

FortiDevSec

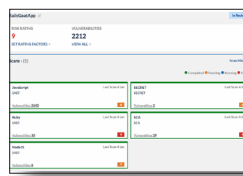
提供形態：



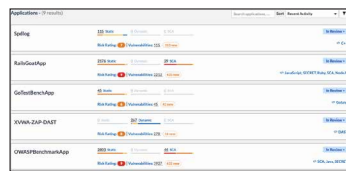
ホスティング

CI / CD パイプラインでの 継続的なアプリケーションセキュリティテスト

ソフトウェアアプリケーションがあらゆる場所に存在するようになり、ビジネスソフトウェアアプリケーションを迅速に開発して展開する能力が、あらゆるビジネスの成功を左右するようになりました。



市場投入までの時間が極めて重要であるため、従来のウォーターフォール方式のアプリケーション開発では対応できなくなりました。ウォーターフォール方式では、アプリケーションの変更は数カ月に1度程度で、開発チームは、前のステップが正常に完了した場合にのみ、次の開発やテストフェーズに進むので、市場投入までの時間が長くなるという課題があります。



アプリケーションの開発と展開を迅速に進めるために、多くのアプリケーション開発チームがアジャイルと DevOps の方法論を採用するようになりました。アジャイルモデルでは、開発とテストの工程が同時進行し、継続的に繰り返されます。アプリケーションの変更はクラウドに展開されることも多く、開発、機能、AppSec（アプリケーションセキュリティ）のテストを担当するチームは、緊密なコラボレーションとコミュニケーションを迅速なターンアラウンドタイムで実行する必要があります。このような状況から、アプリケーションの構築とクラウドへの展開のワークフローの自動化が必要とされるようになり、結果として、CI / CD（継続的インテグレーション / 継続的デリバリー）ツールを使用してこの自動化を可能にする DevOps が大きな役割を果たすようになりました。

AppSec（アプリケーションセキュリティ）テストも自動化することで、この CI / CD パラダイムで動作するようにし、開発サイクルの初期段階に組み込むようにすることが求められています（一般的にシフトレフトと呼ばれます）。ところが、多くの AppSec テスト製品は、AppSec の専門知識が少ない開発者や DevOps のユーザーエクスペリエンスをサポートするようにネイティブに構築されていないため、製品が効果的に使用されているとは言えません。端的に言えば、DevSecOps は実現していないということです。

DevSecOps は、開発（Development）、セキュリティ（Security）、運用（Operations）の略称で、ソフトウェア開発ライフサイクルの初期段階である設計から、統合、テスト、デプロイ、ソフトウェアデリバリーまでのあらゆる段階でセキュリティの統合を自動化するものです。

主なメリット

- DevSecOps の自動化：**アプリケーションセキュリティを DevOps プロセスにネイティブに組み込むため、アプリケーションセキュリティの十分な専門知識は不要
- 攻撃対象領域全体の可視化：**ソースコード、オープンソースコンポーネント、ランタイム攻撃ベクトルなどの Web アプリケーションのあらゆるセキュリティリスクを把握
- 統合ダッシュボード：**使いやすいポータルで、さまざまなタイプのスキャンで見つかったセキュリティリスクを正規化し、集約し、一元管理が可能
- セキュリティ問題の最適な優先度判断：**あらゆるタイプのスキャンがインテリジェントに分析され、セキュリティの問題をランク付けして表示
- 利用と管理の簡素化：**セットアップと管理のオーバーヘッドを排除でき、スキャナのセットアップやアップデートも必要なく、最新のスキャナが自動的にセットアップされる。すべてのスキャンの構成が統一され、サイロ化されたプラグインは不要

ハイライト

革新的な製品

AppSec のテストはさらに、細かく断片化されています。アプリケーションの脆弱性をすべて把握するために実行する必要がある AppSec スキャンには多くのタイプがあり、これらは通常、異なる製品によって提供されています。複数の製品で構成されるソリューションに起因する断片化が、DevSecOps による AppSec の実現を阻害します。

DevSecOps が DNA に組み込まれた革新的な AppSec 製品、すなわち、セキュリティの専門知識を必要とすることなく、開発者や DevOps が簡単に利用でき、SAST、DAST、SCA、Secrets などのあらゆるタイプの AppSec スキャンをサポートする包括的な製品が必要とされています。

フォーティネットの DevSecOps 製品である FortiDevSec は、ソフトウェア開発者と DevOps に特化してゼロから構築された、クラウド / SaaS ベースの継続的なアプリケーションセキュリティテストを提供

最新のアプリ開発方式に対応する シンプルなセキュリティ

最新のアプリケーション開発は、アジャイル方法論による迅速なアプリケーション開発、クラウドネイティブ、マイクロサービスやコンテナベースのアーキテクチャの使用、CI / CD の使用によるビルドとデプロイの自動化の組み合わせによって実現し、そのためには、CI / CD におけるアプリケーションセキュリティテストを自動化する必要があります。

FortiDevSec は、開発者と DevOps の継続的なアプリケーションセキュリティテストのオーケストレーションと自動化により、これらのテストをアプリケーション CI / CD DevOps ライフサイクルに直接組み込みます。数行のコードを CI / CD にコピーするだけで、AppSec の専門知識を必要とすることなく、DevOps に FortiDevSec を統合でき、AppSec を DevOps と同じ速さで進められるようになります。FortiDevSec は、主要な CI / CD ツール、言語、フレームワークをすべてサポートしています。

FortiDevSec を利用することで、統一された yami 構成により、すべてのタイプのアプリケーションセキュリティスキャンに単一の自動化レイヤーが DevOps に提供されます。DevOps に複数のスキャナに対応する複数のプラグインを組み込む必要はありません。スキャナは Docker イメージで提供され、常に最新バージョンに更新されるため、全体として容易な管理が実現します。

します。FortiDevSec は、アプリケーションのセキュリティ脆弱性を開発ライフサイクルの初期段階で発見することで、アプリケーションセキュリティのシフトレフトアーキテクチャを可能にし、アプリケーションの本番稼働前に開発者が問題を迅速に発見して修正できるようにします。

FortiDevSec は、アプリケーションの DevOps CI / CD パイプラインにネイティブに統合、デプロイされ、ソースコード、サードパーティのライブラリ、シークレット、脆弱性やエクスプロイトのスキャンを含む包括的なアプリケーションスキャンを提供し、セキュリティの問題をまとめて、使いやすい Web ポータルで提示します。インテリジェントなノイズリダクションにより、開発者は、過剰な負担を回避しつつ、最も重要な脆弱性に優先的に取り組むことができます。


Easy integration into CI/CD platforms


```


SAST scan:
docker login --username $DOCKERHUB_USERNAME --password
$DOCKERHUB_PASSWORD
docker run --rm --mount type=bind,source=$PWD,target=/app,read-only
registry.fortinet-us.com/fortidevsecops:orgid: your-org-id-here
appid: your-app-id-here
# Optional param section starts
DAST scan:
docker login --username $DOC
$DOCKERHUB_PASSWORD
docker run --rm --mount type=
registry.fortinet-us.com/fortidevsecops:
buildtool: jenkins. # Optional param, values=jenkins|travis
scaanner: sast,dast,sca # Optional param, default is All
language: python, javascript # Optional param, default is Auto Detect


variables:
DAST_URL: https://your.url.com # Optional param
# Optional param section end
# end of file


```



Jenkins
(with plug in)



Harness
CI


GitHub
Action


Circle CI


Bamboo


Travis CI


Azure DevOps

ハイライト

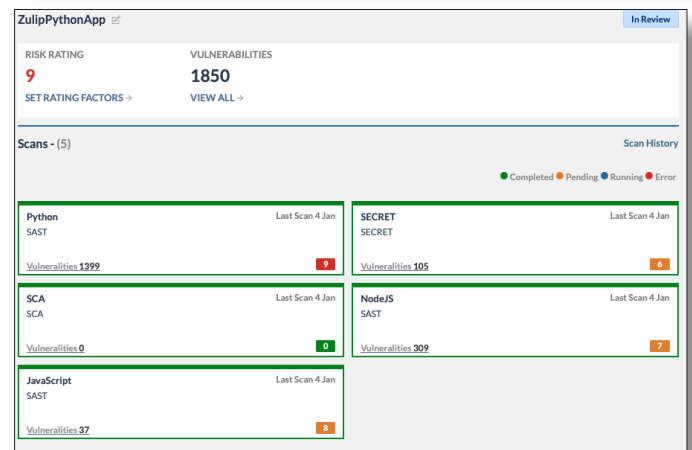
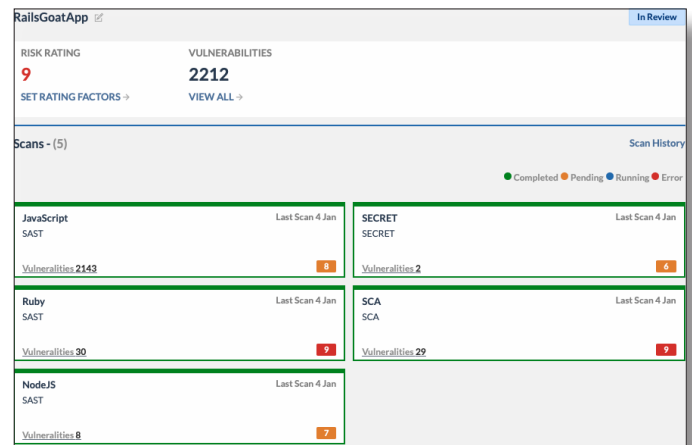
包括的な脆弱性管理

アプリケーションを複数の攻撃ベクトルから保護する必要があり、そのためには多くのタイプのスキャナを使用してセキュリティテストを実行する必要があります。

SAST（静的（またはソース）コードテスト）はアプリケーションそのもののソースコードをスキャンし、SCA / OSS はアプリケーションに含まれるサードパーティのライブラリ（通常はオープンソースライブラリ）をスキャンし、Secrets はコード内のオープンパスワードテキストをスキャンし、DAST（動的テスト）はフロントエンド経由で Web アプリケーションを分析し、攻撃をシミュレーションして脆弱性を発見します。

FortiDevSec は、SAST、SCA / OSS、Secrets、DAST などの複数のタイプのテストを組み込むことで、包括的な脆弱性管理を提供します。

FortiDevSec は、各アプリケーションを分析し、言語やフレームワークなどの属性に基づき、そのアプリケーションに必要な関連性のあるスキャンのタイプを自動的に選択します。スキャナは、FortiDevSec エージェントの Docker イメージとして自動的にダウンロードまたは更新されます。

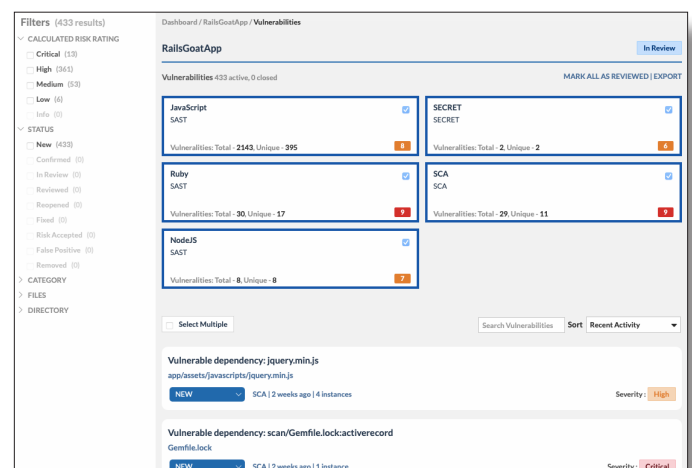


統合ダッシュボード

FortiDevSec には、ユーザーがログインして利用できる使いやすいポータルが提供されており、すべてのアプリケーション、すべてのスキャンタイプ、すべての問題をこのポータルで確認できます。複数の異なる断片化されたスキャナごとに複数のポータルを使用する必要はありません。

スキャン結果が最初に複数のスキャンタイプで正規化され、リスク評価、リスクカテゴリ、記述もすべて正規化されます。結果をさらに集計し、さまざまなフィルターを指定して表示することで、最も重要な項目を優先的に修正できるようになります。

報告される問題があまりに多いと、ほとんどの開発者は圧倒されてしまうものです。そのような状況を軽減するため、FortiDevSec は、複数のスキャンの結果をインテリジェントに相関付け、それに応じてリスク評価を判断します。結果として、報告される問題のノイズリダクションが可能になり、開発者は最も重要な問題の修正に集中できるようになります。



オーダー情報

FortiDevSec は、ユーザー数に基づくライセンスでご利用いただけます。このユーザーグループには通常、FortiDevSec でセキュリティをテストするアプリケーションに関わるすべての開発者が含まれます。DevOps、セキュリティ、管理などの FortiDevSec ポータルにアクセスする必要がある他のユーザーも、ユーザー数としてカウントする必要があります。FortiDevSec は現在、最大 5 ユーザーの SKU を提供しています。この SKU を積み上げ方式で利用することで、利用できるユーザーを増やすことができます。これらのユーザーがアクセスしてオンボーディングする（直接的に関わる）アプリケーションの数に制限はなく、FortiDevSec でのスキャンの数にも制限はありません。

| Product | Description |
|-------------|--|
| FortiDevSec | FortiDevSec - Standard functionality Tier - Unlimited scans and unlimited apps for all scanners for up to 5 developer users (all developers working on the target apps to be scanned are counted) - Annual Subscription. |



フォーティネットジャパン合同会社

〒106-0032

東京都港区六本木 7-7-7 Tri-Seven Roppongi 9 階

www.fortinet.com/jp/contact

お問い合わせ