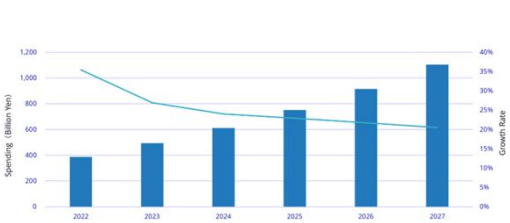
生成AIとOSINTを利用したサイバー対策に関する研究

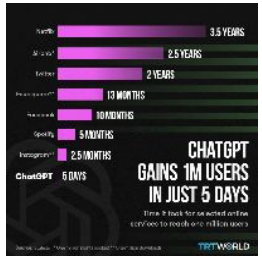
Research on Cyber Measures using Generative AI and OSINT

江　鴻浩・スシテム分科会・情報セキュア大学院大学

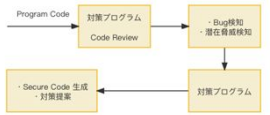
研究背景

- サイバー犯罪が大幅に増加している
- 攻撃者が日々新しい攻撃方法を探索し続けている
- サイバーセキュリティの重要性は高まっている
- 国内生成AIシステムの市場規模の拡大
- 生成AIの活用が急速に広がっている
- 生成AIが革新的なプロダクトとして活用されている



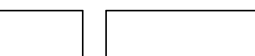


- SECURITY REPORTING
- THREAT INTELLIGENCE
- MALWARE DETECTION
- CYBERDEFENSE AUTOMATION
- INCIDENCE RESPONSE GUIDANCE
- DEVELOPING ETHICAL GUIDELINES
- IDENTIFICATION OF CYBER ATTACKS
- SECURE CODE GENERATION AND DETECTION



Code Review
潜在XSS攻撃の検知

サーバアクセスログ分析
潜在脅威特定
自動化分析スクリプト作成



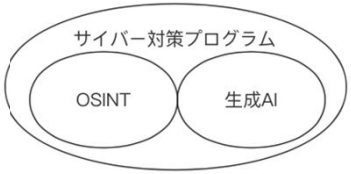
・敵を倒す
重要なガイダンスとコンテキストをセキュリティ チームの手元に置くことで、数時間や数日もかけずに数分でインシデントに対応できるようになる。

・他が見逃すものもキャッチ
膨大なデータ シグナルを主要な分析情報に要約し、ノイズを遮断し、被害が発生する前にサイバー脅威を検出し、セキュリティ体制を強化できる。

・チームの専門性を強化する
段階的なガイダンスを通じて若手スタッフに権限を付与してタスクを進め、シニア スタッフが戦略的優先事項に集中できるよう、面倒な作業を軽減。

提案手法

- OSINT情報源を整理し・対策行動に結びつき得る情報源を選定する
- 具体的な調査手法を確立し手順化する
- セキュリティ対策向上に寄与できるものかを複数の事件を利用して検証する
- 自動的な調査システム、あるいは容易な調査手順を確立する
- 生成AIをシステムに導入する（外部・内臓）
- 各シーンに対して、生成AIを特化したトレーニングを行って、自動化防衛と対策提案を実現する



今まで・今後

今まで

- OSINT情報源の整理：対策行動に繋がるOSINT情報の精査
- 調査手法の確立：具体的なツール選定と手順確立

今後

- 調査手法の効果実証：対策行動に結びついたか？
- 調査手法の自動化・汎用化：大規模な実施に向け汎用
- 生成AIの導入：生成AIをSOCアナリストとして、自動化防衛・対策提案