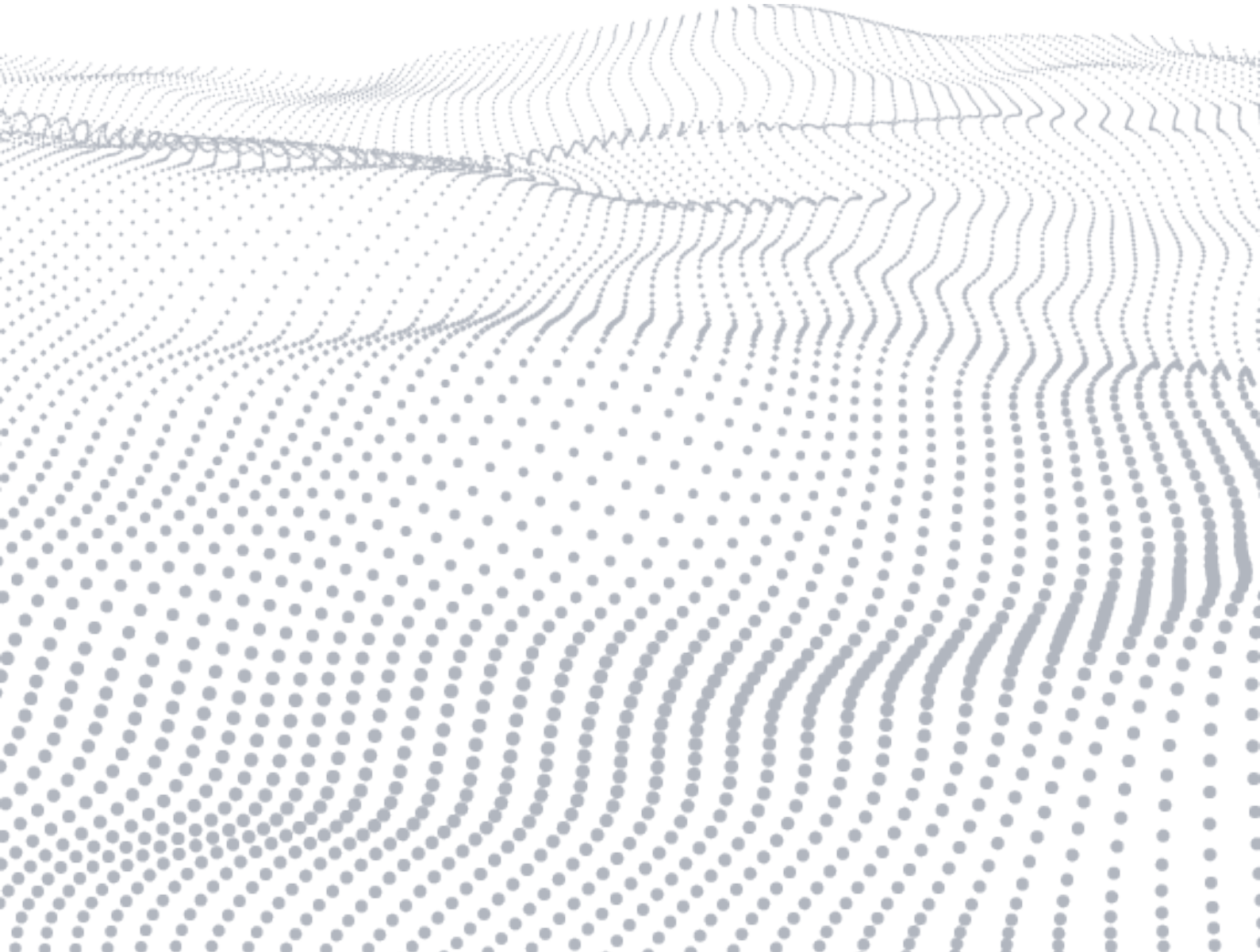
BLACKDUCK®

ホワイトペーパー

サプライチェーンの強靭化



概要

最近報道されたいくつかのインシデントを受け、外部ベンダーから調達したソフトウェアやサービス、ハードウェアに潜む脆弱性のリスク管理方法について、多くのカスタマーからブラック・ダックへ問い合わせが寄せられています。インフラストラクチャのセキュリティ対策の中でも、この問題は法務およびガバナンスのフレームワークから、高度な脅威検知まで、サイバーセキュリティのほとんどすべての領域に影響を及ぼします。

本稿は、潜在的リスクの枠組みを理解してサプライチェーン・セキュリティの目標達成を支援するブラック・ダックのツール、テスト、プロフェッショナル・サービスについて説明したカスタマー向けのリファレンス資料として作成したものです。

実際のニーズは企業ごとに異なるため、どのような施策を実施するかは個々の環境、リスク・プロファイル、組織の特性に応じて細かく調整することが望まれます。以下に、「利用者」と「製作者」の双方に対するブラック・ダックの全体的な推奨事項をまとめます。

利用者

利用者（ソフトウェア製品のエンドユーザー組織）にとってまず必要なのは、潜在的なセキュリティ侵害の存在を検出することです。これは、最近の攻撃によって直接影響を受けた企業にとっては特に重要な点です。次に、国際標準化団体がまとめた枠組みに従って、リスクの発見とフレーミングを実施します。具体的には、以下のような施策を実施します。

- 潜在的リスクの高いシステムを見つける
- これらシステムのセキュリティ・プログラムを納入しているベンダーを評価する
- これらシステムの個々のデプロイ環境に対してリスク評価を実施する
- 業界のガイダンスに基づいてベンダー要求事項を作成する
- 分析結果に基づいて、技術、法務、ガバナンス面の対策を作成する
- サプライチェーン・セキュリティ要求事項の適合証明と成熟度向上をベンダーと共同で検証する

製作者

製作者（利用者にソフトウェア製品を提供する組織）にとってまず必要なのは、個々のコードベースを精査して、現在のビルドおよびデプロイ環境に意図しない機能が混入していないかを確認することです。次に、利用者の場合と同様に国際標準化団体や業界のリーダーがまとめた標準的な枠組みに従って、リスク管理およびフレーミングを実施します。具体的には、以下のような施策を実施します。

- 攻撃者にとって魅力的な機能プロファイルを持つ、潜在的リスクの高いシステムを見つける
- 開発パイプラインに対して脆弱性およびリスク管理評価を実施する
- リスクに対して技術および組織面での対策を作成する
- コードの脆弱性およびコードを悪用される可能性が抑えられるような形でソフトウェア開発ライフサイクル（SDLC）の評価を実施する
- システム・デリバリ / デプロイ・フレームワークに対してリスク管理を実施する
- リスクが見つかった場合、追加の対策を作成する
- 統合されたサードパーティ・コンポーネントのベンダー・リスクを管理する

全体として、戦略的および戦術的目標に関係する以下の 2 つの基本的な質問に答える形で組織としての取り組みを進める必要があります。

- 自社は現在進行中の攻撃の被害者であるか。
- どうすればサプライチェーン攻撃のリスクを緩和できるか。

背景

2020 年 12 月、SolarWinds 社のプラットフォーム Orion にマルウェアが感染し、多くの大企業や政府機関がサプライチェーン攻撃を受けたことが明らかになりました。このマルウェアは SolarWinds のビルド環境に仕込まれ、同社のカスタマーに対するアップデートの一部として、通常のリリース・サイクルによってデプロイされました。更に、このマルウェアが内部ネットワークへの高特権ピボット・ポイントとして使用され、そこで侵入後の活動が実行されました。SolarWinds の Orion は、主に特権サービス・アカウントを使用してシステム監視とデータ収集を実行するモジュールを組み合わせて構成されているため、他のネットワークを標的にする攻撃者にとって非常に価値のある資産であったと言えます。

この攻撃の全容をまとめることは、本稿の趣旨ではありません。攻撃の手口（TTP= 手法、ツール、手順）は、本稿作成時点でまだ完全に解明されておらず、2021 年 1 月中頃にも大きな新情報が報じられたばかりです。これらの TTP は必ずしも目新しいものではありませんが、明確な意図を持って巧妙な細工がなされており、SolarWinds のプロセスとパイプラインについての内部知識を持った者の関与も疑われています。

この攻撃についての最新情報は、以下のリンク先を参照してください。

- FireEye
- CrowdStrike
- SolarWinds
- CISA

以下に、2021 年 1 月 26 日現在での分析結果の要点をまとめます。

- SolarWinds 社のインフラストラクチャ自体に複数の脆弱性があり、これがビルド・パイプラインへの攻撃を招く要因となった
- 攻撃者は SolarWinds 社の環境で使用されているツールやプロセスを熟知していた可能性が高い
- ビルド・ツールのアラートや警告が作動しないように注意が払われた
- マルウェアは署名付きアップデートの一部としてデプロイされた
- 被害を受けたサイトにも、情報セキュリティの基本機能に関する一般的な脆弱性が存在し、これが悪用されて検知に失敗した

結論として、この攻撃は法務面のフレームワークから高度な脅威検知まで、サイバーセキュリティにおける予防的対策や検出対策のすべてに影響を与えるということが言えます。

一般的な攻撃の分類

サイバー・サプライチェーンに対する脅威は今に始まったものではありません。一般的な攻撃は、以下のように分類されます。

1. 開発またはデプロイの段階で、攻撃者が本来の意図にない（悪意のある）機能を挿入する
2. ベンダー自身の正当な製品またはデリバリ手順によって悪意のある機能がデプロイされる
3. 問題のあるコードを顧客が受信してデプロイ、または既存システムのアップデートに使用する
4. 脅威エージェントが侵入後の活動を実行する

こうした攻撃の過去の例（匿名のもの、公開されたものを含む）としては、以下のものがあります。

- 悪意のある製品アップデート
  - Havex（リモート・アクセス型トロイの木馬）
  - Stuxnet
- マルウェアが挿入されたソフトウェア
  - CCleaner（過去 2 回）
  - MeDoc（ウクライナの会計ソフトウェア）
- 開発ツール
  - XcodeGhost
  - GitHub やその他リポジトリのタイポスクワッティング（URL ハイジャッキング）または悪意のあるライブラリ

攻撃の形態は、ハードウェアの改ざんや、SolarWinds の場合のようなエンタープライズ・ソフトウェアへの攻撃などさまざまです。ソフトウェア・ダウンロード・ポータルやプロフェッショナル・サービス・ツールを悪用し、悪意のあるコンテンツを配布するといった攻撃もあります（上記の手順 3 と同様の結果を招きますが、手順 2 については開発後に対処します）。

ブラック・ダックは、サプライチェーンのリスクとセキュリティに関するブログ記事やレポートをいくつか公開しています。以下のリンク先をご参照ください。

- ホワイトペーパー
- アナリストによるレポート
- ブログ記事

ブラック・ダックのソリューション

ブラック・ダックは、さまざまなツール、テスト、プロフェッショナル・サービスを組み合わせることにより、リスクの発見、理解、軽減を支援することを活動の主眼としています。これには、サードパーティから供給されたアプリケーションの脆弱性が、デプロイ後に攻撃者によって悪用されるのを防ぐ取り組みも含まれます。

セキュア開発とコード品質のためのツール

ブラック・ダックのツールは、DevOps 環境にシームレスに統合しながら、セキュリティと品質の不具合への幅広い対処を支援します。自社開発ソースコード、サードパーティ製バイナリ、オープンソース依存ファイルに潜むバグやセキュリティ・リスクに加え、アプリケーション、API、プロトコル、コンテナの実行時脆弱性も特定します。

ブラック・ダックのツールは、個々の環境およびテクノロジ・ニーズに応じたデプロイが可能です。

ペネトレーション・テスト

ブラック・ダックのペネトレーション・テスト・サービスにより、以下に示すさまざまなインフラストラクチャ、システム、および個別製品に対するリスクへの理解を深めることができます。

- 開発環境およびツール
- 特定の関心対象システム
- 個々のアプリケーション（サードパーティ製ソフトウェアを含む）
- 個々の製品（ハードウェアおよび IoT 環境を含む）

コンサルティング・サービス

ブラック・ダックのプロフェッショナル・サービスは多くのお客様にご利用いただいており、サプライチェーン・セキュリティの目標達成に貢献しています。以下に、代表的なサービスを挙げます。

マルウェア検知

自動化したツールと専門のアナリストを組み合わせてコードベースを精査し、マルウェアの可能性が疑われるコードを特定します。多くのマルウェアは外見も挙動も通常の機能と変わらないため、ツール主導の人手による解析を実施することで、意図しない機能がコードに含まれないようにします。

SDLC 評価

ブラック・ダックのチームは初期段階での設計 / コンセプト・リスク評価からクラウドへのデプロイまで、開発ライフサイクル全体でセキュリティの徹底を図るための評価およびプロセス分析サービスを実施しています。

これらの評価を実施することにより、実装済みコードのセキュリティ対策にはどのような施策、プラクティス、手続きを SDLC に含めればよいのかが明確になります。

ベンダーまたはサプライチェーンのリスク管理

ブラック・ダックは SDLC における開発プロセスおよび技術対策の評価で培ったノウハウを活かし、システム開発企業が同じ原則をベンダー評価にも適用できるように支援しています。上記の評価サービスを実施することにより、ベンダーの全体的なセキュリティ成熟度についての現状を把握し、軽減対策およびガバナンス・フレームワークの導入促進を図ることができます。

脅威モデリングおよびアーキテクチャ・リスク評価

実装テストを行う前に、ブラック・ダックのテスト・サービスと同様の方法でさまざまな環境を評価してアーキテクチャ・リスクを特定します。これにより、評価範囲内の各環境やシステムにおける潜在的リスクを完全に理解することが可能となり、この理解に基づいてテスト内容を決定したり、テスト前に問題を修正したりできます（多くの場合、技術評価で実装リスクを見つけることはできますが、より根本的なレベルでシステムに組み込まれたリスクは見つけることができません）。

このサービスは高リスクのデプロイ環境、開発環境、デプロイ・ストラテジー、あるいはサービス・プロセスに対しても実施できます。

実装コンサルティングおよびトレーニング

業界をリードするブラック・ダックのエキスパートが、個々のニーズに合わせて修正プラン、段階を踏んだ成熟度プログラム、ツールに関連した実装ガイダンスの作成を支援します。これにはコンテナ化、クラウドへのデプロイ、継続的インテグレーション / デリバリ（CI/CD）環境、DevSecOps などさまざまなものが含まれます。

次のステップ

利用者のチェックリスト

施策	関連するブラック・ダックのサービス
アクティブなインシデントが発生していないか確認する	マルウェア検知（不審なシステムを特定済みの場合）
高リスク・システムの環境を評価する	• アーキテクチャ・リスク評価 • 脅威モデリング • コンサルティング・サービス：実装コンサルティング • ペネトレーション・テスト
ベンダー評価を実施する	• セキュア開発成熟度モデル（BSIMM） • コンサルティング・サービス：ベンダーおよびサプライチェーン・マネージメント
ベンダーのプログラム成熟度を評価し、リスクの高いものをトリアージする	コンサルティング・サービス：ベンダーおよびサプライチェーン・マネージメント
ベンダー要求事項を作成する	コンサルティング・サービス：実装コンサルティング
高リスク・システムに対する緩和対策を作成する	コンサルティング・サービス：実装コンサルティング
自社開発コードのリスクを評価する	「プロデューサーのチェックリスト」参照

製作者のチェックリスト

施策	関連するブラック・ダックのサービス
アクティブなインシデントが発生していないか確認する	• マルウェア検知（不審なシステムを特定済みの場合） • 使用しているテクノロジーに応じたコード評価ツール
魅力的な機能プロファイルを備えた製品やサービスを評価する	• アーキテクチャ・リスク評価 • 脅威モデリング • コンサルティング・サービス：実装コンサルティング
開発およびデプロイのパイプラインを通して完全な脆弱性管理を実施する	• コンサルティング・サービス：実装コンサルティング • ペネトレーション・テスト（オプション） • 構成評価（クラウドへのデプロイなど）
開発パイプラインおよびデプロイ・プラクティスのリスク評価を完全に実施する	• アーキテクチャ・リスク評価 • 脅威モデリング
適切な対策を作成する	コンサルティング・サービス：実装コンサルティング
ソフトウェア開発ライフサイクル（SDLC）およびデプロイ・プラクティスを評価してセキュリティ・ギャップを特定する	• SDLC 評価 • セキュア開発成熟度モデル（BSIMM） • CI/CD マチュリティ・アクション・プラン（MAP） • DevSecOps MAP • カスタム
製品に統合されたサードパーティおよびベンダーを評価する	「利用者のチェックリスト」参照
利用者の視点から内部環境に取り組む	「利用者のチェックリスト」参照

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