2022 年 4 月

2022 年 4 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

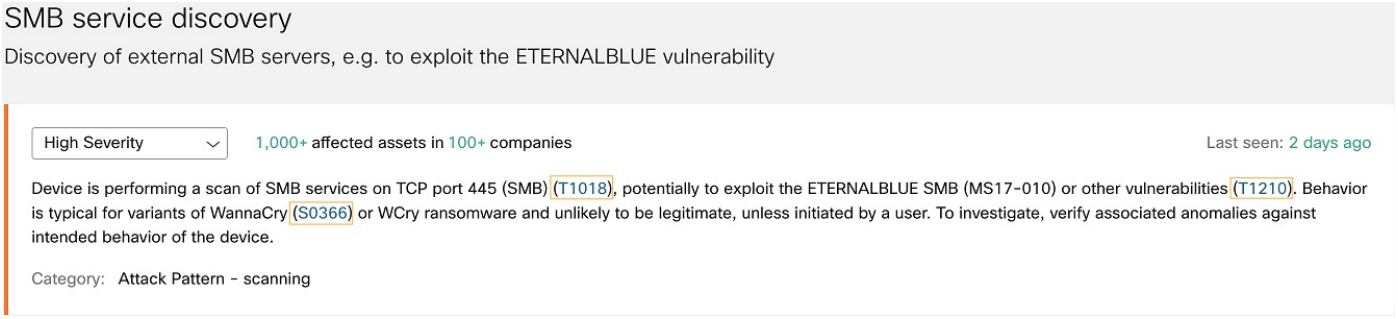
MITRE ATT&CK® との調整

グローバル脅威アラートの脅威インテリジェンスレコードは、MITRE ATT&CK® フレームワークに関して調整されています。

- 必要に応じて、ATT&CK フレームワークからの命名が直接使用されます。
- グローバル脅威アラートの脅威インテリジェンスは、関連する ATT&CK の戦術、テクニック、およびソフトウェアエントリへの参照を提供します。

図 *1 :*

図 *2 :*



これらの改善により、インシデント対応の既存の標準操作手順とのプロセス統合が容易になり、新しいアナリストの学習曲線が短縮されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。