

ブラック・ダック開発者向けセキュリティ・トレーニング

Secure Code Warrior 提供



開発チームとセキュリティ・
チームを支援するため、
ブラック・ダックと
Secure Code Warrior が提携

- ・コードの問題をより迅速に
修正
- ・後の工程での手直しを回避
- ・AI コーディング・アシスタント
を安全に採用

ブラック・ダックと
Secure Code Warrior の
連携により、開発者が
ビジネスにとって最も重要な
方法でセキュリティに
対応できるようになり、
セキュリティ・チームが
真のリスクを測定、管理、
軽減できるようになります。

アプリケーション・セキュリティ・テスト (AST) のリーダーであるブラック・ダックと、デベロッパーのリスク管理のリーダーである Secure Code Warrior は、DevSecOps における開発者主導のセキュリティに最も効果を発揮する共同ソリューションを提供するために提携を結びました。この統合型ソリューションにより、開発中にセキュリティの問題が発生するのを防ぎ、SDLC と CI/CD のパイプライン全体にわたるセキュリティ・テスト中に検出された問題の修正までの時間を短縮するクローズドループ戦略が確立されます。

DevSecOps における自発性を促す セキュリティ対策と教育

セキュリティの問題を最も簡単に解決する方法は、最初からプロジェクトに入り込ませないことです。この AI の時代において、セキュリティに精通したコード・コントリビューターの必要性がこれまで以上に高まっています。セキュリティ・チームと開発チームには、リスク許容度の限度を守り、事業目標の達成を支援するセキュリティ・トレーニング、可視性、ガバナンスが必要です。

Secure Code Warrior の開発者リスク管理プラットフォームでは、SDLC の早い段階でのプログラムによる観測機能、ガバナンス、教育に重点を置き、開発者主導のセキュリティに対する包括的かつ自発性を促す手法を用いることができます。

- ・業界初のベンチマーク・ツールである SCW Trust Score® により、CISO は時間の経過に合わせてプログラムの進捗と価値を測定し、基準に照らして評価し、向上させることができます。
- ・SCW Trust Agent を使用すると、リポジトリ単位でコミット制御を作成でき、開発者が脆弱性の発生を防ぐために必要なセキュア・コーディングの知識を持てるようになります。
- ・SCW プラットフォームは、開発者のワークフローに直接統合された、最も包括的で適切な AppSec トレーニング・コンテンツを提供します。

Secure Code Warrior トレーニングは、Black Duck Coverity® 静的解析、Seeker® インタラクティブ解析、Software Risk Manager™ に組み込まれており、開発者がコーディングする際にセキュリティ問題に直接対処することで、修正までの時間を短縮し、将来における問題再発を防ぎます。また、DevOps のワークフローを妨げることなく、開発チームやエンジニアリング・チームに関連する教育を提供することもできます。

特定のテクノロジー、プロジェクト、コンプライアンス基準、その他のビジネス・ニーズに合わせてカリキュラムをカスタマイズできます。

ブラック・ダックの AST ツールは、修正すべきセキュリティ・リスクの優先順位付けを支援し、開発者に問題に対処するための最も適切で効果的な教育とリソースを提供します。

開発者教育のための最も魅力的なプラットフォーム

開発者は、脆弱なアプリケーションに対する悪用や侵入を回避するための、組織における最初の防衛線です。その一方で、開発チームはセキュリティのツールやプラクティスの導入に苦勞することが多く、開発速度のためにセキュリティを犠牲にしていると思われるがちです。Secure Code Warrior プラットフォームは、セキュア・コーディングに取り組む開発者を育成するために、最も魅力的で適切なリソースを提供します。

- ・ **明確できめ細かいコース**：インタラクティブな短期集中形式で提供されるため、開発者はすでに行っている実際の作業の中で、知識を素早く学び、テストし、応用できます。
- ・ **インタラクティブかつ段階的なガイド付きウォークスルー**：開発者が脆弱性や安全でないコーディング・パターンを理解しやすくなります。
- ・ **没入型のコーディング・シミュレーション**：開発者に、リスクのない環境でセキュア・コーディングと攻撃的セキュリティ対策を実践する使命が与えられます。
- ・ **課題解決型演習**：実戦的シナリオが用意されており、開発者が問題のあるコードを特定し、最適な修正策を選択することで、ポイントを獲得し、チーム対抗戦で上位に進出できます。
- ・ **リアルタイムのフィードバックを伴うハンズオン・コーディング**：セキュアなブラウザベースの IDE で提供され、セキュリティ対策能力を育成します。また開発者がコーディングしている間に状況に応じたフィードバックとコーチングが行われます。
- ・ **セキュリティのトピックとコンセプトの広範なライブラリ**：初心者からセキュリティ・チャンピオンまで、さまざまな水準のスキルの開発者に合わせて作成されており、開発者に最も関連性の高い言語とフレームワークで提供されます。

Black Duck Coverity、Seeker、Software Risk Manager には、Secure Code Warrior プラットフォームの推奨トレーニングが統合されています。これらを組み合わせることで、セキュアなソフトウェア開発のための総合的なソリューションが実現します。

開発者は、Black Duck Code Sight™ IDE プラグインから直接、または個別に用意されたカリキュラムを通じて、検出されたリスクに関連するセキュリティ・トレーニングを受講することもできます。これにより、修正時間を短縮し、セキュリティ・プログラムの ROI を高めることができます。

ブラック・ダックについて

ブラック・ダックは、True Scale Application Security によって、モダン・ソフトウェアの経営レベルのリスクに対応し、規制された、AI を活用した世界におけるソフトウェアの信頼性を保証します。ブラック・ダックのソリューションは、セキュリティ、規制、ライセンスに関するリスクを排除しつつ、組織のスピード、精度、コンプライアンスのトレードオフから解放します。クラウドでもオンプレミスでも、コードが実行されるあらゆる場所でミッション・クリティカルなソフトウェアを保護するには、ブラック・ダックこそが選択肢となるのです。ブラック・ダックを活用することで、セキュリティ・リーダーはよりスマートな意思決定を行い、自信を持ってビジネス・イノベーションを推進することができます。詳しくは、www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社

www.blackduck.com/jp

©2025 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2025 年 11 月