ISRAEL CYBER ALLIANCE

B2B Meetings for Start-Ups

サイバーテック東京 2017, Japan

2017 年 11 月 30 日

Prime Minister's Office
National Cyber Directorate
National Cyber Bureau

ISRAEL EXPORT INSTITUTE

Ministry of Economy and Industry
Foreign Trade Administration

The Israel Export & International Cooperation Institute's (IEICI) Cyber Security Unit

Represents more than 300 Israeli companies in the cyber security field, and works tediously to maximize the effectiveness of their business engagements with foreign counterparts, as well as in foreign markets. The unit exposes Israeli capabilities and innovative cyber security solutions to potential foreign clients and partners, either as stand-alone solutions or as an overarching tailor-made suite of solutions, accommodating their specific short and long term needs. To that end, the unit, which plays a key role in the Israeli ecosystem and is well-acquainted with the needs of the local cyber industry, holds the most comprehensive and up-to-date database of Israeli-based cyber security companies.

The unit is a joint venture of IEICI and its major governmental partners, the Foreign Administration at the Ministry of Economy and the Israel National Cyber Directorate in the Prime Minister's Office, leveraging their expertise and national assets in order to achieve the unit's and the industry's objectives.

Israel's Foreign Trade Administration in the Ministry of Economy, which is responsible for managing and directing the international trade policy of the State of Israel, with its 40 plus economic missions throughout the world that are dedicated to facilitating trade relations and investment opportunities between local companies and Israeli companies.

The Israel National Cyber Directorate in the Prime Minister's Office, serves as the Prime Minister's and government's staff, which devises a national cyber defense policy, promotes its implementation, and provides recommendation on cyber-related matters. It strives to advance the State of Israel's leading posture as a global powerhouse for cyber security-related research and development, by investing dedicated resources in the Israeli academy, human capital, and cyber security industry. It enhances the cooperation and synergy between the private sector, the government and international partners, in order to create a unique and dominant cyber security ecosystem in Israel.

The Israel Export & International Cooperation Institute

Mr. Achiad Alter,
Manager, Cyber Security
achiada@export.gov.il

Ms. Meytal Shavit
Marketing Coordinator, Cyber Security
Meytals@export.gov.il

Ms. Yaara Sabzerou,
Marketing Coordinator, Cyber Security
yaaras@export.gov.il

The Economic Mission to Tokyo, Japan

Mr. Assaf Marco
Trade Officer, Homeland Security & Cyber,
Tokyo, Embassy of Israel
hls@tokyo.mfa.gov.il

Contents

BGProtect は、小規模の法律事務所から国家レベルの幅広い顧客を経路ハイジャック攻撃から保護するサービスを提供しています。テルアビブ大学での 20 年にわたる研究から得た知識をもとに、インターネット上の経路を監視し、経路上の異常を特定する独自のシステムを開発しました。ハイジャックが検知された場合、（顧客の了承を得た上で）ハイジャックによる被害を抑えるための対策を講じます。BGProtect のサービスによって、BGP ハイジャックやデータプレーンの不正操作を中心に、様々な技術によるハイジャック攻撃を防ぐことができます。また BGProtect は、ルーターの IP アドレスの地理的な位置情報を独自にデータベース化し、それを基盤としたネットワークインテリジェンスサービスを、主に政府機関に提供しております。

製品とテクノロジー

昨今、経路ハイジャックの技術は、敵対的政府や犯罪組織に使用されることが多くなりました。攻撃者はオンライン上で被害者になりすまし、インターネットトラフィックを傍受し、記録し、改ざんします。たとえ強度の高い暗号化機能を備えていても、攻撃対象の機関とそのユーザーに対し、様々な中間者攻撃を行うことができるのです。

インターネットに接続している機関はすべて、経路ハイジャックの被害者になりえます。政府機関、重要なインフラを担う企業、金融機関、その他大企業などは特に標的として狙われています。
BGProtectは、あらゆるタイプのハイジャック攻撃を特定し、顧客の被害軽減策を管理するサービスを提供しています。

詳細はこちら- www.bgprotect.com

CyberX

CyberX は、主要産業インフラのリスクを継続的に低減することを目的とした産業用サイバーセキュリティプラットフォームを提供しており、最も幅広く採用されています。弊社は、ガートナー社から「優れたベンダー」と称されていることや、米国国土安全保障省や国防総省が後援しているSINET16 Innovator Award で ICS セキュリティサプライヤーに唯一選ばれるなど、業界内で高い評価をいただいています。CyberX のプラットフォームは、所有者の異常挙動検知システムや自己学習アルゴリズムを、産業用制御システム（ICS）特有の IT 資産を把握する手段や、脅威インテリジェンス（脅威情報）、リスクの分析手法と組み合わせて使用し、ICS に対する脅威を継続的に監視します。また、弊社は顧客の最も重要な ICS 資産への攻撃経路を特定して可視化する、独自の攻撃ベクトルシミュレーションサービスも提供しています。

製品とテクノロジー

CyberX プラットフォームは、継続的にリスク評価を行い、リスクスコアとして管理レポートに記載し提示します。業界内で唯一、重要な ICS 資産を標的とした一連の攻撃ベクトルで最も可能性の高いものを予測し、脆弱性を利用される前に、攻撃を想定した予防策を講じることができます。これにより、顧客はファイアウォールなど、境界を保護する従来のセキュリティ以上に、多重構造の積極的なサイバー防衛戦略を実施することが可能になります。

詳細はこちら- www.cyberx-labs.com

Cyiot

CYIOT は、全てのスマートデバイスとコネクテッドデバイスを対象としたサイバーセキュリティ総合支援サービスを提供するイスラエルのスタートアップ企業です。

製品とテクノロジー

CYIOT ソリューションによって、ネットワークの「電波傍受」、マッピング、そしてモニタリングを継続して行うことで、全てのスマートデバイスとコネクテッドデバイスを完全に可視化することができます。それに加え、データサイエンスを活用し、脅威や悪意のある行為の正確な検知を確実に行います。

詳しくはこちら- www.cyiot.net

Cronus Cyber Technologies

Cronus は、顧客の事業継続性を保つことを目的に、重要な IT 資産と業務プロセスを標的とした攻撃を予測して予防することができる、CyBot というサイバーボットを開発しました。

弊社は、インフラとウェブの両方を対象とした脆弱性をスキャンする次世代の企業で、特許取得済みの Attack Path Scenarios（攻撃経路シナリオ）技術を使用して、顧客の重要な資産を標的とした脅威をリアルタイムに明示します。CyBot は、顧客企業の事業に脅威を与える実質的な深刻度に応じて、効率的に脆弱性に優先順位を付けます。Cronus は Cybersecurity 500 の世界的に最もホットなサイバー企業の一つに認定され、CB Insights からはサイバー業界に変革を起こす 12 の企業の 1 社に選出されました。ぜひ、無料試用版を www.cronus-cyber.com にてご利用ください。

製品とテクノロジー

Cronus は顧客の事業継続性を保つことを目的に、業務プロセスを標的としたサイバー攻撃を予測して予防することができるサイバーボット（CyBot）を開発しました。CyBot は、自社内の本番環境にバーチャルマシンとしてインストールし、24 時間 365 日稼働して、リアルタイムの監視を世界的に行い、攻撃を防止するツールです。このツールは、重要な資産や業務プロセスを標的とした攻撃経路の一部となる脆弱性を、全体の 3%未満に絞り込むので、ウェブやインフラのスキャン中に誤検出されるアラートに悩まされる情報システム部門にとって心強い味方になります。

詳細はこちら- https://cronus-cyber.com/

Intezer

Intezer は、生物の免疫システムの概念をサイバーセキュリティ分野で再現することで、他に例を見ない脅威検知システムを企業に提供し、早急なインシデント対応を可能にします。弊社は CyberArk の創業者や IDF Incident Response Team の元トップなど、経験豊かなサイバーセキュリティのプロによって設立されました。

製品とテクノロジー

Intezer Analyze™ は、クラウド上のマルウェア分析サービスで、マルウェアと信頼できるソフトウェアに関する大量のデータベースとコードを大規模に比較することで、全ての実行ファイルを幅広く把握することができます。直感的なウェブインターフェイスと API アクセスで、顧客企業のインシデント対応策における、あらゆるプロセスのためのプラグアンドプレイソリューションとして機能します。

詳細はこちら- www.intezer.com

Ironscales

人間の知能を機械学習と組み合わせて、多重化・自動化された解決手法で、現代の巧妙な E メールフィッシング攻撃を自動で予防し、検知し、対応する、世界初で唯一の E メールフィッシング対策テクノロジーを提供します。

製品とテクノロジー

IronSights- 世界初にして唯一の、メールボックスレベルのフィッシング検知システムです。

IronTraps- フィッシングインシデントに最も素早く、完全に自動で対応します。

Federation- フィッシング情報をリアルタイムに自動で共有する唯一のシステムです。

IronSchool- 最も高度なシミュレーションと意識向上トレーニングを行います。

詳細はこちら- ironscales.com

Karamba Security

KarambaのAutonomous Securityは、受賞歴もあるソフトウェアで、車両の電子制御ユニット（ECU）をサイバー攻撃から守ります。弊社が開発したCarwall®ソフトウェアは、ECUの工場設定が不正に変更されることを防止します。実行時には、この埋め込まれたCarwall®によって、異質なコードやメモリに潜む攻撃が、工場設定からの逸脱と認識され、ハッカーが車のシステムに侵入する前にブロックできます。Carwall®は開発環境とシームレスに統合されており、ECUのハードやソフト、デベロッパのリソースに変更を加える必要はなく、開発の工程を邪魔することもありません。Karamba Securityは異常を誤検知することなく、且つ、マルウェア対策ソフトをアップグレードし続ける必要もない、サイバー攻撃対策を提供します。

製品とテクノロジー

Carwall は、ECUのソフトウェア実行環境を堅牢にし、全ての攻撃計画を検知し、未然に防ぎます。コード内のセキュリティバグを修正することはせず、車両走行に必要なECUの工場設定にしたがった動作のみを許可することで、セキュリティバグを悪用されないようにします。

Carwallは、顧客のソフトウェア開発環境にシームレスに統合し、自動的にサイバー攻撃から顧客のソフトウェアを隠ぺいして保護します。埋め込まれた動作の軽いCarwallには、複数のセキュリティレイヤーが含まれています。例えば、メモリ内に潜む攻撃を回避するためにメモリ内の機能フローを有効にすること、プログラムを強化して、工場設定どおりにロードするようにすること、アーキテクチャの欠陥が発生しないようにECUのインターネット接続をコントロールすること、外部機器からの入力をコントロールし、周辺機器からのマルウェアの侵入を防ぐことなどです。

詳細はこちら- https://karambasecurity.com/

Kryon

2009年に創業したKryon Systemsは、画期的で高度なロボティックプロセスオートメーション（RPA）ソリューションを提供し、企業のデジタル革新を実現しています。弊社の主力プラットフォームのLeoには、特許取得済みのビジュアルラーニングとディープラーニングテクノロジーを使用しており、企業の業務プロセスを素早く簡単に自動化することで、いち早く生産性を高め、ミスの発生を0％近くに抑え、コストを下げて、大幅なROI向上を実現します。

製品とテクノロジー

弊社のソフトウェアロボット Leo は、仮想知的労働者と人間を同じように支援し、どのような企業アプリケーションの業務プロセスでも正確に効率よく実行できるようにします。Leo RPA プラットフォームは、人の手を介さない作業（バーチャルマシン）と人の手を介する作業（デスクトップ）の自動化と、仮想知的労働者と人間が相互に作用するハイブリッドオートメーションにも活用することができ、オートメーションへの投資に対する ROI を向上させ、全社的な業務プロセスの改善を実現します。

詳細はこちら- http://www.kryonsystems.com/

Nubo Software は、企業モビリティのための仮想モバイルインフラ（VMI）を開発した初の企業であり、今日の移動しながら働く従業員に最適でセキュアなリモート仮想ワークスペースを開発しました。当初から、Nubo の VMI テクノロジーはモバイルコンピューティングに対するニーズと、企業のセキュリティに対する、データセントリックなアプローチを元にして生まれました。

Nubo Software

Nubo の革新的なモバイルセキュリティの手法を使用すれば、個人のデバイスにデータを保存せずに、ネイティブアプリのように処理を実行することを可能にします。

Nubo のテクノロジーを利用すると、顧客企業はデータとアプリケーションを管理し、従業員は端末を管理することになります。企業に所属するユーザーは、個人所有のデバイスからでも安全に、楽しく、且つ極めて簡単に仕事をすることができるのです。

製品とテクノロジー

Nubo は、企業モビリティのための仮想モバイルインフラ（VMI）ソリューションを開発・提供している、先駆的なリーディングカンパニーです。

Nubo Software は、今日の移動しながら働く従業員に最適でセキュアなリモート仮想ワークスペースを開発しました。

Nubo のテクノロジーを利用すると、顧客企業はデータとアプリケーションを管理し、従業員は端末を管理することになります。

Nubo の革新的なモバイルセキュリティの手法を使用すれば、個人のデバイスにデータを保存せずに、ネイティブアプリのように処理を実行することを可能にします。

詳細はこちら- nubosoftware.com

ReSec Technologies

ReSec は、2012 年に軍のサイバーディフェンスの専門家によって設立され、従来のマルウェア対策用検知システムの限界に対処するため、Content Disarm and Reconstruction テクノロジー（コンテンツ武装解除・再構築技術：CDR）を開発しました。ReSec の製品は、銀行、金融、製造、通信、医療、官公庁など、部門の枠を超え、多数の一流企業に採用されています。

製品とテクノロジー

ReSec の CDR は、全てのファイルを処理し、コンテンツ構造を分析し、機能性を保ったまま複製ファイルを再作成します。CDR によって疑わしい要素は排除され、全てのユーザーが確実に安全なダウンロードファイルを受け取れるようになります。また、万が一のときは、オリジナルのコンテンツを参照・分析できるように、ネットワークの外に安全に保存する機能もあります。

詳細はこちら- www.resec.co

SaferVPN

SaferVPN は、2013 年に、IDF インテリジェント技術部隊出身のベテラン達により、設立されました。弊社は、次世代のリモートアクセスと WiFi のセキュリティを専門としており、以下の 3 つの事業部門を持っております。

a. ホーム用 SaferVPN – 世界中のコンシューマーに、インターネットアクセスをセキュアに、ウェブの閲覧を私的なものとします。

b. ビジネス用 SaferVPN – 企業に対して、カスタマイズされたアクセス・ゲートウェイを展開し、従業員が容易に重要なネットワーク・リソースにアクセスでき、クラウド環境を使うことができるようにします。

c. OEM 用 SaferVPN – いくつかの大きなインターネットセキュリティ企業とパートナーシップを進めております。

製品とテクノロジー

弊社の新しい Software defined Perimeter (SDP) サービスであるビジネス用 SaferVPN は、企業に対して、カスタマイズされたアクセス・ゲートウェイを展開し、従業員が容易に重要なネットワーク・リソースにアクセスでき、クラウド環境を使うことができるようにします。企業は、ますます分散化されたクラウドベースのサービスに依存しているので、このような技術の必要性は、急速に高まっています。

上記の認知されたクラウド・セキュアード・ネットワーク・アクセス(Cloud Secured Network Access)製品に加え、SaferVPN が特許出願中の自動 WiFi セキュリティ(Automatic WiFi Security)は、コンシューマー市場とビジネス市場の両方で、使用可能です。これにより、コンシューマーは、ウェブ閲覧やオンラインショッピングをセキュアでない公衆 WiFi ネットワーク上で、安全に使うことができ、企業は、効果的で自動化された方法で、従業員が外出先でも、モバイルデータを保護することが可能となります。

詳細はこちら- https://www.safervpn.com/business