Recorded Future®

ケース
スタディ

導入前の課題

- 自社が注視するべき攻撃者の手口や最新動向の把握が困難
- BASで対処すべき攻撃シナリオの選定や優先順位付けに時間がかかる
- BAS実行後の効果の確認が困難

導入後の効果

- Threat Mapで注目するべきアクターの優先度付けができる
- Threat Mapからチェックするべき攻撃シナリオを絞り込める
- 対策後のサイバー脅威を視覚化し継続的なBAS実行に貢献

SOMPO HOLDINGS

Recorded Future Threat MapとBASを連携して能動的サイバー防御と継続的な脅威検出管理を推進

「“安心・安全・健康のテーマパーク”により、あらゆる人が自分らしい人生を健康で豊かに楽しむことのできる社会を実現する」というパーパスを掲げ、人や社会を守り、支えるため、中長期的な視点で様々な社会課題に向き合っているSOMPOホールディングス株式会社。SOMPOグループでは、国内損害保険事業、海外保険事業、国内生命保険事業、介護・シニア事業およびデジタル事業などを展開し、ユニークかつ先進的な「安心・安全・健康のテーマパーク」の具現化を目指している。同社のIT企画部では、SOMPOグループ企業全体のサイバーセキュリティを強化するために、2020年からRecorded Futureの脅威インテリジェンスを導入し、攻撃者の分析を通して対策を強化してきた。そして、自社の脅威ランドスケープを視覚的に確認できるThreat Mapを活用し、BAS（Breach and Attack Simulation）と連携し継続的な攻撃シミュレーション実行の自動化を推進している。

活用・評価

脅威インテリジェンスを活用しグループ企業全体のサイバーセキュリティを強化

SOMPOホールディングス株式会社のIT企画部で、Recorded Futureを活用し、攻撃者の活動状況や攻撃の事前検知などに取り組んでいる大石明香セキュリティアナリストは、同部の役割と脅威インテリジェンスの運用効果を次のように評価する。

SOMPOホールディングス株式会社
IT企画部 セキュリティアナリスト
大石 明香氏

「当部では、SOMPOグループ会社のサイバーセキュリティ全般を監視しています。以前は、FS-ISACやOSINTなどの情報から手動で脅威情報や脆弱性情報をリサーチしていました。Recorded Futureの脅威インテリジェンスを導入してからは、攻撃性の高い情報の精査が迅速かつ効果的になりました。具体的には、脅威インテリジェンスで収集した脆弱性情報をグループ会社に配信したり、収集したIPアドレス情報のリスク度合いで精査して、関連URLを注意喚起したりするなど、監視及び警戒を行っています。また、SOMPOグループのブランド名を悪用した偽のサイトなどが作られていないか、といった監視にもRecorded Futureを活用しています」。

新たなチャレンジ

BASによるDefense-in-Depth戦略の推進と実施効率の追求

IT企画部のサイバーセキュリティグループで、能動的なサイバー防御（Active Cyber Defense）に取り組んでいるセキュリティエバンジェリストの小中俊典氏は、サイバー攻撃の脅威に対して積極的な防御を実施する重要性について次のように語る。

「SOMPOグループでは、Active Cyber Defenseを強化するために、BAS（Breach and Attack Simulation）の専門チームを編成し、攻撃シミュレーションを定期的に実施しています。BASの実行には、検査対象から収集した情報を元にして、仮想的な攻撃シミュレーションを実施するための自動化シナリオを選定する必要があります。そのため、選定する攻撃シナリオが的確ではないと、時間とコストをかけても適切な防御策を講じられない、という課題があります。加えて、BASを実行する優先順位も重要です。危険性の高いサイトやレイヤーから実施しなければ、対策が後手に回ってしまうのです。さらに、実行後に発見された脆弱性に対する評価や経営層への説明責任なども必要になります。BASによる効果的なActive Cyber Defenseを推進していくためには、攻撃シミュレーション対象の選定や、実施後の効果測定につながる脅威インテリジェンスの活用が求められていました」。

SOMPOホールディングス株式会社
IT企画部 サイバーセキュリティグループ
セキュリティエバンジェリスト
小中 俊典氏（2024年2月取材時）

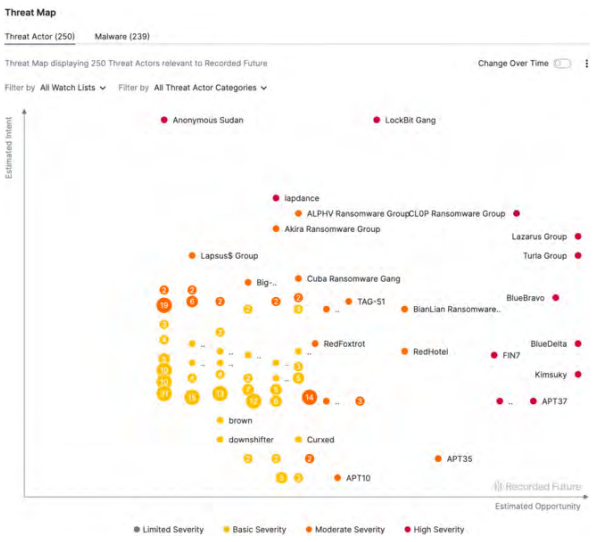
成果

Threat MapとBASを連携して攻撃シナリオ選定の精度を向上

効果的で的確なBASによる攻撃シミュレーションを実施するために、脅威インテリジェンスチームではRecorded Future Threat Mapに注目した。大石氏は「Threat Mapは、マップの右上から脅威が高い順にマッピングしてくれるので、対応しなければならない脅威の内容と優先度を視覚的に一瞬で把握できます。Threat Mapには、業界や利用テクノロジーなど、さまざまな検査対象を登録できます。また、Threat Mapにマップされている脅威アクターをクリックすると、侵害の兆候や攻撃者の過去の攻撃事例、防御や検出のためのルールなども特定できるので、サイバーセキュリティのチームが、現在の脅威の状況を視覚的に確認できます」と活用の効果を話す。

Recorded Future Threat Mapは、業界最大級の100万を超えるデータソースから、自然言語処理、特許技術である機械学習、さらにアナリストによりサイバー攻撃を分析し、脅威マップを作成する。

小中氏は「Threat Mapによって優先付けされた脅威とBASを連携すれば、検査対象となる環境に関連性の高い攻撃シナリオを継続的に実行できると考えました。具体的には、Recorded Futureの Intelligence Cloudに蓄積されている当社の脅威マップのデータをもとに、BASツールを実行するための攻撃シナリオと対象の優先度を決めていきます。また、これまではBAS実行後の効果測定が困難でしたが、サイトの脆弱性などの改善後にThreat Mapで継続的にモニタリングすることで、対策が効果的かどうかも確認できるようになります。Threat MapとBASの連携は、能動的なサイバー防御にとって高い効果の期待できる対策です」と評する。



展望

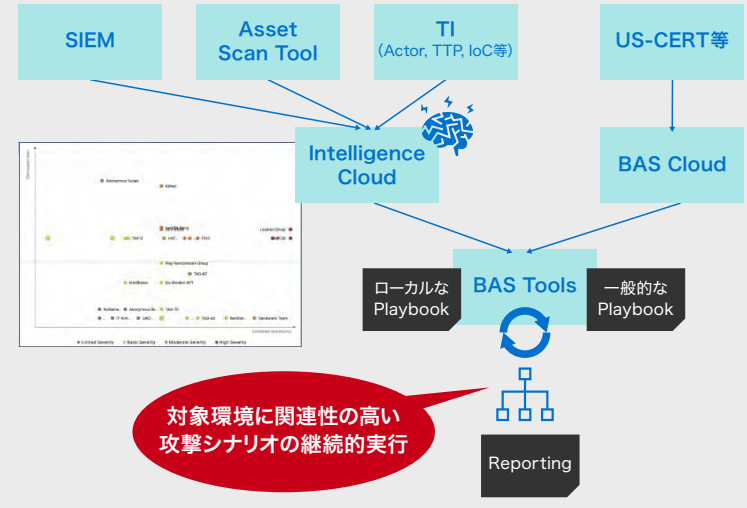
継続的なBAS実行と説明責任を果たす効果測定を推進

Threat MapとBASを連携させた能動的なサイバー防御の必要性について、小中氏は「昨今多くのサイバー攻撃がネットワーク・セキュリティ制御をバイパスしています。そこで効果的なセキュリティ戦略を推進するためには、継続的に脅威の状況をしっかりと理解し、実際のサイバー脅威に対して、セキュリティ制御を定期的にテストすることが必要です。そのテストも、環境に関連した基礎的情報と攻撃者の手口（Tactics, Techniques, and Procedures）を的確に取得した上で、環境ごとに脅威ランドスケープを設計していかなければ、BASの成果が得られません。さらに、BASは継続的に実行していかなければ、脆弱性の改善につながりません。そのために、現在はRecorded FutureのIntelligence Cloudと当社のBAS Cloudを連携させて、自動的にBASツールを実行する仕組みの構築を推進しています」と取り組みに触れる。

大石氏も「Recorded Futureを導入してからは、グループ会社への脆弱性に関するレポートの信頼度も上がりました。今後は、脅威インテリジェンスチームの中でRecorded Futureをより深く活用していく計画です」と語る。

さらに小中氏は「Threat Mapは、BASの実行に役立つだけではなく、脅威が軽減したかどうかの変化も確認できると期待しています。加えて、継続的にBASを実行していく有用性をグループ会社や経営層に説明していく上でも、とても重要な存在です」と利用効果を話す。

脅威インテリジェンスとBASによる能動的なサイバー防御の構成図



Recorded Future について

Recorded Future は、エンタープライズセキュリティインテリジェンスを提供する世界最大級のプロバイダです。継続的かつ広範な自動化されたデータ収集 / 分析と、人による分析を組み合わせることにより、タイムリーかつ正確で実用的なインテリジェンスを提供します。混沌と不確実性が増している時代において、Recorded Future は組織が脅威をより迅速に特定 / 検知する上で必要な可視性を提供するとともに、攻撃を阻止するためにプロアクティブなアクションを取り、人、システム、アセットを保護することで安心してビジネスを展開できるように支援しています。Recorded Future は、世界中の企業や政府系機関で利用されています。