Continuous Dynamic

従来および最新の web フレームワークと アプリケーションのための web アプリケーション・セキュリティ

現在の企業は、社外向け web サイト、顧客向けポータル、ショッピング・カート、ログイン・ページ、社内 HR ポータルなど、多岐にわたる web アプリケーションを運用しています。ビジネスを支えるこれらの基幹系 web アプリケーションは、その脆弱性を悪用することによって企業のバックエンド・データベースへのアクセスが可能になるため、ハッカーにとって魅力的な標的となっています。

Continuous Dynamic

Continuous Dynamic® は SaaS (Software-as-a-Service) 形式の動的アプリケーション・セキュリティ・テスト (DAST) ソリューションのため、スケーラブルな web セキュリティ・プログラムを迅速に導入できます。web サイトの数や、その更新頻度にかかわらず、Continuous Dynamic はあらゆる要求にスケーラブルに応えます。セキュリティ・チームと開発チームは、QA および本番環境において迅速、正確、そして継続的なアプリケーションの脆弱性診断が可能となります。Continuous Dynamic はハッカーと同じ手法を用いて弱点を見つけるため、ハッカーに悪用される前に先回りして弱点を修正できます。

Continuous Dynamic はクラウドベースのソリューションで、特別なハードウェアの設置やスキャニング・ソフトウェアのインストールは必要ありません。Continuous Dynamic には以下のような利点があります。

- 継続的な同時診断を無制限に実行
- web アプリケーションのコード変更を自動で検出して解析
- オープン API によるセキュリティ情報 / イベント管理ソリューション、バグ追跡システム、web アプリケーション・ファイアウォール (WAF) との統合

Continuous Dynamic はあらゆる環境にスケーラブルに適合し、1 万以上の web サイトに対して同時に診断を実行できます。さらに、見つかった脆弱性はすべてブラック・ダックのセキュリティ専門家による検証を受けるため、誤検知がほとんどありません。

人工知能と機械学習を活用

Continuous Dynamic は機械学習 (ML) と人工知能 (AI)、そして専門家による脆弱性分析を組み合わせることにより、動的アプリケーション・セキュリティ・テストの結果精度を最大限に高めています。このため、大量の誤検知による開発スピードの低下を心配することなく、web アプリケーションのセキュリティを検証できます。

Continuous Dynamic 独自の AI/ML モデルは、高度なトレーニングを受けたブラック・ダックの専門家が長年をかけて収集した貴重なデータを使用して開発されています。自動化により短時間で結果を得た後、専門家が検証を加えるこのアプローチにより、脆弱性をいち早く検出してサイバー攻撃への応答を迅速化できます。

Continuous Dynamic の仕組み

Continuous Dynamic は、自動アプリケーション・スキャンと世界最大級のセキュリティ専門家チームを組み合わせており、ユーザーには検証済みの脆弱性と実践的なレポートが提示されます。

オンボーディング

URL、ログイン情報、スケジュールをユーザー側からご提供

初回スキャン

検出、微調整、構成

web サイト診断

無制限の診断、脆弱性検出、および検証

レポート

結果をポータルに表示。レポートはカスタマイズが可能

ニーズに合わせて選べる 3 つのエディションをご用意

Continuous PE (Premium Edition)	Continuous SE (Standard Edition)	Continuous BE (Baseline Edition)
・マルチステップ・フォームを使用した、コンプライアンス要件の厳格な基幹系の恒久的 web サイト向け ・SE の全機能にビジネス・ロジック・テスト機能を追加	・必ずしも基幹系でない恒久的 web サイト向け ・BE の全機能にマルチステップ・フォームおよびログインに関する問題のテスト機能を追加	・基幹系でない web サイトに適した基本構成のソリューション ・自動スキャンと脆弱性検証をサポートしており、低リスクの web サイトに最適

機能	説明	PE	SE	BE
継続的診断	web サイトを継続的にスキャンして、web アプリケーションのコード変更を自動で検出します。	●	●	●
脆弱性検証	検出された脆弱性はすべてセキュリティ専門家による検証を受けており、さらに AI も活用することで誤検知をほぼゼロに抑えています。	●	●	●
オンデマンドの再テスト	検出された脆弱性を修正後、オンデマンドで web サイトを再テストすることにより、正しく修正されたかを確認できます。	●	●	●
本番環境に対応	本番環境に影響しないペイロードのみを使用するため、性能の低下がありません。	●	●	●
Continuous セキュリティ・エンジニアへのアクセス	ポータル経由でセキュリティ専門家に何度でも直接アクセスして、修正ガイダンスを得ることができます。	●	●	●
Black Duck セキュリティ・インデックス	単一のスコアにより、web サイトのセキュリティ強度を一目で概観できます。	●	●	●
内部 QA/ ステージング環境のテスト	本番前の内部ステージング環境を徹底的にテストすることで、脆弱性が本番環境に紛れ込むのを防ぐことができます。	●	●	●
柔軟なレポート、分析機能、およびベンチマーク比較	柔軟なフォーマットをサポートし、事業部門ごとにデータを集約できるエンタープライズ・クラスのレポートおよび分析機能により、web サイト全体のセキュリティ・トレンドを概観できるほか、ベンチマーク機能によってスコアを業界平均値と比較することもできます。	●	●	●
シングルページ・アプリケーション	本番環境への影響なしにシングルページ・アプリケーションを完全に自動でスキャンします。	●	●	
完全な構成とフォームのトレーニング	フォームおよびログインを使用した web サイトを安全にスキャンできるようにスキャナーを設定します。	●	●	
認証されたスキャン	マルチファクター認証を含め、認証を必要とするサイトを自動でスキャンします。	●	●	
ビジネス・ロジック診断	ビジネス・ロジックの評価では、複雑なビジネス・ロジックやワークフローの脆弱性を発見します。これらの脆弱性は、アプリケーションの意図された動作をより深く理解する必要があり、自動化されたスキャナーだけでは発見できません。	●		

Continuous Dynamic の特長

容易な導入、同時テスト、スケーラブル

Continuous Dynamic は導入の容易なクラウドベースの動的セキュリティ・テスト・ソリューションで、10,000 を超える web サイトに対して同時にオンボーディングとテストを実施しても速度が低下しません。あらゆる環境にスケーラブルに適合し、開発ペースを維持できます。

継続的診断の手法

Continuous Dynamic は完全な継続的解析をサポートしており、更新の続く web サイトを常時スキャンできます。web アプリケーションのコード変更を自動で検出して解析でき、新たな脆弱性が見つかるとアラートを受け取ることができるほか、毎回完全なテストを実施しなくても脆弱性を再テストできるなど、「常時オン」のリスク診断が可能です。

本番環境に対応

Continuous Dynamic は本番環境の web サイトに実施しても性能の低下が生じないため、安心して導入できます。ライブ・コードに対して無害のインジェクションを実行することにより、データの完全性を確保します。また、スキャンのカスタム・チューニングにより、性能に影響を与えることなく完全なカバレッジが可能です。

誤検知をほぼゼロに抑えた検証済みの実践的な結果

検出された脆弱性はすべてセキュリティ専門家の検証を受けており、さらに AI も活用することで誤検知をほぼゼロに抑えています。これにより修正プロセスが合理化され、深刻度と脅威に基づく脆弱性の優先順位付けが容易になり、全体的なセキュリティ態勢を考慮しながら修正に専念できます。

柔軟なフォーマットによるエンタープライズ・クラスのレポート機能

Continuous Dynamic は強力なレポート機能を備えており、セキュリティ・プログラムの効果を把握しながら、アプリケーション・セキュリティ態勢の改善を図ることができます。問題修正の進捗率、修正に要した時間、脆弱性の発見からの経過時間など、トレンドや主要な統計値を監視する高度な分析機能もあります。また、リアルタイムおよび履歴データを追跡してリスクへの曝露状況の推移を測定するトレンド分析により、セキュリティの最も強い web サイトと最も弱い web サイトを一目で把握できます。

web セキュリティ専門家への無制限のアクセス

Continuous Dynamic では、web アプリケーション・セキュリティ・テスト専門家に無制限にアクセスしてカスタム修正ガイダンスを得ることができます。「Ask a Question」機能を利用して、いつでもポータルから直接セキュリティ専門家にアクセスできます。

オープン API による統合

Continuous Dynamic は、一般的なバグ追跡システム、セキュリティ情報 / イベント管理ソリューション、ガバナンス / リスク / コンプライアンス製品、web アプリケーション・ファイアウォール（WAF）との統合が可能です。

シングルページ・アプリケーションのスキャンを完全に自動化

Continuous Dynamic は、従来のアプリケーションに加えシングルページ・アプリケーションに対してもスキャンとテストを完全に自動で実行します。web アプリケーションをブラウザーにロードし、ユーザーと同じようにアプリケーションを操作します。本番環境に影響しない診断により、従来のスキャン・ツールでは検出できない脆弱性も見つけることができます。

PCI コンプライアンス

Continuous Dynamic は、内部および外部 web サイトに対し、検証を加えた脆弱性診断を継続的に実施することにより、PCI DSS 3.1 の要件を超える高い基準を満たします。Continuous PE には、PCI DSS の要件であるビジネス・ロジック診断の機能も含まれます。WAF との統合により脆弱性を修正する仮想パッチの作成もサポートされるほか、監査に必要なレポートも生成できます。

Black Duck セキュリティ・インデックス

Black Duck セキュリティ・インデックスは、全体的なアプリケーション・セキュリティを単一のスコアとして示したもので、web サイトのセキュリティ強度を一目で概観できます。このスコアは、インテリジェンス・メトリクスに関するブラック・ダックの豊富な経験、およびさまざまな業種の幅広い顧客基盤に基づいて包括的な指標データから算出されており、ユーザーの web サイト全体におけるアプリケーション・セキュリティの現状を正確に反映します。Black Duck セキュリティ・インデックスから得られる洞察により、リスクの軽減、時間の節約、アクティビティの優先順位付け、全体的なセキュリティの改善が可能になります。

Continuous Dynamic | 検出可能な脆弱性

技術的な脆弱性

脅威の分類

- 機能の悪用
- アプリケーション・コード実行
- アプリケーションの設定ミス
- autocomplete 属性
- ブルートフォース
- バッファオーバーフロー
- キャッシュ可能なセンシティブな応答
- クリックジャッキング
- コンテンツ・スプーフィング
- クロスサイト・リクエスト・フォージェリ
- クロスサイト・スクリプティング
- サービス拒否
- ディレクトリ・リスティング
- フィンガープリンティング
- フレーマブル・リソース
- HTTP レスポンス分割
- 不適切な入力確認
- 情報漏洩
- 安全でないインデックス化
- 自動化の停止が不適切
- 不適切な許可
- 不適切なパスワードポリシーの実装
- 不適切なパスワード回復
- 不適切なプロセス検証
- 不適切なセッション有効期限
- 不十分なトランスポート層の保護
- LDAP インジェクション
- メール・コマンド・インジェクション
- セキュア・ヘッダーの欠落
- HttpOnly 属性のないセッション・クッキー
- OS コマンド・インジェクション
- OS コマンドの実行
- パス・トラバーサル
- 推測可能なリソースの位置
- クエリー言語インジェクション
- リモート・ファイル・インクルード
- ルーティングの迂回
- サーバーの設定ミス
- セッション ID の固定化
- 証明書とセッションの推測
- SQL インジェクション
- SSI インジェクション
- パッチ未適用のソフトウェア
- 安全でないセッション・クッキー
- URL リダイレクトの悪用
- XML 外部実体参照
- XML インジェクション
- XPath インジェクション
- XQuery インジェクション

OWASP Top 10

- A1 - アクセス制御の不備
- A2 - 暗号化の失敗
- A3 - インジェクション
- A4 - 安全が確認されない不安な設計
- A5 - セキュリティの設定ミス
- A6 - 脆弱で古くなったコンポーネント
- A7 - 識別と認証の失敗
- A8 - ソフトウェアとデータの整合性の不具合
- A9 - セキュリティログとモニタリングの失敗
- A10 - サーバーサイドリクエストフォージェリ (SSRF)

* 製品ラインごとの互換性リストについてはお問い合わせください。

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。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