報道関係者各位
プレスリリース

2017年6月13日
グローバルセキュリティエキスパート株式会社

GSX、データ分析プラットフォーム Splunk でセキュリティ監視強化や運用負荷軽減を実現する無償テンプレート「金融機関向け App for Splunk」(仮) をリリース

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：久慈 正一、http://www.gsx.co.jp、以下、GSX）は、データ分析プラットフォーム Splunkによってセキュリティ監視強化やセキュリティ運用負荷軽減を可能にする、金融機関向け無償テンプレート「金融機関向け App for Splunk」をリリースしました。

近年、社会を取り巻くサイバー脅威は圧倒的に外部脅威の台頭となっており、企業は格好のターゲットとなっているのが実情です。殊に金融機関では、インターネットバンキングにおける不正送金被害が甚大なものとなっています（警察庁の発表では、2016年に発生したインターネットバンキングで不正送金された被害は1,291件、被害額は約16億8,700万円）。このように攻撃者優位の構図は変わらず、攻撃者側の分業が進み、情報搾取のための様々なツールやサービスが自由自在に利用できる状況にあります。

企業側では突如発生する情報セキュリティインシデントに対して、既存システムのログ収集や分析はその痕跡を追うための重要なファクターとなります。ログを収集/分析する仕組みがなければ「なぜインシデントが発生したのか？」「どこからインシデントに至ったのか？」という事実（原因）を把握することはできません。実際に起こった事柄を正確に把握するため、システムログ等のデータはインシデント・レスポンスを実現する上で必要不可欠となります。

この度GSXは、マシンデータ分析プラットフォーム「Splunk」に対応したログ分析テンプレート「金融機関向け App for Splunk」を無償で提供致します。「金融機関向け App for Splunk」では、「Splunk」に実装可能なセキュリティレポートやダッシュボードのサンプルをApp※として提供し、セキュリティログ分析を目的として「Splunk」を導入する金融機関様がセキュリティ用途に特化した形で監視強化や運用負荷軽減を実施するためにご利用いただくことを想定しております。

※Appとは
Splunk社やユーザコミュニティなどから提供される各種アプリケーション、デバイス用の公開テンプレートです。
Appを利用することにより、Splunkにおけるログ分析、ダッシュボード、レポート作成などが効率的に行えます。

製品名	金融機関向け App for Splunk (仮)
提供形態	アプリケーション
提供開始日	2017年6月13日（火）
対象ユーザ	「Splunk」をご導入済みで50GB/日以下のライセンスをシングル構成でご利用のお客様

◆「金融機関向け App for Splunk」概要について

金融機関向け App for Splunkは、マシンデータ分析プラットフォーム「Splunk」のセキュリティ利用を支援するサンプルAppです。本Appでは、以下の概要をベースにGSX独自のカスタマイズを実施しています。http://www.gsx.co.jp/informationsecurity/splunk.html#GSXApp

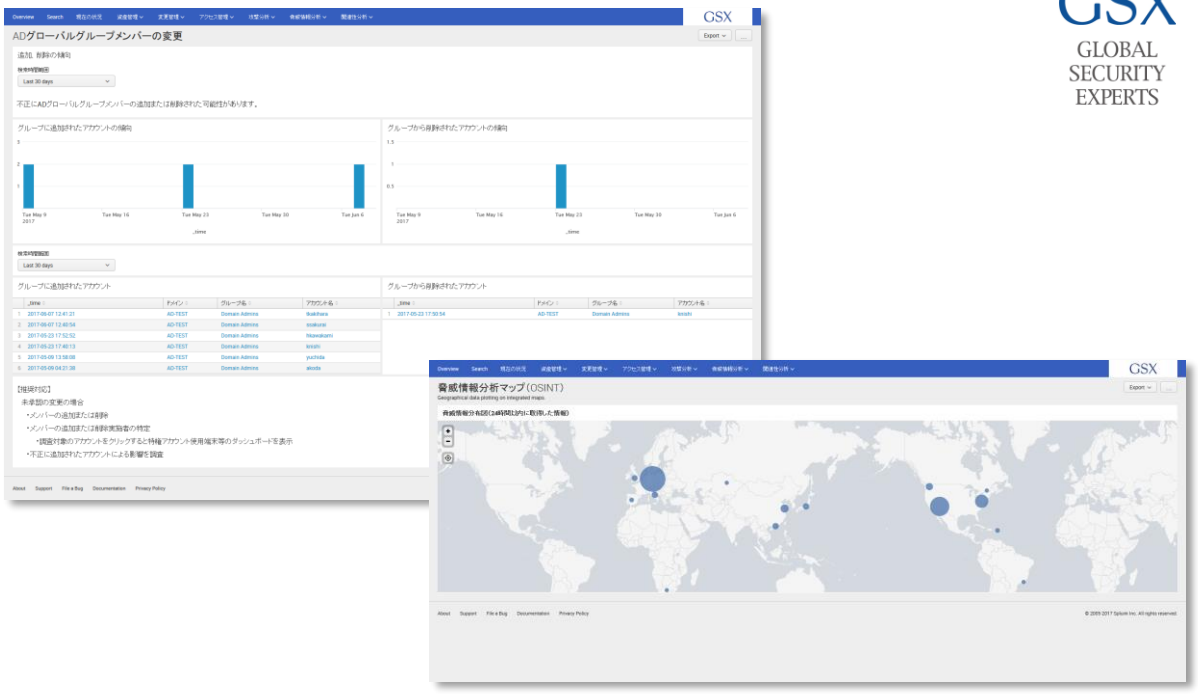
- IPA「高度標的型攻撃に向けたシステム設計ガイド」
- JPCERT/CC「ログを活用したActive Directoryに対する攻撃の検知と対策」
- JPCERT/CC「高度サイバー攻撃への対処におけるログの活用と分析方法」

またお客様のSplunk環境に取り込まれているイベントログ等のデータに対し以下のダッシュボード機能を提供します。

- 現在の状況ダッシュボード ※下図参照
  攻撃検出状況、イベントの概要、不正検知状況、外部からの情報提供（金融ISAC、JPCERT/CC）、IPA（重要セキュリティ情報）を表示するダッシュボート
- 資産管理ダッシュボート
  AD上に登録されているアカウントの一覧を表示するダッシュボート
- 変更管理ダッシュボート ※下図参照
  アカウントの変更状況等を表示するダッシュボート
- アクセス管理ダッシュボート
  サーバへのリモートデスクトップ接続状況等を表示するダッシュボート
- 攻撃分析ダッシュボード
  JPCERT 公表の「ログを活用したActive Directoryに対する攻撃の検知と対策」の分析ロジックを参考にしたダッシュボード
- 脅威情報分析ダッシュボード ※下図参照
  金融ISAC、オープンな脅威情報（OSINT）に該当する不正通信等の分析を行えるダッシュボード
- 関連性分析ダッシュボート
  不審なイベントの調査を支援するダッシュボート

脅威情報としては下記の2種情報を取得の上、活用しています。

- プレミアム脅威情報（金融ISAC、JPCERT/CC）
  金融ISAC、JPCERT/CCから提供される脅威情報を登録することができます。
- オープン脅威情報（OSINT）
  「Macnica CSIRT App Basic」を使用して、自動でOSINTの情報を取得しています。



（注意事項）

・マクニカネットワークス様経由で Splunk をご購入またはご購入を検討されているお客様へご提供致します。

・本 App に関する仕様の確認や動作不具合におけるサポートのお問い合わせにつきましては GSX の Splunk 保守受付窓口では受け付けておりませんのでご注意ください。

・本 App に関するお問い合わせは、GSX 担当営業までご連絡下さい。

・各種ダッシュボードのご利用にはインターネットへの接続が必要となります。

◆本リリースに関するマクニカネットワークス株式会社様からのエンドースメントについて

マクニカネットワークスは、グローバルセキュリティエキスパート様が「金融機関向け App for Splunk」をリリースされることに心より御礼申し上げます。
弊社は、Splunk 社のディストリビューターとして、国内のお客様に Splunk 製品の販売と導入から運用までのサポートを致しております。 グローバルセキュリティエキスパート様がこれまで培った経験と知見を汎用的なテンプレートとして活用することによって、セキュリティログ分析を目的として Splunk を導入する金融機関のお客様が、早期構築と運用を実現できるものと確信しています。

マクニカネットワークス株式会社
代表取締役社長
池田　遵

◆Splunk 社について

Splunk Inc.は、リアルタイムのオペレーショナルインテリジェンス・ソフトウェア・プラットフォームのリーディングプロバイダーです。Splunk のソフトウェアとクラウドサービスは、Web サイト、アプリケーション、サーバー、ネットワーク、センサー、モバイル機器から生成されるビッグデータをサーチ、監視、分析、可視化することを可能にします。世界中の企業、政府機関、大学、サービスプロバイダーが Splunk のソフトウェアを利用し、ビジネスや顧客の理解を深め、サービスや稼働率の向上、コスト削減、サイバーセキュリティリスクの軽減を実現しています。
詳しくは http://ja.splunk.com/company をご覧ください。

◆マクニカネットワークス株式会社について

マクニカネットワークスは、数多くの海外企業との提携により、最先端のテクノロジーを備えた様々なネットワーク機器・ソフトウェアなどを提供する技術商社です。その豊富なラインアップと、製品の導入から運用・保守サポートに至るまでの万全なサービスにより、官公庁や金融機関・一般企業など、数多くのお客様への導入実績を誇ります。

会社名　　マクニカネットワークス株式会社
資本金　　3 億円 (2016 年 9 月 30 日現在)
　　※株式会社マクニカ 100%出資子会社
本社所在地　　〒222-8562 横浜市港北区新横浜 1-5-5
代表者　　代表取締役社長　　池田 遵
ウェブサイト　　http://www.macnica.net/
事業内容 企業向けネットワーク、セキュリティ関連ハードウェア・ソフトウェアの輸入、開発、販売コンサルティング・保守サービスにわたる IT ソリューションの提供

◆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　久慈　正一
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/
事業内容：国内初の情報セキュリティ専門コンサルティング会社として2000年に設立され、脆弱性診断、コンサルティング、サイバーセキュリティサービス、教育事業にいたる広範な情報セキュリティサービスを提供しています。
情報セキュリティポリシーの国際標準基準となった英国規格協会（BSI）のBS7799（現ISO27000）を日本に初めて紹介し、高品質な情報セキュリティコンサルテーションを行っています。
さらに、高い技術を有し、システムの脆弱性の検出のためにプラットフォーム診断やWebアプリケーション診断、スマホアプリセキュリティ診断などさまざまな脆弱性診断を行う【タイガーチームサービス（TIGER TEAM SERVICE）本部】、標的型メール訓練サービスやマルウェア感染調査をはじめとする新しい脅威に対抗するサービス／ソリューションをご提案する【サイバーセキュリティサービス本部】、企業様のセキュリティポリシーの策定・リスクアセスメント・システム監査または、ISMSやPマーク取得支援、PCI DSS準拠認定支援、CSIRT構築運用支援サービスなどを行っている【コンサルティング本部】、情報セキュリティ人材育成（EC-Council）事業として認定トレーニング及び認定資格試験として、認定ネットワークディフェンダー（Certified Network Defender）、認定ホワイトハッカー（Certified Ethical Hacker）などの講座をご提供する【エデュケーション本部】を組織しています。また【R&D本部準備室】には
GSXサイバーセキュリティ研究所（GSX Cyber Security Research Institute）を擁し、セキュリティ製品評価やサイバー攻撃に関する情報収集及び分析、セキュリティインシデント対応要員の育成を進めており、問題指摘のみならず、インシデントに対する解決策までをワンストップで提供できる体制を整えています。

【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　営業本部　マーケティング室
TEL　：03-3578-9001（代）　E-mail　：mktg@gsx.co.jp