CYCRAFT

CRAFT FOR RESILIENCE
CYCRAFT

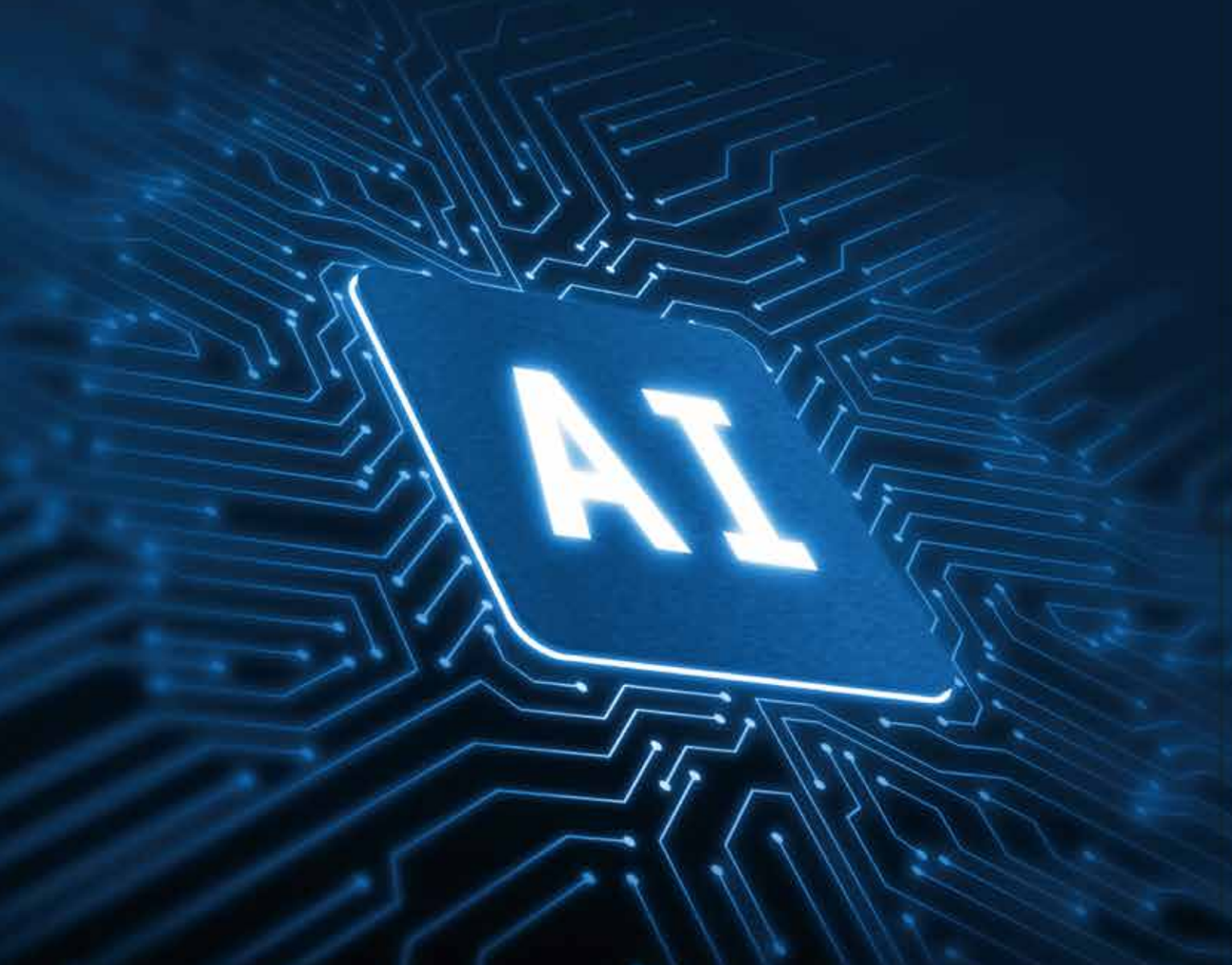
CRAFT FOR RESILIENCE.
CYCRAFT

サイクラフト
CyCraftは、サイバーセキュリティの未来を創造するAI企業です。私たちが提供するCyCraft（サイクラフト） AIRは、自律システムと、人とAIとのコラボレーションにより、MDR、インシデントレスポンス、脅威ハンティングを的確に実行。SOC、フォレンジック、ディテクション、レスポンスなど一連の工程をスマートに自動化します。その実力は、すでに多くの「フォーチュン・グローバル500」企業、政府関連機関で立証されています。

サイクラフト
CyCraft　AIRを構成するアプリケーションは3つ。エンドポイントで脅威のエビデンスを収集するXensor（ゼンサー）。すべてのエビデンスの相関処理と挙動分析を自動的に行うCyCarrier（サイキャリア）。そして、脅威を確認し、グローバルな情報に参照して解析するCybertotal（サイバートータル）。

サイクラフト
CyCraft　AIRは、効率的かつグローバルレベルの実効性を備えたサイバーレジリエンスソリューションです。

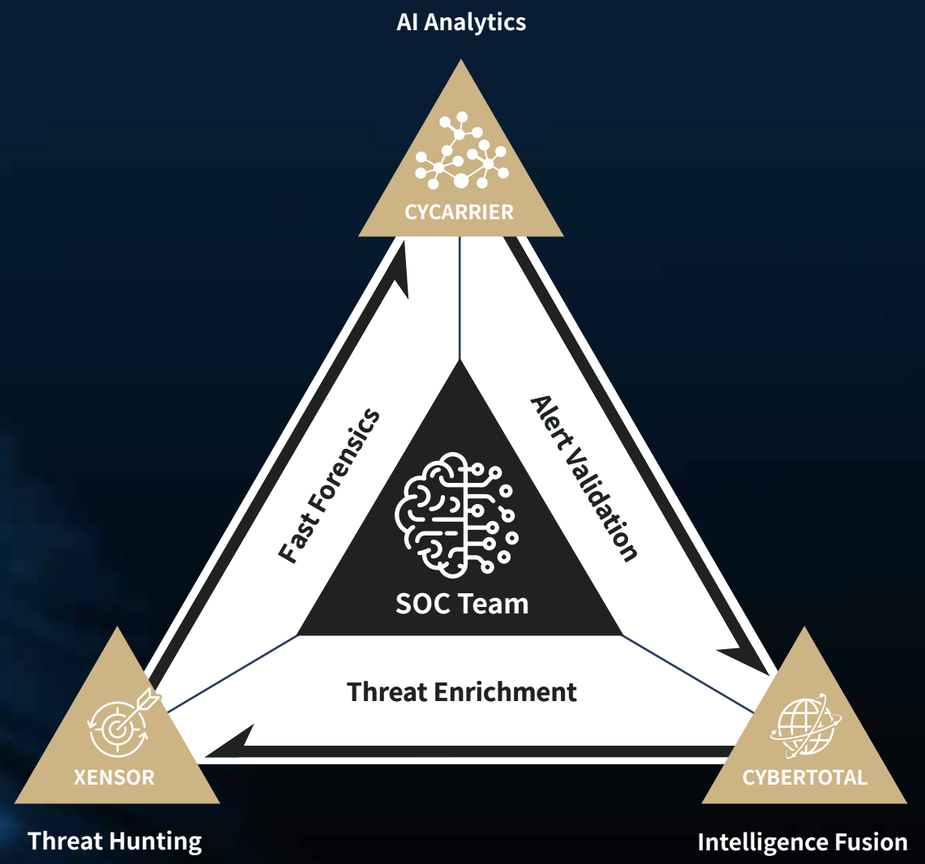
www.cycraft.com



AIが実現する、自動化、高度化、強靭化

自動 | インテリジェンス | レジリエンス

CyCraft（サイクラフト） AIRは、オンプレミスでもクラウドでも、フレキシブルに対応。膨大なエンドポイントからスキャナーが情報を収集し、AIが自動解析。サイバー状況を迅速に把握し、問題に対処します。
インターフェイスはさまざまな情報が視覚化され、簡単にセキュリティ管理が可能。多彩な機能を直感的にコントールできます。
デジタルフォレンジックケースマップ、トポロジーによる根本原因及びストーリーライン分析を、グローバルな脅威インテリジェンスを照合しながら、通常のセキュリティ機器やサービスが検出できない、重大な脅威を暴き出します。



自動

オンプレミス／クラウド対応
リモートで応急対処
カスタマイズ可能なレポート

インテリジェンス

APT状況分析
的確なアラート通知
AIアナリスト機能

レジリエンス

デジタルフォレンジック
根本原因／ストーリーライン解析
グローバルCTI照合

CyCraft（サイクラフト）マシンラーニング機能を備えたCyCraft独自のセンサーが、脅威分析と関連する推論に対応。迅速な自動事例調査、攻撃状況マーカー及び根本原因解析を実行します。隠れた脅威を見つけ出し、セキュリティとレジリエンスを強化することで、SecOps（セキュリティ運用）を効率的かつ高精度に進めます。

XENSOR (ゼンサー)

次世代型MDRエンドポイントセキュリティシステム

XENSOR (ゼンサー)

独自のフォレンジック遠隔測定技術とマシンラーニングの融合により、Xensor（ゼンサー）はエンドポイントに遠隔でアクセス。効率的なトリアージと、インシデント調査、脅威ハンティングを実行します。

一般的なセキュリティ製品とは一線を画すXensor（ゼンサー）は、多元的な脅威インテリジェンス、UEBA、プログラムメモリーフォレンジック、エンドポイントコンピュータフォレンジック、ネットワークトラフィック分析など、多彩な機能を統合的に備えています。ウイルスシグネチャーや機能ルールを追加することなく、素早い対応とコストの削減を実現します。

あらゆる環境に適合

オンプレミス／クラウド、エージェントベース／インストールフリー、環境を問いません。

フォレンジックを強化

Windows、Linuxに対応した積極的な脅威ハンティングを実行。最新の脅威やハッカーの侵入経路を見つけ出すなど、詳細なフォレンジック調査が可能。

セキュリティ業務を効率化

セキュリティチームの作業効率を高め、迅速な対応、費用の最少化を実現することで、事業活動の強化に貢献。

特長

- インテリジェントなATP状況認識
- 効率的、軽量、マルチプラットフォーム
- 24時間365日監視体制による迅速な対応
- マルウェア＆メモリフォレンジック
- 国際的なセキュリティフレームワークMITRE ATT&CK の統合による攻撃チェーンの特定

対応オペレーティングシステム

・Windows
Windows XP SP3/7/8/10
Server 2003 R2 - 2019

・Linux
Ubuntu 9.10 - 20.04
Debian 7.0 - 9.0
RHEL 6.0 - 8.1
CentOS 6.0 - 8.0

・MAC
MacOS X10.10～

CYCARRIER (サイキャリア)

AI主導型セキュリティオペレーションセンター

積極的な脅威ハンティング

ゼンサー　サイバートータル
Xensor、Cybertotalを統合することで、社内外の情報を結集し、最新の脅威を積極的に特定することができます。

多元的な脅威分析

根本原因解析、攻撃シーケンスダイアグラム、事例タイミングダイアグラムなど、相互に関連した情報を多元的に分析することで、迅速かつ正確に脅威に対応できます。

フォレンジック調査事例の概要

当社の状況認識テクノロジーにより、フォレンジック環境や複雑に絡み合う脅威行動の全体像を、容易に把握しています。

CYCARRIER (サイキャリア)

従来のMSSPやSOCでも、迅速にアラートを発することは可能です。しかし、誤検知への対応や、その後のセキュリティ調査、とくに根本原因解析については、非効率的で、リソースも時間もかかりすぎるのが現状です。昨今では、サイバーセキュリティ分野での人材の確保が難しいこともあり、日々進化するハッカーの攻撃にいかに対処するかが、大きな課題となっています。

サイクラフト
CyCraftは、世界トップレベルのAI主導型サイバーセキュリティシチュエーションセンターを構築。当社の特許技術であるAIアナリストと、トップレベルのセキュリティエキスパートチームのコラボレーションにより、常に最新のセキュリティ分析を提供。ハッカーに隠れる余裕すら与えません。

すべてのエンドポイントデータを収集し、ひとつにまとめて解析することで、セキュリティチームは、遠隔によるフォレンジックが可能になります。サイキャリア
CyCarrierのインターフェイスは、さまざまな情報が視覚化され、直感的なセキュリティ管理が可能。企業内のセキュリティ脅威を素早く把握し、最新のAIとエビデンスに基づき、各事例の発生状況を自動的に分析します。

AIエージェントのコンテキスト推定により、マルウェアアソシエーションマップ（ファイル照会）、プログラム行動アソシエーションダイアグラム（コールグラフ）、攻撃コンテキストチャート（ラテラルムーブメント）、そして、侵入事例タイミングダイヤグラム（ストーリーライン）などを自動生成。ワンランク上のセキュリティ管理を実現します。

特長

- セキュリティ状況認識の視覚化
- インテリジェントなAI分析
- オートマティック事例分析
- コラボレーション型調査とチーム管理
- MSSP/SOCチームの効率性の向上
- 脅威分析レポートの迅速な生成
  （HTML、PDF、STIX、YARA、SNORTなどに対応）
- 英語/日本語/中国語版レポートに対応

CYBERTOTAL (サイバートータル)

グローバル脅威インテリジェンスプラットフォーム

リスクに基づく直感的トリアージ

マシンラーニングによって、世界のさまざまなCTIソースを自動集約。
重要度、信頼性など、さまざまな脅威指標を提供します。

重要なアラートに素早くフォーカス

社内外からの脅威を感知すると、統計的処理を通して脅威の重大性を数値化し、最も重要なアラートにすばやくフォーカス。

人件費削減に貢献

格付け、相関処理、集約などを駆使した精度の高いアラートで、セキュリティ担当者は無理なく正確にアラートを分類・処理できます。

CYBERTOTAL (サイバートータル)

脅威インテリジェンスや関連するセキュリティ情報の共有は、攻撃を早期に検知し、抑止しするために重要な施策です。しかし、従来のサイバーセキュリティ脅威インテリジェンス（CTI）は、IP、ドメイン、MD5の既存のブラックリスト情報を交換するのみで、ハイレベルなハッカーに関する情報は不足していました。

サイクラフト
CyCraftのサイバーインテリジェントチームは、ハイクオリティな脅威インテリジェンスの提供するために、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を提供し、また、各種グローバルCTI情報ソースを統合してきました。
そして、自動AI相関分析とナレッジベースの最適化によって、企業が脅威に対し迅速に反応し、識別し、セキュリティアラートを検証できるようサポートしています。

- サイバートータル CyberTotalでは、14種類の脅威指標に対応するする包括的な情報セキュリティディクショナリを提供しています。
- サイバートータル CyberTotalでは、STIX 2.0の状況レポート機能が利用できます。また、ISACで交換される情報を受け渡しするためのTAXIIに対応しています。
- サイバートータル CyberTotalには、充実したAPI統合インターフェイスが用意されているため、脅威ハンティングやセキュリティと容易に統合できます。

*企業は有料のAPIキーを提供してソースを拡張できます。

特長

- 1クリックでグローバル脅威インテリジェンスを照会
- 業種、国別の脅威ソースのAIによるラベリング
- オープンソースインテリジェンス（OSINT）
- 民間かつ私有のインテリジェンスソース
- STIX 2.0 ／TAXII 2.0 をサポート
- ハイレベルなAPI統合インターフェイス
- サイキャリア ゼンサー CyCarrier、Xensorとの統合で、脅威ハンティング、データエンリッチ化を実現

ADDRESS : 〒100-0004 東京都千代田区大手町一丁目９番２号大手町
フィナンシャルシティグランキューブ３階 Global Business Hub Tokyo
MAIL : contact@cycraft.com　TEL : 81-(0)3-6378-1053

www.cycraft.com