SecHack365

SecHuv

Security Hub for Human-Vulnerabilities.

思索駆動コース

梅内 翼

Umeuchi Tsubasa

最終目標 人的脆弱性に起因する問題の責任をユーザへと帰着させずエンジニアリングで解決する世界へ。

はじめに - 問題提起と求められる仕組みの思索

人的脆弱性を突いた攻撃の発生が後を絶たない。

人的脆弱性を突いた攻撃への対策として進められている取り組みは**ユーザへの教育**がメインである。しかし、教育によって**「知識がある」状態**になったからと言っても、それが即座に**「現実に応用される」とは限らない。**

そこで、人的脆弱性への対策として必要な観点を定義し、**望ましい対策のあり方について思索**を行った。その取り組みを通して、人的脆弱性への対策において求められるツールやプラットフォームを4つ定義し、各々が緊密に連携することで有効な対策として効果を発揮することを実証するために以下の思想と目標に基づいて実装を行なった。

設計 - システムの思想と目標

インテリジェンス駆動型の有機的なセキュリティシステム。

場当たり的な対策で終わらないようにするために、インテリジェンス駆動型の**有機的なセキュリティシステム**を構築する。

そのために、人的脆弱性の種別を**CHVE(Common Human Vulnerabilities and Exposures)**として独自に体系化する。そして、**CHVE DB(人的脆弱性データベース)**に蓄積されたインテリジェンスを用いて各種ツールの性能を高めるとともに、各種ツールから得た情報によってインテリジェンスを強化するというサイクルが半自動的に運用されることによ**るセキュリティのエコシステムを構築**を目指す。

SecHuv - システムの構成する要素とCHVEの定義

SecHuv - Security Hub for Human-Vulnerabilities.

上記の設計思想及び目標をシステムとして実装する。

システム上ではあらかじめ定義されたCHVEをもとにインシデントの検知及び狙われた人的脆弱性の識別を行う。

ユーザ側に提供するツール群は以下の通りである。

SecHuv : Web

悪性Webサイト検出用
Webブラウザ拡張機能

SecHuv : Mail

悪性メール検出用ツール

SecHuv : Heart

インシデント相談用
チャットボット

SecHuv : Viewer

CHVE DBに格納された
データを公開するWebサイト

エンジン - 攻撃検知と識別のためのアルゴリズム

自然言語処理技術を活用した文書間の類似度計算。

ペイロードである自然言語を**Maximizing Semantic Volume**[2]に基づいて要約し、各ペイロードがどのCHVEを突いた攻撃である可能性が高いかを**Doc2Vec**やキーワードマッチングを用いて判断する。

フィッシングサイト 800,000件
フィッシングメール 1,000,000通 [1]

対策のアーキテクチャ

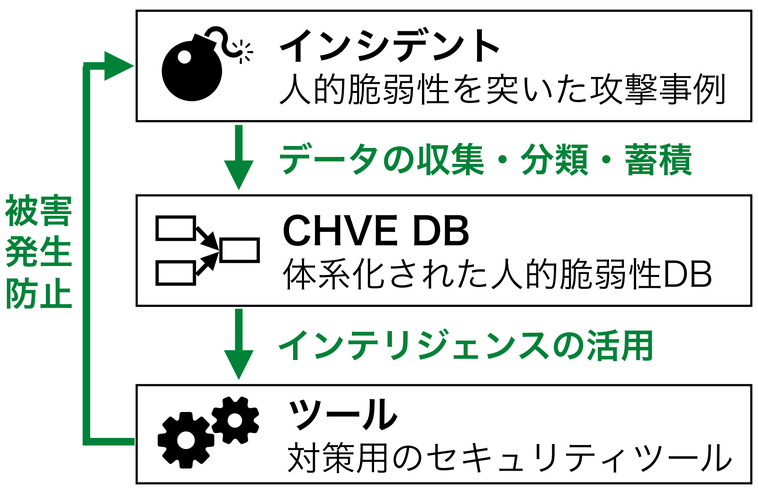
全体がエコシステムとして有機的に機能するような対策。

責任の所在

ユーザの知識ではなくエンジニアリングによって実現する対策。

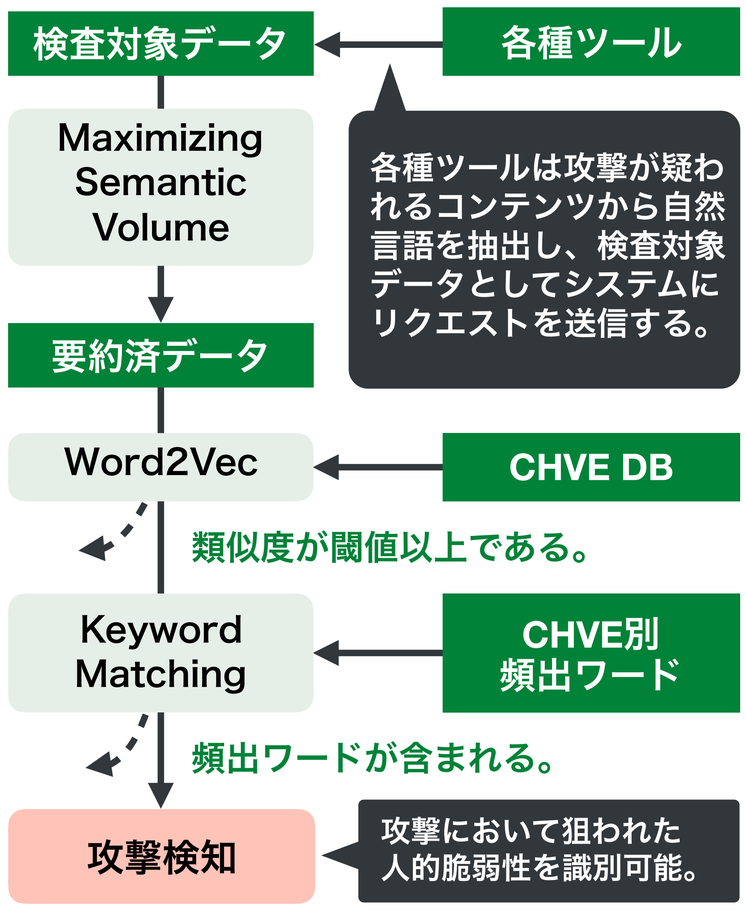
ユーザへの負担

インタフェースが簡潔で本当に対策を必要とするようなユーザから忌避されない対策。



CHVE
Common Human Vulnerabilities and Exposures.

CVEのアイディアを人的脆弱性に応用。
人的脆弱性の種別を体系化することで
攻撃の識別や対策技術の進化へと応用する。



[1] フィッシング対策協議会 フィッシングレポート2019

[2] Dani Yogatama, Fei Liu, Noah A. Smith,: Extractive Summarization by Maximizing Semantic Volume, The 2015 Conference on Empirical Methods on Natural Language Processing(EMNLP 2015).

NICT 国立研究開発法人 情報通信研究機構