DevSecOps

أحدأهداف DevOps هو تقديم تحديثات برامج سريعة وعالية الجودة. ولكي تكون البرامج ذات جودة عالية، يجب أن تلبيمتطلبات الأمن السيبراني الصارمة. وهنا يأتي دور أمان DevOps، أو DevSecOps. في هذا الدرس، ستستكشفDevSecOps وفحوصات الأمان الخاصة به واعتماده على التشغيل الآلي.

ماهو DevSecOps؟

DevSecOpsهو امتداد لـ DevOps الذي يقوم بأتمتة عمليات التحقق من الأمان طوال دورة حياة تطوير البرامج (SDLC) لمنع الثغرات الأمنية في المنتج النهائي. **أوهن**هي نقطة ضعف محتملة، مثل فقدان تشفير البيانات، والتي يمكنلأي شخص استغلالها في النظام.

تقليدياً،قام المطورون بكتابة معظم أكواد الإنتاج دون أخذ الأمان في الاعتبار، وفقط في نهاية SDLC سيقوم فريق الأمانباختبار البرنامج. ينجح هذا الأسلوب عندما تأتي التحديثات عدة مرات فقط في السنة، لكن فرق DevOps تنتج التحديثاتكل بضعة أسابيع أو أقل.

باستخدامDevSecOps، يقوم المطورون بدمج الأمان في كل خطوة من خطوات SDLC. تدرس الفرق التهديدات الأمنيةالمحتملة وتخطط لها في وقت مبكر، وتقوم باختبار التعليمات البرمجية وفحصها وتدقيقها ومراجعتها طوال فترةالتطوير.

عناصر

تشملالمكونات الرئيسية لـ DevSecOps المسؤولية المشتركة والسرعة والجودة والفحوصات الأمنية والأتمتة.

المسؤوليةالمشتركة

فيDevSecOps، يتقاسم الجميع - فرق التطوير والعمليات والأمان - المسؤولية عن الأمن.

- يجبأن يفهم أعضاء الفريق استراتيجيات أمان التطبيق والتخفيف الأساسية.
- يجبعلى أعضاء الفريق متابعة التحديثات الخاصة بـمشروع أمان تطبيقات الويب المفتوحة (OWASP) أعلى10، قائمة قياسية بالمخاطر الأمنية الحرجة لتطبيقات الويب.
- يجبعلى المطورين الموافقة على ممارسات الترميز الآمنة واتباعها.

السرعةوالجودة

تتطلبالمشكلات الأمنية في التطبيق الوقت والمال لإصلاحها، خاصة تلك التي تم العثور عليها متأخراً في SDLC، ويمكنأن تؤخر الإصدار بشكل كبير.

باستخدامDevSecOps، تتولى الفرق مسؤولية الأمان بدءاً من مرحلة التخطيط فصاعداً، وتقوم بتحديد المشكلات الأمنيةومعالجتها مبكراً وبسرعة. وبهذه الطريقة، يمكنهم الاستمرار في تقديم تحديثات صغيرة ومستمرة وعالية الجودة.

التفتيشالأمني

معDevSecOps، يخضع البرنامج للعديد من فحوصات الأمان عبر SDLC. دعونا نناقش بعض الفحوصات القياسية.

- **نمذجةالتهديد**هي عملية تقوم فيها الفرق بتحديد وتصنيف التهديدات الأمنية لمراعاة تطوير البرامج ودعمها.تحدث نمذجة التهديدات عادةً أثناء مرحلة التصميم أو التخطيط للتطوير قبل أن يكتب المطورون التعليماتالبرمجية.
- **عملياتفحص الثغرات الأمنية**تحديد نقاط الضعف في التطبيق ومن المكتبات (مجموعات التعليمات البرمجيةالقابلة لإعادة الاستخدام) التي يعتمد عليها التطبيق. يمكن للفرق أتمتة عملية التصحيح لمعالجة الثغراتالأمنية في أسرع وقت ممكن. هناك نوعان من عمليات فحص الثغرات الشائعة وهما اختبار أمان التطبيقالثابت واختبار أمان التطبيق الديناميكي.
- **اختبارأمان التطبيقات الثابتة (SAST)**تقوم الأدوات بالبحث عن نقاط الضعف داخل الكود ومكتباته. "ثابت " يعني أن التطبيق لا يتم تنفيذه؛ انها في راحة.
- **اختبارأمان التطبيقات الديناميكي (DAST)**تكتشف الأدوات نقاط الضعف التي يمكن ملاحظتها خارج التعليماتالبرمجية أثناء تشغيل التطبيق. وللقيام بذلك، تحاكي هذه الأدوات تقنيات القرصنة الحقيقية مثلحقن SQL لاكتشاف نقاط الضعف التي يمكن لمجرمي الإنترنت استغلالها.
- **كشفالأسرار**تبحث عمليات المسح عن الأسرار التي يتركها المطورون عن طريق الخطأ في التعليمات البرمجيةأو ملفات التكوين. الأسرار هي بيانات اعتماد حساسة مثل كلمات المرور ومفاتيح التشفير، ويجب علىالمؤسسات حمايتها من التسريبات. إذا وجدت الأسرار طريقها إلى قاعدة التعليمات البرمجية للتطبيق، فقديجدها مجرمو الإنترنت.
- **اختباراتالوحدة**هي اختبارات تقيم مكوناً واحداً أو وحدة واحدة من التطبيق للتحقق من أداء المكون بشكل صحيح.يتم تشغيل هذه الاختبارات عندما يرسل المطورون تعليمات برمجية مكتوبة حديثاً لدمجها في قاعدة التعليماتالبرمجية الرئيسية للبرنامج. في DevSecOps، يصمم المطورون اختبارات وحدة إضافية تسمى **اختباراتوحدة الأمن**التي تحقق من وجود مشاكل أمنية.

- **المراقبةالأمنية**تقوم الأدوات بمراقبة التطبيقات المباشرة لمشاكل الأمان مثل الهجمات الإلكترونية وإرسال تنبيهاتفورية عند حدوث مثل هذا النشاط. وبهذه الطريقة، يمكن للموظفين الاستجابة بسرعة لتقليل الضرر وتصحيحالتطبيق إذا لزم الأمر.

أتمتة

تعدالأتمتة أمراً ضرورياً لـ DevOps، ولا يختلف DevSecOps عن ذلك.

يمكنلأدوات التكامل المستمر والتسليم المستمر (CI/CD) أتمتة عمليات التحقق من الأمان خلال كل مرحلة من مراحلSDLC تقريباً، مما يتيح للجميع التركيز على المهام الأخرى.

- تتحققأدوات الأتمتة من اجتياز التعليمات البرمجية لاختبارات وحدة الأمان ومن أن تبعيات البرامج موجودةعلى أحدث التصحيحات الخاصة بها.
- تكتشفأدوات SAST الثغرات الأمنية في التعليمات البرمجية الجديدة قبل أن يقوم المطورون بدمجها في قاعدة التعليمات البرمجية الخاصةبهم.
- تقومأدوات DAST بتقييم التحديثات في بيئة ما قبل الإنتاج.
- يمكنللأدوات أتمتة تكوين الأنظمة والخدمات، مما يضمن الامتثال الأمني ويقلل الأخطاء البشرية.