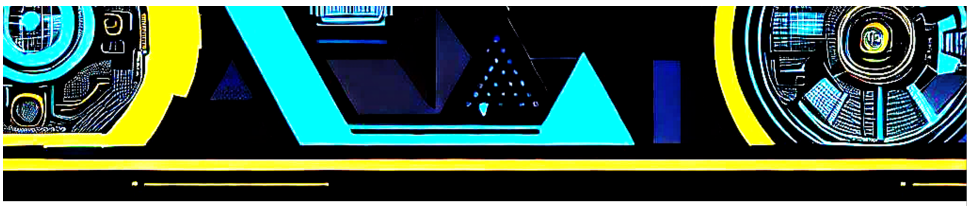

ICSCoE 中核人材育成プログラム
第6期 卒業プロジェクト

SOARを活用した セキュリティ運用の効率化

SOAR活用プロジェクト

SOAR を活用した
セキュリティ運用の効率化

独立行政法人 情報処理推進機構
産業サイバーセキュリティセンター
中核人材育成プログラム 6 期生
SOAR 活用プロジェクト

2023 年 7 月

目次

はじめに

近年、サイバー攻撃の増加[*1]に加えて、セキュリティ人材の不足がグローバル規模で課題となっており[*2]、企業におけるセキュリティ運用業務の負荷が高い状態が常態化している。また、現状のセキュリティ運用業務では定例的な単純作業にリソースを大きく割かれてしまい、検知ルールの作り込みや脅威ハンティングなどの高度な対応に着手できない状態となっている。

このようなリソースが限られた状況において、セキュリティ運用を実施していく解決策のひとつとして、セキュリティ運用業務を自動化するソリューションの導入が挙げられる。自動化ソリューションの選択肢は数多く存在するが、本プロジェクトでは、近年注目されている SOAR（Security Orchestration, Automation and Response）に着目した。SOAR は、現時点で導入事例や公開情報がほぼ存在しておらず、導入によって得られる効果や、導入・運用におけるポイントを把握することが難しい。

そこで、SOAR の実態を調査するため、企業の IT 環境を模擬した検証環境を構築し、SOAR の導入および効果検証を実施した。本書では、導入による効率化の評価結果やその際に得られた知見を記載する。

セキュリティ運用の定義および用語集

「セキュリティ運用」というフレーズは、人や組織によって様々に解釈することが可能である。本書では、「セキュリティ運用」をインシデントの兆候を検知する「検知」、インシデントの分析を実施する「分析」、関係各所との情報連携や処理の判断を実施する「連携・判断」、インシデントによる被害拡大を防ぐために実施する「封じ込め」と定義している[*3]。

図1: セキュリティ運用の定義

また、本書に記載する各用語は次のとおりとする。

[*1] 総務省 令和 4 年版 情報通信白書 NICTER におけるサイバー攻撃関連の通信数の推移 参照 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nf307000.html

[*2] (ISC)² 2022 Cybersecurity Workforce Study 参照 https://www.isc2.org/Research/Workforce-Study

[*3] NIST SP800-61 Computer Security Incident Handling Guide を参考に筆者らで定義。https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

用語	説明
API	Application Programming Interface の略で、ソフトウェアアプリケーション同士が情報をやり取りするためのインターフェース
CSIRT	Computer Security Incident Response Team の略で、コンピュータセキュリティインシデントへの対応を専門に行うチームまたは組織
EDR	Endpoint Detection and Response の略で、エンドポイントにおけるセキュリティ監視と対応のための技術
OSINT	Open Source Intelligence の略で、オープンソース情報を収集・分析する手法やプロセス
SLA	Service Level Agreement の略で、サービス提供者と顧客との間で合意される、サービス品質とレベルに関する契約書や合意事項
SOC	Security Operations Center の略で、組織内でセキュリティ監視、インシデント対応、脅威インテリジェンス、セキュリティイベントの分析などを中心に行うセキュリティ専門チームまたはセキュリティオペレーションの組織
アノマリ検知	データセットやシステムの中で、通常とは異なる異常な振る舞いやパターンを検知するための技術
クエリ	情報を取得するためにデータベースや情報システムに送信される要求
属人化	組織や業務において特定の個人に過度に依存してしまう状況
トリアージ	セキュリティインシデントや脆弱性に対して優先順位をつけ、リソースの効果的な配分や対応の計画を立てるプロセス
ハッシュ値	データやメッセージから数学的な関数によって生成される固定長の一意の値（バイト列や数字）
マネージドセキュリティサービスプロバイダ（MSSP）	組織や顧客に対してセキュリティ監視、脅威検知、インシデント対応などのセキュリティ関連サービスを提供する企業やプロバイダ
ローコード	ソフトウェア開発やアプリケーション開発を容易にするためのアプローチやプラットフォーム ローコード環境では、フローチャートやワークフローを使用して視覚的にロジックを定義することが可能である また、コンポーネントやテンプレートが事前に用意されていることが一般的である

本書の構成

第 1 節「SOAR について」では、企業におけるセキュリティ運用の効率化を進めるためのツールとして SOAR を紹介する。

第 2 節「SOAR の導入手順」では、SOAR の導入における実施手順を説明する。

第 3 節「SOAR の効果検証」では、企業を模擬した検証環境に SOAR を導入して評価を実施し、評価結果

と SOAR の有用性について説明する。

第 4 節「導入や運用における注意点」では、導入や運用において注意すべき点について説明する。

第 5 節「まとめ」では、本書のまとめを記載する。

本書の想定読者

本書は、以下の方を対象としている。

- セキュリティ運用業務の自動化に興味・関心がある方
- SOAR を用いたセキュリティ運用を検討・実施している方
- CSIRT や SOC などに従事するセキュリティ担当者の方

免責事項

- 本書は単に情報として提供され、内容は予告なしに変更される場合がある。
- 本書に誤りがないことの保証や、商品性または特定目的への適合性の黙示的な保証や条件を含め明示的または黙示的な保証や条件は一切ないものとする。
- 本書に記載の内容は、独立行政法人 情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、著者の見解に基づいている。
- 本書の利用によるトラブルに対し、本書著者ならびに監修者は一切の責任を負わないものとする。
- 本書の有効期限は、発行日から 2 年間とする。

1　SOAR について

1.1　SOAR とは

SOAR とは、Security Orchestration, Automation and Response の略であり、Gartner 社によって以下のとおり定義されている[*4]。

> SOAR とは、組織がセキュリティ運用チームによって監視される入力を収集できるようにする技術を指す。例えば、SIEM やその他のセキュリティ製品からのアラートは、人と機械の力を組み合わせてインシデント分析とトリアージを実行でき、標準化されたインシデント対応活動の定義、優先順位付け、推進に役立つ。SOAR を使用すると、組織はデジタルワークフロー形式でインシデント分析と対応手順を定義できる。

SOAR では、対応フローを定義した手順書である「プレイブック」を作成することにより、アラートのトリアージからオペレーションまでの一連の対応を自動化することが可能である。つまり、SOAR を活用することでセキュリティ運用業務の負荷を軽減することができ、そのリソースを高度な対応に割り当てることが可能になる。

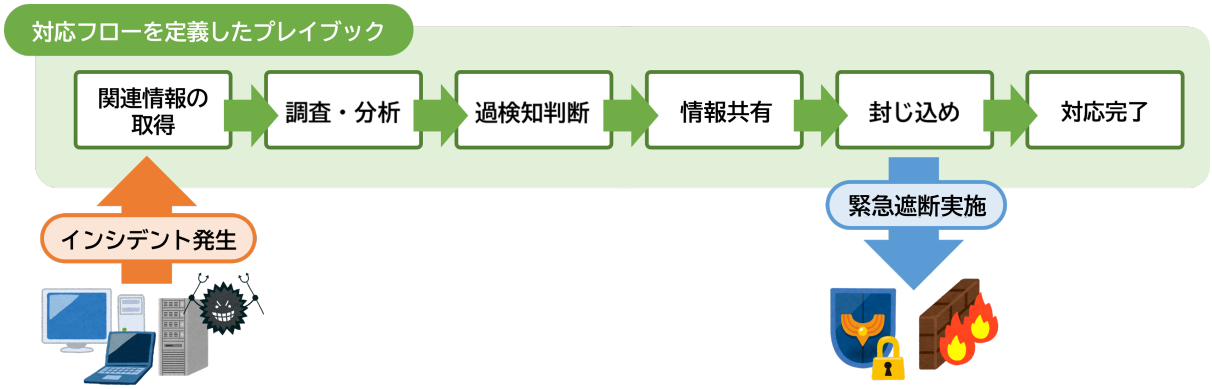

図2: SOAR の仕組み

1.2　SIEM との違い

セキュリティインシデントを統合的に扱うツールとして、SIEM(Security Information and Event Management) というソリューションがある。SIEM とは、各所に設置してあるセキュリティ機器などからログやアラートを集約して 1 箇所で確認できるようにし、相関分析によってインシデントを検知することができるセキュリティ情報イベント管理ツールである。一方、SOAR では、SIEM で検知したアラートと連携し、トリアージや対応の自動化を実施することが可能である。

[*4] Definition of Security Orchestration, Automation and Response (SOAR) - IT Glossary より引用し日本語に翻訳 https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

1.3 他の自動化手法との違い

自動化手法として、他に活用されている手法について説明する。

- RPA
  RPA とは、日本 RPA 協会によって以下のとおり定義されている[*5]。
  > RPA とは、これまでの人間のみが対応可能と想定されていた作業、もしくはより高度な作業を人間に代わって実施できるルールエンジンや AI、機械学習等を含む認知技術を活用した新しい労働力を創出する仕組み (Digital Labor)

  これまで人が行ってきた定型的なパソコン操作をロボットにより自動化するものであり、具体的には、GUI 上の操作を認識する技術とワークフロー実行を組み合わせ、表計算ソフトやメールソフト、ERP（基幹業務システム）など複数のアプリケーションを使用する業務プロセスを自動化する手段として使用されている[*6] 。
- プログラミング言語を用いたスクリプト
  Python などのプログラミング言語を用いたスクリプトを作成することによって、自動化できるセキュリティ運用業務も存在すると考えられる。ただし、セキュリティ運用の理解に加えて、プログラミング言語のコーディングの技術力が必要となる。その両方を複数人が身につけることは容易ではなく、自動化を実装できたとしても属人化を招く恐れがある。また、昨今の転職事情などを踏まえると、そのような高い技術を持った人材を確保し続けられるとは言い難い。

[*5] 一般社団法人日本 RPA 協会 より引用 https://rpa-japan.com/news/33/
[*6] 総務省 情報通信統計データベース RPA（働き方改革：業務自動化による生産性向上）参照 https://www.soumu.go.jp/menu_news/s-news/02tsushin02_04000043.html

2　SOAR の導入手順

SOAR の導入手順として、自動化対象項目の洗い出し、プレイブック作成・運用について説明する。

2.1　目標設定

はじめに、企業として目指すべき姿や、SOAR を導入することにより達成したいことなどの目標を明確にしておくことが重要である。目標を明確にしておくことで、導入を進めていく過程で目的を見失わずに進めることができる。

2.2　課題整理

課題整理では、現状のセキュリティ運用業務における課題を整理する。セキュリティ運用業務に関する対応フローの洗い出しを行い、業務負荷などの課題となっている個所を明確化する。なお、対応フローの洗い出しを行う際には、公開されているフレームワークを活用すると網羅的に整理することができる。本プロジェクトでセキュリティ運用を定義する際に参考にした「NIST SP800-61 Computer Security Incident Handling Guide」や セキュリティ対応組織を構築・運用するためのフレームワークとして公開されている「JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク[*7]」などを参考にするとよい。SOAR 製品開発企業によっては、インシデント対応フローが公開されているものもあるため、参考にするのもよい。

2.3　自動化対象項目の優先順位付け

次に、前項で整理した対応フローをもとに、自動化対象項目を決定し、SOAR で自動化を実現するための対応フローを決定する。自動化対象項目を決定するにあたっては、発生頻度が高いか、定例的な作業であるか、ミスが発生しやすいかということがポイントとなる。効率化という点で SOAR の恩恵を最も受けやすい自動化対象項目から優先順位をつけて段階的に導入していくことが重要である。また、自動化対象項目をプレイブックに落とし込む際には、対応フローとして整理する必要がある。既存の対応フローから変更不要であることがほとんどだが、自動化対象項目や使用するログによっては順番を前後し、まとめた方が効果的な場合もある。なお、遮断などの重要な判断を行う際は、状況や局面に応じた柔軟な意思決定が必要になると考えられる。プレイブックの作りこみにより対応フローの完全自動化を実現できる可能性もあるが、その工数が自動化によるメリットに見合うものになるか、運用を行う上で必要な柔軟性を備えているかを慎重に検討する必要がある。このように、対応フローには、自動化に適さない項目が少なからず存在すると考えられるため、そのような項目は自動化対象にしないという選択肢もある。

2.4　プレイブックの作成

次に、前項で洗い出した自動化対象項目をもとにプレイブックを作成する。プレイブックの作成にあたっては、対応フロー全体を一つのプレイブックで作成するのではなく、モジュールごとにプレイブックを作成する

[*7] JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク https://www.ttc.or.jp/document_db/information/view_express_entity/1423

方法がある。具体的には、対応フロー全体に相当するメインプレイブックを作成し、具体的な自動化対象項目をサブプレイブックとして作成し、メインプレイブックからサブプレイブックを呼び出す方法である。

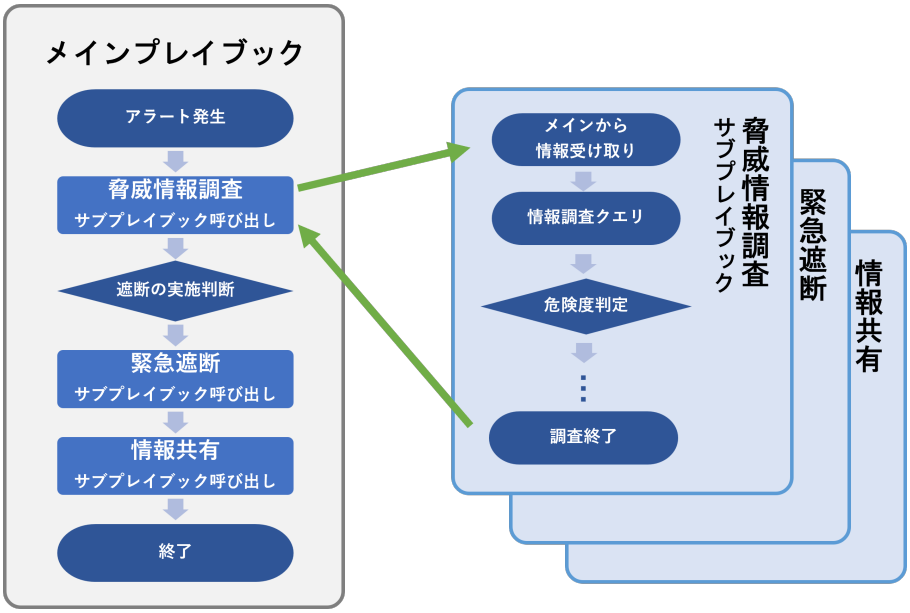

図3: メインプレイブック・サブプレイブックの概要

このようにサブプレイブック化（モジュール化）することで、優先度の高い自動化対象項目から段階的に実装しやすく、プレイブックの修正が必要になった際のメンテナンスが容易になるというメリットがある。加えて、対応フローによらず同じ作業内容が求められる場合でも重複する作業を何度もプレイブック化する必要がなくなるため、プレイブック作成に要する時間を最小限に抑えることができる。

また、サブプレイブック化をせずに作成したプレイブックは、対応フローの分岐が細かく複雑な構成になる可能性が高い。そのようなプレイブックは、作成者以外には全体像が理解しにくく、メンテナンスも困難になってしまう。そのため、できる限り細かな分岐は設けず、サブプレイブックとして分割することが望ましい。なお、サブプレイブックごとにプレイブックを作成する場合にも、対応フローの全体像や自動化対象項目の実施内容の理解は必要である。具体的なプレイブック作成例は 3節に、作成における注意点については 4節に記載する。

2.5 動作検証

最後に、作成したプレイブックを実行し、正常に動作するか動作検証を実施する。プレイブック単体で動作検証を行い、メインプレイブックとサブプレイブックを結合した状態で動作検証を実施する。想定通りに動作するかを確認するだけでなく、条件分岐が含まれている場合は網羅的に動作を確認する必要がある。その際には、プレイブック内の処理でエラーが発生しないか、エラーが発生した場合の例外処理が入っているか、処理完了までの待ち時間が考慮されているか、などの観点から確認する。また、API 連携を行うプレイブックの場合は、API 使用回数制限に注意し、再試行回数等の調整を実施する。なお、連携機器の設定変更を伴うプレイブックの動作検証を実施する場合は、運用に影響が出ないように細心の注意を払う必要がある。例えば、実施する時間帯への配慮や、関係各所への事前の情報共有などを行うとよい。

3　SOAR の効果検証

本節では、本プロジェクトで実施したセキュリティ運用における現状の課題とそれに対する自動化対象項目の検討、および自動化の効果検証について説明する。

3.1　自動化検討対象項目

検証を行うにあたり、 2.3項で示した「発生頻度が高いか」、「定例的な作業であるか」、「ミスが発生しやすいか」という 3 つの観点から、自動化対象項目を検討した。

本プロジェクトにおいてセキュリティ運用と定義した「検知」、「分析」、「連携・判断」、「封じ込め」という 4 つのフェーズに分け、検討したセキュリティ運用項目を以下の図. 4に示す。

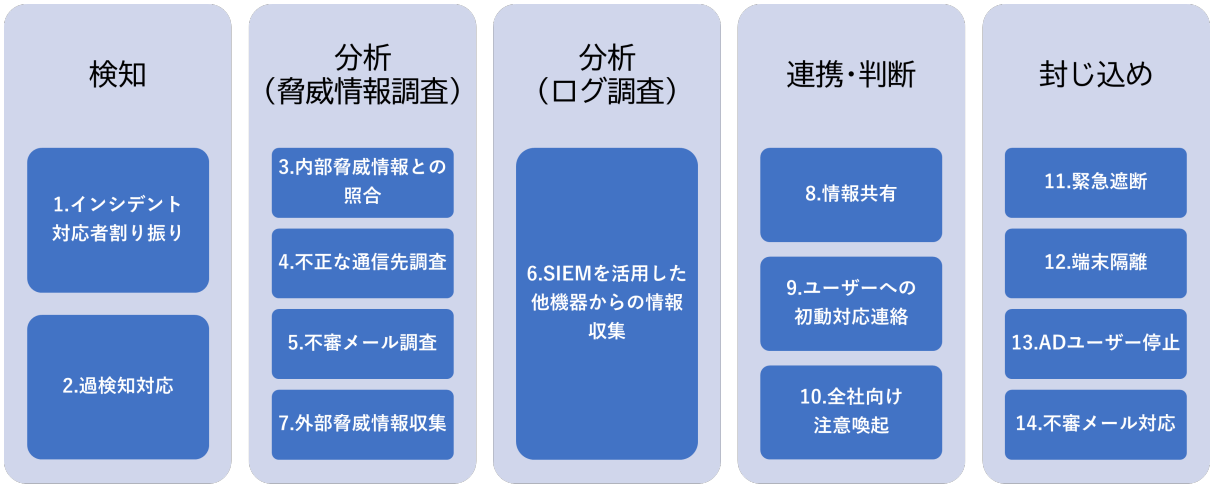

図4: 自動化を検討したセキュリティ運用項目

各項目について、現状のセキュリティ運用における課題や自動化方法の検討内容を順に説明する。

検知フェーズ

1. インシデント対応者の割り振り
   担当者ごとのインシデントの対応状況が把握しにくいことやインシデントが多発した際の取りこぼしが発生する可能性があることが課題として挙げられる。SOAR の機能として挙げられるインシデントのチケット管理システムを活用し、シフト管理システムと連携することにより、担当者の対応状況の把握、担当者への対応要否の確認、最終的に担当者の割り当てまでを自動化することを検討した。
2. 過検知対応の処理
   ユーザーアクティビティに関するアノマリ検知は、発生頻度が高く、過検知であることが多い。対応として、担当者だけでなく検知ユーザーにヒアリング対応をしてもらう必要があり、双方で負荷となっていることが課題である。アノマリ検知に関するインシデントが上がった際には、検知ユーザーに対してメール等で自動連絡を行い、ユーザーの意思による操作だったのかを簡易的に回答し

てもらう方法を検討した。

分析フェーズ

3. 内部脅威情報との照合
   企業にて独自の脅威情報を保有している場合、インシデントに紐づいた IP アドレスや URL、ハッシュ値等の情報が一致していないかを確認している。脅威情報を保管しているデータベースに照合した結果をインシデントのチケットにコメントとして書き込みを行う方法を検討した。
4. 不正な通信先に関する調査対応
   各種 OSINT ツールを使用した調査を実施しているが、活用するツールが分散しており、インシデントに紐づいた IP アドレスや URL 等の情報を一つずつコピー＆ペーストする方法で調査しているため、作業に時間を要していることが課題である。API を活用し各種 OSINT ツールと連携することで、自動で調査を行い、調査結果をインシデントのチケットにコメントとして書き込む方法を検討した。
5. 不審メールに関する調査対応
   項目4と同様にメールに記載されているリンクや添付ファイルのハッシュ値を一つずつコピー＆ペーストする方法で調査しているため、作業に時間を要していることが課題であり、同様の自動化を検討した。
6. SIEM を活用した他機器からの情報収集
   プロキシサーバー等のログをもとに、攻撃によるものなのかの判断や被害範囲の特定を行うための詳細調査を実施しているが、確認項目が多数に渡ることやログの量によっては調査に時間を要することが課題である。また、メールに関しては配送や開封状況の確認、同様のメールが他のユーザー宛に届いていないかの追加調査が必要となる。SIEM に保管しているログの中から判断に必要な情報を取得するためのクエリを作成し、検索結果をインシデントのチケットにコメントとして書き込みを行う方法を検討した。
7. 外部脅威情報の収集
   外部で公開されている脅威情報の収集を行うにあたり、費用面の問題からフリーの収集先から脅威情報を適応したり、Twitter 等の SNS から有識者が公開している最新の攻撃動向や脆弱性情報に関する情報収集を行っている。API を活用し、公開情報や Twitter から収集した情報を自動的にデータベースに取り込む方法を検討した。

連携・判断フェーズ

8. 情報共有
   インシデント発生時に上長や関連部署へ情報共有を行う際、SLA の厳守が求められる一方で、インシデント対応に追われてスムーズに行うことができていない。必要なタイミングで必要な情報をすみやかに各所へ展開できるように自動化する方法を検討した。
9. ユーザーへの初動対応連絡
   ウイルス感染の疑いがある端末の所有者に対して、ネットワークからの切断や状況のヒアリングを実施する必要があるが、主に電話での対応となり、スムーズに進まないことがある。項目2と同様

の方法で、必要な情報を所有者であるユーザーに事前通知する方法と、電話帳情報との連携をとることで電話対応時に必要な電話番号の検索を自動化する方法を検討した。

10. 全社向け注意喚起
    不審メール対応において、メールフィルタリングシステムではすべての不審メールを防ぐことはできないため、定期的に確認し注意喚起を実施しているが、リアルタイムでの通知は難しく運用負荷となっている。インシデントに上がった不審メールの情報をもとに、全社向け掲示板等との連携やメール発信により注意喚起を自動化する方法を検討した。

封じ込めフェーズ

11. 不正な宛先の緊急遮断設定
    調査結果により IP アドレスや URL 等の情報が不正であると判断した際に、ファイアウォール等での緊急遮断を実施している。設定を行うにあたり、手順書の作成やダブルチェックが必要となる等、作業に割かれるリソースが多く、緊急の作業にも関わらず対応を実施するまでに時間がかかっていることが課題である。API を活用し、インシデントに紐づく IP アドレスや URL 等の情報から、ファイアウォールへの緊急遮断の設定を自動で実施する方法を検討した。
12. 端末の隔離
    インシデント発生時もしくは調査結果により通信の発生元となる端末の健全性が確認できない場合、ネットワークからの隔離が必要となる。隔離の方法はいくつか考えられるが、本プロジェクトでは EDR を使用した隔離を自動で実施する方法を検討した。
13. AD ユーザーの停止
    インシデント発生時もしくは調査結果により AD ユーザーが侵害された可能性がある場合、AD ユーザーの無効化が必要となるため、AD ユーザーの停止を自動的に実施する方法を検討した。
14. 不審メール対応
    メールシステムとの連携により不審メールの隔離や送信者アドレス、件名や添付ファイル名でのブロックを自動化する方法を検討した。

3.2 自動化完了項目

前項で検討した自動化対象項目のうち、本プロジェクトにおける SOAR による自動化の実装結果を図. 5に示す。

本プロジェクトで自動化未実施となった項目は、その他の機器との連携が必要であり、連携方法や自動化対象項目の実装方法が分からずに断念したものが主である。SOAR の製品選定や導入を検討する時点で、ベンダーサポートの有無やサポート範囲の確認、自動化対象項目が実現可能なものであるかを検討項目として盛り込む必要があると感じた。なお、プレイブックの作成を通して感じた注意点については、 4節にて説明する。

3.3 評価

効果検証の評価について、時間、費用、人材の 3 点を評価軸として評価した結果を説明する。

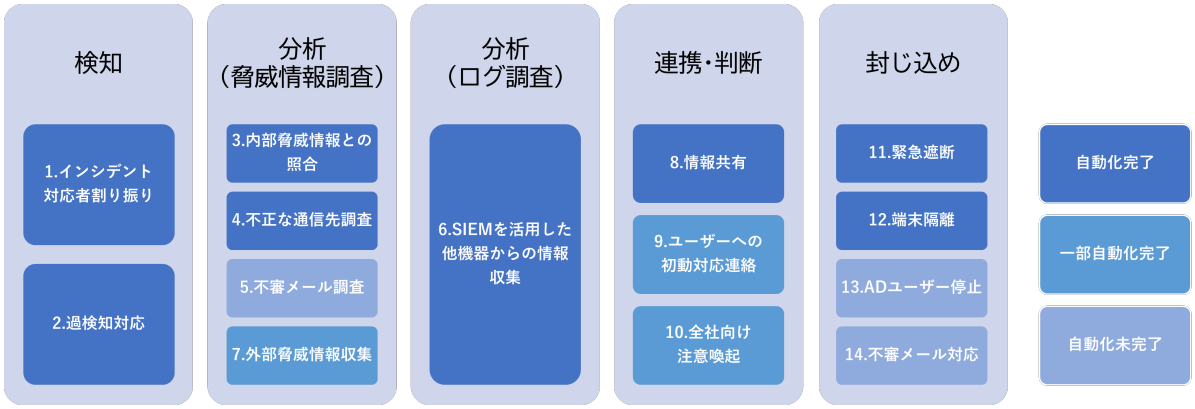

図5: 自動化実装結果

時間

本プロジェクトでは、不正通信の発生もしくはマルウェア検知をトリガーとする模擬インシデントに対して、SOAR を使用した場合の対応時間と SOAR を使用しなかった場合の対応時間（従来の対応方法での対応時間）を比較した。模擬インシデントに対する対応フェーズと、SOAR あり・なしの対応時間の結果は以下の表. 1のとおりである。

表1: SOAR 利用による対応時間削減効果

対応フェーズ	SOAR なし対応時間 in 時: 分: 秒	SOAR あり対応時間 in 時: 分: 秒	削減率
検知	0:02:12	0:00:12	91%
分析（脅威情報調査）	0:07:51	0:00:31	93%
分析（ログ調査）	0:11:35	0:00:31	93%
連携・判断	0:05:25	0:00:02	99%
封じ込め	0:04:40	0:02:18	51%
合計	0:31:43	0:03:31	89%

【注】結果は SOC 業務経験者 3 名、未経験者 2 名で実施したものの平均値

検証の結果、SOAR ありの場合、SOAR なしの対応時間と比較して約 9 割削減できることが実証された。特に、分析や連携・判断のフェーズにおいて対応時間に大きく差が出ており、インシデントに IP アドレスや URL、ハッシュ値等の情報が複数含まれている場合や、インシデントが多発している場合には、SOAR による自動化の効果が十分に発揮されると考えられる。

封じ込めのフェーズのうち緊急遮断の実施について、検証環境との兼ね合いもあり、設定前の事前確認やダブルチェック等の通常実施する作業は省略した形で検証を実施した。そのため、実際には本検証結果よりも大きく対応時間が短縮されることが期待される。ただし、遮断により可用性が失われる可能性も考えられるため、すべてを自動化するのではなく、遮断前に人の判断を挟んだり自動化を行うインシデントを制限したりすることが望ましい。

費用

SOAR の導入に伴い発生する費用として、SOAR 製品自体の費用以外に検討しておく必要があるものを説明する。SOAR 自体に各種ログを取り込む必要がある場合には、ログのサイズや転送に関する費用が発生するため、自動化に必要なログの選定や取得期間を検討する必要がある。プレイブックによっては API 接続に際してライセンス費用が発生するものもあるため、事前に自動化対象項目として挙げられる場合には、費用として含めておく必要がある。プレイブックの作成の際にはノウハウの収集が必須であるため、メーカーサポートの費用を含めること、メーカーサポートの充実さを検討項目として盛り込んでおく必要がある。

また、SOAR 製品自体の料金体系が、従量課金制、ライセンス制のどちらを採用しているかも検討のポイントとなる。SOAR 導入による費用対効果を示す際に、自動化の範囲を徐々に拡大していくことを念頭に置いている場合は、従量課金制の方が効果が見えやすくなる。

人材

SOAR を導入することにより、セキュリティ運用に必要な工数の削減が見込まれるが、一方でプレイブックの作成やメンテナンスなどの SOAR の運用を行う工数が必要となる。SOAR の運用においては、セキュリティ運用の全体的な流れとそれに必要な知識だけでなく、SOAR の機能を理解した人材を確保しておくことが求められる。

3.4 SOAR の有用性

検証結果より、SOAR によりセキュリティ運用の効率化は実現できることが明らかになった。また、効率化以外に対応の平準化や対応フローの整備という点でも SOAR を導入することによる効果は大きい。担当者の業務経験の差に左右されず一定のインシデント対応が可能となり、調査や対応結果としてインシデントのチケットに記録されるコメントが統一化されるため、対応品質の向上にもつながる。プレイブックの作成がインシデント対応フローの整備につながることもメリットの一つである。

また、クラウド環境の活用が増えてきている状況で、監視対象をクラウド環境まで拡大するとなるとアラートが膨大な量になるが、SOAR の導入により現在の運用体制のまま監視範囲を拡大できる可能性がある。ただし、SOAR を利用する企業形態やセキュリティ運用組織の成熟度によって、導入の効果には大きな差が出てくると考えられる。

MSSP の場合は、プレイブックの作成に時間や費用を費やしても、顧客数が多ければ採算が合うためメリットは大きい。一方で、ユーザー企業の場合は MSSP と契約しアウトソースする選択肢もあるが、SOAR を活用して効率化することにより工数の削減を見込めるのであれば、自社内で SOAR を導入しセキュリティ運用を行う方が費用を抑えられる可能性がある。プレイブックの作成に関しては、メーカーサポートを駆使することやプレイブックを共有できるようなコミュニティが存在する場合はそれを活用しながら、プレイブックの作成に割くリソースを可能な限り低減させることで、SOAR 導入効果の最大化を図ることが望ましい。

4　導入や運用における注意点

4.1　プレイブック作成時の注意点

プレイブックを作成する際には、以下の点について注意する必要がある。

人の判断の介在

3節でも述べたとおり、対応フローによっては完全自動化が適さないものもあるため、処理内容に応じて人の判断を介在させることが必要である。例えば、不審な通信先をファイアウォールで遮断するプレイブックを導入する際、前段で調査フェーズを経ても、100%不審かどうかを機械的に判断させることは難しい。そのため、調査結果をもとに継続処理の遮断を実施するか人の判断を介在することで、誤遮断による可用性の損失というリスクを減らすことができる。また、ウイルスに感染したと思われる端末を隔離するプレイブックを導入する際、その端末の利用用途によっては即時隔離を判断することはリスクが大きい。事務業務を行う社員の端末であれば、企業の業務影響に直結することはあまりないが、制御システムに関連する端末の場合は業務停止につながる可能性も考えられる。制御システムに限らず、可用性に影響を与えるものに対して遮断等の設定変更を自動化する場合は、関連部門や社員の理解を得ることが必須であり、可用性に影響を与えない導入方法を十分に検討する必要がある。一定時間応答がない場合の対応フローを用意しておくことも必要である。

他の機器との連携

他の機器と連携し、設定変更等を行うプレイブックを作成する場合は以下の 2 点に注意すべきである。なお、他の機器との連携を行うにあたり、API 接続を使用することがほとんどであるが、API 接続の利用における注意点は次の項目で説明する。

- **設定変更の実行結果の確認**

  遮断等の他の機器の設定変更を自動化する場合には、機器によって設定反映に時間を要するものもある。設定反映が正常に完了したかどうか確認するアクションも自動化の中に組み込めるとよい。
- **誤対応の復旧**

  他の機器との連携により遮断や隔離を実施するプレイブックを導入する際には、誤対応を実施してしまった場合に備えて復旧用のプレイブックも併せて作成しておくべきである。

API 接続の利用

自動化による対応範囲を広げるために、他の機器との連携や外部ソースとの連携に API 接続を利用することは必須である。しかし、API 接続を利用するにあたって注意すべき点がある。

- **処理時間や使用制限**

  API 接続をする際の処理の待ち時間を想定した設定を組み込む必要がある。プレイブック上でデフォルトで設定されている待ち時間以内に API 接続処理が完了しなかった場合、API 接続処理が繰り返し実行され、API 接続の使用回数が消費されたり、プレイブックがエラーで途中終了したりすることとなる。使用回数に関して、API によっては上限が設けられているものもあるため、API の

使用制限を確認したうえで実装する必要がある。

・**認証**

API 接続に伴い認証が行われるが、認証にユーザーアカウントを使用するものについては注意が必要である。API 接続を使用する処理によっては、連携機器の設定変更を行うことも考えられるため、最小権限を与えたユーザーを使用したり API 専用のユーザーを作成することが望ましい。

・**信頼性**

API を介した情報漏洩やデータの不正更新というセキュリティリスクに注意する必要がある。特に外部ソースとの連携を組み込む際には、ソースの信頼性を明確にしておくべきである。

テンプレートの活用

SOAR にはプレイブックのテンプレートが用意されていることが多い。テンプレートを活用することでプレイブックの作成を容易に行うことができるが、テンプレートを有効にするだけでは動作しない場合がある。

・**権限**

先に述べた API 接続を利用するプレイブックの場合、API 接続の設定や認証に使用するアカウントの権限設定などの注意が必要である。

・**互換性**

連携機器のバージョンによって対応しているテンプレートが異なる場合もあるため、テンプレートの使用要件を事前に確認しておく必要がある。

ローコードで作成するリスク

プレイブックはローコードで作成できるものが多く、GUI で操作しながら視覚的に作成できるため、開発やコード作成の経験や技術がない人でも容易に作成できるメリットがある。一方で、GUI で作成した内容がエラーによりコミットできない場合の原因調査やプレイブックの作りこみにはコード自体の理解が必要な場面もある。

・**教育**

メーカーサポートを活用することはもちろんのこと、コミュニティ等で公開されているノウハウを収集したりメーカー提供のトレーニングを活用することで SOAR 製品やプレイブック作成に関するスキルを習得する必要がある。

・**属人化の防止**

作成者に属人化しないよう簡潔で分かりやすい対応フローを意識することや、作成者によって揺らぎが出ないように作成ルールを定義しておくことが望ましい。

ログ調査におけるクエリの作り込み

ログ調査の自動化を実装するためのクエリの作り込みには以下の注意すべき点がある。

・**ログ構成の理解**

調査に必要なログやログの構成を理解しておく必要がある。例として、検索時間の範囲においては、

検索範囲が短すぎると必要な情報が取得できず、一方で検索範囲が広すぎると情報量が多くなりすぎたり、他のインシデントのログが取得されたりする可能性があるため、適切な検索範囲について検討しておく必要がある。

・クエリ結果に応じた例外処理

クエリの結果がない場合や適切な結果が取得できない場合などの例外を適切に処理できるように実装する必要がある。例外発生時の挙動については、事前の検証が重要となる。

・インシデントチケットへ記録する情報の精査

調査結果をインシデントのチケットに記録する際、情報量や内容が適切であるか検討する必要がある。判断がしやすいように記載内容を工夫することや、記載内容をもとにどのように判断すべきかを記載しておくと、対応者のスキルによる対応の差をなくすことができる。ただし、クエリを作りこみすぎると、機器更新等によるログフォーマットの変更や取得情報を変更する際のメンテナンスに時間を要する可能性が考えられるため、記録する情報は十分に検討する必要がある。

4.2 運用時の注意点

SOAR の導入後、運用においても注意すべき点がある。

プレイブック実行のヘルスチェック

何らかの原因でプレイブックが正常に実行されなかった場合、対応が行われずインシデントによる被害が発生してしまう可能性がある。プレイブックが正常に実行されているかを可視化する方法として、SOAR のダッシュボード機能を活用しプレイブックの実行結果を表示したり、プレイブックが失敗した際にコミュニケーションツールやメール等で通知したりする方法を検討する必要がある。ダッシュボード機能は、プレイブックの正常性確認以外にもアラート件数や対応状況の可視化にも活用できる。

また、プレイブックによってどのような対応が実行されたかも可視化すべきである。本プロジェクトで実際に発生した例として、プレイブックの実行により端末が隔離されたことに気づかず、端末に接続できなくなり、その原因調査に時間を要してしまった。端末の隔離以外にも、何か設定を変更する対処を行った際には、チケットのコメントに記載したり関係各所に通知したりする方法を検討する必要がある。

プレイブックのメンテナンス

一度作成したプレイブックにおいて、対応フローに変更がない限り、メンテナンスの必要性はほとんどないと考えているが、必要となり得る場面を説明しておく。

まず、連携機器の仕様変更によりログ形式が変更された場面が挙げられる。ログ分析を行う対応をプレイブックで作成している場合、ログ形式の変更により、クエリによる検索で本来の結果が出力されなくなったり、検索結果を条件分岐に使用している場合は正常な分岐がなされなくなったりするなど、自動化の処理に影響が発生する。プレイブックで使用しているログやログ形式を把握・管理しておくことが必要である。

また、API の仕様や使用条件が変更された場面が挙げられる。API の使用回数制限が変更されたり、もともと無料だったものが有料化されることも考えられる。API の機能自体が終了する可能性もゼロではないため、使用している API に関する情報を定期的に収集し、事前にメンテナンスとして対応できるように注意すべきである。

プレイブックおよび API 接続の管理

SOAR の運用に伴い、自動化の対象範囲が拡大すると、プレイブックの作成数が増加するとともに、API 接続の使用数も増加すると考えられる。既に不要になったものや用途が不明なものが放置されることがないよう、プレイブックおよび API 接続の用途を十分に管理しておく必要がある。また、不要な API 接続は削除することで、前項で述べた API 接続の利用におけるセキュリティリスクを防ぐことができる。

SOAR を使用しない手順の整備

何らかの原因でプレイブックが正常に動作しなかった場合や SOAR を使用できなくなった場合を考慮し、従来通りの運用手順もしっかりと整備しておくことを忘れてはならない。

4.3 SOAR 選定時の注意点

SOAR 製品を選定する上で、注意すべき点を記載する。

連携可能な製品や API の種類

自組織で使用している製品や連携したいサービスに対応しているのか、事前に確認しておく必要がある。例えば、自組織で脅威インテリジェンスサービスを契約している場合、SOAR と連携し活用していくことが望ましい。SOAR がそのサービスに対応していない場合、脅威インテリジェンスを活用した自動化を行う際には追加で別サービスの契約が必要となるため、費用面で最適ではない。

ソリューションの提供形態

SOAR 製品は、オンプレミスのサーバーに導入するものと、クラウドサービスとして提供されているものに大別される。オンプレミス環境とクラウド環境を連携させることになると構成が複雑になるため、どちらかのネットワーク構成に重きを置いた方が良い。社内のネットワーク構成や自動化対象項目に関連する機器の構成を理解しておく必要がある。ログの収集が必要な場合は、情報の取り扱いについても注意が必要となる。また、対象項目の自動化が実現できるのか、前述の連携したい機器や API と合わせて事前に調査しておく必要がある。

製品の得意分野

SOAR 製品によって、得意とする自動化対象項目が異なる場合がある。同一メーカーのセキュリティ製品と連携した自動化が得意なものや、セキュリティ運用における検知・調査・封じ込めのうち何れかの自動化が特に得意なものなど、製品によって得意分野は様々である。そのため、自組織の目的に応じた選定が必要となる。

メーカーサポートの充実度

本検証での実態として、プレイブックの作成に一番時間を要した。特に自動化対象項目をプレイブックに実装していく段階で、その方法がわからず大変苦戦した。プレイブックの作成に時間を掛けず、SOAR

のメリットを最大限に生かすためには、メーカーサポートの対応範囲やプレイブックに関するノウハウをどれだけ提供してもらえるかといった点も、製品選定時の評価項目として盛り込むべきである。

5　まとめ

本書では、セキュリティ運用の効率化を目的としたSOARの導入手法の紹介と効果検証の結果に基づいた有用性、導入や運用における注意点について記載した。効果検証の結果、本プロジェクトで実装した自動化対象項目において対応時間が短縮され、セキュリティ運用の効率化につながるとともに、対応フローの整備や対応品質の向上も見込めることが明らかになった。

一方で、SOARを導入・運用する上で理解しておくべき点がある。

一つ目に、SOARを導入する際には、自組織におけるセキュリティ運用に関する課題を整理することや自動化により効率化したい運用項目を明確にすることが重要である。どの製品やサービスを導入する際にも言えることだが、SOARを導入することが目的とならないよう、SOARという手段を用いて目的となるセキュリティ運用の課題解決に対してどのように活用できるのかを導入時点で十分に検討する必要がある。導入後も、導入時点の状態で継続運用していくのではなく、プレイブックの見直しや自動化の範囲を徐々に広げていくなどの改善を重ねていく必要がある。

二つ目に、SOARによってすべてのセキュリティ運用業務を自動化でき、効率化できるわけではないということを念頭に置いておくべきである。企業におけるネットワーク構成や自動化対象項目に関連する機器によっては、SOARと連携するための基盤構築やプレイブック作成に時間や費用を要してしまい、費用対効果が小さくなる恐れもある。

上記について理解した上で、企業の課題や構成に適したSOAR製品を選定し、SOARによる自動化を実施することで、セキュリティ運用の効率化を実現できる。

本書で示したSOARの導入手法や自動化対象項目、プレイブック作成におけるポイントは、企業へのヒアリングおよび検証結果をもとに作成したが、あくまで本プロジェクトメンバーで考察した結果であり、ヒアリングにご協力いただいた企業の主張とは異なる点がある。そのため本書の内容が唯一無二の正解だと考えるのではなく、一つの参考として各企業における課題や目的に適した方法にアレンジして活用してもらいたい。

本書が、SOARの有用性および実態の理解の一助になり、企業におけるSOAR導入の後押しとなれば幸いである。さらに、実際にSOARを導入することによりセキュリティ運用が効率化され、より高度なセキュリティ業務に専念できる環境が整備されていく未来に期待したい。

謝辞

本書の作成にあたりまして、先駆者である ICSCoE 修了生やご協力いただいた組織の皆様にセキュリティ運用における課題や SOAR の導入・運用方法についてヒアリングさせていただくなど、多大なるご支援・ご尽力を賜りました。お世話になりました皆様にこの場を借りて心より御礼申し上げます。

また、産業サイバーセキュリティセンター中核人材育成プログラム講師の門林雄基先生、並びに満永拓邦先生には、本書の元となるプロジェクトのメンターとして、ご指導・ご助言、ご支援を賜りました。改めて御礼申し上げます。

そして、本書の作成や本プロジェクトをともに実施した、下記メンバーの皆様にも感謝を伝えたいと思います。

＜ **SOAR** 活用プロジェクトメンバー＞

リーダー

平岡 侑祐

サブリーダー

伊東 亘

メンバー

伊藤 昌範
髙橋 奈央美
土屋 拓仁
友藤 了佑
名畑 皓正
藪田 樹