CYCRAFT

テレワークに応じたセキュリティ対策

無料提供中

CyCraftは新型コロナウイルス感染症影響下での事業継続に貢献します。テレワークによる業務が必須条件となった今、新しく購入された端末や社員が個人所有している端末など、直接管理されていない端末によるVPN経由での社内ネットワークへの接続の増加に対策が必要になります。多くの場合それらの端末は社内環境で管理されている端末より安全性が低く、Mac・Windows・Linuxを問わず、未知の脆弱性を含めたあらゆる脅威を潜在的に抱えています。
加えて、VPNは一般的なセキュリティソリューションを回避できるように設計されているため、ファイアウォールや他のゲート製品ではこれらの脅威を防ぐことができません。攻撃者にとって、こんな魅力的な攻撃ルートは無いでしょう。保護されていない端末から社内ネットワークに直接アクセスできるチャンスを得られたも同然ですから。こういう状況をふまえ、貴社には新たなサイバーセキュリティソリューションが必要です。

SECURE FROM HOME

アンチウィルスやOS自体のソリューションではもはや限界がきており、企業はかつてないリスクにさらされている可能性があります。一般的なソリューションでは、このような課題に直面します。

1. 事件の根本原因を特定できない。
2. マルウェアの潜伏した拡散活動を検知できない
3. 未知のデバイスを見つけられない
4. 組織全体のサイバーセキュリティ状況を確認できない
5. インシデントの全貌把握に多くの時間を要する

CyCraft Secure From Homeソリューションではこれらの課題解決の為、次世代アンチウィルス（予防措置）とMDR（マネージド・ディテクション・アンド・レスポンス）の機能を１つのサービスで、負荷のかからない軽量エージェントとして提供しますので容易に導入可能です。ご自宅でもオフィスでも、24時間365日世界で最も高度な脅威に対して貴社の貴重な情報資産を守ることができるでしょう。

CyCraft Secure From Homeソリューションは場所を問わず安心安全な作業環境を提供します。

導入事例

「スケルトンキー作戦」に直面した二社物語

「それはすべての時代の中で、最良の時代であり、最悪の時代でもあった。叡智の時代であるとともに、愚鈍の時代であり…」（チャールズ・ディケンズ「二都物語」より）
A社とB社はともに半導体業界のリーディングカンパニーで、A社はCyCraftのクライアントで、B社はクライアントではありませんでしたが、この経験の後にクライアントとなりました。そんな両社が、世界で最も悪名高い脅威の一つによる高度なゼロデイ攻撃に直面した時の実例です。
その攻撃とは、「スケルトンキー作戦」という新しいタイプのファイルレス攻撃で、Windowsドメインコントローラのメモリを悪用してスケルトンキー（複製された鍵）を作成し、ネットワーク上のあらゆるシステムに管理者権限でログインできるというものでした。セキュリティ上、最悪の事態です。しかし、A社にとって幸運なことに、CyCraftのMDR機能ではこのタイプの攻撃を検知することが可能で、攻撃者からの侵入を未然に回避することができました。一方、B社はこの攻撃により問題が発生、CyCraftに助けを求めてきました。CyCraftは直ちに調査を行い、攻撃者がどのような攻撃を行ったのか、侵入経路と攻撃対象を明確にし、攻撃手法とすでに漏洩してしまった情報資産を明らかにすることができました。CyCraftのソリューションをもっと早くから導入していれば、未然に事故を回避できたことでしょう。

CyCraftは前例のない高度なAPT攻撃を発見し、日々ブロックしています。併せてCyCraft AIエンジンは、クライアントごとに攻撃対象となったあらゆる情報を網羅したレポートを短時間で作成できます。
残念なことに現在のテレワーク環境を支えるVPN接続はこの種の攻撃を受ける可能性を高めてしまうだけです。CyCraft Secure From Homeソリューションを利用することで、貴社の在宅勤務環境における脅威を未然に防ぐことができます。しかも無料で。

自宅から無料でセキュアに

新型コロナウイルス感染症の影響による急なテレワークへの切り替えは、誰にとっても大変困難です。
そんなあなたを応援するため、CyCraftは3月26日から6月30日まで、企業のテレワーク用端末に対し、無償でMDRを提供します。加えて、基幹産業の事業継続を支援するため、すべての企業及び政府機関に対して、無料のサイバーセキュリティヘルスチェックと完全なMDR付きのSecure From Homeサービスを3ヶ月間提供しています。期間中であれば、端末台数無制限でライセンスを使用できます。
今すぐお問い合わせください：contact@cycraft.com

日本におけるお問い合わせ先：株式会社セキュアブレイン　info@securebrain.co.jp

CYCRAFTオールインワンエージェント + クラウドプラットフォームで実現

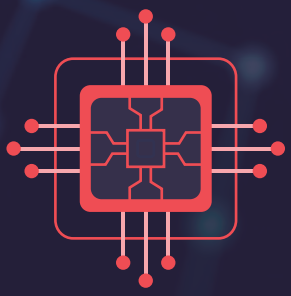
- NGAV：既知および未知の脅威をリアルタイムでブロック
- MDR:：分単位でのフォレンジック解析と対応、世界で最も高度な脅威の検出
  - 脅威インテリジェンス
  - UEBA 分析
  - プレイブック
- レポーティングと可視性
  - システムフォレンジック(キャッシュ、ログイン記録、認証ログやイベントログなど)
  - プロセス、メモリおよびファイルの検査
  - MITRE ATT&CK マッピング
  - 未知のデバイスの可視化
  - あらゆるハッキング活動のストーリーライン
  - 根本原因分析
  - 悪意のあるドメイン、IP、URL分析
  - 疑わしいユーザアカウントの可視化
  - マルウェア分析
  - 影響を受けるすべてのノードと実行の図式化
  - 対処プランと対処後の確認

  （※有料版フル機能利用時）

端末が組織のネットワークに未接続の環境にいても、CyCraft Secure From Homeは次世代アンチウィルスと単体MDRであなたを守ります。もうあなたの大切な時間をログの分析や新しい端末の確認に浪費する必要はありません。端末調査の優先順位をつけなくても、自分で個別に調査しなくても、あなたのセキュリティは守られます。今すぐCyCraftに連絡し、新しいサイバーセキュリティソリューションを体験しましょう。

導入の流れ

CyCraft Secure From Home
スキャナをインストールする



CyCraftで継続的に
スキャナデータを受け取り

CyCraft AIと専門家による
データ分析により、
アラートとレポートを生成

CyCraft専門家の協力の下に
ハッキング根絶

実際の取り組み

GAN、DeepRL、UEBAなどのAIの最新技術を活用して、アーティファクト、エンドポイント、ユーザ、ネットワーク、脅威インテリジェンスなどの複数のレイヤーからの電磁的証拠を分析し、マルウェア、侵害、データ損失、インシデントなど、あらゆるハッカー行為を防止します。

対応端末：

Windows: 7/8/10, Server 2008 - 2019
Mac: macOS 10.10 - 10.15
Linux: Ubuntu 9.10 - 18.04, Debian 7.0 - 9.0, RHEL 6.0 - 8.1, CentOS 6.0 - 8.0

CYCRAFTを知る

cycraft.com
twitter.com/cycraft_corp
medium.com/@cycraft_corp
linkedin.com/company/cycraft/

第三者による評価

MITRE | ATT&CK™

- アメリカMITRE ATT&CK（マイター・アタック）評価第2ラウンドに選定（APT29攻撃に基づく）

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

- サイバーセキュリティ優秀賞を20項目以上受賞。具体的には、MDR、フォレンジック、インシデント対応、人工知能部門での金賞などのほか、サイバーセキュリティにおける最優秀企業賞金賞など。

FIRST

- インシデント対応に関する最大組織であるFIRST加盟。

CYCRAFTについて

CyCraftは台湾・シンガポール・日本・ベトナム・タイをはじめとするAPAC諸国において、政府機関、フォーチュン・グローバル500企業、アジアの主要銀行や金融機関、基幹インフラ・航空・通信・ハイテク企業と、中小企業へセキュリティを提供しています。またSOC（セキュリティオペレーションセンター）に対し、海外で受賞歴のある独自のAIベースのMDR（管理された検出と応答）、SOCオペレーションソフトウェア、TI（脅威インテリジェンス）、ヘルスチェック、自動フォレンジック、インシデント対応（IR）にてSecure From Homeサービスの強化ソリューションを提供しております。