ULTRARED

2023 年 1 月

外部攻撃サーフェス管理

Gaining the Upper Hand

～優位に立つ～

ULTRA RED Threat Exposure Management Platform はエンタープライズ攻撃サーフェスの検出とサイバー管理を自動化するユニファイド SaaS ソリューションです。他の多くの EASM ソリューションと異なり、ULTRA RED は優先順位を付けた確認済みの脆弱性を継続的に提示します。これらの脆弱性は追加の調査を行わなくても対処することができるので、エクスポージャの検出機能と対応スピードが向上します。各ベクターに関する追加のインテリジェンス、PoC、修復のためのガイダンスによって修復を担当するチームへの作業移行がスムーズに行えます。

www.ultrared.ai

ほとんどの企業や組織は継続的な技術革新を前提とした非常に競争の激しいビジネス環境で事業を行っています。ただしインターネットが関係する場合、革新には犠牲がつきものです。

変化し続ける外部攻撃サーフェス

デジタルトランスフォーメーションの取り組み、クラウドへの移行、サードパーティの SaaS アプリケーション、WFH のサポート、新たにインターネットに接続する API、IoT デバイスはいずれも急拡大および常に変化する攻撃サーフェスの要因になっています。企業の攻撃サーフェスに潜む脆弱性に対するエクスプロイトは現在発生している侵害の 3 分の 1 を占め、この割合は増加しています[1]。

文書化されている脆弱性やエクスプロイトの数は毎年継続的に増加しています。これにより成功率が高くなるので脅威アクターにとっては朗報です。Initial Access Brokers や Ransomware as a Service などの新たな犯罪ビジネスモデルに加え、地政学的な緊張の高まりや国家的活動によって事態は悪化の一途をたどっています。

ゼロデイ脆弱性はメディアの注目を集めていますが、脅威アクターはパッチが提供されたばかりの脆弱性を悪用し、パッチ未適用のシステムを探してエクスプロイトを仕掛けます[2]。エクスプロイトされた脆弱性の上位 5 つのうち 4 つが新たな脆弱性だったという調査結果もこれを裏付けています。リスクの高い脆弱性が公表されてから影響のある全システムを修復するまでの間、企業の脆弱性が特に高まります。

クラウドホスティングとサードパーティの SaaS アプリケーション導入の場合、脆弱性の検出と解消における固有の課題があります。Gartner によるとパッチ適用不可能な攻撃サーフェスの割合は現在 10%ですが、2026 年までに 50%に達する見込みです[3]。

---

[1] IBM X-Force Intelligence Index 2022 - https://www.ibm.com/downloads/cas/ADLMYLAZ

[2] Symantec – The Threat Landscape in 2021（2021 年の脅威環境） - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-2021

[3] Gartner Predicts 2023（Gartner の 2023 年予測）：Enterprises Must Expand From Threat to Exposure Management（エンタープライズは脅威管理だけでなくエクスポージャ管理に拡大すべき）