技術検証

ジュニパーネットワークスによる脅威検知および修復の自動化

Sky Advanced Threat Prevention と SRX シリーズ ファイアウォール

シニア アナリスト、ジャック・ポーラー

2019 年 7 月

この ESG 技術検証は、ジュニパーネットワークスから委託され、ESG のライセンスを得て配布されるものです。

目次

ESG 技術検証

ESG 技術検証の目的は、IT 技術者に対し、あらゆるタイプや規模の企業向けの情報技術ソリューションに関する教育を提供することにあります。ESG 技術検証は、購入の意思決定を行う前に実施すべき評価プロセスを代替するものではなく、これらの新しいテクノロジを深く理解していただくためのものです。我々の目的は、IT ソリューションのより価値のある機能について調査し、それらをどのようにしてお客様の実際の問題解決に役立てることができるかを示すとともに、改善が必要な領域を特定することです。ESG 検証チームのエキスパートによる第三者的見解は、当社のハンズオン テストの結果と、本番環境でこれらの製品を使用しているお客様への聞き取り調査に基づくものです。

はじめに

この ESG 技術検証では、脅威検知と修復の自動化の効果と効率に注目しつつ、ジュニパーネットワークスの Juniper Networks Sky Advanced Threat Prevention（ATP）および SRX シリーズ次世代ファイアウォールを評価しています。ESG はこの評価プロセスの中で、マルウェアを使ってエンドポイントを侵害し、Sky ATP を使ってこの攻撃を検知します。これにより、ファイアウォールによってエンドポイントの垂直方向のトラフィックがブロックされ、ローカル スイッチによってエンドポイントの水平方向のトラフィックがブロックされ、エンドポイントはネットワークから切断されます。

背景

ESG が年 1 回実施している技術支出アンケートにより、サイバーセキュリティが IT 部門の最優先業務となっていることが分かりました。組織の 40% は、サイバーセキュリティの強化が今後 1 年間における技術支出目的の第 1 位になると回答しています。[1]

こうした組織は、サイバーセキュリティのさまざまな側面を改善することは容易なことではないと認識するでしょう。ESG の調査によると、組織の 4 分の 3 以上（76%）が、脅威の検知と対応は 2 年前に比べて難しくなっていると考えています。回答者は、脅威の検知および対応の主な課題として、脅威の数の増加と巧妙化（34%）、脅威を検知/対応するワークロードの増加（17%）、攻撃対象領域の増加（16%）、各種脅威検知/対応ツールの数の増加（11%）、サイバーセキュリティ スキルの世界的な不足（8%）などをあげています。[2]

今後 1 年間における組織の技術支出に占める割合のうち、**サイバーセキュリティの強化**が最も高いと考えている回答者の割合。

2 年前に比べ、**脅威の検知と対応**が難しくなったと考えている回答者の割合。

実際問題として、脅威を検知し、対応するために複数のベンダーのさまざまなツールが導入されています。このためアナリストは、アラートを管理して保護対策を実施するために、さまざまなシステムにログインする必要があります。これが原因で、手動による介入が発生し、検知、調査、対応、修復のプロセスに時間がかかり、平均対応時間（MTTR）が増え、攻撃者が留まる時間が延びています。

複数のポイント ツールの機能を集約するソリューションが必要になります。脅威の検知と対応のワークロードを自動化することで、このようなツールの使用と管理が簡素化されるソリューションです。アンケートに回答した人の 82% は、脅威の検知/対応を改善することが優先順位が高いと述べています。また、87% は、脅威の検知/対応を改善するための正式な計画と予算があると回答しています。[3]

ジュニパーネットワークスの Sky Advanced Threat Prevention と SRX シリーズ ファイアウォール

ジュニパーネットワークスの Sky Advanced Threat Prevention は、ジュニパーネットワークスの SRX シリーズ サービス ゲートウェイと連携し、仮想拠点、分散拠点、コア拠点向けのルーティング インターフェイス、スイッチング インターフェイス、WAN インターフェイスを使い、高パフォーマンスのネットワーク セキュリティ機能と高度な脅威緩和機能を実現します。

Sky Advanced Threat Prevention

ジュニパーネットワークスが構築した Sky Advanced Threat Prevention（ATP）は、クラウドからのリアルタイムの情報を利用する SaaS ソリューションです。マルウェアを防御して、APT（高度な持続的脅威）やランサムウェアといったサイバー攻撃から組織を守ります。Sky ATP は SRX シリーズ次世代ファイアウォールと連携し、パケットを詳細に検証して脅威をインライン ブロックします。Sky ATP は、サイバー攻撃を検知および防

[1] 出典：ESG 調査レポート、『2019 Technology Spending Intentions Survey』、2019 年 2 月
[2] 出典：ESG Master アンケートの結果、『The Threat Detection and Response Landscape』、2019 年 4 月
[3] 同上

御するために、機械学習、動的分析、アンチサンドボックス回避技術、静的解析、ウィルス対策シグネチャーを使用します。組織に Sky ATP を導入するメリットは次のとおりです。

- **クラウドベースの分析**—損害を与えるおそれのあるファイルをクラウドに送信し、高度な分析を使って良性か悪性かを判別します。
- **マルウェアの修復**—マルウェアを検知した情報が SRX シリーズ ファイアウォールに送信され、攻撃をブロックします。
- **レポートと分析**—設定や更新などの管理タスクを簡素化できる Sky ATP Web インターフェイスを備えています。また、脅威と侵害を受けたシステムを可視化するためのレポート ツールと分析ツールが用意されています。
- **システムの隔離**—SRX シリーズ ファイアウォールが Sky ATP からの情報を使い、侵害されたシステムを隔離します。
- **脅威情報の統合**—ジュニパーネットワークスの SecIntel 脅威情報サービスとリアルタイムに通信し、SRX シリーズ ファイアウォールに脅威情報を送信して即座に対応します。Sky ATP はオープン API を使い、サードパーティーの脅威情報フィードを、ATP を契約しているすべての SRX ファイアウォールに配信します。これにより、即座に対応して攻撃対象領域を削減できます。
- **コマンド&コントロール防御**—Sky ATP は SRX シリーズ ファイアウォールと通信し、マルウェアが社内に広まるのを防止し、コマンド&コントロール サーバーとの通信をブロックします。
- **メールと Web の分析/修復**—機械学習アルゴリズムを使ってメール ファイルおよび Web ファイルを分析し、悪意のある添付ファイルおよびファイルを検知します。ファイアウォールでこのようなファイルをブロックすることで、メールが攻撃ベクトルとして利用されることを防止します。
- **統合管理**—Sky ATP および SRX シリーズ ファイアウォールは、ジュニパーネットワークスのすべてのデバイスおよびサービスの管理を 1 つのコンソールに一元化できる統合アプリケーション、Juniper Networks Junos Space Security Director に統合できます。Security Director を使うと、ステートフル ファイアウォール、統合脅威管理、侵入防御、アプリケーション ファイアウォール、VPN、NAT に関する、すべてのフェーズのセキュリティ ポリシー ライフサイクルを管理できます。

SRX シリーズ サービス ゲートウェイ

ジュニパーネットワークスの SRX シリーズ サービス ゲートウェイは、次世代のファイアウォールです。クラウド、支社オフィス、小規模企業、中規模企業、大規模企業、大規模なデータ センター、サービス プロバイダ向けの仮想アプライアンスまたは物理アプライアンスとして利用できます。SRX ファイアウォールの目的は以下のとおりです。

- **あらゆる規模の組織に対応したセキュリティ**—SRX ファイアウォールは、オールインワン（物理および仮想のセキュリティ ネットワーク デバイスを統合）から、非常に拡張性の高い、シャーシベースのデータ センター ソリューションまで、多くの筐体で利用できます。
- **脅威に対する包括的な保護**—多層セキュリティ サービスで構成された包括的スイートを使い、既知の脅威および未知の脅威を防御できます。
- **パフォーマンスと拡張性**—最大 285 Gbps の IMIX ファイアウォール、同時セッション数 9,000 万、230 Gbps IPS により、1Tbps までのスループットに対応できるように拡張できます。
- **信頼性**—ハードウェアおよびソフトウェアのインサービス アップグレード、コンポーネントの冗長構成、およそ 99.9999% の信頼性により、継続的なアップタイムを実現します。業務、セキュリティ、アプリケーションを、停止することなく継続できます。

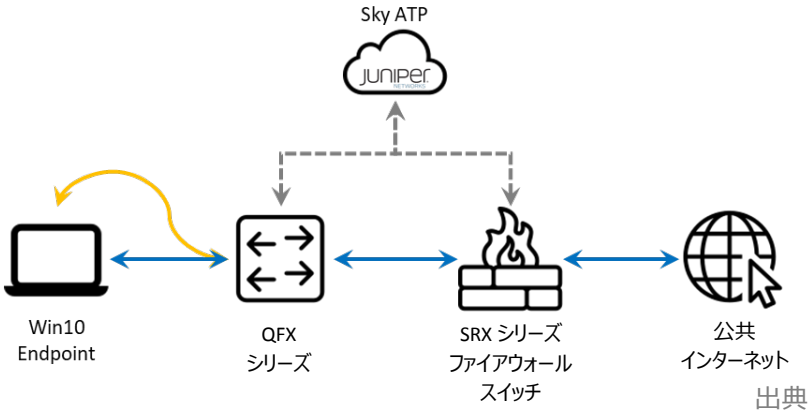
ESG 技術検証

ESG が実施した、Sky Advanced Threat Prevention および SRX シリーズ ファイアウォールの評価およびテストでは、悪意のあるファイルをエンドポイントにダウンロードすると、SRX ファイアウォールから Sky ATP に送信されて評価されることを検証しました。確認したのは主に、エンドポイントが感染されたことが Sky ATP によって検知されたときに、検知、対応、修復が自動的に行われることです。

今すぐ始めてみませんか

最初にテスト ベッドを作成しました（図 1 参照）。仮想マシンとして稼働している Windows 10 エンドポイントから始めました。このエンドポイントを、VLAN 4025 上の、ジュニパーネットワークスの仮想 QFX シリーズ スイッチに接続し、VLAN 3025 上の別の接続に切り替えることができるようにしました。QFX スイッチを SRX シリーズ仮想ファイアウォールに接続し、公衆インターネットに接続しました。QFX スイッチおよび SRX ファイアウォールを、Sky ATP と統合しました。

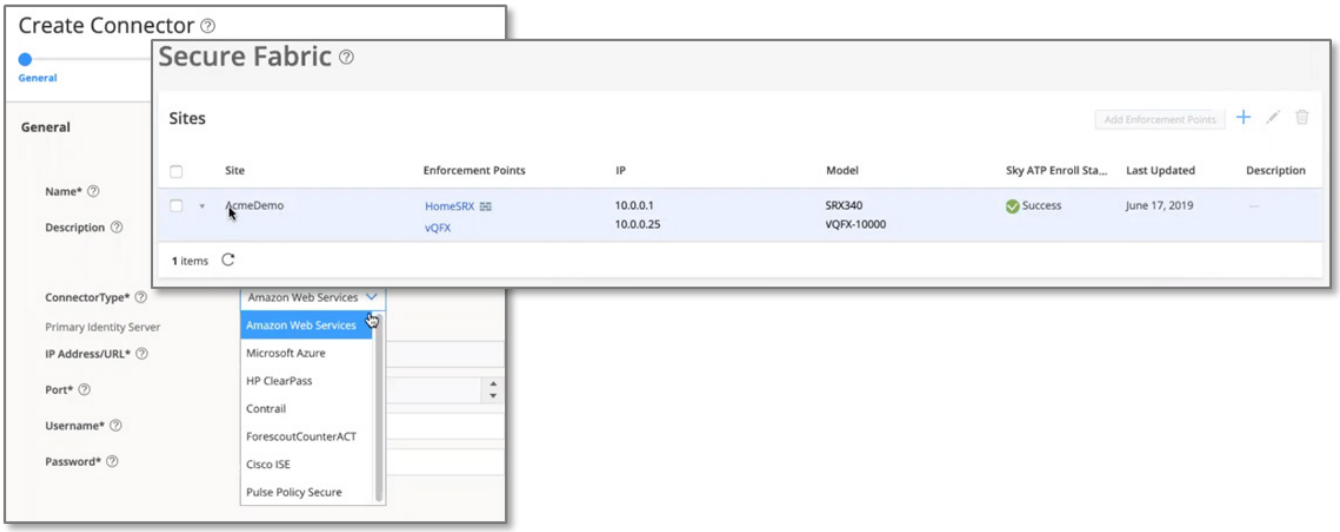
図 1. ESG テスト ベッド



出典：Enterprise Strategy Group

Juniper Networks Junos Space Security Director を、すべてのジュニパー システムを管理する統合コンソールとして使用しました。図 2 のように、ファイアウォールとスイッチを単一のセキュリティ ドメインとして管理できるように、セキュア ファブリックを作成しました。また、Sky ATP でサードパーティーのサービスおよびスイッチ（AWS、Azure、ClearPass、Contrail、Forescout CounterACT、Cisco ISE、Pulse Policy Secure など）に接続できるコネクターを作成する機能についても検証しました。

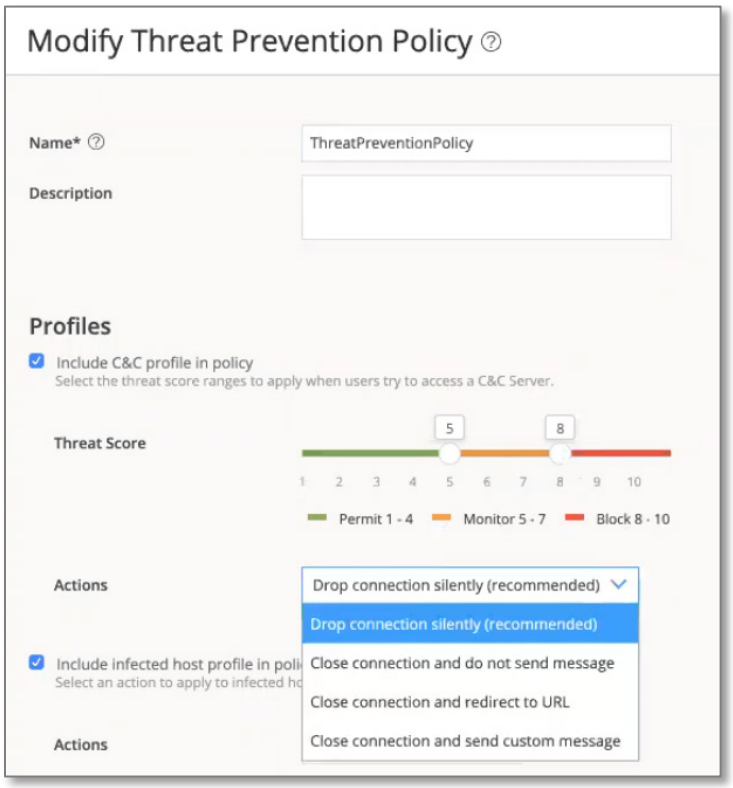
図 2. Sky ATP セキュア ファブリックとコネクター



出典：Enterprise Strategy Group

続いて、Sky ATP 脅威防御ポリシーを検証しました。図 3 のように、Sky ATP を使えば、脅威スコアに基づいて、事前に設定されている処理をセットできます。脅威スコア 8 以上のすべてのオブジェクトについて、[Drop connections silently] （通知なしで接続を切断）を選択しました。

図 3. Sky ATP 脅威防御ポリシー



出典：Enterprise Strategy Group

その重要性とは

サイバーセキュリティは、複雑かつ難易度が高い業務です。経験豊富なスタッフや教育を受けたスタッフの数が不足していることと、異なったベンダーの複数のポイント ツールを組み合わせて使うことによる複雑さ（操作方法とインターフェイスが異なるため）により、脅威を検知および防止することがますます困難になっています。このような複雑さに対応するには、サイバーセキュリティのインフラストラクチャおよびプロセスを簡素化するソリューションが必要になります。

ESG が実施した検証により、ジュニパーネットワークスのソリューションで導入を簡素化できることが証明されました。セキュリティ ファブリックを簡単に作成できたためです。デバイスごとにポリシーを個別に設定する代わりに、異種システムで構成されるグループごとにポリシーを定義して設定できました。セキュリティ ポリシーの定義は、さまざまなリスク レベルごとにしきい値とアクションをスライダーで設定できるので簡単でした。

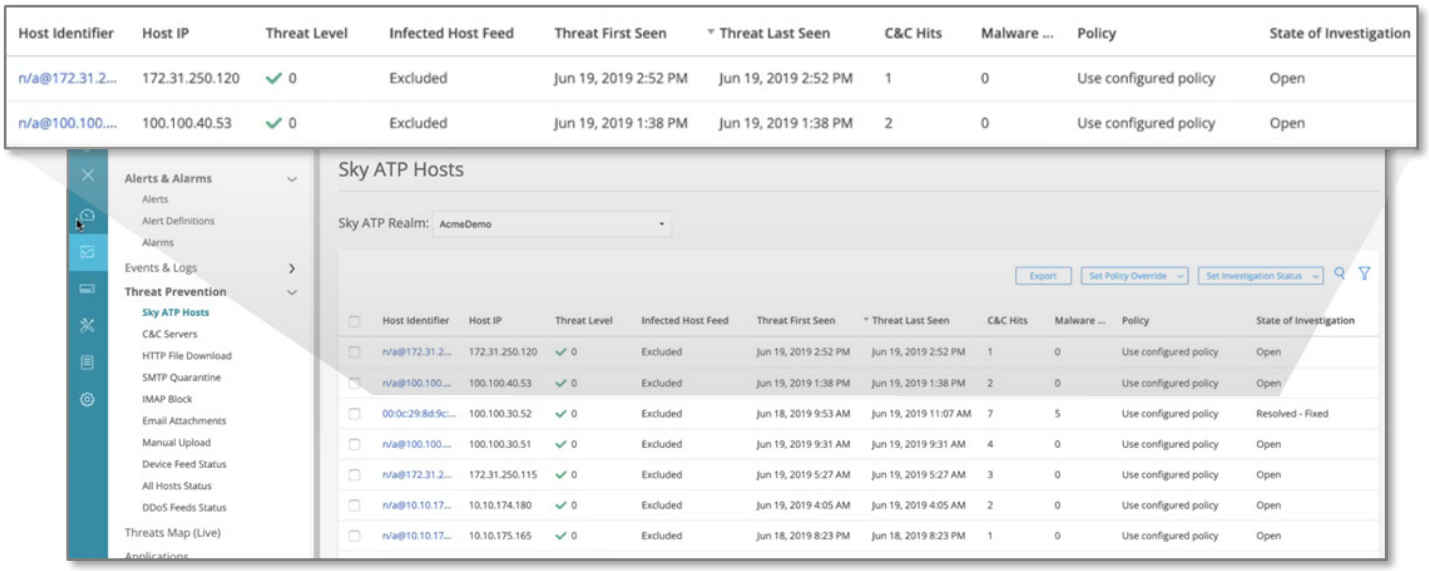
ESG はまた、ジュニパーネットワークスの物理デバイスおよび仮想デバイスで構成される任意のグループごとにポリシーを定義し、設定できることも確認しましました。複雑な環境におけるセキュリティおよびネットワークの管理を簡素化できます。セキュリティ アナリストは、Sky ATP および SRX ファイアウォールを使うことで、ツールの設定と管理に使う時間を節約できるため、アラートへの対応や、脅威および攻撃の調査など、重要な作業に使える時間が増えます。

感染、検知、対応

ESG は、ファイルをダウンロードするときの脅威を防止するためにジュニパーネットワークスが使用しているプロセスに注目しました。エンドポイントにマルウェアをダウンロードすると、ダウンロードしたファイルは SRX ファイアウォールによって Sky ATP に送信され、分析されます。Sky ATP はファイルを分析し、ファイルがマルウェアで、ホストに感染していることが確認されました。Sky ATP が、ネットワークからそのエンドポイントを切断するように、SRX ファイアウォールおよび QFX スイッチに命令しました。これにより、垂直方向のトラフィック（SRX ファイアウォール）および水平方向のトラフィック（QFX スイッチ）を防止します。

まず、環境の現在の状態を確認しました（図 4 を参照）。Sky ATP には、管理対象エンドポイントのリストにあるテスト Windows 10 エンドポイントが含まれており、IP アドレス 100.100.40.53 のエンドポイントを、**感染したホスト フィード**から**除外**しました。Sky ATP はこのリストを使い、侵害されたホストを追跡します。

図 4. Sky ATP ホストの監視



出典：Enterprise Strategy Group

次に、仮想 SRX ファイアウォールおよび仮想 QFX スイッチにログインし、エンドポイントが、内部（水平方向）および外部（垂直方向）で正しく通信できるように設定されていることを確認しました。

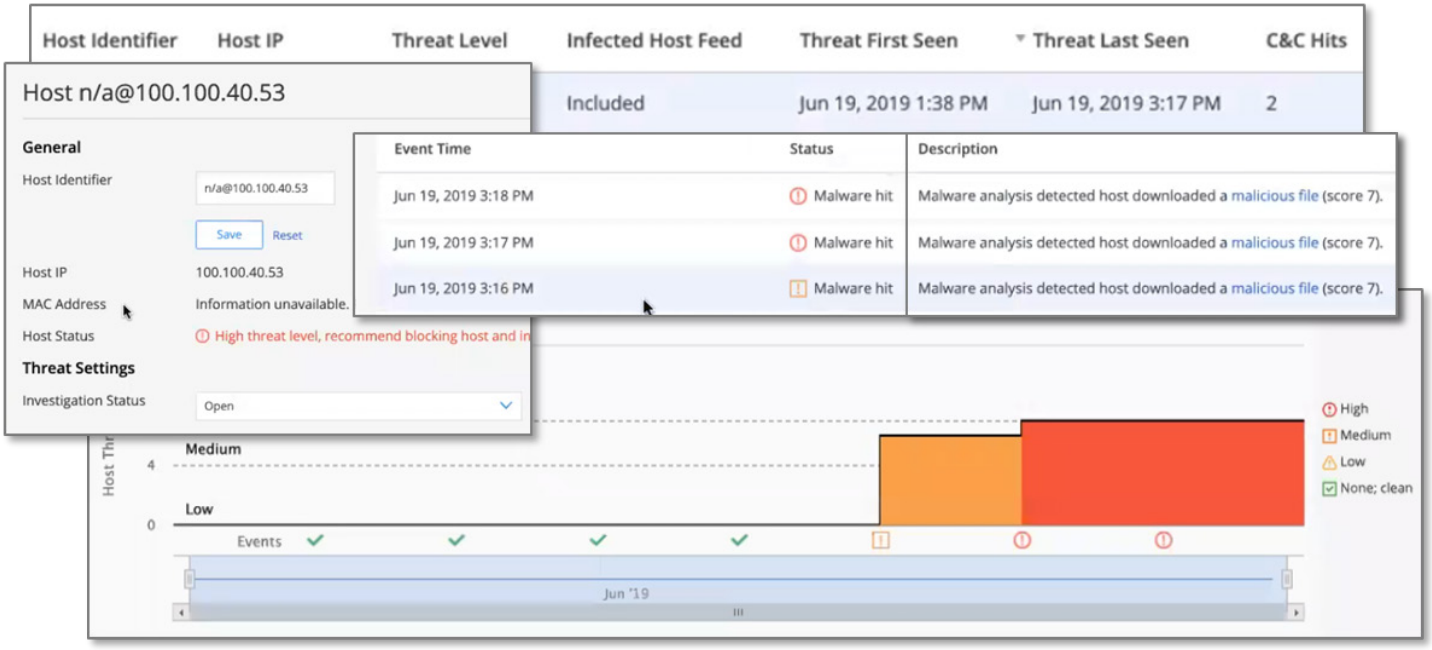
Windows 10 エンドポイントにログインし、Web ブラウザーを使って、マルウェアのサンプルがホストされている Web サイトを開き、マルウェアが含まれているファイル 3 つをダウンロードしました。

ファイルのダウンロードが終了するたびに、SRX ファイアウォールによってファイルのコピーが、分析のために Sky ATP に送信されました。Sky ATP は、各ファイルに一連のチェックを実施しました。チェックとしては、シグネチャーをマルウェア データベースと照合、機会学習を使用した静的解析、サンドボックスを使用した動的分析、行動分析などがあります。Sky ATP はこれらのチェックによって、各ファイルにマルウェアが含まれていることを確認しました。Sky ATP は、自動分析フェーズで収集した情報に基づいて、各ファイルに脅威スコアを割り当て、エンドポイントの脅威スコアを集計しました。

Sky ATP は、集計した脅威スコアおよび事前に設定した脅威防御ポリシー（図 3）に基づき、[Host Status]（ホスト ステータス）を [**High threat level**]（脅威レベル高）に、[Investigation status]（調査ステータス）を [**Open**]（未解決）に設定するとともに、このエンドポイントを感染ホストのリストに追加しました（[**Infected Host Feed**]（感染したホスト フィード）、図 5 ）。

セキュリティ アナリストの通常のワークフローに従い、調査を開始しました。ホスト ID のリンクをクリックすると、ホストに感染したマルウェアのリスト、時間ごとの感染を示すグラフなど、詳細な情報が表示されます。この情報は、調査、根本原因の分析、エンドポイントの修復、問題の解決に役立ちました。

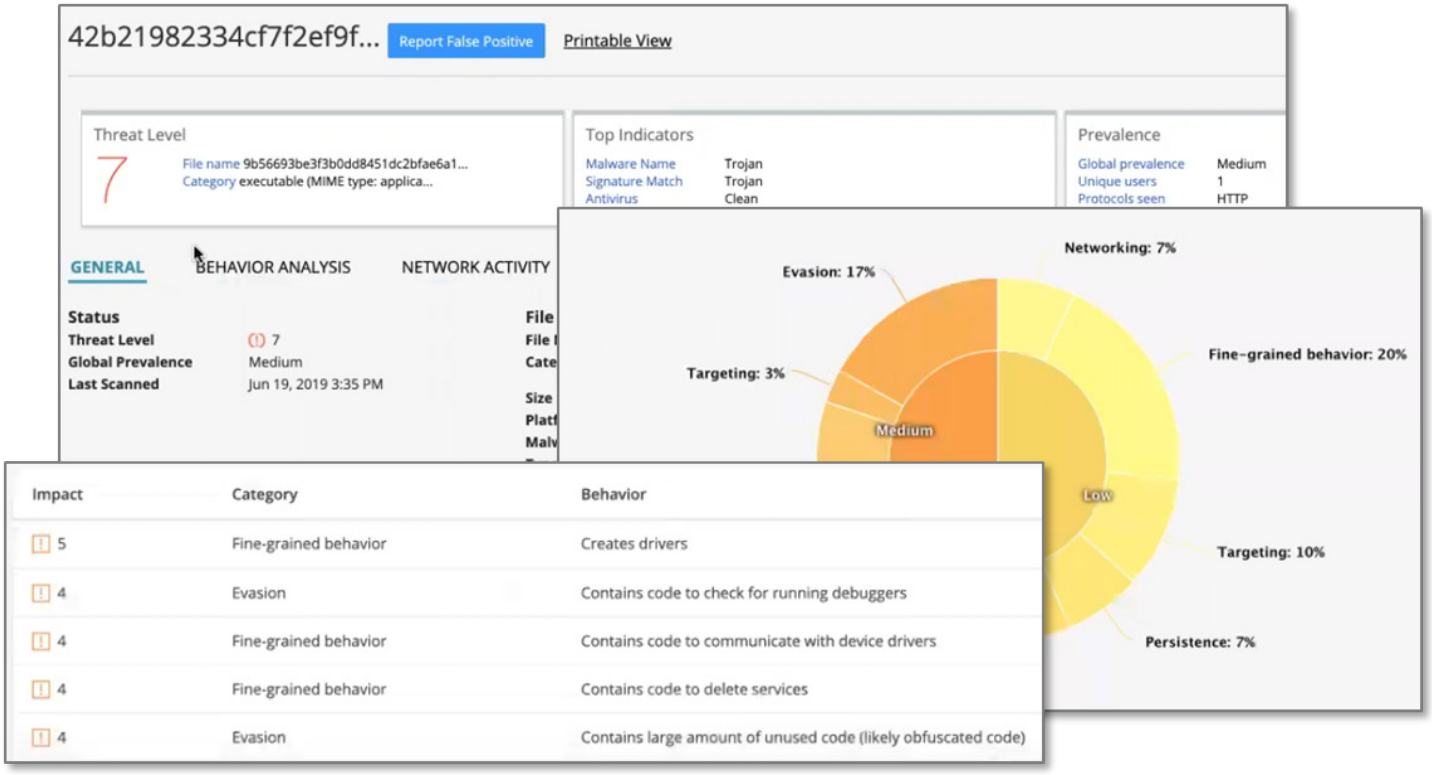
図 5. 感染したホストの詳細



出典：Enterprise Strategy Group

次に、ダウンロードしたマルウェアのリンクをクリックすると、感染に関する詳しい情報が表示されました（図 6）。上部に、概要情報（脅威レベル、上位の指標、脅威の蔓延など）が表示されました。概要データの下のタブ形式の画面に、一般的な情報が表示されました。[Behavior Analysis]（動作分析）タブをクリックすると、リスクに基づいた円グラフ（さまざまな動作をリスクに基づいて分類したもの）が表示されました。このマルウェアは、回避およびターゲット設定の各技術はリスク中、ネットワーク、回避、ターゲット設定、永続の各技術は低リスクで、トロイの木馬に分類されました。表も表示され、識別したそれぞれの動作の詳細を確認できます。別のタブに、このマルウェアのネットワーク アクティビティを示す詳細な表が表示されました。

図 6. マルウェアの詳細



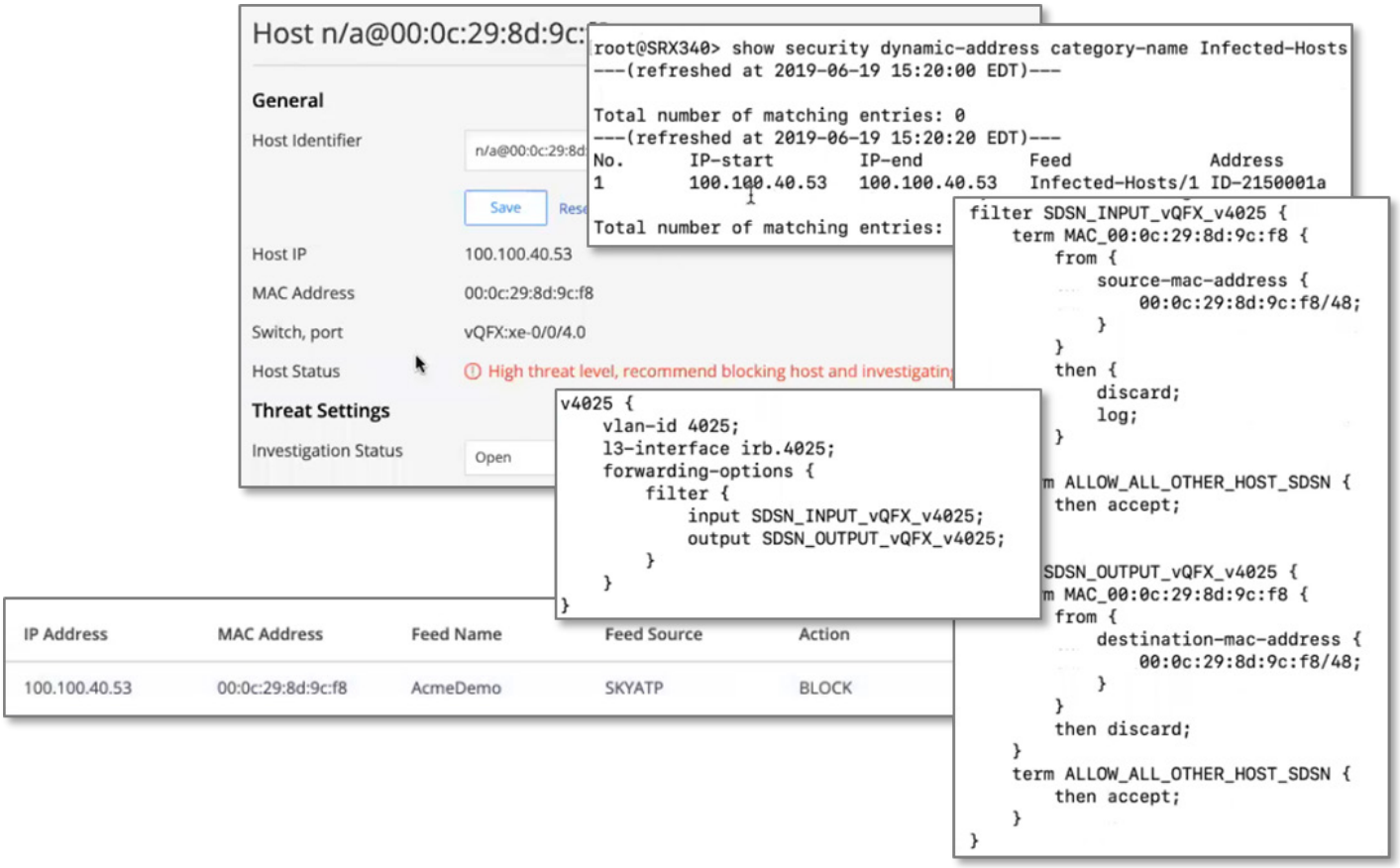
出典：Enterprise Strategy Group

ファイルをダウンロードしてから 5 分以内に、エンドポイントがネットワークから隔離されていることを確認しました。内部 IP アドレスにも外部 IP アドレスにも ping できなかったことで、Sky ATP によって自動的に脅威が修復されたことが分かりました。感染されたホスト フィードにエンドポイントが追加され、SRX ファイアウォールによってエンドポイントによる垂直方向の通信がブロックされました。さらに、エンドポイントの DHCP リースが取り消され、エンドポイントの IP アドレスの割り当てが解除されました。

IP アドレスが無効になったため、Sky ATP により、感染したエンドポイントを MAC アドレスで参照するように、データベースが更新されました（図 7）。

Sky ATP は、ジュニパーネットワークスのすべてのデバイスと通信できるようにする内蔵コネクターを使い、このエンドポイントを隔離するように QFX スイッチに命令を出し、水平方向のトラフィックを防止しました。QFX スイッチによってフィルターが作成され、このエンドポイントの MAC アドレス（00:0c:29:8d:9c:f8）との間でやり取りされるパケットをブロックしました。このフィルターはこのエンドポイントの VLAN（4025）に適用されました。

図 7. 自動修復



出典：Enterprise Strategy Group

エンドポイントがネットワークと通信できなくなったことが分かると、イライラしたユーザーは、ネットワークに問題が発生している可能性があると考え、別のイーサネット ポートを試そうとすることがあります。仮想サーバーを使って仮想ネットワークを切り替えて（エンドポイントは VLAN 4025 から VLAN 3025 に移動）、この状況をシミュレーションしました。切り替えるとすぐに、エンドポイントに新しい IP アドレスが付与されて、社内および社外と両方で通信できるようになりました。

およそ 5 分後、再び通信はブロックされました（社内および社外の両方）。Sky ATP および SRX ファイアウォールは引き続きネットワークを監視し、MAC アドレスでこのエンドポイントを識別しました。エンドポイントはすでに、感染したホスト フィードにあるため、SRX ファイアウォールによって新しい垂直方向のブロックが適用されました。Sky ATP は QFX スイッチに、ステートレス ファイアウォールを更新して VLAN 3025 にこの MAC アドレスのブロックを適用するように命令しました。

その重要性とは

サイバーセキュリティのスキルを持った人材が慢性的に不足しているため、習得に非常に時間のかかる、複雑な製品を複数導入することはできません。結果的に、脅威を検知して防止するために、大変な労力と手作業によるプロセスが必要となります。

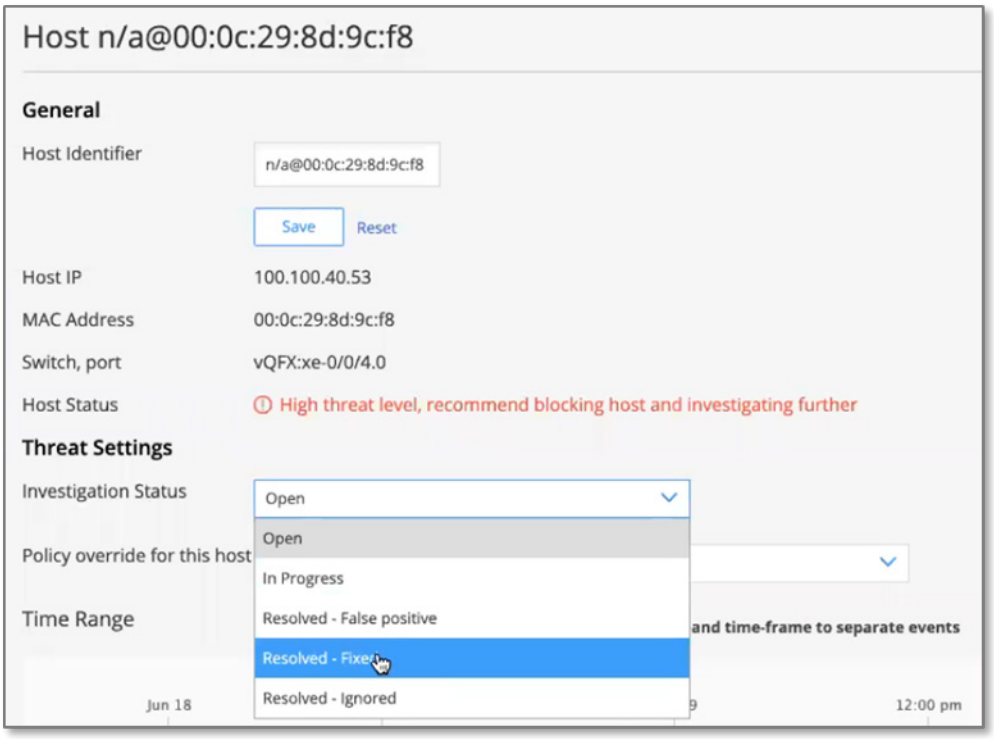
ESG は、ジュニパーネットワークスの SRX シリーズ ファイアウォールによって、分析してマルウェアを検知するために、ダウンロードしたファイルが Sky ATP に自動的に転送されることを確認しました。Sky ATP によってエンドポイントが感染されていることが確認されると、エンドポイントは感染したサイトのリストに追加されました。内蔵の自動化機能およびオーケストレーション機能により、エンドポイントはネットワークから切断され、社内および社外両方の通信ができなくなりました。

Sky ATP および SRX シリーズ ファイアウォールを使うことで、サイバー攻撃をできるだけ早期に検知し、サイバー キル チェーンの進行をストップさせて、重要な資産を保護し、マルウェアの滞在時間を削減できます。

運用管理による解決と修復

ESG は、ホストからマルウェア ファイルすべてを削除することでホストからマルウェアを駆除するという、セキュリティ アナリストが使う典型的なワークフローをシミュレーションしました。続いて Sky ATP インターフェイスを使い、調査のステータスを変更してこの問題を解決済みにしました。ホスト監視セクションで、このホストをクリックしました。プルダウンを使い、[Investigation Status]（調査ステータス）で [**Resolved – Fixed**]（解決済み - 解消）を選択しました。[Investigation Status]（調査ステータス）は図 8 のように、[**Open**]（未解決）、[**In Progress**]（対応中）、[**Resolved – False positive**]（解決済み - 誤検知）、[**Resolved – Fixed**]（解決済み - 解消）、[**Resolve – Ignored**]（解決 - 無視）に設定できます。

図 8. 調査ステータスの更新



出典：Enterprise Strategy Group

調査ステータスを、いずれかの解決済みオプションに設定すると、システムはもう感染されておらず、ネットワークで通信を再開できることを意味します。Sky ATP によって、感染されたホスト フィードからそのシステムが解除され、SRX ファイルウォールおよび QFX スイッチによって、そのホストのファイルウォール エントリーすべてが削除されます。[Investigation Status]（調査ステータス）を [Resolved - Fixed]（解決済み - 解消）に設定してすぐに、エンドポイントが社内および社外両方で通信できることを確認しました。

その重要性とは

サイバー攻撃はますます巧妙化し、その数は増えています。企業がそのような状況に取り組む中、セキュリティ アナリストは継続的に、侵害されたおそれのあるシステムを迅速に調査することが求められています。統合機能、自動化機能、オーケストレーション機能がなければ、繰り返し発生する日常のタスクに、膨大な時間と労力がかかります。

ESG は、セキュリティ アナリストが調査を [Closed]（終了）に設定すると、ジュニパーネットワークスの自動化機能が、該当するファイルウォールおよびスイッチすべてと通信し、ネットワーク通信のブロックを解除して、ホストは社内および社外と通信できるようになることを確認しました。これによりアナリストは、どのスイッチおよびファイルウォールのセットに更新が必要かを確認し、各デバイスにログインし、ルールを更新して新しい設定を保存するという処理を手作業で行う必要がなくなります。ジュニパーネットワークスの自動化機能は、セキュリティ アナリストの負担を軽減するだけでなく、ヒューマンエラーの防止にも役立ちます。

より確かな真実

サイバーセキュリティの状況は、ますます複雑化し、管理が困難になっています。知的財産、顧客情報、財務データが、侵害のリスクにさらされる可能性が増えています。侵害されると、罰金、ブランドおよび企業査定への影響、訴訟など、その影響は甚大です。企業はその間も、急速に増加するセキュリティ インシデントを調査し、対応する必要があります。新しいシステムおよびアプリケーションが増える中、作成されるセキュリティ インシデント シナリオが増えている一方、優れた検知ツールによって生成されるアラートが増えています。サイバーセキュリティのスキルが非常に不足していると回答している企業は、2019 年で 53% で、2018 年の 51% から増加しています [4]。企業は、さらなる効率と効果を求めて、手作業および繰り返しの作業の負担を軽減するために、自動化ツールおよび自動化可能ツールに移行しています。

ジュニパーネットワークスは、サイバーセキュリティを自動化する Sky ATP を構築しました。リアルタイムの情報を使い、アンチマルウェア脅威を防止します。この SaaS ソリューションは、SRX シリーズ次世代ファイルウォールおよび各種ジュニパー製品と統合できます。各種のコネクターを使えば、サードパーティー製品と統合することもできます。Sky ATP は、脅威情報、ウィルス対策シグネチャー、静的分析/動的解析、機械学習といった技術を使い、脅威の検知と修復を自動化します。

SRX シリーズ次世代ファイルウォールは、ダウンロードしたファイル、メールの添付ファイルなど、悪意があると思われるオブジェクトを Sky ATP に転送して分析する処理を自動化します。脅威を検知すると、SRX ファイルウォールは Sky ATP、QFX シリーズ スイッチ、その他のネットワーク デバイスと連携し、感染したシステムをネットワークから切断します。垂直方向のトラフィックを自動的にブロックして、マルウェアがデータを抜き取ってコマンド サーバー/コントロール サーバーに送信することを防止します。また、水平方向のトラフィックを自動的にブロックして、社内への拡散を防止します。

ESG は、Sky ATP によって、導入、設定、管理が簡素化されることを確認しました。セキュア ファブリック（ネットワーク デバイスの集まり）を定義できました。シンプルな操作で多数のシステムを制御できるため、規模が大きく、複雑な環境で有効です。ユーザー インターフェイスは分かりやすく、シンプルなので、セキュリティ ポリシーを短時間かつ効率的に定義できました。

SRX シリーズ ファイアウォールによって、分析してマルウェアを検知するために、不審なオブジェクトが Sky ATP に自動的に転送されることを確認しました。Sky ATP によって分類された感染ホストは、SRX ファイアウォールによってネットワークから自動的に切断され、垂直方向のトラフィックがブロックされました。さらに、Sky ATP および SRX の自動化機能が QFX スイッチと連携し、感染したシステムを切断して、水平方向のトラフィックをブロックしました。この自動化機能により、社内への拡散と、コマンド サーバー/コントロール サーバーとの通信が防止されました。

Sky ATP は、感染、根本原因、是正措置を特定するために必要な正確な情報を出力することで、感染したホストを調査する作業を効率化します。問題を解決し、調査を解決済みにマークすると、Sky ATP および SRX ファイアウォールによってネットワーク接続が自動的に回復されました。セキュリティ アナリストのワークフローにおける、手作業による冗長で複雑なプロセスがまた 1 つ不要になります。

複雑で間違いが起こりやすい、手作業によるワークフローをなくし、自動化機能およびオーケストレーション機能を自社の環境で活用して脅威を検知および防止したいと考えている企業にとって、ジュニパーネットワークスの Sky ATP および SRX シリーズ次世代ファイアウォールは一見の価値があります。

[4] 出典：ESG 調査レポート、『2019 Technology Spending Intentions Survey』、2019 年 2 月

Enterprise Strategy Group 社は、IT 分野における分析、調査、検証、戦略立案を行う企業で、世界中の IT コミュニティに市場情報と実用的な情報を提供しています。

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188