ブラック・ダックのソリューションを使用した EU サイバー・レジリエンス法への対応

製品セキュリティに対する包括的アプローチ

PDE とは

デジタル要素を備えた製品には、直接的または間接的なデータ接続機能を備え、製品機能に不可欠なデジタル・コンポーネントを持つすべてのソフトウェア / ハードウェア製品が含まれます。

- スマートフォン、ノート PC、IoT 機器
- 産業用制御システム
- スマート TV、コネクテッド・カメラ、スマート・サーモスタット
- モバイル・アプリ、デスクトップ・アプリケーション、組み込みファームウェア

欧州連合のサイバー・レジリエンス法（EU CRA）は、デジタル要素を備えた製品（PDE: Products with Digital Elements）に対する透明性、脆弱性管理、長期的セキュリティ維持ガイドラインの確保を目的に、ソフトウェア・ベンダー向けの重要な新要件を導入するものです。これらの新たな要件により、開発から販売後の監視までの製品ライフ・サイクル全体にわたって製品の品質とセキュリティを優先するように迫る、さらなる圧力がベンダーにかけられます。このような要件を満たすことは、特に成熟したアプリケーション・セキュリティ（AppSec）プログラムを持たない企業にとっては困難になる可能性があり、コンプライアンス・コスト、制裁金、市場投入の遅延、リスクの増大につながる恐れがあります。

EU CRA の主な要件

セキュリティ・バイ・デザインとセキュリティ・バイ・デフォルト

PDE は、リスク評価に基づいて適切なレベルのサイバーセキュリティを確保した状態で、設計、開発、製造しなければなりません。製品を市場に出すには、製品に既知の悪用可能な脆弱性が含まれないことを確認し、セキュア・バイ・デフォルト、つまり出荷時にセキュアな状態に構成する必要があります。

脆弱性への対処と報告

CRA は製品のライフ・サイクル全体にわたる堅牢な脆弱性管理プロセスを義務付けています。これには、継続的な監視、定期的なテスト、迅速な脆弱性への対処、組織的な脆弱性開示ポリシーの確立が含まれています。また、メーカーが活発に悪用されている脆弱性を認識した場合、24 時間以内に適切な EU 機関に通知する義務があります。

SBOM の準備

メーカーは自社製品に含まれるコンポーネントを特定して文書化する必要があり、これにはソフトウェア部品表（SBOM）の作成が含まれます。SBOM は一般に使用されている機械読み取りが可能な形式で作成し、少なくとも直接的なアプリケーション依存関係を含む必要があります。

適合性評価

メーカーは PDE を EU 域内で販売する前に、適合性評価を実施して CRA の必須要件に準拠していることを示さなければなりません。

ブラック・ダックの CRA ソリューション

ブラック・ダックの AppSec ポートフォリオは、統合された自動化セキュリティ・アプローチを提供し、独自開発のソース・コードと外部依存関係の両方を解析することで、早期に、またソフトウェア開発ライフ・サイクル全体を通じて継続的に、脆弱性と品質上の問題を特定します。
この複合的な知見とシームレスな開発の統合を組み合わせることで、規制のタイムラインと要件に沿った効果的な優先順位付けおよび緩和策が可能になります。

CRA の要件	ブラック・ダックのソリューション
セキュリティ・バイ・デザインと セキュリティ・バイ・デフォルト	• 静的アプリケーション・セキュリティ・テスト（SAST）で、設計 / コード・レベルの欠陥を早期に検出 • ファジング・テストにより実行時のセキュリティ問題を発見 • ソフトウェア・コンポジション解析（SCA）により脆弱な外部依存関係を特定
脆弱性の対応と報告	• SCA による既知の脆弱性と悪意あるパッケージに対する警告 • ファジング・テストによりゼロデイ脆弱性を発見
SBOM の提供	• SCA は自動的に依存関係を特定して、標準化された形式で SBOM をエクスポート
適合性評価	• SCA、SAST、ファジング・テストが、テスト、テスト結果、コンポーネント使用状況の詳細レポートを提供 • アプリケーション・セキュリティ態勢管理（ASPM）が、アプリケーションに対して実行されたすべてのテストの統合ビューを提供

ソリューション・ハイライト

- **Black Duck® SCA** はアプリケーションをスキャンすることで、オープンソースおよびサード・パーティの依存関係を特定し、関連するセキュリティ、ライセンス・コンプライアンス、またはコンポーネント健全性のリスクについてチームに警告します。Black Duck SCA は、標準もしくはカスタム・フィールドを含む SBOM を SPDX または CycloneDX 形式で生成します。また、スキャンされたアプリケーション、見つかったリスク、コンポーネント使用状況に関する詳細なドキュメントを提供します。
- **Coverity® 静的解析**は独自開発のソース・コードを解析し、品質とセキュリティに関するコーディングの欠陥を早期に検出して修正することで、セキュア・バイ・デザイン開発をサポートします。また Coverity は、ISO 26262、CERT C/C++、MISRA を含む規格に対応するコンプライアンス・レポートを生成します。
- **Defensics® ファジング**は、厳格なフォルト・インジェクションを含むジェネレーション型ファジング・テスト技術を通じて、プロトコルとインターフェイスに含まれる未知の脆弱性を発見することで、製品の堅牢性、悪条件下での安定性、回復力を検証します。
- **Software Risk Manager™**は、特定の製品に対して実行されるすべてのアプリケーション・セキュリティ・テストのレコードを統合して提供する ASPM ツールです。このセキュリティ記録システム（SoR）は 150 を超えるツールから取得されるテスト結果に対応し、品質管理システムに情報を提供する主要プロバイダの役割を果たします。

ブラック・ダックを選ぶ理由

ブラック・ダックはアプリケーション・セキュリティ・テスト分野の Gartner® Magic Quadrant™で 7 回、ソフトウェア・コンポジション解析分野の Forrester Wave™で 5 回、静的アプリケーション・セキュリティ・テスト分野の Forrester Wave™で 3 回リーダーに選出されています。ブラック・ダックには、ソフトウェア・ベンダーおよびハードウェア・メーカーが、車載 / 産業 / 医療機器および航空宇宙 / 防衛などの業界における法規および安全規格に準拠できるように支援してきた確かな実績があります。ブラック・ダックの包括的なポートフォリオ、忠実度の高い結果、専用サポート・チームは、EU CRA の要件への準拠に確信を持ちたいと考えるソフトウェア・ベンダーに最適な選択肢です。

Arm 社の顧客が EU CRA の要件を満たす際に、どのようにブラック・ダックが貢献しているかご確認ください。

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