ニュースリリース

＊英語版と日本語版の間に内容の相違がある場合は、英語版を正とします

シンガテルと米ファイア・アイ、企業による高度なサイバー攻撃への対抗を支援するため、アジア太平洋地域に初の共同アドバンスト・セキュリティ・オペレーション・センターを開設

シンガポール、2015 年 2 月 25 日 – Singapore Telecommunications Limited（シンガテル）と FireEye, Inc.（NASDAQ: FEYE）は、本日、両社の初の提携事業となるアドバンスト・セキュリティ・オペレーション・センター（ASOC）を開設しました。この新しい ASOC では、業界をリードするファイア・アイのセキュリティ専門知識と、シンガテルの優れた情報通信能力および広範囲の域内データ・インフラストラクチャーを統合します。

シンガテルとファイア・アイによる ASOC は、最新の技術、専門知識および情報を組織に提供し、アジア太平洋地域で急増する高度なサイバー攻撃に対するセキュリティ保護を強化します。

シンガポールを拠点とするこの ASOC は、シンガテルの既存のネットワーク・オペレーション・センターに統合される初のセキュリティ・オペレーション・センターとなります。この統合により、サイバー・セキュリティのエキスパートが、インターネット・トラフィック、企業ネットワークおよびユーザー・エンドポイントをエンドツーエンドで可視的に認識できるようになるため、セキュリティ・インシデントに対する迅速な対応が可能となります。

ASOC に地域内に 50 名のセキュリティ専門担当者を配置しており、ファイア・アイの SOC[1] のグローバル・ネットワークにアクセス可能で、高度なサイバー脅威とフォレンジックに精通したファイア・アイのセキュリティ・エキスパートを有しています。シンガテル-ファイア・アイの顧客は、サイバー脅威を検出して被害を防ぎ、攻撃に対処するために 24 時間 365 日体制で'follow-the-sun（太陽を追う）'サービスを提供するエキスパートのサポートを受けることが可能になります。（ASOC の詳細については、付録を参照してください。）

ASOC の開設に伴い、シンガテルとファイア・アイは、共同で初の東南アジア・サイバー脅威レポートを発表しました。このレポートでは、同地域の顧客から収集した実際の攻撃

データに基づいた脅威の見通しを詳細に調査しています。たとえば、レポートでは、2014年7月から12月の間に、シンガポールの顧客の23%が高度な攻撃にさらされていたことが報告されています。

シングテル Group Enterprise の CEO である Bill Chang 氏は、「サイバー攻撃は、特にアジア太平洋地域において頻度を増し高度化しており、多くの企業の経営陣にとって重大な懸念となっています。サイバー攻撃がもたらす被害は、技術上の問題にとどまりません。企業はこのことを認識しており、自社の資産、ブランド・イメージ、顧客の信頼を守るため、より優れたサイバー・ディフェンス能力を求めています」と述べています。

さらに Chang 氏は、「ASOC は、シングテルのサイバー・セキュリティ能力の基盤となるでしょう。ファイア・アイとのパートナーシップによって、シングテルは、進化の速いこれらのサイバー脅威に、より効果的に対処する最善のサイバー・セキュリティ・ソリューションとサービスを企業に提供できるようになりました」と付け加えています。

———（脚注）

[1] ファイア・アイのセキュリティ・オペレーション・センター（SOC）は、米国、ヨーロッパ、オーストラリア（近日開設）に拠点を構えています。

———

ファイア・アイの CEO 兼会長である David DeWalt 氏は、「私たちは、匿名で活動し、ほぼあらゆるネットワークに自由に侵入する国民国家や高度化した犯罪組織との間に発生する新手のサイバー軍備競争を目の当たりにしています。東南アジアは、経済成長と地理的な近接性のせいで、世界でも最も激しく高度なサイバー攻撃が行われている地域の1つとなっています。シングテルと提携すれば、これらの攻撃に対するより優れた可視性を顧客に提供し、私たちが業界最高であると確信するツールや専門技術を用いて顧客のネットワークを安全に保つことができます」と述べています。

ASOC は、ローカル・データ・ストアを備え、シンガポール国内におけるデータ保管が可能なため、データの保管場所を制限されている企業や政府機関は規制への準拠を維持することができます。

ASOC は、クラウドベースのファイア・アイ Dynamic Threat Intelligence Network にも接続しています。このネットワークは、ファイア・アイのラボで新規に発見された脅威情報だけでなく、隠れコールバック・チャネルなどの脅威情報もリアルタイムに交換するプラットフォームを提供するため、新しい攻撃を識別した場合でも世界中の顧客を保護できます。

シングテルとファイア・アイによる東南アジアのサイバー脅威レポート

最新の調査で、東南アジア地域でサイバー攻撃の被害が増加していることが判明しています。シングテルとファイア・アイによる共同レポート「東南アジア: 進化するサイバー脅威の見通し」では、シンガポール、フィリピン、マレーシア、タイ、ベトナム、インドネシアおよびブルネイ内の標的に強い関心を持つ攻撃者のうち、Advanced Persistent Threat（APT: 高度かつ持続的な脅威）を用いる攻撃者とその他のサイバー攻撃グループに関する状況が詳細に報告されています。

2014 年 7 月から 12 月の間に、東南アジアの顧客の 29%が、APT 使用者によるマルウェア攻撃と自社ネットワークへの不正アクセスの試行を検出しました。

最も頻繁に高度な攻撃グループの標的とされたのは次の分野です。

- 政府機関 – 27%
- 通信産業 – 24%
- 金融サービス産業 – 16%
- ハイテク産業 – 10%
- 輸送産業 - 10%

Chang 氏は、「このレポートは、この地域における APT 脅威の性質に関する情報を提供し、サイバー攻撃者の手口を浮き彫りにしています。企業は、この知識を基に新しい脅威の見通しを把握し、自社のセキュリティ体制を最新の状態に保つことで、サイバー攻撃の新たな犠牲者となることを回避できます」と述べています。

###

シングテルについて

シングテルは、固定、無線、およびインターネットプラットフォームを通した音声およびデータ通信ソリューションに加え情報通信技術と有料テレビ放送を含むサービスのポートフォリオを提供するアジア最大級のグループ企業です。当グループは、バングラディッシュ、インド、インドネシア、フィリピン、タイを含むアジアやアフリカなどの 25 か国で 5 億人以上のモバイル顧客を有しています。また、アジア太平洋、ヨーロッパ、アメリカ全域にわたってグローバル拠点を展開しています。

FireEye, Inc.について

ファイア・アイは、次世代のサイバー攻撃に対するリアルタイムの脅威保護を世界中の企業および政府機関に提供する、仮想マシンベースのセキュリティ対策専用プラットフォームを開発しました。これらの非常に高度化したサイバー攻撃は、次世代ファイアウォール、IPS、アンチウィルス、ゲートウェイのような従来のシグネチャ・ベース防御は簡単に回避します。

メディア問い合わせ先:

Singtel
Sonny Phua
Corporate Communications Manager
Tel: +65 6838 6527
Mobile: +65 8511 7996
Email: sonnyphua@singtel.com

FireEye
Vitor DeSouza
FireEye, Inc.
Tel: +1 415-699-9838 Email: vitor.desouza@fireeye.com

付録

シングテル-ファイア・アイの強み
アドバンスト・セキュリティ・オペレーション・センター（ASOC）

シングテルとファイア・アイの ASOC は、アジア太平洋地域における高度なサイバー・セキュリティ・センターであり、次のような多くの強みを有しています。

1. **世界各地の拠点 –** シングテルとファイア・アイの ASOC は、米国、ヨーロッパおよびオーストラリア（近日開設予定）に拠点を置くファイア・アイ ASOC のネットワークに接続しています。

2. **24 時間 365 日のプロアクティブ監視 –** シングテルとファイア・アイは、世界各地のファイア・アイ ASOC にアクセスし、両社の顧客に絶え間ない‘follow-the-sun’サービスを提供することができます。これにより、24 時間体制で常にサイバー脅威を検出して被害を防ぎ、攻撃に対処することが可能となります。

3. **グローバルな脅威情報 –** ASOC は、ファイア・アイの Dynamic Threat Intelligence と統合されています。ファイア・アイの Dynamic Threat Intelligence は、世界各地の顧客ネットワーク、パートナー・ネットワーク、およびサービス・プロバイダーに展開するファイア・アイの技術を相互に連携させるクラウドベースのネットワークです。このグローバル・クラウドでは、可能な限り最新の脅威情報データで顧客を保護するため、ファイア・アイのラボで新規に発見された脅威情報だけでなく、隠れコールバック・チャネルなどの脅威情報も効率的に共有します。

4. **サイバー・セキュリティ・エキスパートのチーム –** ASOC には、50 名のセキュリティ・エキスパートが配置され、悪意のあるサイバー活動をエンドツーエンドで監視しています。シンガポールのチームは、世界中の組織から送信される通常と異なるトラフィックや脅威活動に対し、厳重な監視を続けるセキュリティ・エキスパートのグローバル・チームに参加します。

5. **統合されたネットワークおよびセキュリティ・オペレーション・センター –** ASOC は、ネットワークの監視とセキュリティ・オペレーションを 1 か所に統合します。これにより、シングテルとファイア・アイのサイバー・セキュリティ・エキスパートは、ネットワーク、エンド・ポイントおよびデバイスのすべてにわたる、エンド

ツーエンドの可視性を得ることができ、セキュリティ・インシデントに対する迅速な対応が可能となります。

6. **データ・ストア –** ASOC は、シンガポールにデータ・ストアを配置しています。このため、データ保管場所を制限されている企業や政府機関は、シンガポール国内にデータを保管して規制への準拠を維持することができます。