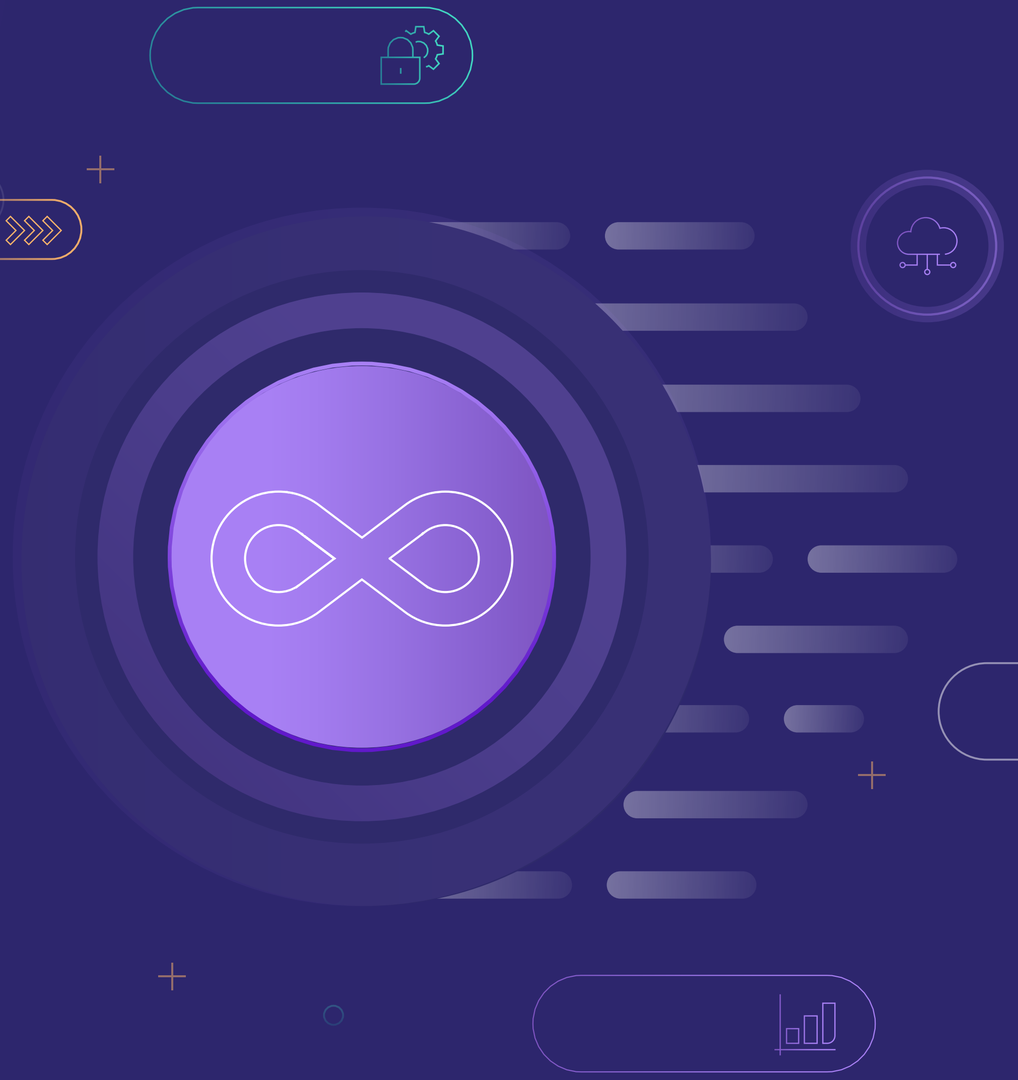
GitLab

Ein praktischer Leitfaden zur schnelleren Entwicklung sicherer Software mit DevSecOps

Erfahre mehr über die Erfolgsgeschichten von Unternehmen wie CARFAX, Lockheed Martin und Southwest Airlines



Inhalt

Da DevSecOps heute eine wichtige Komponente in der Softwareentwicklung darstellt, suchen Führungskräfte oft nach bewährten Strategien, die sie einführen oder mit denen sie ihre bestehenden Verfahren verbessern können. Heutzutage ist jeder für die Sicherheit verantwortlich. Deshalb ist es unerlässlich, sie nahtlos in den Entwicklungszyklus zu integrieren.

DevSecOps ist ein umfassender Ansatz, der Entwicklung, Sicherheit und Vorgang in einem integrierten Prozess vereint. Dieser Übergang kann wie eine große Herausforderung wirken: Welche Vorteile hat es, die Sicherheit nach links zu verlagern? Welche Rolle spielt die Automatisierung von Sicherheitsscans? Wie lässt sich die Software-Lieferkette am besten absichern? Wie können Teams die Vorteile der künstlichen Intelligenz (KI) nutzen? Was können sie tun, um die Konformität mit verschiedenen Vorschriften leichter zu gewährleisten? Aber mit praktischen Einblicken von Branchenexpert(inn)en, die diese Maßnahmen erfolgreich umgesetzt haben, wird der Weg klarer und verständlicher.

Verschiedene zukunftsorientierte Unternehmen, von global agierenden Reiseagenturen bis hin zum öffentlichen Sektor, haben DevSecOps und die dazugehörigen Methoden eingeführt – mit dem Erfolg der KI-gestützten Plattform von GitLab. In diesem Leitfaden erfährst du, wie du die Sicherheit mit automatisierten Tools erhöhst, wie du eine einzige Quelle der Wahrheit für die Konformität mit Vorschriften schaffst, wie du sicherstellst, dass die Tools auf dem neuesten Stand sind, und wie du die besten Sicherheitsmethoden in den gesamten Softwareentwicklungszyklus integrierst. Erfahre, wie Lockheed Martin, CARFAX und andere führende Unternehmen ihre Sicherheitstaktiken neu definiert haben, um die Bedürfnisse ihrer Kund(inn)en besser zu erfüllen.

Legen wir los.

> „Und die Sicherheitsfunktionen der Plattform sind so effizient, dass sie alles abdecken, wonach ich suche. Jetzt habe ich eine einzige Quelle der Wahrheit für Governance-, Konformitäts- und Sicherheitsaudits.“
>
> **Nadav Robas,**
> **DevOps- & DevSecOps Manager,**
> **Agoda**

78 %

der Befragten gaben an, dass sie eine DevSecOps-Plattform nutzen, und bewerteten die Sicherheitsbemühungen ihrer Organisation eher als „gut“ oder „ausgezeichnet“, verglichen mit 66 % der Nichtnutzer(innen).

(Laut dem Globalen DevSecOps-Bericht 2023)

27 %

der Befragten gaben an, dass sie eine DevSecOps-Plattform nutzen, und sie erwähnten mit höherer Wahrscheinlichkeit, dass sie die Sicherheit nach links verschoben haben, verglichen mit 13 % der Nichtnutzer(innen).

(Laut dem Globalen DevSecOps-Bericht 2023)

CARFAX erhöht die Sicherheit durch Automatisierung und Linksverschiebung

CARFAX, Inc. mit Sitz in den USA hilft jeden Tag Millionen von Menschen bei der Suche nach einem Fahrzeug. Mit mehr als 31 Milliarden Datensätzen verfügt CARFAX über die umfangreichste Fahrzeugdatenbank Nordamerikas. Viele der CARFAX-Kund(inn)en interagieren online mit dem Unternehmen. Deshalb ist CARFAX auf Software angewiesen, um Kundenbeziehungen zu pflegen und auszubauen und der Konkurrenz einen Schritt voraus zu sein. Um dies zu erreichen, muss das Unternehmen effizient und sicher neue, innovative und sichere Software entwickeln.

Für CARFAX machte die Einführung einer zentralisierten DevSecOps-Plattform den Unterschied aus. Mark Portofe, Director of Platform Engineering bei CARFAX, sagt, dass das Unternehmen durch die Nutzung automatisierter Testtools, die in die End-to-End-Anwendung integriert sind, wie z. B. die Abhängigkeitssuche und Container-Scanning sowie die Erkennung von Geheimnissen, an Effizienz gewonnen und ein ganz neues Maß an Sicherheit erreicht hat.

„Wir denken immer an Sicherheit, während wir Software entwerfen und entwickeln“, sagt Portofe. „Es geht nicht nur darum, Funktionen zur Verfügung zu stellen, sondern auch darum, sicherzustellen, dass diese Funktionen sicher sind. Das ist Teil jedes Schritts im Softwareentwicklungszyklus. Das spart Zeit und erhöht unsere Sicherheit.“

Lies mehr darüber, wie CARFAX fast ein Drittel seiner Sicherheitslücken viel früher in der Entwicklung erkennt.

30 %

der Sicherheitslücken wurden früher im SDLC gefunden

„Sicherheit ist zwar ein ständiger Kampf, aber die Sicherheitsfunktionen von GitLab machen es den Entwickler(inne)n leichter, Probleme frühzeitig zu erkennen.“

Mark Portofe,
Director of Platform Engineering, CARFAX

Lockheed Martin verbessert die Sicherheitslage und vereinfacht Konformitätsaufgaben

80 x

schnellere CI-Pipeline-Builds

„Die Teams sind sich jetzt der Sicherheitslage des Codes, den sie schreiben, auf eine Weise bewusst, die sie vorher nicht kannten. Das ermöglicht Gespräche über die Sicherheit unserer Software, die auf die bisherige Weise nicht möglich waren.“

Alan Hohn,
Director of Software Strategy,
Lockheed Martin

Die Lockheed Martin Corp. ist ein amerikanischer Gigant in den Bereichen Luft- und Raumfahrt, Verteidigung, Informationssicherheit und Technologie. Es handelt sich dabei um das größte Verteidigungsunternehmen der Welt. Seine DevSecOps-Teams haben die Aufgabe, Software für Tausende von Programmen effizient, sicher und schnell zu entwickeln und bereitzustellen – von Satellitenplattformen und Luftfahrtsystemen bis hin zu Bodenkontrollsoftware und maritimer Software für den Über- und Unterwasserbereich.

Da Lockheed Martin mit dem Verteidigungsministerium und anderen Bundesbehörden zusammenarbeitet, entwickelt das Unternehmen Systeme, die für die nationale Sicherheit entscheidend sind. Das bedeutet, dass die Entwicklung sicherer Software und die Konformität mit staatlichen Vorschriften sowohl für Lockheed Martin als auch für seine Kunden von zentraler Bedeutung sind. Um dieses Ziel zu erreichen und die komplexe Toolchain zu vereinfachen sowie die Zusammenarbeit zu verbessern, entschied sich das Unternehmen für einen umfassenden Ansatz, der Entwicklung, Sicherheit und Vorgänge in ein einheitliches Framework integriert.

Eine Herausforderung für jedes Unternehmen, das Toolchains einsetzt, besteht darin, dass man aufgrund der schieren Größe und Komplexität der Kette leicht einmal ein Update verpassen kann. Mit dieser Plattform muss sich Lockheed Martin keine Sorgen mehr über nicht aktualisierte Tools machen, denn mit einer einzigen, umfassenden Anwendung muss ein Update nur einmal durchgeführt werden und jede Instanz ist abgedeckt. Zudem ist eine standardisierte Reihe von automatisierten Sicherheitsfunktionen nahtlos integriert.

Außerdem nutzt das Unternehmen das Compliance Framework von GitLab, um die Softwarequalität durchzusetzen, und die Automatisierung, um Releases und Abhängigkeitsmanagement effizienter und schneller zu machen.

Hier findest du weitere Informationen darüber, wie eine DevSecOps-Plattform Lockheed Martin dabei hilft, Konformitätsaufgaben zu vereinfachen.

Die Deutsche Telekom geht gegen Ineffizienzen vor, ohne die Sicherheit zu beeinträchtigen

Die Deutsche Telekom AG, Europas führendes Telekommunikationsunternehmen, bedient mehr als 240 Millionen Mobilfunkkunden, 26 Millionen Festnetzanschlüsse und 22 Millionen Breitbandanschlüsse in über 50 Ländern. Um die Softwareentwicklung zu optimieren und die Zusammenarbeit zu verbessern, entschied sich das Unternehmen für DevSecOps. All das wurde erreicht, und auch die Sicherheitsmaßnahmen wurden effizienter.

Durch die Integration von Sicherheitsfunktionen in eine Anwendung konnte die Deutsche Telekom die Sicherheit nach links verlagern, so dass ihre Teams Probleme finden und beheben konnten, bevor sie in der Entwicklungspipeline voranschritten – und schwieriger und kostspieliger zu beheben gewesen wären.

Thorsten Bastian, Business Owner des CI/CD Hubs der Telekom IT, stellt fest, dass die in einer Anwendung integrierten Sicherheitsfunktionen es ihnen ermöglichen, sofort an die richtige Stelle zu springen und jedes Problem zu beheben. „Dies erhöht die Effizienz im Umgang mit Sicherheitsvorfällen“, sagt er.

Norman Stamnitz, Produktmanager für die CI/CD-Toolsuite der Telekom IT – die auf GitLab, und im Fall der Deutschen Telekom auf GitLab Ultimate, aufbaut – stellt ebenfalls fest, dass sie mit einem einzigen Dashboard ihre Bemühungen um Sicherheit und Konformität verbessern konnten. „Wenn man die manuellen Sicherheitsprozesse reduzieren und all diese Sicherheitsscans vor dem Go-Live durchführen kann, erhält man die Möglichkeit, die Entwicklungsgeschwindigkeit zu erhöhen oder die Zeit bis zur Markteinführung noch weiter zu verkürzen“, sagt er. „Und natürlich wollten wir die Linksverschiebung einführen. Wir wollten, dass Sicherheitsscanner zu den täglichen Aufgaben unserer Entwickler(innen) gehören.“

Weitere Informationen darüber, wie die Deutsche Telekom eine 6-mal schnellere Markteinführung und verbesserte Sicherheit erreicht hat.

6 x

schnellere Markteinführung

„Wir haben uns für GitLab Ultimate entschieden, weil wir die Sicherheits- und Konformitätsfunktionen sowie ein All-in-One-Sicherheits-Dashboard nutzen wollten.“

Norman Stamnitz,
Product Manager,
Telekom IT

Der Online-Reiseriese Agoda reduziert das Überangebot an Sicherheitstools und setzt auf KI

3.000

Stunden eingesparte Entwicklerzeit pro Quartal

„Und die Sicherheitsfunktionen der Plattform sind so effizient, dass sie alles abdecken, wonach ich suche. Jetzt habe ich eine einzige Quelle der Wahrheit für Governance-, Konformitäts- und Sicherheitsaudits.“

Nadav Robas,
DevOps & DevSecOps Manager,
Agoda

Agoda hat seinen Sitz in Singapur und bietet seinen Kund(inn)en günstige Angebote für ein globales Netzwerk von 3,6 Millionen Hotels und Ferienunterkünften sowie Buchungen für Flüge, Flughafentransfers und Aktivitäten. Das Unternehmen, das mehr als 6.600 Mitarbeiter(innen) in 31 Märkten beschäftigt, konzentriert sich darauf, seine Softwareentwicklungsteams in die Lage zu versetzen, schnell zu arbeiten, effizient zusammenzuarbeiten und sicherzustellen, dass die Apps, die sie entwickeln, für Kund(inn)en weltweit sicher sind.

Nadav Robas, DevOps & DevSecOps Manager bei Agoda, sagt, dass das Unternehmen vor der Einführung einer DevSecOps-Plattform im Jahr 2021 viel Zeit damit verbracht hat, Upgrades und Sicherheitspatches nachzuziehen. Jetzt, da sie eine einzige Anwendung verwenden, konnte Agoda die Sicherheit erhöhen und gleichzeitig die Erfahrung der Entwickler(innen) verbessern, so dass diese zufriedener denn je sind, egal ob sie eine mobile App entwickeln oder die Unterstützung für eine neue Sprache einführen. „Wir sind produktiver, sicherer und unsere Entwickler(innen) haben eine bessere Arbeitsatmosphäre“, sagt er.

Für die Zukunft bereitet sich Agoda darauf vor, die in die Anwendung integrierten KI-Funktionen zu nutzen, um die Softwareentwicklung und die Sicherheit weiter voranzutreiben. „Wir sind begeistert von den KI-gestützten Funktionen von GitLab, nicht nur für die Programmierung, sondern für den gesamten Lebenszyklus der Softwareentwicklung, wie es der Vision von GitLab entspricht“, sagt Nadav.

Erfahre, wie Agoda DevSecOps einsetzt, um Sicherheitsrichtlinien aufzustellen und durchzusetzen und die Sicherheit nach links zu verlagern.

CACI ist besser auf die Einhaltung von Sicherheitsanforderungen vorbereitet

CACI International Inc. ist ein 6,7-Milliarden-Dollar-Unternehmen, dessen Technologie und Fachwissen eine wichtige Rolle für die nationale Sicherheit der USA und die Modernisierung der Regierung spielt. Das Unternehmen hat sich einen Namen gemacht, indem es kritische Software und softwaregestützte Hardware an US-Regierungsbehörden, den US-Geheimdienst und das Verteidigungsministerium geliefert hat. Einer der Gründe für den Wechsel zu einer DevSecOps-Plattform war die Erhöhung der Sicherheit bei gleichzeitiger Steigerung der Effizienz und Produktivität im gesamten Softwareentwicklungszyklus.

Der technische Projektleiter bei CACI, Wesley Monroe, sagt, dass sie nach einer Anwendung gesucht haben, die alle DevSecOps-Funktionen, wie z. B. Automatisierung, vereint. „Mit all den Roadmapping-, Problemverfolgungs- und Sicherheitsscans an einem Ort ist es sschwierig, die neue Lösung mit unseren vorherigen Tools zu vergleichen“, fügt er hinzu.

Die Einhaltung von Gesetzen, Vorschriften und Standards der Regierung ist für einen staatlichen Auftragnehmer von entscheidender Bedeutung. Einer der größten Vorteile der GitLab-Plattform besteht darin, dass CACI damit auf neue Anforderungen an die Sicherheit vorbereitet ist. Das bedeutet nicht nur, konform zu sein, sondern dies auch nachweisen zu können. Da die gesetzlich vorgeschriebenen Daten nachverfolgt und gespeichert werden, kann das Unternehmen die Einhaltung der Sicherheitsstandards bescheinigen und mit den Daten untermauern. „Wir haben uns so aufgestellt, dass wir die zukünftigen Sicherheitsanforderungen erfüllen können“, sagt Kyle Craft, CSDE Service Lead bei CACI.

Erfahre noch mehr darüber, wie CACI automatisierte Testwerkzeuge einsetzt und die gesetzlichen Vorschriften erfüllt.

3 x

schnelleres Sicherheits-Scanning

„Wir haben uns an GitLab gewandt, um die Art und Weise, wie wir Software schnell entwickeln und erstellen, zu überdenken und zu verändern, ohne dabei die Sicherheit zu gefährden.“

Glenn Kurowski,
Senior Vice President und CTO, CACI

2019

Beginn der Zusammenarbeit mit GitLab

„Wir wollen, dass Entwickler(innen) schnell ein Problem nachschlagen und eine Lösung finden können. Außerdem sollte Kontextwechsel reduziert werden.“

Jim Dayton,
Vice President und CISO,
Southwest Airlines

Southwest entdeckt Scan-Konsistenz und spricht über die Verheißungen von KI

Southwest Airlines Co. ist mit 800 Flugzeugen, 4.000 Flügen pro Tag und rund 60.000 Beschäftigten die größte Billigfluggesellschaft der Welt. Das Unternehmen mit Sitz in den USA hat sich für einen DevSecOps-Ansatz bei der Anwendungsentwicklung entschieden, um die Arbeit seiner Softwareentwickler(innen) zu erleichtern. Die Umstellung ermöglichte es ihnen, Entwickler(inne)n mehr Self-Service-Funktionen und Wissensmanagementprozesse anzubieten.

Jim Dayton, Vice President und Chief Information Officer von Southwest, sieht großes Potenzial in den KI-Funktionen, die in den DevSecOps-Prozess der Plattform integriert sind.

Generative KI, ob in Form von Erklärungen zu Sicherheitslücken, Codevorschlägen oder Codevervollständigung, hat die Fähigkeit, die Arbeitsabläufe im gesamten Softwareentwicklungszyklus drastisch zu beeinflussen. Der Einsatz von integrierten KI-Tools kann die Sicherheit erhöhen und den Zeitaufwand für Code Reviews und Anwendungsentwicklung verringern. „Ich denke, ein gutes Beispiel ist, wenn es eine Lösung für eine Sicherheitslücke bietet, die gerade entdeckt wurde, oder wenn es uns sagen kann, was ein Teil des Codes tut“, sagt er. „Womit wird es integriert? Auf welche Daten wird zugegriffen und warum? Sag mir zum Beispiel im Klartext, dass dieser bestimmte Code für 20 % der Vorfälle in dieser Anwendung im letzten Jahr verantwortlich war. Hier kann KI meiner Meinung nach helfen.“

In diesem Blogbeitrag erfährst du, welches Potenzial der Chief Information Security Officer von Southwest in KI sieht.

Möchtest du die bewährten Methoden für DevSecOps in die Praxis umsetzen?

Starte mit einer **kostenlosen Testversion** der DevSecOps-Plattform von GitLab. Oder wende dich an **unsere DevSecOps-Expertinnen und -Experten**.

Mehr erfahren

Sprich mit einem Experten/einer Expertin >

GitLab

Software.
Faster.