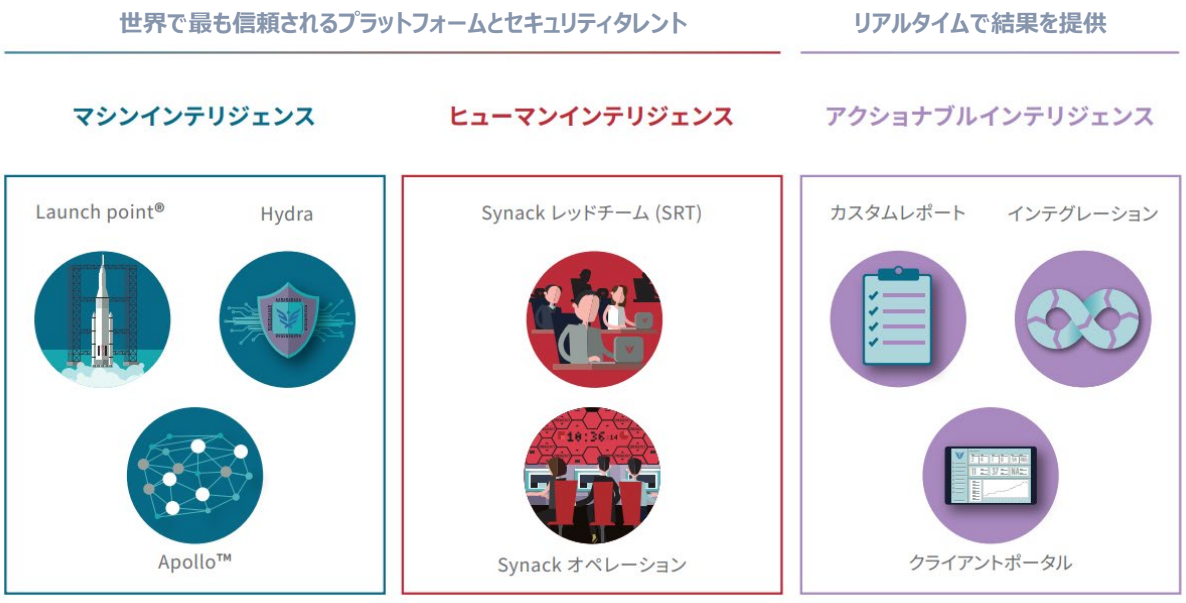
クラウドソーシング・セキュリティテストの概要

スマートな方法で保護を

ペネトレーションテストを拡張するためには、ただのクラウドではなく、最高のクラウド（補足：集団の意味）が必要です。クラウドを拡張するためにはマシンインテリジェンスが必要です。私たちは従来のペネトレーションテスト、またはバグバウンティより有効なテストのソリューションを提供するため、ヒューマンインテリジェンスで増強された最高の人間知能を組み合わせたペネトレーションテストのプラットフォームを開発しました。機械の効率性、優秀な人間の深い洞察能力および上質なサービスを組み合わせ、エクスプロイタブルな脆弱性の大規模な発見と修正を可能にするシステムを Synack は提供しています。

Synack は最も信頼されるクラウドソーシング・セキュリティテストのプラットフォームです

Synack は業界で唯一のペネトレーションテストを提供し、クラウドソーシングによる人間の検査能力と、独自の AI 技術をシームレスに組み合わせ、最高の検査効果と効率性を実現します。Synack の新しいスマートクラウドソーシング・セキュリティテストのプラットフォームは、自動化と拡張知能が含まれており、攻撃対象範囲のカバレッジ向上、継続検査、より高い効率性、直面している課題に対するより深い洞察を提供します。プラットフォームは 24 時間 365 日、人間の検査能力と Smart Scan の最適化を行い、制御。資産を検査するために、Synack は優秀な Synack Red Team（SRT）を配置するだけではなく、同時に SmartScan も展開します。Synack の SmartScan は、プラットフォームの専用スキャナーである Hydra を利用して、SRT のために被疑の脆弱性を継続的に発見し、SRT が最高の結果を手に入れるためのトリアージを実施します。更に、SRT のリサーチャが積極的に脆弱性を探し出し、コンプライアンスチェックリストを完成させ、独自のツールや技術を用いて、クラウドソーシング・ペネトレーションテストを実施することで、独特な人間の創造性と厳格さを検査に提供します。Synack のプラットフォームを活用して、すべてのアプリの高度な自動評価を実施し、Synack Red Team に継続的かつ創造的な関与を奨励する一方で、Synack は、2 つの手法を独自に組み合わせ、市場の中で最も効果的かつ効率的なクラウドソーシング・ペネトレーションテストを Synack は実現します。



信頼の置けるプラットフォーム

Hydra— Synack の独自の自動スキャナは継続的にスキャンを実施し SRT にアラートを出し、潜在的な脆弱性を発見するための調査を行います。スキャナは SRT の手法に対して高度な脆弱性スキャン、変動調査、防御テクノロジの検出をします。

Launch point®— Synack の LaunchPoint および LaunchPoint +は、独自の安全なゲートウェイとエンドポイントコントロールで、すべての検査トラフィックデータを記録し、最も厳しいプライバシー要件を満たす安全なワークスペースで、クラウドソーシングによる検査方法に信頼性、透明性、および監査能力を提供します。お客様は、クライアントポータルを用いて、オンデマンドですべての検査アクティビティとデータ分析の完全なログを受け取ることができます。

Apollo™— Synack のプラットフォームの継続的学習エンジンである Apollo はデータサイエンスと機械学習を利用して、反復可能な作業を自動化し、新たな洞察力で検知機能を増強するために開発されました。SRT の作業から得た知識によって Apollo は Hydra を強化し、継続的にスキャンを実施することで結果の質を向上させます。

セキュリティ能力

Synack Red Team (SRT)— SRT は世界中から集まった高度な専門性を持つ、熟練し、精査されたセキュリティリサーチャーで構成される Synack のプライベートネットワークです。このエリートチームの一員となるためには、業界で最も厳しいスクリーニング、面接、スキル検査、審査を合格しなければなりません。

Synack オペレーション— Synack のオペレーションチームはノイズを排除し、あらゆるエンゲージメントの側面を管理するチームです。これらのオペレーションの作業はすべての SRT の文書をトリアージし、顧客報告書を作成し、お客様の組織のリスク認識度に合わせて、お客様と協力してアセスメントのスコープと関与のルールを定義します。

リアルタイムの結果

クライアントポータル— Synack は包括的な脆弱性の情報と検査トラフィックを記録し、該当データをリアルタイムでダッシュボートとプラットフォームの指標に変換します。被疑のものから報告された脆弱性、パッチ適用済みの脆弱性、検証済みの脆弱性まで、脆弱性のライフサイクル全体を、企業やリサーチャが信頼できる情報として Synack ポータル上でリアルタイムに提供しています。

カスタムレポート—当社の監査報告書はハッカーの視点で、お客様のデータと検査結果を統合し、セキュリティのあるべき姿の推奨を提供します。これには、監査人向けのコンプライアンスチェックリストに限らず、発見されたすべての脆弱性の詳細な説明、脆弱性の修正方法の提案、競合他社との比較なども含まれています。

インテグレーション—私たちは DevOps のツールとの複数のインテグレーションに対応してり、社内のセキュリティ方針とコンプライアンスに関する企業要件を満足するとともに、脆弱性管理のためのセキュリティ運用のワークフローを最適化します。

利用事例と利点：

1. **より厳格なペネトレーションテスト**
   - マシンインテリジェンスを結合したクラウドの多様性を利用して、より効果的なペネトレーションテストを実現
   - 攻撃対象領域の変化と被疑の脆弱性に関するマシンインテリジェンスを提供することにより

     人間のテスターが脆弱性を発見するまでの時間を短縮
   - 継続的かつリアルタイムの報告を利用してより効果的な脆弱性の修復を実現
2. **大規模な脆弱性管理**
   - 継続的に SDLC の中で更新される資産上の脆弱管理を簡単に拡張
   - 最も高いリスクの資産を特定し、優先順位付けすることで、迅速な修復が可能
   - テスターによる継続的な関与を通じ、365 日 24 時間常に継続的なセキュリティの保護を実現
   - 脆弱性発見のための各ステップをリアルタイムで表示
3. **リソースの増強**
   - ノイズレスなスキャンと SDLC のタイミングに合わせた継続的なセキュリティ保護により、セキュリティチームの効率を向上させ、トリアージのコストをかけずに SRT を活用することができます
   - 攻撃対象範囲全体に対する SRT と Hydra の検査状況をリアルタイムで表示
4. **DevSecOps**
   - DevOps ツールとのインテグレーションにより、チームが SDLC プロセスにセキュリティを組み込むことを実現
   - 最も高いセキュリティリスクの領域を特定し、組織的におけるリソースを適切に割り当てることで、修復を迅速化
   - 新しい脆弱性のインテリジェンスにより様々なビジネス関係者に対してより良い洞察を提供
5. **コンプライアンスの要求事項を満足**
   - お客様のインフラストラクチャはリサーチャによる特定の VPN または、ゲートウェイの利用が必要
   - データプライバシーの要求事項または、特定規制上のコンプライアンスのためのフレームワーク/業界基準に準拠

Synack, Inc.

855.796.2251 | www.synack.com | info@synack.com

v2019.1—INT US