報道関係者各位
プレスリリース

2024年9月24日

グローバルセキュリティエキスパート株式会社

増え続けるITシステム、増え続けるサイバー攻撃を自動で継続的に監視・管理する「ULTRA RED」を提供開始。同時に運用サービスを提供し、企業の外部公開ITシステムのセキュリティ対策をフォロー

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1-16-1、代表取締役社長 CEO：青柳 史郎、証券コード：4417、https://www.gsx.co.jp/、以下、GSX）は、ULTRA RED, Ltd.（イスラエル テルアビブ、CEO：エラン・シュタウバー、https://www.ultrared.ai/、以下、ULTRA RED）が提供する「ULTRA RED」の取り扱いおよび運用サービスの提供を開始しました。

システムの脆弱性を突かれるサイバー被害は留まることを知りません。しかしながら、DX化の広がりなどからITシステムは増え続け、多くのITシステムには脆弱性が潜在し、攻撃者から見ると日々攻撃するポイントが増え続けているというのがサイバー攻撃の実態です。

中でも、昨今、最も攻撃の的となっているのが外部公開資産と呼ばれる一般ユーザーがアクセスしやすいITシステムです。企業は、システムを公開してビジネスに活用していく一方で公開するIT資産の脆弱性を管理しなければなりません。

ULTRA REDは、攻撃を受ける可能性のある外部公開資産を継続的に検出し評価する自動化ツールです。GSXは、「ULTRA RED」のライセンス販売を開始すると共に導入する企業が手間なく利活用出来る運用サービスを提供することでサイバー攻撃被害から企業を護ります。

■脆弱性を悪用した攻撃が止まらない

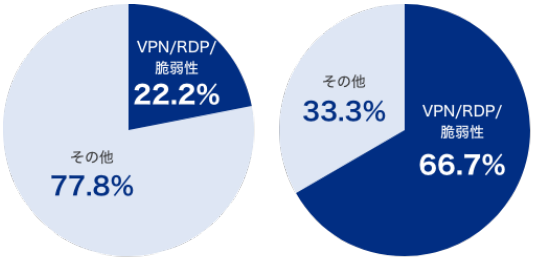
業種・業態・企業規模を問わず脆弱性を突いた攻撃が止まりません。ランサムウェア被害、Webページ改ざん、個人情報漏洩など多様な被害へとつながっていきます。企業担当者は脆弱性への対処が必要であることは重々承知しながらも、護り切れない実態があります。

被害組織	発生時期	被害内容	初期侵入経路
自動車関連	2024年3月	個人情報の漏洩	クラウド設定不備でキー露出
病院	2024年2月	ランサムウェア	外部から認証なしRDP
学会	2024年2月	個人情報の公開	脆弱性悪用の不正アクセス
ICTシステム	2024年2月	ランサムウェア	VPN機器の脆弱性悪用
エレクトロニクス	2023年 12月	ランサムウェアがグループ全体に	VPN機器の脆弱性悪用
臓器移植関連組織	2023年 3月	メールのデータ消失	外部からの不正アクセス
音響メーカー	2023年3月	従業員の個人情報が漏えい	VPN装置から侵入
大手不動産業	2023年3月	第三者から個人情報にアクセス可能	クラウドの制御設定不備
映像制作会社	2023年3月	ランサムウェア被害	不正アクセス
エンターテインメント	2023年2月	Webページが改ざん	不正アクセス
信用調査会社	2023年2月	ランサムウェア	侵入型ランサムウェア（VPN）
衣料品販売	2023年2月	クレジットカード情報及び個人情報が漏えい	脆弱性の悪用
アパレルメーカー	2023年1月	顧客の個人情報が漏えい	不正アクセス
国内大手メーカー	2022年12月	ネットワーク機器から外部への不正通信 認証バイパスやロギング停止	アクセス制御設定不備
仮設建材製造販売	2022年12月	海外のサーバが侵害, ランサムウェアが本社及び関連子会社9社にまで拡大	サーバへ不正アクセス（脆弱性悪用か？）
化学メーカー	2022年11月	ランサムウェアと情報漏洩	VPN機器の脆弱性悪用
独立行政法人	2022年11月	個人情報の漏洩	ゼロディ脆弱性を悪用

作成：ULTRA RED, Ltd.

■直接侵入の増加

トレンドマイクロ社の調べでは VPN や RDP といった社外から社内システムへ接続するプログラムなどの脆弱性を悪用し、内部ネットワークへ直接侵入する経路が増加しています。これは当社が年間約 300 件のセキュリティ被害相談を受ける実態とも合致しています。



2019年1月～2020年12月（24ヶ月）　2021年1月～2023年6月（30ヶ月）

侵入経路	2019年1月～2020年12月	2021年1月～2023年6月
VPN/RDP/脆弱性	22.2%	66.7%

※トレンドマイクロ社のデータを基にGSXで再作成

出典：トレンドマイクロ社「4 年半にわたる国内組織のインシデントレスポンスから見えてきた「ランサムウェア攻撃のリアル」とは？」

https://www.trendmicro.com/ja_jp/jp-security/23/l/securitytrend-20231211-03.html

■企業が抱える 2 つの課題

-DX 化により広がるシステム利用

DX 化によりシステム利用が増えており、攻撃者視点で言えば攻撃対象が増えていることと言えます。企業側の視点に立つと、護るべき範囲が広がっていることになります。

-人材不足

護る対象範囲が広がる一方で、慢性的にセキュリティ人材は不足しており、あらゆるシステムの脆弱性を継続的に監視・評価することは現実的ではありません。また、監視・評価するための知見を十分に有することも難しいという現実があります。

■ULTRA RED の特徴

脆弱性を突いたサイバー攻撃から企業を護るためには、日々変化するシステム環境やサイバー攻撃手法を把握し対処していくことが求められます。

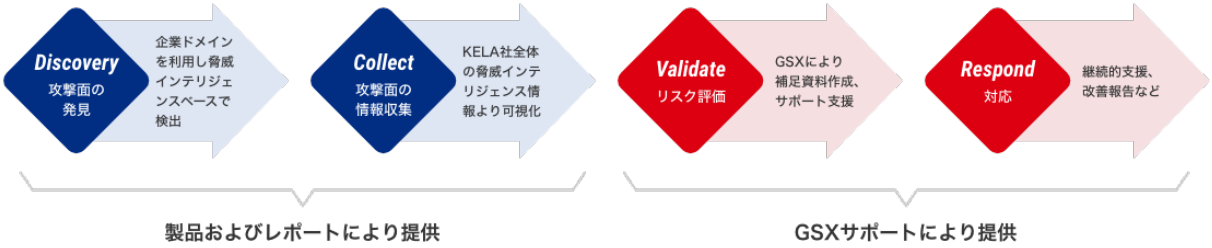
ULTRA RED は企業が保有する外部公開資産を継続的に把握、攻撃者視点で脆弱性や弱点を特定し、それらへの対策を講じることができる継続的な脅威エクスポージャ管理(CTEM)プラットフォームです。
また、見つかった脆弱性等は独自の脅威情報データベースの情報とも合わせて評価するので、より正確に脅威を把握することができるようになります。それにより、企業担当者は監視・評価に関する工数を抑制することができるため、リスクへの対処に工数を充当することができるようになります。

[特徴的な機能]

✓ アセットの検出能力の高さと管理の自動化
✓ ビジネスインパクトに基づく優先順位付け
✓ 繰り返しの検出作業を自動化
✓ 攻撃者の立場でアセットをスキャンし脆弱性や弱点を検出
✓ 脆弱性やウィークネス修復の確認用 POC コードを提供
✓ アセットやパッチ管理に適したユーザーインターフェース
✓ CTEM に必要な機能をオールインワンで提供
✓ 完全エージェントレスの SaaS 型ソリューション

■GSX の運用サービス

セキュリティ人材の不足などによる運用課題に対応すべく、GSX はコンサルティングなど様々なプロジェクトで獲得した知見に基づいた ULTRA RED 運用サービスを提供します。ULTRA RED が検出した脅威情報を精査し、対応すべき事案やその対処方法までお示しします。



[提供サービス]

✓ アタックサーフェスに関するスキャン結果のとりまとめ、トリアージ作業
✓ システムオーナー等のコミュニケーション・サポート支援
✓ 最小 20asset からの提供

◆ULTRA RED, Ltd.

社名：ULTRA RED, Ltd.
本社：イスラエル
代表者：Eran Shtauber
設立： 2021 年
コーポレートサイト URL：https://www.ultrared.ai/jp/home

◆グローバルセキュリティエキスパート株式会社

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1-16-1 ニューピア竹芝サウスタワー10F
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：544,999千円（2024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/

【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　戦略統括部　マーケティング部
TEL：03-3578-9001　MAIL：mktg@gsx.co.jp