SecurityScorecard

SecurityScorecard社ブログ

発行日：2021年4月26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＃3

第三講：「脅威インテリジェンスを活用するための“サイバー攻撃への理解”」

前回のコラムで、オシント／シギント／ヒューミントについて、少し踏み込んだ話をしました。
お伝えしたかったのは、

オシント／シギント／ヒューミントはインテリジェンス自体の分類ではなく、インテリジェンスの収集方法の分類である

ということでした。
では、実際にこれら脅威インテリジェンスを利用してセキュリティ対策を行う場合、どのような活用方法があるのでしょうか。
最も大切なのは「目的設定をしっかり行う」と言うことです。

脅威インテリジェンスを活用する目的を定義する

少し前まで、これまで多くの企業の取り組みは、「マルウェアの侵入を防げば良い」「スパムメールを除外できれば良い」といった、”攻撃の侵入を防ぐこと”に重きが置かれていました。ただ、最近では、その目的が多様化してきたことを、私もお客様と接する中で感じています。例えば、このような目的を持っていらっしゃいます。

「侵入を食い止めたい」
「侵入された後、早く気付きたい」
「データを搾取されることを防ぎたい」
「攻撃のターゲットになりやすいのか知りたい」

なぜ、目的が多様化しているのでしょうか。それは、「どんなに侵入を防ぐためのセキュリティ対策を施しても、完全に攻撃の侵入を防ぐことは難しい」ということが年々明らかになってきたからです。

続きを見たい場合は
メーカーBlogへ
HTTPS://SECURITYSCORECARD.COM/UNDERSTANDING-CYBER-ATTACKS-JP