SOLUTION BRIEF

FortiSOAR によるセキュリティオペレーションの強化とインシデント レスポンスの高速化

概要

進化する脅威と新たなデジタルイノベーションによって、ネットワーク攻撃対象領域が拡大し続けています。多くの組織は、ポイントソリューションを追加することで追いつこうとしていますが、セキュリティがこのように複雑化すると、管理対象のベンダーや調査の必要なアラートが過剰となって手作業のプロセスではレスポンスが遅れることになり、増え続けるワークロードの処理に必要な知識を持つ人材が不足するといった多くの問題が発生します。

このような状況では、既存のセキュリティアーキテクチャに SOAR（セキュリティオーケストレーション、自動化、レスポンス）の機能を追加することでこれらの問題を軽減できます。FortiSOAR を利用することによって、セキュリティオペレーションチームは独自に自動化フレームワークを作成して組織のすべてのセキュリティツールを統合できるため、大量のアラートへの対応から解放され、コンテキストの切り替えが少なくなります。その結果、セキュリティオペレーションチームはセキュリティプロセスの適応はもちろん、最適化も可能になります。

集約されていないセキュリティが担当者を疲弊させ、リスクを生み出している

セキュリティアナリストは現在、一日も休むことなく発生する大量のセキュリティアラートに悩まされています。この問題はますます複雑化しており、断片化されるセキュリティインフラストラクチャ（異なるベンダーの膨大な数のポイント製品）が主な原因となっています。平均的な企業では、新たな脅威やリスクに対応するために 47 もの異なるセキュリティソリューションやテクノロジーが導入されています [1]。

問題の大半は膨大な量のアラートによるものですが、異なる多数のソースから発生するアラートを追跡し、調査そして減災しようとすると、SOC（セキュリティオペレーションセンター）の担当者による大量の手作業が必要になります。これらの非効率的なワークフローはインシデントレスポンスのプロセスを遅らせることになり、現状では 1 件のセキュリティ侵害の特定と封じ込めに平均で 279 日を要することがわかっています [2]。

それと同時に、多くの組織でセキュリティオペレーションの担当者が不足する傾向が続いています。現在、全体の 3 分の 2 近い（65%）企業でセキュリティオペレーションの維持に必要なスキルの高い人材の不足が問題になっています [3]。これらのさまざまな要素が複雑に絡み合うと、セキュリティ侵害が見過ごされてしまう可能性がさらに高まります。

2019 年に発生した、継続期間が 200 日未満のセキュリティ侵害を 200 日以上の侵害と比較した場合、平均損失額は 122 万ドルも少なく（前者が 334 万ドル、後者が 456 万ドル）、その差が 37% であることが明らかになりました [4]。

SOAR 市場では、2019 ～ 2024 年に 15.6% の年平均成長率（CAGR）が予測され、18 億ドル近くに達すると見込まれています [5]。

SOAR ソリューションは、セキュリティツールの統合によってコンポーネント同士のやり取りを可能にし、連携型の防御を実現します。このソリューションは、ネットワークの可視性の向上だけでなく、アラート全体の件数を削減し、サイバーセキュリティに関連するより戦略的なアラートに集中できるというメリットもあります [6]。SOAR を使用することで、セキュリティオペレーションチームはワークフローにおいて人による監視を必要としない面倒で反復的な要素を自動化できます。最良の SOAR ソリューションは、脅威の情報を補強してコンテキストを追加するので、アナリストはリスクの深刻度や機密性、あるいはビジネス部門における脅威の重大度に基づいて迅速にケースをトリアージ可能になります [7]。

FortiSOAR によるセキュリティの統合とレスポンスの自動化

FortiSOAR は、多様なセキュリティ製品が発信するアラートの集約と情報の補強を可能にします。明確に定義されたプレイブックの活用によって、オーケストレーションと管理を簡素化します。また、自動レスポンスによって、時間のかかる手作業のワークフローを排除します。

FortiSOAR は、フォーティネット セキュリティ ファブリックの統合アーキテクチャの一部としてセキュリティツールを 1 つに集約します。FortiSOAR は多くの下位レベルのアラート処理を自動化可能で、SOC アナリストは重要度の高いタスクに集中できるようになります。FortiSOAR の採用によって、問題を抱える SOC チームが直ちにメリットを得ることができる 4 つのユースケースを以下に紹介します。

ユースケース 1：SOC ワークベンチの統合

FortiSOAR は、多様なポイントセキュリティソリューションを一元的なオーケストレーションシステムに統合してほぼすべての環境に導入できるようにすることで、SOC の複雑さを軽減します。FortiSOAR には、すぐに活用できる 280 以上のコネクタが提供されています。これらを利用することで、SOC チームは FortiSOAR と他のベンダーの既存のセキュリティソリューションとのシームレスな運用やアラート情報の取り込みが可能になり、組織全体の可視化と制御が一元化されます。この統合によってエコシステムの断片化が解消されると同時にセキュリティオペレーションのプロセスが簡素化され、既存のツールを長期に渡って利用できるようになり、購入したソリューションの ROI（投資収益率）が最大化されます。

ユースケース 2：アラートの自動トリアージ

FortiSOAR は、アラートを 1 ヶ所に集約してコンテキストを追加することで、問題解決に要する時間を短縮します。さらに、「誤検知」によるアラートを削減すると同時に高度なケース管理機能を提供し、調査の定義、ガイダンス、高速化を支援します。FortiSOAR は、アラートの取り込み、深刻度に基づく優先順位付け、タスクの割り当てなどのシンプルな SOC タスクを合理化します。また、トリアージ、情報の補強、調査、減災などの複雑な E2E（Exchange-to-Exchange）タスクを自動化します。これらの高度な統合と自動化の機能によって、大量のアラートの処理の背後に共通する面倒な作業の多くを排除できるため、SOC アナリストは脅威の追跡や活動中の脅威に晒されている攻撃対象領域の縮小に注力できるようになります。

ユースケース 3：インシデント レスポンスの高速化

手作業のワークフローは、アラートの調査から解決に要する時間を遅らせ、人手による見落としやエラーを発生させることにもなります。FortiSOAR は、すべての SOC プロセスの堅牢なオーケストレーションと自動化を促進します。これにより、FortiAnalyzer および FortiSIEM の SIEM（セキュリティ情報 / イベント管理）が提供する自動化機能がさらに強化されます。セキュリティチームは、すべてのタスク、変更、更新の各作業を組織の特定のニーズに合わせて自動化し、効率化を推進することができます。FortiSOAR は、単一のエンティティの自動化だけでなく、SOC 全体の強化と企業組織の包括的なセキュリティの向上を実現します。

さらに、あらゆるレスポンスを自動化する独自の機能を提供します。特定の重大度に達した場合、セキュリティチームはアイデンティティを直ちにオフライン化し、製品内でプレイブックやコネクタを利用することを決断できます。

ユースケース 4：SOC チームの限られたリソースの負荷軽減

手作業によるタスクの排除は、作業時間と人件費の点で SOC チームに対する過剰なプレッシャーを解消し、セキュリティの TCO（総所有コスト）の向上にも貢献します。FortiSOAR は、ワークフローの自動化によってセキュリティオペレーションとプロセスの高度な合理化を実現します。SOC チームは、個々の SOC 要件に合わせてプロトコルや自動化されたセキュリティレスポンスをカスタマイズすることもできます。

初期登録の容易さという点では、ドラッグアンドドロップですぐに活用できる FortiSOAR のプレイブックオプションを活用することで構成が瞬時に完了し、短時間で価値がもたらされます。FortiSOAR は、SOC チームによる組織内の知識の維持にも役立ちます。従業員が退職した場合も、ワークフローに関する実用的インテリジェンスや経験が文書化され、システムに保持されます。

リスク、リソース、結果の管理

SOC チームは、常に攻撃対象領域の拡大とリソースの不足という二重のプレッシャーに直面しており、増大するリスクに追いつけず、その対応に苦労しています。あらゆる機能が統合され、効率化を実現する SOAR ソリューションを利用することで、SOC チームはこれらの問題を解決すると同時に、組織のセキュリティプロセスの強化と最適化を促進することができます。

FortiSOAR は、進化し続ける脅威環境に対するセキュリティオペレーションのレスポンスに役立つ、俊敏でカスタマイズも可能なソリューションを提供します。FortiSOAR の自動化とオーケストレーションの機能は、セキュリティエコシステムの簡素化、大量のアラート対応負荷の軽減、レスポンスに要する時間の短縮を実現し、SOC チームの限られたリソースの負荷軽減に貢献します。

FortiSOAR には、コストの予測が可能でシンプルなユーザーベースのライセンスモデルで利用できるというメリットもあります。拡張性を備えた FortiSOAR のアーキテクチャは、成長する企業に優れた可用性を提供すると同時に、大規模な導入や管理に要求されるリソースに大きな影響を与えることなく、成長する企業や分散型の組織に合わせたソリューションの拡張を可能にします。

[1] 「53% of enterprises have no idea if their security tools are working」、Help Net Security、2019 年 7 月 31 日（英語）：
https://www.helpnetsecurity.com/2019/07/31/are-security-tools-working/

[2] 「2019 Cost of a Data Breach Report」、Ponemon Institute および IBM Security、2019 年（英語）：
https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report

[3] 「Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019」、(ISC)²、2019 年（英語）：
https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx

[4] 「2019 Cost of a Data Breach Report」、Ponemon Institute および IBM Security、2019 年（英語）：
https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

[5] 「Security Orchestration Automation & Response (SOAR) World Markets, Outlook to 2024: The High Number of False Security Alerts Presents Lucrative Market Opportunities」、Research and Markets、2019 年 11 月 15 日（英語）：https://www.globenewswire.com/news-release/2019/11/15/1947898/0/en/Security-Orchestration-Automation-Response-SOAR-World-Markets-Outlook-to-2024-The-High-Number-of-False-Security-Alerts-Presents-Lucrative-Market-Opportunities.html

[6] 「Why SOAR is a Good Bet For Fighting Mega Cyber Security Breaches」、Muhammad Omar Khan 氏、Entrepreneur、2019 年 5 月 23 日（英語）：
https://www.entrepreneur.com/article/334189

[7] Cian Walker、「SOAR: The Second Arm of Security Operations」、Security Intelligence、2019 年 4 月 9 日（英語）：
https://securityintelligence.com/soar-the-second-arm-of-security-operations/

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

Copyright© 2020 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。

SB-FortiSOAR-202005-R1