報道関係者各位
プレスリリース

2018年7月12日
グローバルセキュリティエキスパート株式会社

GSX-SOC が EDR 市場の複数製品に対応する MDR サービスをリリース

～ もはやインシデント・レスポンスに不可欠な EDR 製品の実運用（MDR）を支援する ～

グローバルセキュリティエキスパート株式会社（本社：東京都港区海岸1-15-1、代表取締役社長：青柳 史郎、http://www.gsx.co.jp、以下、GSX）は、

- カーボン・ブラック・ジャパン株式会社の提供するCb Defense
- ファイア・アイ株式会社の提供するFireEye Endpoint Security（HXシリーズ）

（上記は提供会社名50音・アルファベット順）などの複数製品に対応したGSX-SOC MDRサービスをリリースしました。

GSX-SOC MDRサービスは、各製品導入後のサポートとして、24時間365日のセキュリティ監視サービスです。エンドポイントでの不正な挙動の検知の通知と、検知後の即時遮断や感染後の対応方法のご助言などを行います。今後も順次EDR市場製品に対応したMDRサービスをローンチして参ります。

◆企業にとってEDR（Endpoint Detection & Response）が必要とされる背景とは

近年の企業を取り巻くセキュリティ脅威の変化として、かつては愉快犯が中心であった外部脅威がランサムウェアに代表されるように身代金目的や企業の機密情報の窃取など、仮に被害にあった場合には金銭的実害が出るケースが増加しています。更に、外部脅威として攻撃の変化も見過ごすことはできず、これまで脅威への対策は特定の原因（例．マルウェアなど）を発見する試みとして「侵入検知」が代表的な対策例でしたが、近年は特定の原因が存在しない攻撃（例．正規プログラムによる侵害）も増加しています。

また攻撃の変化と深化として、「Port Scan（偵察）」「ツールを用いたExploit」「既知のマルウェアを用いたExploit」「未知の脆弱性を突くExploit」などの攻撃は日々深化しており、様々な手段で攻撃者は侵入を試みます。続々と生まれるマルウェア、ファイルレス攻撃などの台頭に対峙するには、仮に侵入されたとしても、その脅威を発見できる仕組みの必要性も去ることながら、脅威の侵入を止めるということも重要な要素になります。

すなわち、攻撃の深化により侵入後の検知能力を向上する必要があり、初期侵入先である端末を5W1H的に正確に検知できることが肝要になります。

- When：いつから感染しているのか？
- Where：どこで感染したのか？
- Who：どのノードが感染したのか？
- What：何の脅威によって感染したのか？
- Why：何が原因で感染したのか？
- How：どのような経路で感染に至ったのか？

侵害の進行を検知し、範囲を特定し、隔離するまでの早期発見と対処が今、企業に求められています。

◆GSX-SOC MDRサービスとは

冒頭複数製品のエンドポイント・セキュリティにおける各製品導入後のサポートとして、24時間365日のセキュリティ監視サービスです。エンドポイントでの不正な挙動の検知の通知と、検知後の即時遮断や感染後の対応方法のご助言などを行います。

MDRサービスのインシデント重要度定義については、以下をご覧ください。GSX-SOCではアラート通知の重要度を以下の3種に分類し、重要度に応じて電話やメールにてお客様に通知しております。

重要度	重要度詳細	GSX-SOCでの対応	通知方法	お客様側対応例
高	セキュリティ侵害によりお客様の資産にとって重大な脅威となり得るイベントが確認されたインシデント	・電話及びメールでご連絡します ・ネットワーク隔離を実施します ・解析レポートをご提出します ※お客様との事前取決により、お客様の確認を待たずに、先行して隔離する事も可能です	アナリストが重要度の判定後、60分以内を目途に速報通知をお送りします。その後、翌営業日以内を目途に詳細な解析レポートをお送りします。	・当該ホストの調査もしくは再セットアップなどのご対応 ・対応完了時の隔離解除連絡
中	検知時点でセキュリティ侵害活動は防止されているが、マルウェア除去などエンドポイントに残る脅威への対応が必要なインシデント	・メールでご連絡します ・解析レポートをご提出します	アナリストが重要度の判定後、60分以内を目途に速報通知をお送りします。その後、翌営業日以内を目途に詳細な解析レポートをお送りします。	・解析結果のご確認 ・マルウェアの駆除
低	お客様の資産にほとんど影響がないと思われるインシデント	月次レポートでアラート統計をご連絡します	月次レポートでご連絡します	必要に応じてアラートを確認します

GSX-SOC MDR サービス詳細については下記 URL をご覧ください。
http://www.gsx.co.jp/soc/index.html#MDR

◆本リリースに関する賛同文（提供会社名50音・アルファベット順）

・カーボン・ブラック・ジャパン株式会社からのエンドースメント

情報セキュリティ・サイバーセキュリティに特化した専門会社であるGSX様にCb Defense（クラウドベースのNGAV+EDR）のMDRサービスをリリース頂き、非常に心強く思っております。「A World Safe from Cyber Attacks」という弊社VisionをGSX様と共に日本のお客様へご提供させて頂く所存です。

カーボン・ブラック・ジャパン株式会社 カントリーマネージャー　西村 雅博

・ファイア・アイ株式会社からのエンドースメント

国内組織を狙ったサイバー攻撃は増加の一途を辿っています。より迅速に脅威を検出して対応するには、強力なエンドポイント技術の採用が必要です。ファイア・アイはグローバルセキュリティエキスパート（GSX）様との提携を通じて、引き続き国内組織・企業のセキュリティ強化を支援したい考えです。

ファイア・アイ株式会社　代表取締役社長　西村 隆行

◆グローバルセキュリティエキスパート株式会社について

社名　　：グローバルセキュリティエキスパート株式会社
本社　　：〒105-0022 東京都港区海岸1-15-1 スズエベイディアムビル4F
代表者　：代表取締役社長　青柳 史郎
資本金　：1億円
設立　　：2000年4月
コーポレートサイトURL：http://www.gsx.co.jp/

ー GSX は、サイバーセキュリティ教育カンパニーに生まれ変わります ー

わたしたちは、情報セキュリティ・サイバーセキュリティに特化した専門会社であり、セキュリティコンサルティング、脆弱性診断、サイバーセキュリティソリューションをはじめ、日本初のセキュリティ全体像を網羅した教育メニューや情報セキュリティ特化事業再生支援サービスをご提供しています。
以下のように「教育」という観点を各事業の軸に据え、お客様へセキュリティへの気づきを与え、セキュリティ市場を活性化する事で、日本の情報セキュリティレベル向上に貢献します。

➢　直接的な教育貢献
総合的な教育事業提供社として、EC-Council セキュリティエンジニア養成講座を介してセキュリティエンジニアを輩出し、標的型メール訓練サービスや IT セキュリティ e ラーニングである Mina Secure®及びサイバーセキュリティ演習サービスを介してお客様のセキュリティリテラシーを向上します。

➢　間接的な教育貢献
GSX の既存事業（脆弱性診断サービス、コンサルティングサービス、サイバーセキュリティソリューションサービス）を介して、各サービスに関係するサイバー犯罪やそのリスク、さらにお客様の現状の課題についての"気づき"と、対策の正しい進め方を提供することで、あらゆる事業活動を教育啓蒙の場として活用します。

➢　市場活性化としての教育貢献
この度の協業のように、お客様の情報セキュリティリテラシー向上のため、共にお客様をサイバー脅威などから守れる業界のプレイヤー（パートナー様）を増やすことを目指します。志を同じくするプレイヤーを増やすことで、さらなる市場の活性化を推進します。

【本リリース内容に関するお問い合わせ先】
グローバルセキュリティエキスパート株式会社　経営企画本部　マーケティング部
TEL　：03-3578-9001（代）　E-mail　：mktg@gsx.co.jp