CYCRAFT

侵害調査サービス

現在と過去の攻撃者の行動を「F / A / S / T」で特定
Fast(高速) / Accurate(正確) / Simple(簡単) / Thorough(徹底)

CyCraftの侵害調査

CyCraftのIRサービスチームはサイバーセキュリティとサイバー脅威情報の最前線で活動し、政府機関、フォーチュングローバル500の企業、重要インフラを、最も高度なサイバー攻撃から保護しています。

CyCraftでは、進行中の脅威や新規の脅威に対する最前線での経験や、これらの脅威の技術、戦術、手順、行動プロファイルを活用し、顧客によるサイバー環境の現状の評価、重大なセキュリティインシデントの調査、詳細なデジタルフォレンジック分析の実施、長期的なセキュリティソリューションの成熟化を支援しています。

侵害調査の必要性

この10年で、サイバー犯罪では保護システムの侵害、信頼されていたツールや証明書の不正使用、正当なユーザー動作の精密な模倣が見られるようになりました。自分の環境が侵害されたかどうかを確実に把握すること、脆弱性を特定すること、リスクを取り除くことは、2020年代においてSOCを効果的に行う上で重要です。MTTD（平均検出時間）やMTTR（平均対応時間）が長くなると、ビジネスに影響する重大なデータ漏洩につながる可能性があります。

当社のアプローチ

1日以内 - 当社のエージェントレススキャナーを実行してから1日以内に、詳細かつ正確な侵害調査レポートが届きます。この処理は、当社のアナリストの専門チーム、仮想フォレンジックアナリストAI、攻撃動作モデリング技術の連携により実現しています。侵害調査レポートには、リスクと露出についてのサイト全体の分析、セキュリティ検疫の問題、疑わしい動作の分析が記載されます。当社の侵害調査サービスチームは侵害調査レポートに従って、皆様の組織を標的とした将来のセキュリティインシデントに迅速かつ効果的に対応できるようにするための指導を行います。

対象となる主な脅威

データの盗難
脅威グループが標的としているのはあなたの金銭だけでなく、顧客情報や知的財産も標的になります。

サービスの停止
多くの組織で、ユーザーがシステムに常時アクセスできるようになっているため、メンテナンスが難しくなっています。当社の脅威調査スキャンにより、サービスを侵害する恐れがある、悪意のあるアクティビティや潜在的なリスクを明らかにします。

時間とコストがかかる復旧
2020年代のサイバー攻撃は、オンプレミスやクラウドベースのネットワークシステムに極めて甚大な物理的損害を与えます。

多大な罰金
GDPRやCCAのような規制では、規模の大小にかかわらずすべての組織が国家単位の脅威グループから保護することが求められます。これに反すると多大な罰金が課せられます。

顧客の信頼の喪失
侵害が発生した場合、十分な情報発信ができず、透明性を確保できない場合、最終的にはこれまで苦労を重ねて獲得してきた顧客の信頼を失うことになります。

1. 

エンドポイントで調査用スキャナーを実行します。

2. 

当社でスキャナーのデータを受け取って分析し、ヘルスチェックレポートを作成します。

3. 

レポートの内容を皆様と確認します。

CyCraftの特徴

CyCraftの侵害調査サービスと他のサイバーセキュリティ評価との比較

	CyCraftの侵害調査サービス	レッドチーム評価	侵入テスト評価	脆弱性評価
分析にかかる時間	1日以内	数か月	数週間	数日
結果の種類	現在発生中の事案	今後発生が見込まれる事案	今後発生が見込まれる事案	今後発生が見込まれる事案
組織にとっての価値	高	中	中	中
実行の難易度	簡単	困難	中程度	簡単

CyCraftの侵害調査サービスとEDR / AV / SIEMの比較

	CyCraftの侵害調査サービス	EDR	AV	SEIM
根本原因の特定までの時間	1日以内	数日～数週間	(該当なし)	数日～数週間
クエリの量	ゼロ	大量	(該当なし)	大量
組織にとっての価値	高	中	低	中～低
実行の難易度	簡単	困難	簡単	困難
状況全体の把握度	高	中～低	低	低

CyCraftの侵害調査サービスはGDPRや日本当局の法令を遵守

- データ収集量はWindowsよりはるかに少ない
- 支払データ、プレゼンテーションファイル、メッセージや電子メールの内容、その他GDPRやプライバシー関連法令に違反する情報は収集しない
- **GDPRやプライバシー関連法令の遵守を支援する**
  - ハッカーによるデータ盗難を防ぐ
  - 法令遵守のため短時間でレポートを作成する

CyCraftのサービスについて

CyCraftのサービスにより、世界中の組織が、2020年代のサーバー脅威を防ぐために必要となる革新的なAI主導のテクノロジーを利用できるようになりました。CyCraftのテクノロジーは、悪意のある行動の最新の傾向の検知、調査の自動化、アラートの重要度を自動設定するように設計されているため、CyCraftの顧客はほぼリアルタイムで脅威の検出、追跡、抑制、根絶ができるようになります。

詳しくは www.cycraft.com/services/compromise-assessment をご覧いただくか、engage@cycraft.com

「F / A / S / T」のメリット

Fast：高速

当社のエージェントレススキャナーを実行してから1日以内にリスクと露出についてのサイト全体の分析、セキュリティ検疫の問題、疑わしい動作の分析が記載された侵害調査レポートが届きます。

Accurate：正確

非常に詳細かつ正確な侵害調査レポートをお送りします。この処理は、当社のアナリストの専門チーム、仮想フォレンジックアナリストAI、攻撃動作モデリング技術の連携により実現しています。

Simple：簡単

当社の侵害調査サービスチームは侵害調査レポートに従って、皆様の組織を標的とした将来のセキュリティインシデントに迅速かつ効果的に対応できるようにするための指導を行います。

Thorough：徹底

現在および過去の悪意のあるアクティビティの発見を重視した、徹底した環境分析を行います。