SOC業務支援のためのオープンソースインテリジェンスシステムの提案と評価

Proposal and evaluation of Open Source Intelligence system to support SOC operations

大村篤生・マネジメント分科会・情報セキュリティ大学院大学

As cyber attacks become more sophisticated OSINT , which utilizes public information to quickly collect threat and vulnerability information, is attracting attention, and in-house OSINT to support SOC is considered effective for security defense and expanding security-related knowledge in organizations. In-house OSINT for the purpose of supporting SOC is considered to be effective for security defense of organizations and expansion of security knowledge.

研究概要

OSINTの定義：自組織へのセキュリティ脅威に対する予防と、セキュリティチームの知見・関心の向上を目的とする脅威・脆弱性情報の早期認識のため、公開情報から情報収集を行いその情報を有効に活用すること

SOC業務の課題
・スキルを持った人材の確保が困難
・現場運用のウェイトが重く、脅威動向を追えていない

SOC業務支援のためのOSINTシステム提案
・セキュリティに関する最新の脅威動向を自動的に収集する
・緊急性の高い脅威や脆弱性についてはその他の情報と区別して収集する
・要約された収集情報をチェックすることでSOCの通常業務への負担を少なくして**攻撃**の高度化を追う

OSINTシステムの実装・評価

既存のOSINTシステムに新規要件を付加
要件①収集情報の保存
要件②情報収集の脅威排除
要件③収集情報の翻訳
要件④収集情報の要約

↓

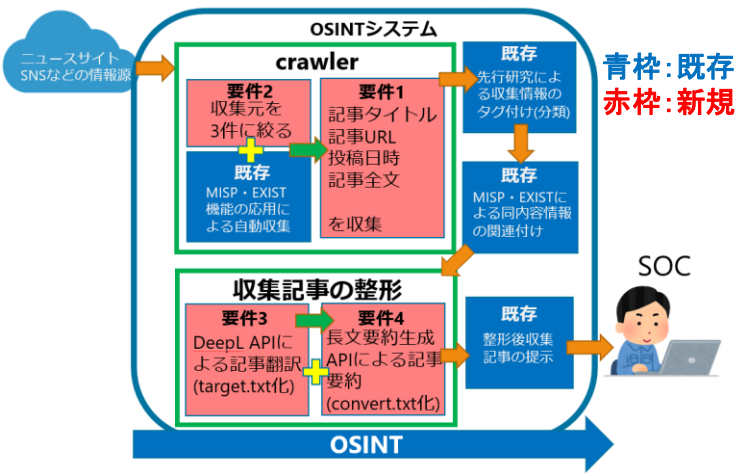
SOC業務従事者にアンケートを実施
・既存OSINT機能より、新規OSINT機能の方が評価が高い
・要件①、要件③の評価が高い

出力イメージ

記事タイトル、URL、本文(冒頭300字)等がcsvでリスト化される↓
※本文全文はtxtで個別に格納される

title	URL	投稿日時	キーワード	本文
Google、「Chrome 109」をリリース	https://www	2023/1/12	セキュリティ/対策/脆弱	Googleは、Windows・macOS、Linux向けにブラウザの最新版「Chrome 109」をリリースした。複数の脆弱性を修正
教員認定講習の論文が所在不明	https://www	2023/1/11	セキュリティ/対策	大阪府は、大阪府教育委員会免許法認定講習の受講者が作成した論文が所在不明になったことを明らかにした。同府に
アンケートフォームで設定ミス	https://www	2023/1/11	セキュリティ/対策/個人	大阪府守口市は、イベント参加者向けのアンケートフォームにおいて、他団体者に関する個人情報が閲覧できる状態と
Synology製ルータのOSやVPNサ	https://www	2023/1/11	セキュリティ/対策/脆弱	Synology製ルータのOSやアドオンパッケージのVPN機能に深刻な脆弱性が明らかとなった。アップデートが提供され
米政府、「DWASSRF」など悪用	https://www	2023/1/11	セキュリティ/対策/脆弱	2022年11月に明らかとなった「Microsoft Exchange Server」の脆弱性や、年明け2023年1月の月例パッチで修正された
「Adobe Acrobat/Reader」に深	https://www	2023/1/11	セキュリティ/対策/脆弱	Adobeは、PDFファイルの生成や編集機能を提供する「Adobe Acrobat」や閲覧機能を提供する「Adobe Reader」向け
「PHP」にセキュリティアップ	https://www	2023/1/11	セキュリティ/対策/脆弱	PHPの開発チームは、最新版となる「PHP 8.2.1」「同8.1.14」「同8.0.27」をリリースした。今回のアップデートでは
MS、2023年1月の月例セキュリ	https://www	2023/1/11	セキュリティ/対策/脆弱	マイクロソフトは、2023年最初となる月例セキュリティ更新プログラムを公開した。98件の脆弱性に対処しており、
トレンドマイクロが新ロゴ - 「T	https://www	2023/1/10	セキュリティ/対策	トレンドマイクロは、1月10日よりあらたなコーポレートロゴを使用すると発表した。従来と同様に円形の赤を主体と
解約完帳やローン導入申込書な	https://www	2023/1/10	セキュリティ/対策/個人	信用金庫の営野滝支店において、顧客情報が記載された書類の所在がわからなくなっている。医療業者に誤って引
健保組合向け管理システムでダ	https://www	2023/1/10	セキュリティ/対策	健康保険組合向けに人間ドック受診管理システムを提供しているイーウェルは、健保加入事業者へダウンロード権限を
「Apache Kylin」にアップデー	https://www	2023/1/10	セキュリティ/対策/脆弱	10月にオープンソースの分散分析エンジン「Apache Kylin」のアップデートにて脆弱性が修正されたが、対策をパイ
「Zoom Rooms」のクライアント	https://www	2023/1/10	セキュリティ/対策/脆弱	ビデオ会議サービスを展開するZoomは、Windows・macOS向けの「Zoom Rooms」においてアップデートを通じて脆
2022年12月のフィッシングURL	https://www	2023/1/10	セキュリティ/対策/フィ	フィッシング対策協議会は、2022年12月に報告を受けたフィッシング攻撃の状況について取りまとめた、報告数全体が
宅食サービス会社がランサム被	https://www	2023/1/6	セキュリティ/対策/ラン	食事宅配サービス「ナッシュ」を展開するナッシュは、パソコンが不正アクセスを受けてランサムウェアに感染し、デ
医療従事者向け求人サイトにサ	https://www	2023/1/6	セキュリティ/対策/サイ	医療機関向けのコンサルティングサービスや、医療従事者向けの求人検索サイトを運営するメディウェルは、「病院等
胃がん検診票が所在不明、郵便	https://www	2023/1/6	セキュリティ/対策	神奈川県相模原市は、個人情報含む胃がん検診票が所在不明になっていることを明らかにした。同市によれば、検診を
EC事業者の6割弱がサイバー攻	https://www	2023/1/6	セキュリティ/対策/サイ	ECサイト事業者の6割弱がサイバー攻撃による被害を経験していることがわかった。また3割弱が不正注文による被害
セブンイレブンのマルチコピー	https://www	2023/1/6	セキュリティ/対策	セブン・イレブン・ジャパンの店舗に設置されているマルチコピー機において一時障害が発生し、一部代替サービスを

提案モデル



利用者評価

アンケート結果：1(分かりにくい・無効)～5(分かりやすい・有効)

氏名	研究内容・説明の分かりやすさ	既存OSINT機能の評価	新規OSINT機能の評価	内容の取り込み機能(要件1)	情報収集の脅威排除機能(要件2)	情報の翻訳機能(要件3)	情報の要約機能(要件4)
A	4	3	4	5	1	5	3
B	5	4	5	4	3	5	4
C	5	3	5	5	2	5	5
D	4	4	5	5	3	5	4
Avg.	4.5	3.5	4.75	4.75	2.25	5	4

氏名	コメント
A	1つ目のシステムと2つ目のシステムでは、2つ目のシステムの方が使いやすかった。特に要件1の一覧と全文が分かれている部分については、詳細に調べたい記事をすぐにみることができるようになっていたのでよかった。要件2は、普段閲覧しているサイトが使えなかったため使いにくさを感じた。要件4は、使用する状況によっては助かる機能かもしれない。
B	説明が分かりやすく、使用したシステムも使いやすかった。翻訳は手動で翻訳機にかける手間が省けたのでとても良いと感じた。
C	2回目のシステムの方が比較して利用しやすい。要件2はもっと複数のサイトから記事を集められると良いと感じた。
D	

結論

・SOC業務支援のため、OSINT機能を活用した対策を提案
・提案システムの全体評価では、既存システムより提案システムの方が扱いやすいという評価を得た
・要件単体では、内容の取り込み機能(要件1)、情報の翻訳機能(要件3)においては高い評価を得た
⇒したがって、提案システムはSOC業務に必要な情報収集の面で支援されていることを示した