MITRE ATT&CKを実践するための10の方法

脅威に基づく防御策を
組織全体で構築するためのガイド

splunk>
turn data into doing™

MITRE ATT&CKを**実践する**ための10の方法

MITRE ATT&CKフレームワークが公開されてからすでに数年が経ちますが、今日、組織の間で強力なITセキュリティチームの必要性が認識され、情報セキュリティプログラムの成熟度を高めるための予算確保が以前よりも容易になったおかげで、ようやくその導入が進み始めています。

そして組織の投資対象は防御対策以外にも広がっています。その中で多くの組織が目指すのは、脅威の早期検出能力を高め、インシデント対応の体制を築くとともに、ベンダー依存のアプローチから分析主導型セキュリティのアプローチへと移行することです。

セキュリティプログラムの成熟度を高めるには、脅威グループによって異なるサイバー攻撃の戦術とその具体的な技法を、セキュリティ担当者だけでなく組織全体で理解することが重要です。

> **“デジタル化が進む世界で、セキュリティチームが脅威検出とインシデント対応のための適切な戦略を立てて組織のビジネス、顧客、従業員を守るには、データが欠かせません”**
>
> – Splunk CISSP/CEH/セキュリティエバンジェリスト、Matthias Maier

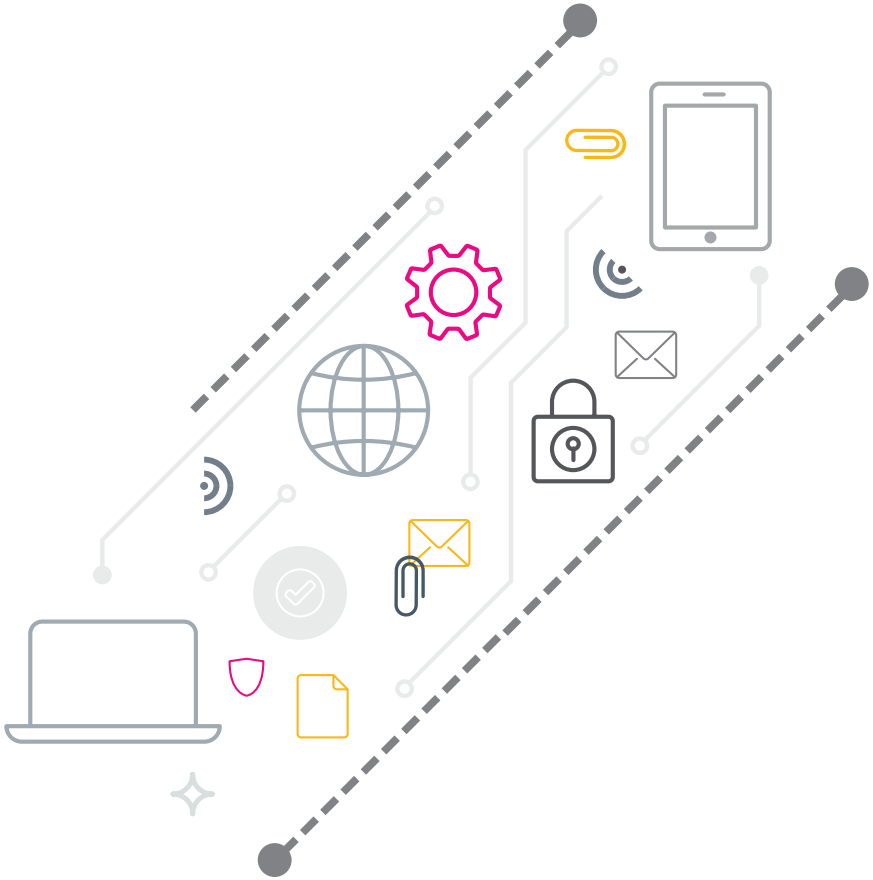
このアプローチは、組織がサイバーリスクにより効果的に対処し、セキュリティインシデントの調査に必要なデータを事前に見極め、従来の防御主体の対策ではカバーできないか、その組織の働き方の中では対応が難しい早期検知ポイントを確立するために役立ちます。

MITRE ATT&CKフレームワークは、セキュリティ担当者にとって有用なだけではありません。セキュリティチームの規模にかかわらず、組織のセキュリティ対策の透明性を高めて、対策が効果を発揮していることを示すなど、さまざまな方法で活用できます。MITRE ATT&CKフレームワークのその他の活用例については、こちらのブログを参照してください。

組織のチームごとの
MITRE ATT&CK
フレームワークの活用法

この電子書籍では、MITRE ATT&CKフレームワークの活用法を組織内の役割ごとにご紹介します。

1. セキュリティ運用責任者：防御、検出、対応、改善戦略を確立する
2. セキュリティコンテンツ開発者/ブルーチーム：対応時の分析時間を短縮する
3. SIEMアーキテクト：カバー範囲を検証する
4. SOCエンジニア：IT運用チームに対してデータの必要性を正当化する
5. ITセキュリティマネージャー：対象となるログやコンポーネントに基づいてリスクに関する意思決定を行い文書化する
6. CISO：資産の重要度に応じた監視体制の構築によって投資を正当化し、ロードマップを作成する
7. SOCアナリスト：リスクベースアラート(RBA)モデルを開発する
8. SIEM管理者：オンボーディング時のデータ品質とカバー範囲を確保する
9. 侵入テスト担当者/レッドチーム：改善の取り組みを文書化して伝える
10. 購買部門/ITリーダー：インシデント対応と監視に関するITセキュリティの戦略的なベースラインを定義し、サードパーティのサプライヤーの透明性を高める



1

セキュリティ運用責任者：
防御、検出、対応に基づく戦略を確立する

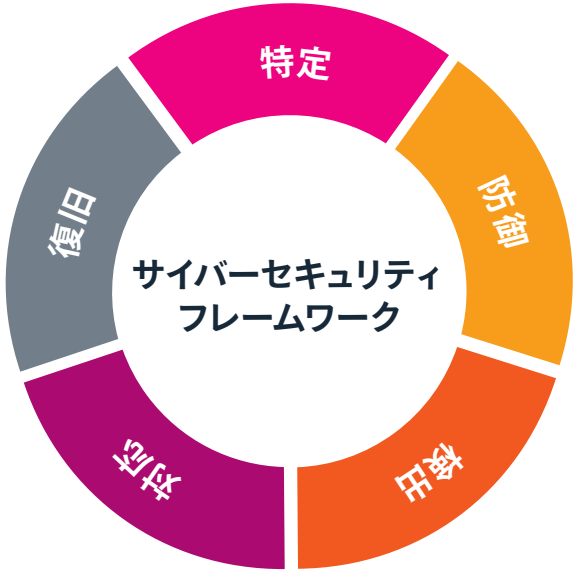
MITRE ATT&CKフレームワークに定義された技法を想定することで、組織は防御にとどまらず、検出、対応、改善プロセスに重点を置いたロードマップを作成できます。

Siemens社のEAGLEデータセンターを担当するセキュリティチームは、このアプローチに従って品質保証と継続的な改善プロセスを構築しています。このチームの最優先事項は、可能な限り脅威を未然に防ぐことです。未然に防げない脅威については、早期に検出してアラートを受信できるようにします。アラートを受信したら、調査を行って対応し、その後、事例を分析して、可能であれば検出方法を調整するか防御策を講じて改善につなげます。

NISTサイバーセキュリティフレームワークでも、リスクの特定と、防御、検出、対応、復旧について、同様のコンセプトが提唱されています。

“毎日対応に追われずに済むように脅威をできるだけ未然に防ぎたいと考えています。未然に防げなかったときは、適切な方法で漏れなく検出して対応することを目指しています。日常業務から得た知識を改善に活かして次回からは防止できるようにしています”

– Siemens社EAGLEデータセンター、Oliver Kollenberg氏



NISTサイバーセキュリティフレームワーク：基本的なサイバーセキュリティ活動を構成するコア機能の大分類

どちらのフレームワークでも、基本的に、セキュリティチームが脅威に基づいて防御する姿勢を持ち、環境の現状を把握するために適切なデータを利用できることが前提となっています。

2

セキュリティコンテンツ開発者/ブルーチーム：対応時の分析時間を短縮する

セキュリティコンテンツ開発者やブルーチームは、MITRE ATT&CKフレームワークを使用することで、新しいサイバー攻撃が登場した際に攻撃で使われる技法をすばやく洗い出し、狙われるデータを特定して、その攻撃戦術のすべての段階で脅威を検出するための分析手法を開発できます。

“攻撃ではなく動作を検出することを検討すべきです。キルチェーンやMITRE ATT&CKフレームワークはよくご存じでしょう。その中で攻撃の侵入段階だけを検出しようとすると、運悪く取りこぼしてしまうことがあるかもしれません。しかし、侵入、調査、C2接続の段階ごとに分析を行えば、それぞれの動作を検出できます。

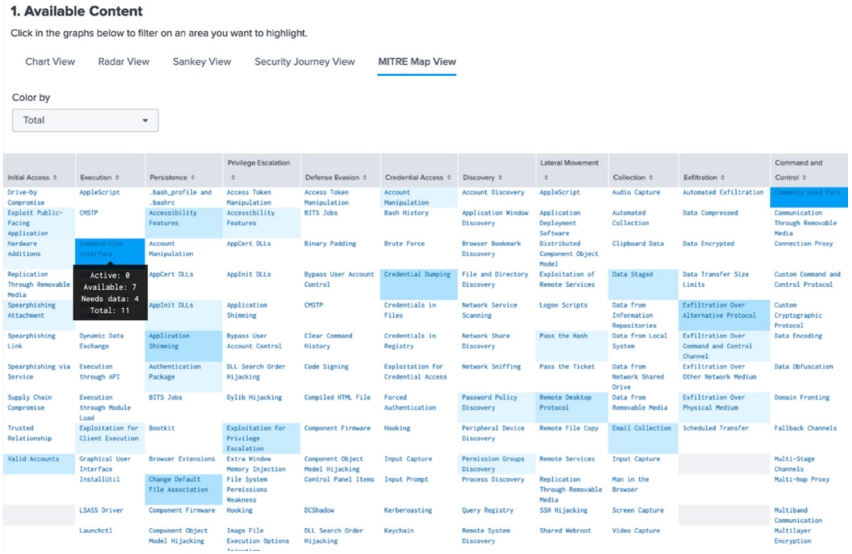
新しい挙動に関する情報を入手したときは、攻撃の新たな検出方法をすばやく開発します。最短2時間で開発したこともあります。もしベンダーに問い合わせて検出機能を製品に組み込むよう依頼するとしたら、3カ月は待たなければならないでしょう”

–イングランド銀行セキュリティ防御センター責任者、Jonathan Pagett氏

3

SIEMアーキテクト：カバー範囲を検証し、適用状況を測定する

SIEMアーキテクトにとって、自身が設計するSIEMが実際にどのくらいの範囲をカバーしているかを見極めるのは容易ではありません。特に、カバー範囲を定義する上で、ログデータを提供しているシステムやシステムコンポーネントだけでなく、ソースデバイスでログに記録されたイベントに適切なアクションが実行されているかどうかも考慮する必要がある場合はなおさらです。さらに、アクティブなSIEMコンテンツで適切な状態を検出できているかどうかも確認する必要があります。これらの点で、MITRE ATT&CKフレームワークは、SIEMのカバー範囲を検証するためのマップとして理想的です。



ATT&CKのすべての戦術と技法をまとめた表。Splunkで利用可能な分析が強調表示されています。アクティブなコンテンツ、アクティブではないが利用可能なコンテンツ、またはデータが必要なコンテンツを強調表示できます。色が濃いほど、多くのコンテンツが存在します。ソース：Splunk Security Essentials App (バージョン2.4)のAnalytics Advisor

4

SOCエンジニア：IT運用チームに対してデータの必要性を正当化する

SOCエンジニアは通常、保護対象のシステムやアプリケーションのオーナーではありません。そのため、SOCチームに必要な可視性を確保することは面倒な作業になりがちです。たとえば、特定のタイプのアクションを監査および保存する必要が生じた場合、IT運用チームに時間を取ってログレベルや設定を確認してもらうために、その必要性を十分に伝えなければなりません。

MITRE ATT&CKフレームワークを使用すれば、特定のアクティビティ (Windowsコンピューターのタスクスケジューラーで新しいタスクが作成された、PowerShellのログが取得されたなど)についてイベントが必要な理由を文書化して伝えることができます。また、MITRE ATT&CKフレームワークを使用して、IT運用チームに、アーキテクチャに基づいて技術的に最適なデータ収集方法を判断してもらうこともできます(SwiftOnSecurity氏によるsysmon設定を使用してエンドポイントのアクティビティをネイティブで取得する、エンドポイント保護ソリューションを使用して収集するなど)。

5

ITセキュリティマネージャー：対象となるログやコンポーネントに基づいてリスクに関する意思決定を行い文書化する

ITセキュリティマネージャーは、MITRE ATT&CKフレームワークを使用して、組織のセキュリティコントロールの対象となる監査やログについてより具体的なガイダンスを示すことができます。これには、SOCエンジニアが組織で許容されるリスクレベルをより正確に理解できるといったメリットがあります。

たとえば、ISO/IEC 27002のコントロールセクションのガイドラインでは、イベントログに含めるべき項目として具体的なシステムアクティビティが列挙されています。

MITRE ATT&CKフレームワークを使用すれば、[初期アクセス]の戦術に含まれる[10%]の技法についてイベント収集からイベント相関付けまでをカバーする、などのようにコントロールを細かく定義できます。

6

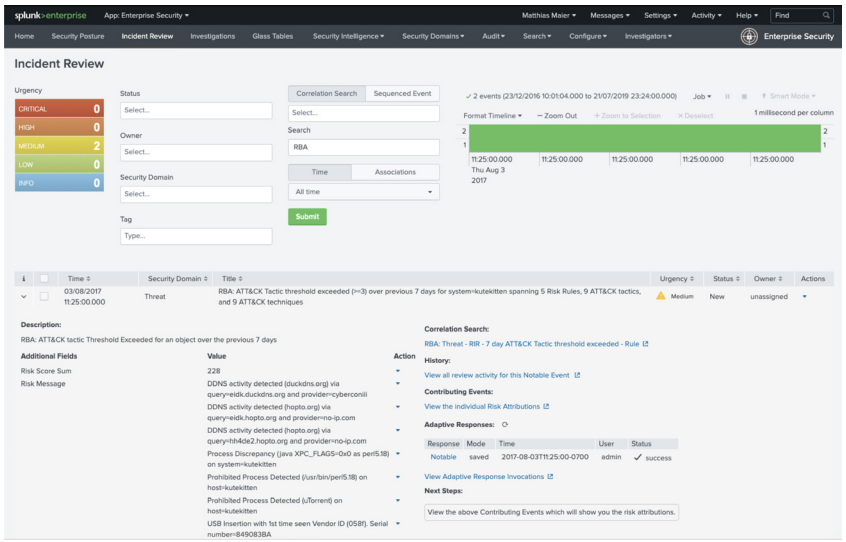
CISO：セキュリティ体制と監視の取り組みを強化し、投資を正当化する

CISOは、ATT&CKフレームワークを使用して、汎用的なポリシーを策定するのではなく、組織のニーズとリスクプロファイルに基づいたセキュリティ体制を構築できます。セキュリティ管理者は、特定のリスク、受けた攻撃、脅威グループ、文書化されたAPT脅威レポートをATT&CKとマッピングすることにより、戦略のギャップを特定して、スタッフの補強、可視性の向上、新しいセキュリティツールの導入などの方法で組織のセキュリティ体制を強化するためのロードマップを作成できます。CISOは、ATT&CKフレームワークを使用することで、抽象化レイヤー、アプリケーションの重要度、ログレベルに基づいてセキュリティを集中的に強化できます。たとえば、一部のMITRE技法によって重要な資産の脆弱性を補えることができるが、その他の技法は自組織にはあまり関係がない場合、前者の技法の実装に必要なSOCのリソースに集中的に投資して、適切なデータをより高い頻度で収集し、重大なセキュリティインシデントの発生時に一元的に利用できるようにすることができます。

7

SOCアナリスト：リスクベースアラート(RBA)モデルを開発する

SIEMコンテンツ開発者がMITRE ATT&CK技法に基づいて検出対象を決定および実装すると、SOCアナリストは、生成されるアラートの量に圧倒されるかもしれません。その場合は、MITRE ATT&CK技法の優先順位を判断できるように、アラートを、資産に基づくリスクスコアを示すシグナルに変換できます。たとえば、検出された技法や挙動のタイプに応じてスコアを高くしたり、関係する資産やユーザーに応じてスコアに加重をかけたりします。これにより、SOCアナリストの抽象化レイヤーでは、アラート数に圧倒されることなく、リスクスコアの高い資産やユーザーの対応に集中し、重大な問題を優先的に調査できます。



アラートタイトル：RBA: ATT&CK Tactic threshold exceeded (>=3) over previous 7 days for system=kutekitten spanning 5 Risk Rules, 9 ATT&CK tactics, and 9 ATT&CK techniques、リスクスコア合計：228、ソース：Splunk Enterprise Security

8

SIEM管理者：オンボーディング時のデータ品質とカバー範囲を確保する

セキュリティ運用チームと組織全体が、脅威の追跡、セキュリティの監視、インシデント調査に必要なデータ、ログ、イベントを特定できれば、SIEM管理者の仕事は楽になります。SIEM管理者は、MITRE ATT&CKフレームワークを使用して、オンボーディングプロセスでデータをチェックし、SOCのニーズを満たしているか、追加のツールが必要かどうかなどを判断できます。また、データの品質とカバー範囲を確保するための追加手順として、脅威のアクティビティや異常をシミュレートすることもできます。

> **“検出メカニズムがエンドツーエンドで機能しているかどうかを検証するには、攻撃をシミュレートし、必要なデータを作成します”**
>
> – Splunkスタッフセキュリティストラテジスト、Dave Herrald

9

侵入テスト担当者/レッドチーム：改善の取り組みを文書化して伝える

侵入テスト担当者やレッドチームの仕事は、情報ネットワークの弱点を見付けることです。その際には、重大な脆弱性をつい優先してしまい、すべての脆弱性について同じように調査することを怠りがちです。しかし、平等に調査すれば、悪用につながるにもかかわらずSOCで見落とされたアクティビティを洗い出すことができます。MITRE ATT&CKフレームワークは、侵入テストを外部組織に依頼する場合でも、社内のSOCが実行する場合でも、コミュニケーションを標準化することができます。全員が同じフレームワークを使用して作業すれば、対象となる戦術や技法をより効果的に調査して、セキュリティシステムの弱点を特定できます。

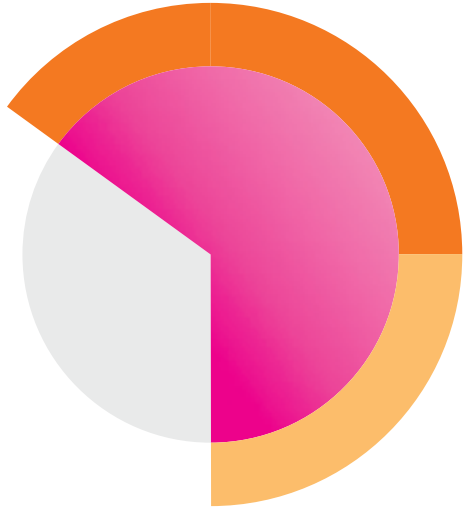
10

購買部門/ITリーダー：インシデント対応と監視に関する戦略的なセキュリティベースラインとニーズを定義する

サードパーティのツールやサービスを購入することは、ITリーダーやビジネスリーダーが講じる標準的な手段の1つです。ベンダーは、自社製品の安全性とコンプライアンスの確保を最重要課題として、顧客や規制機関の監査を定期的に受けてセキュリティ対策を検証します。MITRE ATT&CKフレームワークを使用すれば、要件を詳細に定義して、ISO27001認証やNIST-800-53認証などのITガバナンスフレームワークを上回るセキュリティを実現するための、優れたレイヤーを確立できます。特に、サービスの一部の責任が組織の情報セキュリティチームに託される責任共有モデルでは、サービスプロバイダーが監査証跡を自動的に収集できるようにするとともに、監査証跡に適切なイベントデータを含めることが重要です。プロバイダーのアーキテクチャとは切り離された抽象化レイヤーでその「適切なイベントデータ」を定義すれば、脅威が進化したり、新しいオペレーティングシステムが登場して標的となる新しい機能が登場したりしても、適切に対応できます。

“デジタル化が進む世界で、セキュリティチームが脅威検出とインシデント対応のための適切な戦略を立てて組織のビジネス、顧客、従業員を守るには、データが欠かせません”

– Splunk CISSP/CEH/セキュリティエバンジェリスト、Matthias Maier



始めましょう

適切なデータを使用して適切な答えを導き出していますか?

Splunkと強力なサーチ処理言語(SPL)で何ができるかをぜひお確かめください。
Splunk Security Essentials AppはSplunkbaseからダウンロードできます。
こちらもぜひお試しください。

20-47401-10-Ways-to-Take-Your-MITRE-ATT_CK-From-Plan-to-Action-JA-202012

splunk> turn data into doing™