SecurityScorecard

SecurityScorecard社ブログ

発行日：2021年5月4日

執筆：SecurityScorecard 中村 悠
編集：SecurityScorecard 橋本 詩保

今だから知りたい、『脅威インテリジェンス』 シリーズ＃５

第五講：「“ セキュリティ リスク レイティング”とは何か？」

『組織のセキュリティ態勢が攻撃者から見た時にどのように映っているのか。』を知る

前回のコラムでは、「脅威インテリジェンスを活用する目的を設定する。そのために、サイバー攻撃のライフサイクルを理解する」というテーマで話を進めてきました。
その中で、「(1) 情報収集段階」への脅威インテリジェンスの活用を今後広げていく必要があると伝えました。
ここで、念のために、「(1) 情報収集段階」について、簡単に振り返ってみます。

(1)情報収集段階
このステージでは、攻撃者は、標的とする組織の実態調査を行います。つまり、セキュリティの弱い点を詳らかにし、標的とすべきか否かを決断します。
従って、セキュリティ対策も、（自社組織、並びに、関連企業の）現状把握が目的になります。自社のセキュリティ態勢はどうなっているのか、また、ビジネス上に関連する企業のセキュリティ態勢はどうなっているのか。そして、それらのセキュリティ態勢が攻撃者から見た時にどのように映っているのか。これらを推し量るために脅威インテリジェンスの活用が考えられます。

その中で、「セキュリティ リスク レイティング」というソリューションがこの段階の脅威インテリジェンスの活用の一形態だということをお伝えしました。

「セキュリティ リスク レイティング」とは？

では、この「セキュリティ リスク レイティング」というソリューションは、どのようなものなのでしょうか、おそらく日本では、まだ、あまり耳なじみのない方が多いのではないでしょうか。

続きを見たい場合は
メーカーBlogへ
HTTPS://SECURITYSCORECARD.COM/THREAT-INTELLIGENCE-5-JP