CyCraft AIR を利用したサイバー攻撃監査サービス

ホワイトペーパー（2021 年 9 月版）

株式会社セキュアブレイン

CyCraft AIR MDR：2020 年代に順応した管理された検出と応答

自動化され、インテリジェントで回復性の高い CyCraft のプラットフォームにより、これまで以上に迅速、正確、シンプル、徹底した検出と対応が可能に

2020 年代以降のセキュリティの状況

企業は、複雑で変化の激しいハイブリッドクラウド／オンプレミス環境、新旧のシステム、複数の地域にまたがる運用、在宅勤務の従業員、高可用性、コンプライアンス、使いやすさなどの要件の確保に苦労しています。

悪質で絶え間ない巧妙なサイバー脅威や、攻撃者からの検出しにくい攻撃に直面しながら、SOC（セキュリティオペレーションセンター）を運営するには、貴重なセキュリティ人材を採用・維持する必要があるため、真のサイバーセキュリティは、ほとんどの企業にとって不可能で夢のようなものでした。

台湾：サイバーセキュリティ研究の最前線

台湾の会社である CyCraft は、その特殊な地政学的状況から、世界のどの国々よりも先に、最も高度、執拗、攻撃的な脅威と行為者に頻繁に遭遇するという独特なセキュリティ環境に直面しています。これらは多くの場合、国家の支援を受けた攻撃者や犯罪シンジケートの攻撃者であり、自らの課題を推進するために台湾を標的として、最新にして最も巧妙で悪意のある技術を試しています。世界規模で展開されている有名なセキュリティソリューションは他にもありますが、このレベルの脅威の前には無力です。CyCraft はこの最も悪意のあるサイバーセキュリティ問題に対処できる、まったく新しい技術を開発しました。

CyCraft AIR は、このサイバーセキュリティの最前線で、台湾が世界に誇る AI およびサイバーセキュリティ人材が練り上げた新しいソリューションです。他のソリューションでは実現できない、世界で最も困難なサイバー攻撃を阻止するために、CyCraft AIR は台湾政府、銀行、テクノロジー産業で広く導入されており、企業セキュリティをより安全に保つために必要な独自の機能と価値を提供します。

CyCraft AIR が 2020 年代において競争に勝ち、独自の価値を生み出し、企業を安全に維持できる 20 の理由

1. *フォレンジックファースト*

   ブロックリストや隔離されたアーティファクト、さらには隔離されたエンドポイントやネットワークの入口から操作することで、AV、EPP/EDR、IDS/IPS のベンダーは、最新の攻撃を検索する際に暗礁に乗り上げていました。セキュリティベンダーは、すべてを単独で見てしまうと、2020 年代の最新の攻撃の特徴である巧妙な動作、ファイルレス攻撃、信頼されたツールの悪用を見逃す恐れがあります。SIEM や汎用製品では表示されるデータが多すぎて、草むらの中から一本の針を見つけるような作業を強いられます。しかも最新の攻撃はユーザーの正当な行動を偽装していることが多いため、その針は周囲の草と見分けがつかなくなっています。セキュリティテクノロジーを前進させる唯一の賢明な方法は、個別の端末のログに注目したり、全体をまとめて注目したりするこれまでの方法を捨て、フォレンジックに基づく考え方を取り入れ、「何が」「どこで」「いつ」の要素に注目することです。CyCraft AIR はフォレンジック

ファーストのプラットフォームです。フォレンジックファーストの考え方に基づかないテクノロジーでは最新の脅威に対応できません。

2. *7 段階のコンテキストを分析*

フォレンジックファーストのアプローチの一環として、CyCraft AIR は悪意があると考えられるすべての動作の調査において、複数レベルのコンテキストについて自動フォレンジック分析を実行し、各レベルの間の関係を分析します。

- レベル 1 は「分離された端末のログのコンテキスト」です。分離された端末のログの例として、パケット、実行、メモリセグメント、ログファイルのエントリなどが含まれます。
- レベル 2 は「ネットワークのコンテキスト」です。システム間の接続を、その接続の様々なプロトコルと行動目的の観点から調べます。
- レベル 3 は「エンドポイントのコンテキスト」です。CyCraft AIR はエンドポイントのイベントログ、メモリ、スタートアップファイル、プロセスなどをフォレンジックスキャンします。
- レベル 4 は「ユーザーのコンテキスト」です。ユーザーの動作、ログオンの成功、試行の失敗などを調べます。
- レベル 5 は「企業全体のコンテキスト」です。CyCraft AIR は下位のコンテキストで見つかった証拠をリンクし、企業全体のコンテキストでそれを調べます。
- レベル 6 は「全世界の脅威情報のコンテキスト」です。CyCraft AIR は全世界の脅威情報（後述のポイント 3 を参照）を綿密に調べ、下位レベルで見つかった行動やアーティファクトと関連付けます。
- レベル 7 は「AI 分析のコンテキスト」です。CyCraft AIR は AI による調査方法の行動自動化を活用し、下位レベルをすべてまとめて最終分析を行い、サイバーセキュリティの現状を完全に把握できるようにします。

3. *最も正確で徹底した脅威情報*

CyCraft AIR では、20 を超える主要な独自の情報源から得た脅威情報と、台湾で発生している最新かつ最も悪意のある脅威から得た独自情報と組み合わせ、ISAC (Information Sharing and Analysis Center)、FIRST（Forum of Incident Response and Security Teams）、大企業、政府機関からなる情報コミュニティと連携し、その情報を CyCraft AIR の CyberTotal 脅威情報プラットフォームの AI 主導の綿密な調査プロセスで調査することにより、最新かつ最も高度な脅威をこれまでにない精度と完全度で検出し、阻止することができます。

4. *完全自動フォレンジック調査*

CyCraft AIR は、フォレンジックファーストのテクノロジーとコンテキストのレベルを利用し、バーチャルフォレンジックアナリスト機能でフォレンジックアナリストの作業を自動化することにより、より速く、より正確で、より徹底したフォレンジックプロセスを実現します。CyCraft では AI 分析の作業を自動化しているため、CyCraft AIR の分析はより高速です。熟練したフォレンジックア

ナリストでも 1 台のマシンの調査には 2 時間かかり、全体では感染した可能性があるマシンの台数に乗算した時間がかかることになるため、請求対象となる業務時間は数百時間にものぼりますが、CyCraft AIR では詳細なフォレンジックを数分で実行できます。また、人間のフォレンジックアナリストには疲労や誤りがあり、何も検出できない場合もあります。自動化された AI 主導の CyCraft AIR では、完全で高速なフォレンジック結果が得られ、人為的な誤りもありません。

5. *最も巧妙で悪意のある攻撃を記録的な短時間で阻止*

攻撃の状況は急速に変化しています。インターネットを介し、誰もが最新の最も巧妙な攻撃の標的となる可能性があります。最新の攻撃では、大手クラウドプロバイダーなどの信頼できるソースを悪用したり、信頼できるベンダーのデジタル証明書を偽造したりすることにより、保護システムを突破し、暗号化された PowerShell コマンドライン攻撃などのファイルレス攻撃を仕掛けて、他の巧妙で検出しにくい方法で動作します。コンテキストの各レベル、最も正確な脅威情報、AI 分析、CyCraft が開発した攻撃者モデリング行動技術を結びつけることにより、CyCraft AIR は最も悪質で巧妙な攻撃を、他のシステムが検出する前に阻止します。これにより企業は時間と費用を節約でき、ブランドと従業員を守ることができるのです。

6. *結果重視の AI と自動化：MITRE ATT&CK の複数の指標で最高の評価*

最近はどのベンダーも何らかの形で AI や機械学習を取り入れていると宣伝していますが、実際のパフォーマンスは購入者に明らかにされていません。MDR で重要なのはツールではなく、結果のみです。CyCraft では、革新的な AI と自動化により、世界中のどのベンダーよりも優れた結果を最短時間で得ることができます。その自動化や AI がどのようなものであるかは重要ではありません。重要なのは、CyCraft AIR は MITRE ATT&CK の評価における主要ステップのすべてで警告できる唯一のプラットフォームであるという事実です。また、CyCraft AIR はどのベンダーよりも多くの警告を出すことができ、一般的、戦術的、技術的検出もどのベンダーよりも広範囲です。これらすべてが、デフォルトの設定だけで最初から可能です。遠隔測定、検出、UI の設定を変更する必要はありません。MITRE ATT&CK は高度な永続的脅威のエミュレーションにおける公正さと洗練度で業界のゴールドスタンダードとなっています。CyCraft は世界中の大小あらゆるベンダーの先を進んでいます。

7. *最適な警告*

警告に関する問題の多くは、しばしば検証されていないこと、コンテキストが十分でないこと、セキュリティ上の問題の解決にはつながらないことが挙げられます。IT/SOC チームにとっては余計でストレスの多い作業が増えるばかりで努力に見合う価値が得られないため、事態が悪化することも多くあります。CyCraft AIR はすべての警告に事前検証を実行し、多段階フォレンジック AI 分析によりその数を減らし、警告を組み合わせ、それぞれの警告に対して具体的に何が必要かを特定します。IT/SOC チームは、警告を受け取った後、何が必要かを把握できま

す。CyCraft は警告を送信する際に AI 分析を活用し、完全で詳細なフォレンジックスキャンを企業全体に対して実行します。これにより、疑いのある動作を検証し、悪意のある動作をすべてリンクさせ、企業のサイバーセキュリティの状況について、効率的かつ完全で具体的対応が可能な分析を行います。

8. 自動トリアージ警告とインシデント

CyCraft AIR の自動システムで SOC アナリストとフォレンジックの機能を実行することにより、SOC チームに対して警告トリアージが次のように処理されます。1）警告が事前検証され、誤検知が除外されます。2）警告に重大度が設定され、企業と CyCraft の AI 分析が何をどの順序で処理すべきかを把握できるようになります。3）CyCraft AIR はインシデントのフォレンジック分析を自動化してすべての警告を処理するため、人間によるトリアージが不要になります。

9. 企業全体の分析をこれまで以上に高速で実行

警告により AI 分析による次の段階が開始されると、アナリストは企業全体を数分間で調べ上げ、すべてのイベントとログを結び付け、すべてのセキュリティインシデントの全体像を形成します。フォレンジックアナリストの業務や行動の徹底的な研究と革新的な AI を組み合わせることにより、CyCraft は世界中のどのセキュリティベンダーよりも短時間で綿密に分析を行うことができます。

10. 常時稼働の分析により結果重視のセキュリティを実現

AI 分析の自動化により、企業は常時保護されます。CyCraft AIR では、人間のアナリストによるインシデント処理だけに頼らず、どの競合他社よりも高速、正確、簡単、そして綿密なサービスを提供し、可視化と行動分析の点で優れた結果を出して企業のセキュリティを確保します。

11. 間違いのない企業全体のインシデントストーリーライン

CyCraft AIR は企業全体ですべてのフォレンジックコンテキストを高速かつ綿密に調べ、悪意のある行動や端末のログとそのコンテキストレベルの関係を調べてリンクさせることにより、攻撃の総合的なストーリーラインを生成できます。これは 1 つのエンドポイントに限られたものではなく、デバイス間で自在に動き回る攻撃者のすべての行動が対象です。実行されたコマンド、関連する悪意のあるファイルとネットワークのログをすべて記録したリストが、わかりやすいストーリーラインの中に組み込まれます。これは人間のアナリストが行うことと大きくは変わりませんが、詳細なスキャンを一貫して行うことができ、企業全体にまたがる攻撃の証跡を得られるため、はるかに短時間かつ綿密です。

12. 間違いのない企業全体の根本原因分析

セキュリティインシデントのすべてのイベントとログをリンクすることにより、CyCraft は攻撃の一部や特定のデバイスのみならず、攻撃者による企業への侵入の初期ベクトルまですべてさかのぼることができます。セキュリティ体制や技術を調整してインシデントから復旧し、将来のインシデント発生を防ぐために必要な知識が得られるため、この情報は非常に重要です。

13. サイバーセキュリティ状況を完全に把握

企業は資産がどの程度安全に保護されているかを把握できず、セキュリティ状況について不安を持つことが多くあります。CyCraft AIR テクノロジーはすべてのデバイスで発生したすべてのイベントに注目することにより、企業のサイバーセキュリティの状況を詳細に把握できます。内部のユーザーと外部の攻撃者による、隠れたデバイス、巧妙で悪意のある操作、異常な動作が、簡単で理解しやすい形で明らかになり、異常への対応についても指示があります。

14. 自動レポート：照会は不要

CyCraft AIR の MDR の自動レポート機能により、IT/SOC チームは攻撃の全貌を把握できたかどうかわからないままコンソールの前で何時間も費やす必要がなくなりました。分析の結果は即時かつ自動的にチームに通知されます。チームは遠隔測定データを照会することなくセキュリティ体制を調整してインシデント対応を完了することができます。

15. 世界最先端の脅威分析チーム

CyCraft の研究・脅威分析チームは、これまでになかった攻撃についても調査しており、WIRED※が取り上げた研究の中で、新興の攻撃グループである「Chimera」の存在を突き止めました。この研究チームはマルウェアの消去や、世界で最も新しく悪質な脅威の詳細分析を日々進めています。チームのインターン生も DEFCON のコンペティションで名誉ある賞を受賞しています。チームはその知見を CyCraft AIR の AI、脅威情報、自動化に日々取り入れ、最新の攻撃に対応しています。
※https://wired.jp/2020/08/09/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/

16. GDPR（およびその他のプライバシー関連法律）を忠実に遵守

CyCraft AIR は個人特定情報の読み取り、分析、記録、アクセスを行いません。CyCraft AIR は企業をセキュリティ保護して情報漏洩を防ぎ、企業がコンプライアンス要件を満たすために必要な書類の作成を支援します。CyCraft AIR はサーバーに個人特定情報を保存しません。CyCraft AIR は市場で最もプライバシーに配慮した MDR ソリューションです。CyCraft はマシン上で分析を行い、独自のフォレンジックメタデータを生成して、マシンから AI 分析クラウドに送信します。そのため、CyCraft では不要な情報を閲覧も保存もしません。さらに、CyCraft AIR の MDR は非常に高速で綿密な処理を実行するため、開示に関する要件は遵守され、セキュリティ状況に関する社内外のコミュニケーションが容易になります。

17. SOC チームは落ち着いてタスクに集中できる

SOC を運用したり、セキュリティ責任を負ったりすることは、企業にとって最も負担の大きい作業のひとつです。侵害の可能性は常に存在し、業務のセキュリティが低く、警告が溢れていると、攻撃者はさらに活発で高度な攻撃を仕掛けてきます。CyCraft AIR の MDR が SOC での警告、トリアージ、調査、セキュリティイベントへの対応を取れるようにすれば、SOC は現在の多忙な SOC アナリストに求められているベースライン設定、内部の連絡、セキュリティテストなどの業務に集中でき、CyCraft AIR の MDR にあとを任せることができます。

18. 負荷が最も低い MDR ソリューション

エンドポイントエージェントと MDR の仕組みについて抜本的に再考し、AI や自動化と組み合わせることにより、CyCraft では競合他社よりもはるかに効率的な処理が可能です。CyCraft AIR の MDR エージェントの CPU 使用率は 1%未満で、一日のエンドポイントあたりのネットワーク帯域幅は 1MB 未満です。インシデントの検証、トリアージ、調査を自動化することで、組織は時間とコストを削減し、多額のコストや時間の浪費、パフォーマンスの低下を招くことなく、セキュリティ状況を完全に把握することができます。

19. 業界で最も重要な形で評価

MITRE ATT&CK の数多くの指標で最高の評価を得ました。 日本では Interop の「Best of Show」を受賞し、Forrester のアナリストの研究の対象となり、Momentum Cyber のさまざまなカテゴリーで取り上げられ、Cybersecurity Excellence で 25 を超える賞を受賞し、WITSA などでも受賞しています。どれも非常にすばらしい実績ですが、評価として最重要ではありません。業界内で最も重要な評価は、政府、銀行、ハイテク分野で、世界でこれまで見られなかった高度なサイバー脅威に対する防衛の手段として頼られていることです。

20. 侵害の防止

最後に、最も重要なことは、CyCraft の MDR があれば、企業は侵害を防げるということです。他のベンダーより先に攻撃を検出し、正確かつ論理的な警告を行い、世界においても業界最高水準で、最も速く多段階のフォレンジック調査から得られた攻撃の兆候をたどることにより、企業は今後侵害について心配をする必要がなくなります。

セキュリティへの最短距離

世界でも独特の台湾のサイバー脅威の現状を踏まえ、世界で最初の本格的なフォレンジックベースの AI 分析を構築し、人間のアナリストの行動を自動化し、新しい AI を作り上げ、世界レベルの研究者のチームを採用することにより、CyCraft の MDR は他のソリューションでは得られない安心感をもたらします。セキュリティの状況が完全に制御されているという事実はかけがえのないものです。CyCraft の無料トライアルで、最も速く、正確で、簡単で、綿密な MDR ソリューションをご体験ください。

CyCraft

政府機関、Fortune Global 500 の企業、大手の銀行や金融機関、主要インフラ、航空会社、遠距離通信企業、ハイテク企業、SME などで、CyCraft の高速・正確・簡単・綿密なセキュリティソリューションが導入されています。

CyCraft は独自の AI と自動化テクノロジー（CyCraft AIR）を SOC に導入し、管理された検出および応答（MDR）を、統合グローバルサイバー脅威情報（CTI）、脅威情報ゲートウェイ（TIG）、エンドポイント保護（EPP）、ネットワーク検出および応答（NDR）、エンドポイント検出および応答（EDR）セキュリティオペレーションセンター（SOC）ソフトウェア、自動生成インシデント対応（IR）レポート、システム規模のネットワーク健全性チェック、「Secure From Home」サービスの形でご提供しています。

2020 年に、CyCraft は MITRE ATT&CK®の評価対象となっている他のすべてのベンダーを、設定変更なしで、テクニック、戦術、一般の検出で上回りました。CyCraft AIR と CyberTotal は Interop Tokyo 2020 でセキュリティソリューションについて「Best of Show」の最優秀賞を受賞しました。また、CyCraft は 2020 Cybersecurity Excellence で、管理された検出と応答、インシデント対応、脅威情報、人工知能などの分野で、25 を超える賞を受賞しました。CyCraft はインシデント対応セキュリティチームの最高の企業である FIRST のメンバーです。

エンドポイントからネットワークまで、調査からブロックまで、社内からクラウドまで、CyCraft AIR は、中小企業から大企業まで、現代のあらゆるセキュリティ脅威から守るために必要な、プロアクティブでインテリジェント、かつ適応性の高いセキュリティソリューションを提供するために必要なすべての側面をカバーしています。

AI 主導型フォレンジック・ソリューション CyCraft AIR を利用した「サイバー攻撃監査サービス」

AI によって導かれたサイバー攻撃監査レポートを活用し対策することで、フォレンジック調査時間の大幅短縮や二次被害のリスクを軽減します。

エンドポイントから収集した情報をAIで分析する仕組みにより「早期の脅威発見」、「専門知識不要で調査可能」、「人員面での作業負荷軽減」を実現

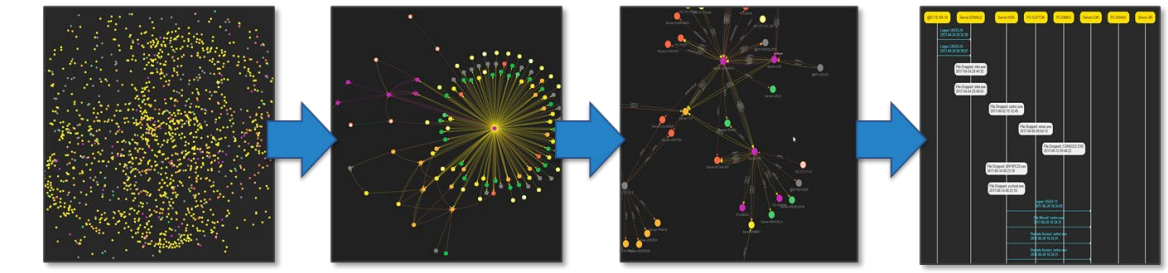
早期対処
- 脅威発見から3時間でリスク可視化と優先順位付け
  短時間で即座に対象デバイスを特定 （隔離、駆除するため）
  ※事故後でも対応可能。残存する情報に基づく調査

簡単確実
- AI により速やかに分析、レポートを提供
  専任者不在や専門知識が不要に

高効率
- ネットワーク全体の脅威全貌を網羅的に把握可能
  一部調査 → 空振り → 別セグメント再調査 といったロスを削減

調査が短時間で済む理由～AI の活用

AI （CyCraft AIR）による調査



PC全ての情報を自動収集（スキャン） → 相関性の検出 データの最適化 → 自動ストーリーライン インシデントのみを特定 → 根本原因解析 タイムライン生成

1ヶ月から3時間へ

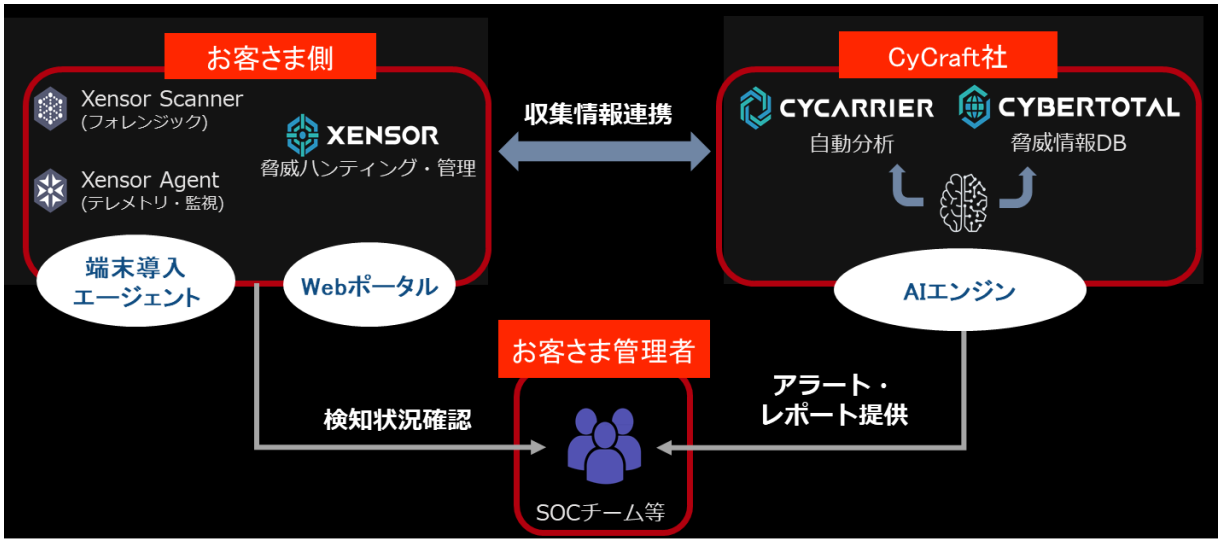
その他の利点：大量データの効率的処理、見落とし・間違い等ミスが削減、調査結果にムラが生じない等

CyCraft AIR のプラットフォームについて

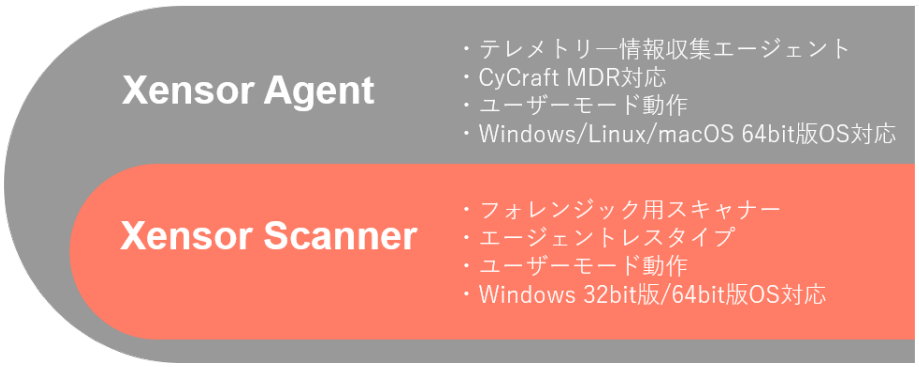
お客様への情報提供は2つのプラットフォームで構成しています。

・情報収集/端末状況：Xensor

・AI 分析/脅威情報 DB：CyCarrier/CyberTotal



クライアントツール XENSOR(ゼンサー)について



常駐監視・サーバ指示対応機能を持ち、常駐版ではScannerと合わせて提供

端末フルスキャン機能を提供。ワンタイム版ではScannerのみの提供

※Linux/MacOS 版は XensorAgent に XensorScanner 機能を搭載しています。

※クライアントツールはお客様側にて端末への配布を行って頂きます。

項目		サポートの必要条件
対応 OS		Windows (x64): XP SP3/7/8/10, Windows Server 2003R2 – 2019
		Linux (x64): Ubuntu9.10 - 20.10, Debian7.0 - 10.8, RHEL6.0 - 8.3, CentOS6.0 - 8.3, OpenSUSE 15.1
		Mac (x64): MacOS10.10 - 10.15, 11.2
		(※Windows XP SP3、Windows Server 2003 R2 については Scanner のみ対応、HTTPS 非対応)
ハードスペック	CPU	2 コア以上
	RAM	4GB 以上
	HDD	100MB 以上
Linux/Mac のみ		Python 2.7 以上が必要

※2021 年 9 月現在

提供サービス（ワンタイムサービスと常駐型 MDR サービス）

ワンタイムサービスは、CyCraft AIRを用い端末に一時的なエージェントを配布し、スキャンして収集した情報をAIが自動解析を行い、脅威の有無、脅威の内容、感染拡大状況等について短時間で自動レポートを提供するものです。

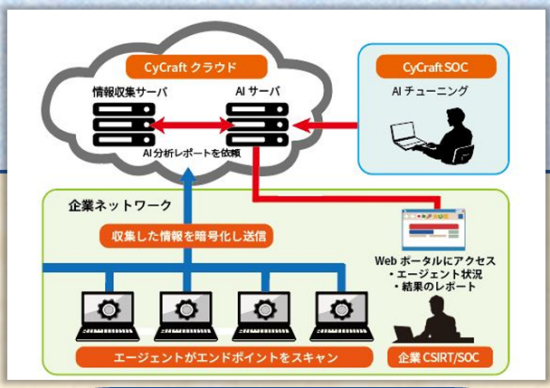
■1000台までの1回のスキャンとレポートの提供が基本サービス単位となります。

■ライセンスの有効期間は1年間です。

ワンタイムサービス

■提供レポートは１種類となります。

■一度レポートを発行すると、以降ライセンスは無効となりますのでご注意ください。



■100台以上の単位でのご契約となります。

■ライセンスのご契約期間は1年間を基本とし、複数年契約による割引がございます。

常駐型MDRサービス

■サービスレベルにより、レポート提供時間や提供種類が異なります。

■レポートには脅威の都度発行されるものと、定期的に提供されるものとがございます。

常駐型MDRサービスは、CyCraft AIRを用い端末に常駐するエージェントを配布し、スキャンして収集した情報をAIが自動解析を行い、脅威があればアラートを発報し、脅威の内容、感染拡大状況等について短時間で自動レポートを提供するものです。

レポートサンプル

ワンタイム・常駐型 MDR いずれのサービスでもご提供の「サイバーシチュエーションレポート」のご紹介

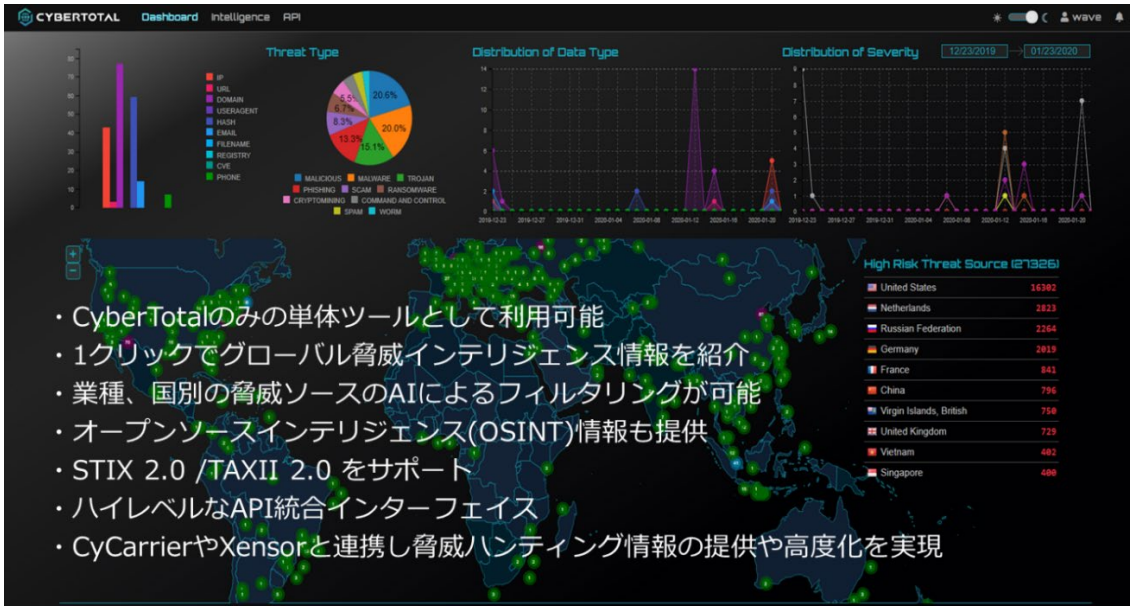
全体として指定期間に監査がどの程度行われ、結果としてどの程度脅威が見つかったかダッシュボード形式でわかりやすく提供

端末単体での脅威の実行状況や、他の端末との相関作用について、ストーリーラインとして詳細情報をご提供

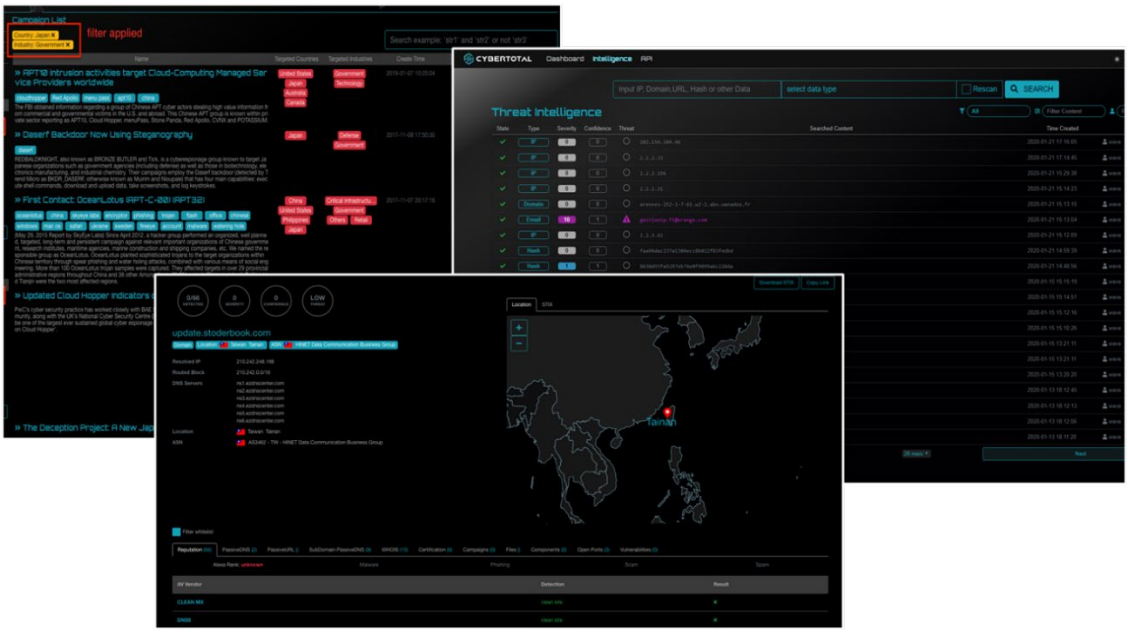
その他、実行されたコマンド詳細、脅威のファイルやプロセス情報、監査を行った端末リスト、分析コメントなどの情報も併せてご提供いたします。

グローバル脅威インテリジェンスプラットフォーム 「CyberTotal」について

CyberTotal は、ハイクオリティな脅威インテリジェンスを提供するために、各種グローバル CTI 情報ソースを統合し完成したプラットフォームです。CyCraft 社のサイバーインテリジェントチームが、長年にわたりさまざまな形態の侵入を追跡し、APT グループに関する履歴情報も含まれています。



検索 Query を活用することで、様々な脅威インテリジェンスデータを同時に閲覧可能、SOC/CSIRT のアナリストご担当者様に最適なツールです。



※CyCraft AIR は台湾 CyCraft 社の製品です。

【販売会社】株式会社セキュアブレイン
〒102-0094　東京都千代田区紀尾井町 3-12 紀尾井町ビル 7F 電話：03-3234-3001、FAX：03-3234-3002
e-mail:　sales@securebrain.co.jp　　https://www.securebrain.co.jp/