報道関係者各位
プレスリリース

2023年7月19日

グローバルセキュリティエキスパート株式会社

GSX、Active Directory上のデータを「CrowdStrike Falcon Identity Protection」で保護・監視する運用支援サービスを開始

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、https://www.gsx.co.jp/、以下、GSX）はこの度、CrowdStrike（本社：米国テキサス州オースティン、CEO：George Kurtz、https://www.crowdstrike.com/ 、以下、CrowdStrike）が提供するCrowdStrike Falcon® Identity Protectionを使用して、顧客のActive Directory上のデータをIDベースの脅威から保護するオリジナル運用支援サービスを開始しました。

■近年のサイバー攻撃の巧妙化と認証情報への対策が急がれる背景

CrowdStrike2023 年版グローバル脅威レポートによると、マルウェアフリーの活動は 2021 年の 62%から急増し、2022 年には全検知数の 71%を占めました。これは、攻撃者がマルウェアの使用からシフトし続け、クレデンシャルの乱用と脆弱性の悪用の使用頻度が高まっていることを強調しています。認証情報（インターネット上のサービスを利用する際に入力するアカウント ID/パスワード）が窃取されることで、突破されたシステムを契機に次のシステム、次のシステムと侵攻を許すことになり、重要なデータを抑えられてしまう、業務停止に至るシステムを停止させられてしまうことに繋がっていきます。ID 関連のセキュリティインシデントは枚挙にいとまがありません。

攻撃者が特に標的としているのは Microsoft の Active Directory(AD)で、これは組織にとってサイバー防衛戦略の弱点と考えられます。攻撃者は、AD が Microsoft Windows アカウントや従業員端末を一元管理し、組織のシステムへのアクセスを提供するために使用されていることを知っています。AD のセキュリティ侵害は、ID インフラ全体を弱体化させます。組織にとって、AD が攻撃者からどれだけ脆弱であるかを理解することが重要であり、潜在的なデータ漏えいだけでなく、潜在的なシステムの破損／乗っ取り、破滅的なランサムウェア攻撃やサプライチェーン攻撃を防ぐための措置を講じることができます。

適切な AD セキュリティハイジーン（AD セキュリティの衛生管理）を維持するためには、どのような AD モニタリングが必要とされるのでしょうか。

- ✓ 特権ユーザが管理外のホストで利用されている
- ✓ 90 日以上利用されていない特権ユーザが存在する
- ✓ ダークウェブ・データベースで見つかった認証情報をもつユーザが存在する

このような状況の可視化をすることで、組織管理者は自社組織に内在する脆弱な設定状況や攻撃者の侵入の兆候を知ることが可能になります。

この度 GSX では、CrowdStrike Falcon プラットフォームのサポートにより、AD でのアカウント保護に有効な 2 つの運用支援サービスを開始しました。本サービスをご利用いただくことで、以下のような自動化やセキュリティ対策への運用負荷軽減を実現します。

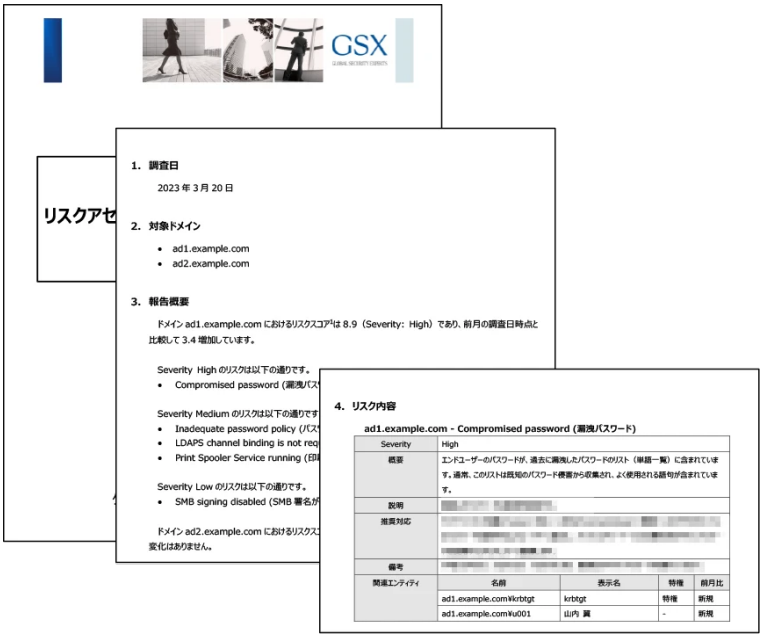
- ✓ AD の脆弱な設定が可視化できる
- ✓ AD 上に存在するリスクの高いアカウントを検出できる
- ✓ 不正なアカウント動作を検出できる
- ✓ アラート発生時に組織管理者は受信レポートを確認し、初動対応ができる

■GSX オリジナル運用支援サービスについて

◆リスクアセスメントサービス for CrowdStrike Falcon Identity Protection

月次でリスクの状況を確認し、必要な対処をレポート形式でご案内します。

- ➢ 脆弱なパスワードが設定されているユーザの一覧をリスト化します
- ➢ AD の脆弱な設定例の提示と対処方法をご案内します
- ➢ 追加された特権ユーザ一覧をリスト化します

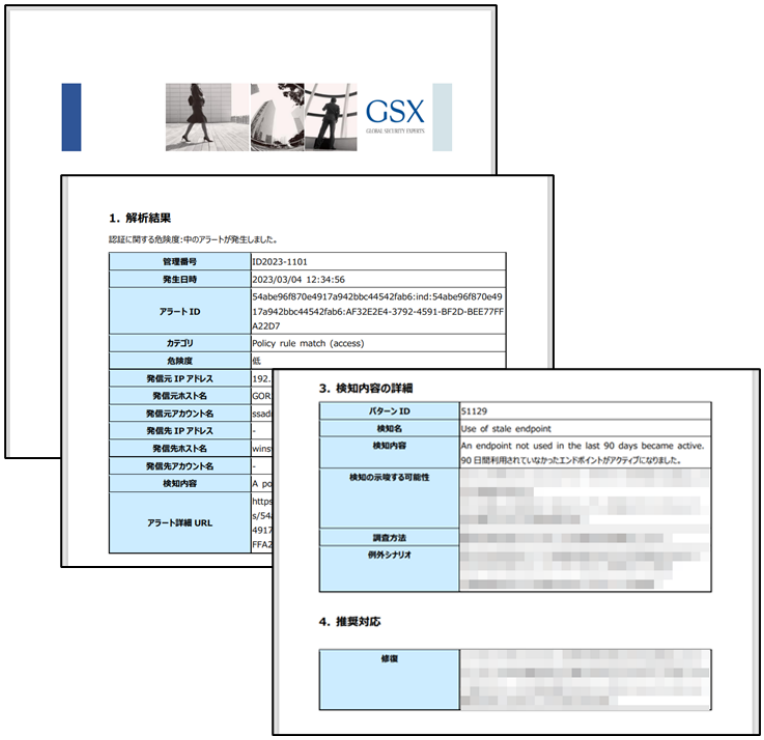


当該レポートでは、検出されたリスク、対処方法や参考情報、特権アカウントの増減、増加した特権アカウントの詳細などを可視化し、詳細にご指南します。評価期間終了の翌日から 5 営業日以内にご提供させていただきます。

◆アラート監視サービス for CrowdStrike Falcon Identity Protection

不正なアカウント動作を検知した際に、事象と対処方法をレポート形式でご案内します。

- 異常検知を発生した日時、ホスト、ユーザ名を通知します
- 検知内容、検知発生理由として想定される事象と対処方法をご案内します



当該レポートでは、発生日時、アラートの危険度、ホストやアカウント詳細、セキュリティイベントの詳細、推奨される対応などを詳細にご指南します。アラート発生後 60 分以内にご提供させていただきます。

◆リスクアセスメントサービス for CrowdStrike Falcon Identity Protection および
アラート監視サービス for CrowdStrike Falcon Identity Protection 詳細はこちらから
https://www.gsx.co.jp/services/incidentavoidance/crowdstrikefalcon-idps.html

上記 2 種運用支援サービスについての料金体系や導入要件などの詳細については、別途お問い合わせをお願いします。
https://www.gsx.co.jp/inquiry?service=crowdstrike_falcon

■本リリースに関する賛同文

・CrowdStrike Japan 合同会社からのエンドースメント

CrowdStrike2023 年版グローバル脅威レポートによると、サイバー攻撃の 80%近くがアイデンティティベースの攻撃を利用して、正規の認証情報を侵害しています。さらに、ダークウェブのアクセスブローカー広告が 112%増加しており、最初のアクセスと水平展開の両方で認証情報と権限を盗み出すという攻撃者の需要が高いことを示唆しています。これらのサービス導入により、GSX は Microsoft Active Directory 固有の弱点を悪用する一般的な攻撃ベクトルに対する防御に関して、組織に大きなアドバンテージを与えています。CrowdStrike が支援するこれらの GSX のサービスを通じて、より多くの企業が Active Directory 対策に取り組むことを期待しています。

CrowdStrike アジア太平洋・日本地域のチャネル担当シニアディレクター
ジョン・フォックス（Jon Fox）

◆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
東京本社：〒105-0022 東京都港区海岸1-15-1 スズエベイディアム4F
西日本支社：〒541-0047 大阪市中央区淡路町3-1-9 淡路町ダイビル8F
西日本支社名古屋オフィス：〒451-6040 愛知県名古屋市西区牛島町6-1名古屋ルーセントタワー40F
西日本支社福岡オフィス：〒812-0054 福岡県福岡市東区馬出1-13-8　ソフネット県庁口ビル4F
代表者：代表取締役社長　青柳 史郎
証券コード：4417
上場証券取引所：東京証券取引所グロース市場
資本金：529,833千円（2023年3月末）
設立　：2000年4月（グローバルセキュリティエキスパートへの商号変更日を設立日として記載）
コーポレートサイトURL：https://www.gsx.co.jp/

GSX は、日本全国の企業の自衛力向上を目指し、セキュリティ業界全域で事業を展開する
サイバーセキュリティ教育カンパニーです

―Purpose―
全ての企業をセキュリティ脅威から護るそのために必要なことを惜しげもなくお伝えする
―Mission―
日本全国の企業の自衛力を向上すること

情報セキュリティ・サイバーセキュリティの実装・運用支援をワンストップで提供する「コンサルティング事業」「ソリューション事業」と企業のセキュリティ水準向上を内面から支援する「教育事業」を展開しています。

【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　経営戦略室　マーケティング部
TEL：03-3578-9001　MAIL：mktg@gsx.co.jp