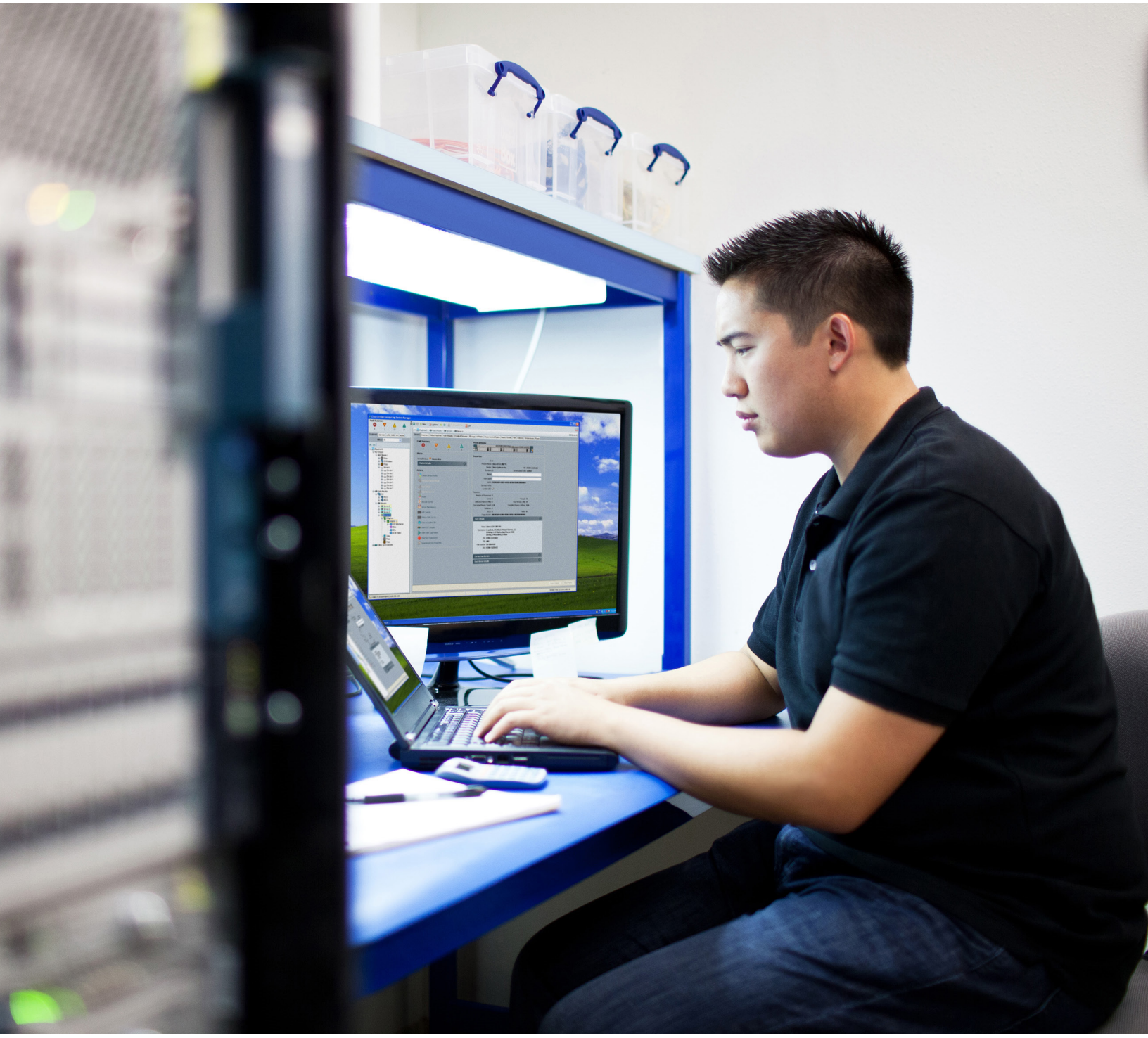
# セキュリティ分析とその先へ

## 効果的なインシデント対応計画の作成



## 概要

このホワイトペーパーでは、IT とセキュリティ チームのメンバー向けに、効果的なインシデント対応計画に必要な要素について説明します。

- 現在のインシデント対応計画が失敗している理由を理解する
- 適切なインシデント対応チームを編成する
- 成功する対応手順を開発する
- 適切なセキュリティ技術を選択する
- NetFlow とセキュリティ分析を使い、インシデント対応とフォレンジックを大幅に改善する

## 攻撃の増加

今日の標的型サイバー攻撃は巧妙化が進んでおり、大規模な小売業者から医療機関、さらには政府機関に至るまで、誰もが安全ではありません。財務データ、企業秘密、機密情報など狙われているものはさまざまですが、絶え間なく進化する脅威や急速に拡大するネットワーク環境は、攻撃者に付け入る隙を多く与えています。

もはや攻撃者がネットワークに侵入するかどうかは問題ではありません。侵入は必ずあるものとして、それがいつなのかが問題なのです。攻撃者は、ゼロデイ攻撃、盗んだアクセス認証情報、ウイルスに感染したモバイル デバイス、無防備なビジネス パートナーなど、さまざまな手段を利用します。

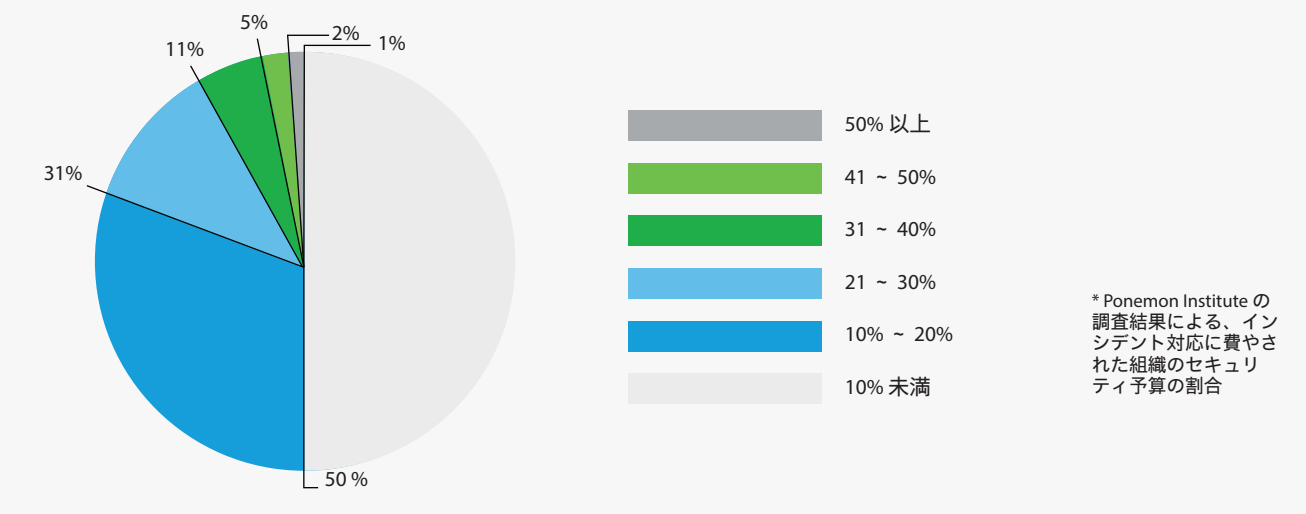
セキュリティの成功は、脅威をネットワークから排除するだけのことではありません。攻撃が発生したら迅速に対応し、阻止することも求められます。

Gartner 社によると、「組織は侵害を早期に検出できずにいて、侵害の 92% 以上が被害組織で検出されていない」状況です。[1]組織を保護する上で、私たちがもっと積極的な役割を果たす必要があることは明らかです。攻撃によって組織のネットワークと評判が大きく損なわれる前に、インフラストラクチャ内で何が起こっているかを常に監視できる、継続的な対応を確立する必要があります。

## インシデント対応の欠点

Ponemon Institute が実施した調査では、侵害の影響に対して事前に施せた緩和策として、ほとんどの組織がインシデント対応機能の改善を挙げています。その一方で、これら回答者の半数が、インシデント対応にかける費用は情報セキュリティ関連の予算全体の 10パーセント未満であったとも答えています(図 1)。[2] また、別の調査によると、大企業の 90パーセントで 1 年を通して重大な IT インシデントが発生しているにもかかわらず、わずか半数あまりしかインシデント処理チームを確保できていません。[3]

図 1. インシデント対応関連の支出




世界有数の有名ブランドや機関に対する攻撃が継続的に増大していることから判断すると、満足できるインシデント対応までの道のりはまだまだ長いことがわかります。ここ最近のハッカーは検出されないままネットワークに潜み続け、その期間は許容レベルを超えて平均 100 ～ 200 日にもなります。[4]

[1] Gartner 社、「Magic Quadrant for Security Information and Event Management」、2013 年 5月
[2] Ponemon Institute、「Cyber Security Incident Response - Are we as prepared as we think?」 2014 年 1 月
[3] Dimensional Research、「Major Incident Management Trends 2016」、2015 年 12 月
[4] シスコ 2015 年中期セキュリティ レポート

「組織は侵害を早期に検出できずにいて、侵害の 92% 以上が被害組織で検出されていない」

– Gartner

## インシデント対応計画の強化

インシデント対応には、セキュリティ インシデントの検出と対応にあたる人員、それらで使用するプロセス、テクノロジーのすべてが含まれます。これらパズルのピースとも言える 1 つ 1つ、つまり人員、プロセス、テクノロジーは効果的な対応計画の確立と実行でどれも同等に重要です。

## 人員

組織のインシデント対応計画に関与する必要があるのは誰でしょうか。そうです全員です。

### CSIRT

企業組織は何よりもまず、トレーニングを受けた専任のセキュリティ プロフェッショナルで構成され、十分な機能を果たせる Computer Security Incident Response Team(CSIRT)を用意する必要があります。規模に関係なく、すべての組織でコンピュータ セキュリティ インシデントに対応する担当者を少なくとも 1 名指名する必要があります。残念ながら、セキュリティのエキスパートだからといって、必ずしもインシデント対応のエキスパートであるわけではありません。インシデント対応担当者は、差し迫った状況の対応で実務経験がある、またはそういった状況を処理できるトレーニングを受けている必要があります。また、さまざまな他の IT およびセキュリティ関連の職務を兼務していない、専任のインシデント対応担当者を設置することも重要です。

インシデント対応チームにはネットワークと資産に関する深い知識が必要です。最近の攻撃者はターゲット ネットワークについて徹底的な調査を行うため、被害組織の IT やセキュリティ チームよりそのネットワークに詳しいことも珍しくありません。適切なテクノロジーを使うことで、インシデント対応担当者はネットワーク上の資産を検出し、最も保護が必要なものを判断できるほか、通常の動作を基準にして攻撃の前触れの可能性がある異常な動作を迅速に特定できます。

### IT チームだけの問題ではない

ところで、適切な技術チームを用意するだけがインシデント対応ではありません。組織のインシデント対応計画では、IT チームだけでなく、法務、経営幹部、人事、広報、その他の部門の主要な関係者も欠かせない役割を果たします。インシデント発生時における各グループの役割について、組織全体で理解しておく必要があります。つまりインシデントが発生する前に役割と責任を明確にし、早い段階から各自を関与させるのです。また、インシデント対応の手順、成果、課題について経営幹部に逐一報告し、これら取り組みに適切な関心と予算が集まり十分な効果が発揮できるようにすることも重要です。

最終的に、組織が連携する全従業員の一人ひとり、さらにはサードパーティが一丸となってインシデント対応チームに協力する環境が理想です。従業員をトレーニングし、ソーシャル エンジニアリングが疑われる場合に何を確認すればよいか理解してもらいます。慎重に見極め、身元調査を行い、自社のネットワーク、さらには社内の機密情報にもアクセスできるサードパーティのセキュリティについて問い合わせる必要があるでしょう。また、内部の脅威についても忘れてはなりません。マネージャには不審な従業員の行動に常に注意して何かあれば人事に報告するように指導し、人事にはこれら報告を必ず IT に伝えるように指導します。

「Stealthwatch により、セキュリティおよびインシデント対応チームは、以前よりも迅速にインシデントを修復できるため、ダウンタイムを短縮し、結果としてネットワークとネットワーク サービスを管理する全体的なコストを削減できます」

– Telenor Norway

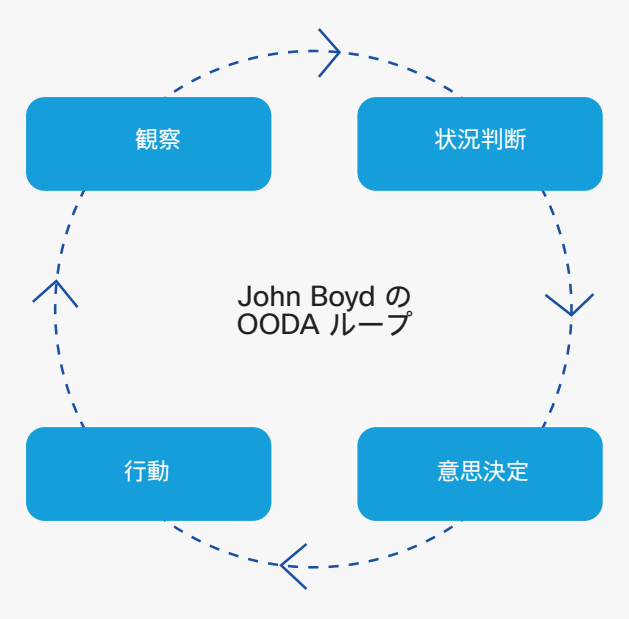
## プロセス

インシデント対応は後付けできません。企業組織には、社内各方面の主要な個人とグループを組み込んで十分に考え抜かれた、しっかりとした対応計画が必要です。

真に効果的なインシデント対応計画とは次の通りです。

1. **明確な役割、責任、承認プロセス**をすべての関係者に用意し、特定のアクションについて実行の可否を決めるルールを定義します。たとえば、インシデント対応チームは、攻撃を封じ込めるために追加承認なしでマシンをオフラインにすることが許可されていますか。コンピュータのワイプや特定サービスへのアクセスのブロックについてはどうですか。これらのアクションは必要に応じて許可されていますか。さらに、侵害が発生した場合の会社の法的、規制上、契約上の義務は何ですか。インシデントが発生する前に、これらの質問の回答を書面にまとめることが重要です。インシデント対応計画では、危機的な状況で適切な意思決定が行われるように、ポリシー間で適切なバランスを取るようにしてください。つまり、得なければならない承認が多すぎてスキルの高い対応担当者の力が十分に発揮できないことがないようにしてください。
2. **トレーニングとアセスメント演習を定期的に行います。** 企業ではインシデントが発生する間隔がかなり空く場合があります。その間も、関連するすべてのスタッフのトレーニングを継続すると共に、インシデント発生時の準備状況を評価する演習を実施することが重要です。さらに、インシデントが発生した場合は、チームの対応力を測定する機会として利用することを忘れないでください。セキュリティ問題の特定までの平均時間(MTTI)、根本原因判明までの平均時間(MTTK)、修正までの平均時間(MTTF)などのメトリックの活用は、対応プロセスを改善するための取り組みや経営幹部への投資回収率の具体的な説明で大いに役立ちます。
3. **インシデント対応計画の取り組みと成果を経営幹部に伝える標準的な手段**を用意し、プロセスに適切な関心と投資が集まるように、また業務を継続するためにはインシデント対応が重要であることが理解されるようにします。
4. **組織のインフラストラクチャと「最も貴重な資産」がある場所をしっかり理解します。** ネットワーク内の一般的なアクティビティの詳しい情報と、外部から得られる信頼性の高い脅威インテリジェンスは、どちらもインシデント対応の重要な要素です。
5. **インシデントを単に取り除くだけでなく、調査も行うフィードバック ループ**を用意します。同様の攻撃を防ぐために、攻撃者と彼らが使う方法に関する重要な詳細情報を調査・収集して取り出す必要があります。軍事戦略家であった John Boyd は、戦闘活動で意思決定を行う際のフレームワークとして OODA ループを開発しました(図 2)。現在、多くの他の分野でも使われており、効果的なインシデント対応に必要な継続プロセスの優れた例として利用できます。

図 2. OODA ループ




## テクノロジー

インシデントが発生する前に、適切な人員とプロセスを用意することは、正しいテクノロジーを導入することと同じくらい重要です。

既知の攻撃への対処では外部から得られる脅威インテリジェンスが重要ですが、インシデント対応としての成果を上げるには、社内ネットワークのアクティビティを深く掘り下げて重要な情報が得られるツールが対応チームに必要です。見えないものを防御することはできないからです。

単にマルウェアを取り除いて感染したコンピュータをオンラインに戻すことがインシデント対応ではありません。詳細な調査を行って、攻撃の範囲、他に影響を受けたマシン、攻撃者が使った戦術のタイプなどを判断する必要があります。このようにすることで、環境からその攻撃が一掃され、同じ攻撃が再度発生することがなくなります。

> 「Stealthwatch は問題解決に必要な時間を数日から数秒に短縮します。StealthWatch のおかげで、潜在的な攻撃や侵害の一歩先を行くことができます」
>
> – Edge Web Hosting

### ネットワーク監査証跡

今日の大規模で複雑なネットワーク内で何が起こっているかを確認する最良の方法は、ネットワーク監査証跡を収集して分析することです。実際、Ponemon が実施した調査の回答者の 80% が、NetFlow やパケット キャプチャなどのソースから入手した監査証跡の分析が、セキュリティ インシデントと侵害の検出に最も効果的なアプローチであると答えました。[5]

ネットワーク アクティビティ ログを使用すると、組織は攻撃の試行をより簡単に認識して阻止できます。特に NetFlow は、専用のプローブを設置せずにネットワーク全体でデータを収集できるため、かなり効果的なテクノロジーです。また、データはそれほどコストをかけずに長期間保管できます。

### NetFlow のパワー

シスコが最初に開発し、現在ではさまざまなネットワーク インフラストラクチャ デバイスに搭載されている NetFlow は(他のタイプのネットワーク テレメトリと共に)、既存のルータ、スイッチ、ファイアウォールから貴重なメタデータを収集し、可視性と状況認識力を高めます。ネットワーク上で発生する各接続について、「宛先」と「送信元」のアドレス、ポート番号、転送されるデータ量、その他の情報を記録します。

NetFlow ではネットワークの資産と動作について、誰が誰と通信しているのか、どのアプリケーションが使われているのかなど、無数の貴重な詳細情報を明らかにできます。

ほとんどの組織は、それぞれの環境内で NetFlow にすでにアクセスできます。つまり、収集と分析を開始するだけでネットワークの新たなレベルの洞察を得ることができます。ただし、すべての NetFlow モニタリング テクノロジーがまったく同じというわけではありません。

現在のネットワークは絶えず進化しており、大量のデータ、つまりビッグデータを作り出し続けています。これらデータにとりあえずアクセスできても、そのデータの意味を理解し、状況認識の向上や意思決定の改善に活用できなければ、インシデント対応チームにとっては残念ながら何の意味もありません。そこで、Cisco® Stealthwatch などの高度なフローベースのモニタリング ソリューションの出番となります。

### Cisco Stealthwatch

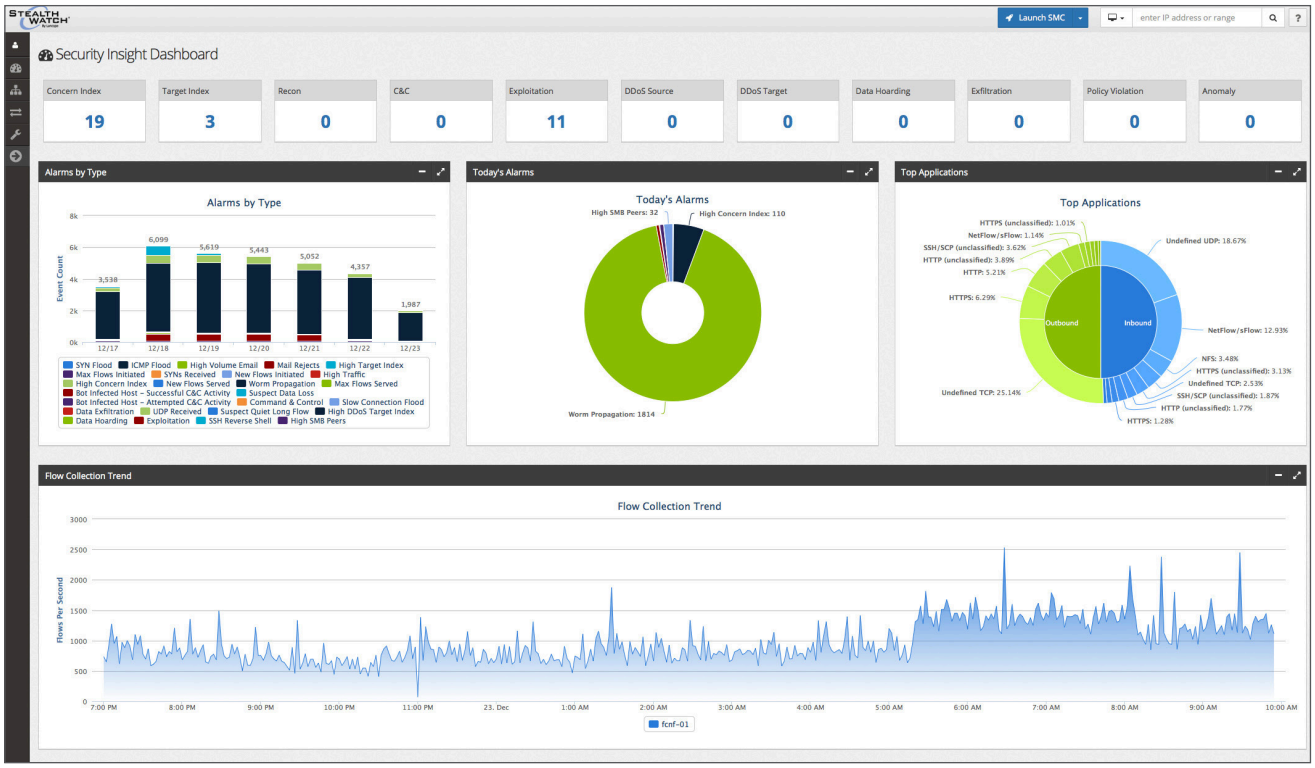
Cisco Stealthwatch は、ネットワークのレーダーとして機能します。莫大な量の NetFlow データを迅速に収集および分析し、セキュリティ チームおよび対応チームに詳細な視覚化情報と実践的なノウハウを提供します。これにより、先に説明したネットワークの詳細な理解とネットワーク アクティビティのベースラインとなる基準が得られます。これは、強力なインシデント対応手順の確立に不可欠です。

さらに、Stealthwatch を他のシスコのセキュリティ テクノロジーと組み合わせることで、既存のインフラストラクチャをコスト効率に優れた方法で活用できます。つまり、組織はそれぞれのネットワークを常時オンのセキュリティ センサーとして使い、よりシームレスに脅威を検出できるのです。また Stealthwatch は、高度な動作分析を通じて、ゼロデイ マルウェア、分散型サービス妨害(DDoS)攻撃、Advanced Persistent Threat(APT)、内部の脅威など、さまざまな攻撃につながる可能性がある疑わしい振る舞いを自動的に検出できます。

これにより、インシデント調査に関連する手動による分析を劇的に減らします。多くの場合、トラブルシューティングにかかる時間が数日、または数ヵ月からわずか数分に短縮されます。直感的なダッシュボードとレポートにより、セキュリティとインシデント対応のプロフェッショナルは、ネットワーク アクティビティの全体像、潜在的問題のリスト、特定のホストのビューなど、必要な情報に数回クリックするだけですばやくアクセスできます(図3)。また、これらの情報は経営幹部などの他の関係者とも簡単に共有できます。

[5] Ponemon Institute、「Cyber Security Incident Response – Are we as prepared as we think?」2014 年 1 月

図 3. Stealthwatch ダッシュボード




Cisco Stealthwatch は、高度なネットワークの可視性とセキュリティ インテリジェンスを提供し、インシデント対応の迅速化を実現します。

たとえば、内部の人間がネットワークの制限されたエリアに繰り返しアクセスしようとしている、異常に大量のデータがネットワークから送信されている、内部ホストが外国の不審な IP アドレスと通信している、といったことがあります。ネットワークの可視性とセキュリティ分析を提供する効果的なツールは、このような動作をピックアップし、詳しく調査するように管理者に警告できます。

「セキュリティ インシデントと侵害の検出に最も効果的なアプローチを尋ねたところ、NetFlow やパケット キャプチャなどのソースから入手した監査証跡の分析を挙げたのは回答者の 80% でした」

– Ponemon Institute

## Stealthwatch の違い

ネットワーク トラフィックをモニタするだけの多くの競合製品と異なり、Stealthwatch は水平方向（末端間）のトラフィックもモニタすることで、ネットワーク内で広がる攻撃を検出し、内部関係者による脅威をあぶり出します。ネットワークの異常な動作を常にモニタし、セキュリティ分析、アラーム、レポート機能を使用して潜在的な問題を管理者に警告することで、Stealthwatch はより迅速で効率的なインシデント対応を可能にします。

通常、NetFlow の処理は、フルパケット キャプチャなどの他の方法よりもリソース消費が少なくて済みます。しかし、グローバル企業の広範なロギングでは、1 秒あたり 100 万フローを超えるレコード ボリュームが生成される場合があります。効果的なソリューションは、ストレージと消費電力を削減するために適切に調整できる必要があります。Stealthwatch では、優れた拡張性と単方向のフロー レコードを重複除外して集約する機能により、きわめて大規模で複雑なエンタープライズ ネットワークにおいてもコスト効率の高いフロー モニタリングとフロー ストレージを実現できます。

Stealthwatch は、リアルタイムの脅威検出の改善に加えて、より迅速で徹底的なフォレンジック調査の実施にも役立ちます。数ヵ月または数年にわたってフローデータを保存できるため、高度なクエリ機能を使って以前の攻撃に関する関連情報をすばやく抽出できます。過去の状況を見返すことは、インシデント対応手順を微調整して脅威に対する防御を改善するために不可欠です。ネットワークがクラウド、Software Defined Networking(SDN)、Internet of Things(IoT)アーキテクチャを通して拡大と進化を続ける中、ネットワークとセキュリティに関する膨大なデータを効率的に収集、分析、解釈する機能はますます重要になります。

> 「Stealthwatch の導入前は、ネットワーク アクティビティ データを手動で分析して相関付けていました。Stealthwatch は、深く掘り下げた詳細なネットワーク情報を単一の使いやすいインターフェイスから自動的に提示するため、セキュリティ、ネットワーク運用、コンプライアンスの取り組みで役立ちます」
>
> – BlueCross BlueShield of Tennessee

### 強化されたセキュリティ コンテキストと統合

調査によると、組織の 69% が自分たちのセキュリティ ツールはリスクを理解するための十分なコンテキストを提供していないと述べています。[6]

Stealthwatch は、独自のテクノロジーと業界のコラボレーションの両方を通じて(シスコの他のテクノロジーとの緊密な統合を含む)、セキュリティ コンテキストのレイヤを強化し、インシデント対応とフォレンジックの実施をさらに推し進めて改善します。

付加価値のあるインテリジェンス レイヤの例を以下に示します。

- ユーザとデバイスの認識
- クラウドの可視性
- アプリケーションの認識
- 脅威フィード データ
- エンドポイント セキュリティの統合
- プロキシの可視性
- パケット キャプチャ

単一のコンソールからすべての情報にアクセスできるため、脅威の調査と修復が劇的に合理化されます。実際、Enterprise Strategy Group によると、インシデントの検出と対応プロセスがうまくいかないのはセキュリティ テクノロジーが統合されていないことが原因であると組織の 80% が考えています。[7] 残念ながら、ソリューションが分断されていると、脅威の緩和に時間がかかるほか、攻撃者が悪用しやすいセキュリティ ギャップが放置されます。コンテキストと緊密な統合のレイヤが強化されたことで、現在組織が直面するあらゆる種類の脅威に対して自動化された、流動的で効果的な対応が可能になります。

## まとめ

残念ですが、エンタープライズ ネットワークからハッカーを完全に排除できる技術は今のところありません。しかし、組織が人員、プロセス、テクノロジーを適切に組み合わせてそれぞれの環境を定期的にモニタすれば、セキュリティ チームは攻撃を受けている場所を正確に特定し、進行中であってもその攻撃を阻止できるため、データ漏洩に伴う悲惨な結果や大きな損害を避けることができます。

[6] Ponemon Institute、「Privileged User Abuse & The Insider Threat」、2014 年 5 月
[7] Enterprise Strategy Group、「Tackling Attack Detection and Incident Response」、2015 年 4 月

## 関連情報

Stealthwatch はシスコの広範なセキュリティ ポートフォリオと組み合わせることで、エッジからネットワーク、データセンター、エンドポイント、モバイル デバイス、クラウド全体へのアクセスで包括的な保護を提供するほか、インシデント対応を合理化できます。

シスコの CSIRT が Stealthwath を使ってどのように悪意のあるトラフィックを検出・分析してインシデント対応とフォレンジックを改善しているかについては、ここをクリックしてご覧ください。

**詳細はこちらをご覧ください。デモをリクエストしてください。**

stealthwatch@cisco.com

「組織の 80% が、インシデントの検出/応答プロセスがうまくいっていないのはセキュリティ テクノロジーが統合されていないことが原因であると考えています」

– Enterprise Strategy Group



C11-737531-00 07/16