SecurityScorecard

SecurityScorecard社ブログ

発行日：2021年8月12日

執筆：SecurityScorecard 中村 悠
編集：SecurityScorecard 中島 朝可・橋本 詩保

プロアクティブにサイバー攻撃の脅威に対応する3つの価値

このブログを読んでくださっている皆様の組織でも、これまでも多くのセキュリティへの投資をされてきたと思います。ネットワークセキュリティ製品・メールセキュリティ製品・エンドポイントセキュリティ製品・脆弱性診断ツール・脅威インテリジェンスサービスなどが挙げられるでしょうか。

皆様の組織で行われたこれらの投資、振り返ってみるとどのような分野への投資が多く、これから強化すべきはどのような分野なのかを改めて考えてみませんか？
セキュリティ投資をカテゴリーに分ける方法は様々ありますが、このブログでは、こんな分け方をして整理をしてみます。

『リアクティブな対応』 VS 『プロアクティブな対応』

『リアクティブな対応』とは
文字通り、“サイバー攻撃が確認されてから、セキュリティ運用担当者はその侵害への対応を開始する”といった対応方法です。攻撃を精査し、攻撃者をネットワークから追い出し、組織への損害度合いが評価され、状態復旧を試みます。

『プロアクティブな対応』とは
“サイバー攻撃の前に何かしらの対応（“対策”といった方が正しいかもしれませんが、あえて“対応”という言葉を利用します。）を行います。おそらく、多くの方が、事前に行う対応の大切さはご理解いただいていると思いますが、実際にどのような観点で対応を行ったらよいかの理解がなかなか進まず、実行に移し切れていないのではないでしょうか。
『プロアクティブな対応』を平易な言葉で置き換えてみます。ズバリ、“予防策”です。この言葉ならば、途端にわかりやすくなると思いますし、「それなら、既にやっている」、「ああ、そういうことか」と思われた方もいらっしゃると思います。

続きをご覧になりたい場合は
メーカーBlogへ
HTTPS://SECURITYSCORECARD.COM/REACTIVE-VS-PROACTIVE-CYBERSECURITY-3-BENEFITS