SAMPAN security inc

STAY PROTECTED FROM LIVE PC INTRUSION

エンドポイント プロテクター

FireTower

セキュリティー ソリューション

オーバービュー

SAMPAN security inc

コンテンツ

1. イントロダクション

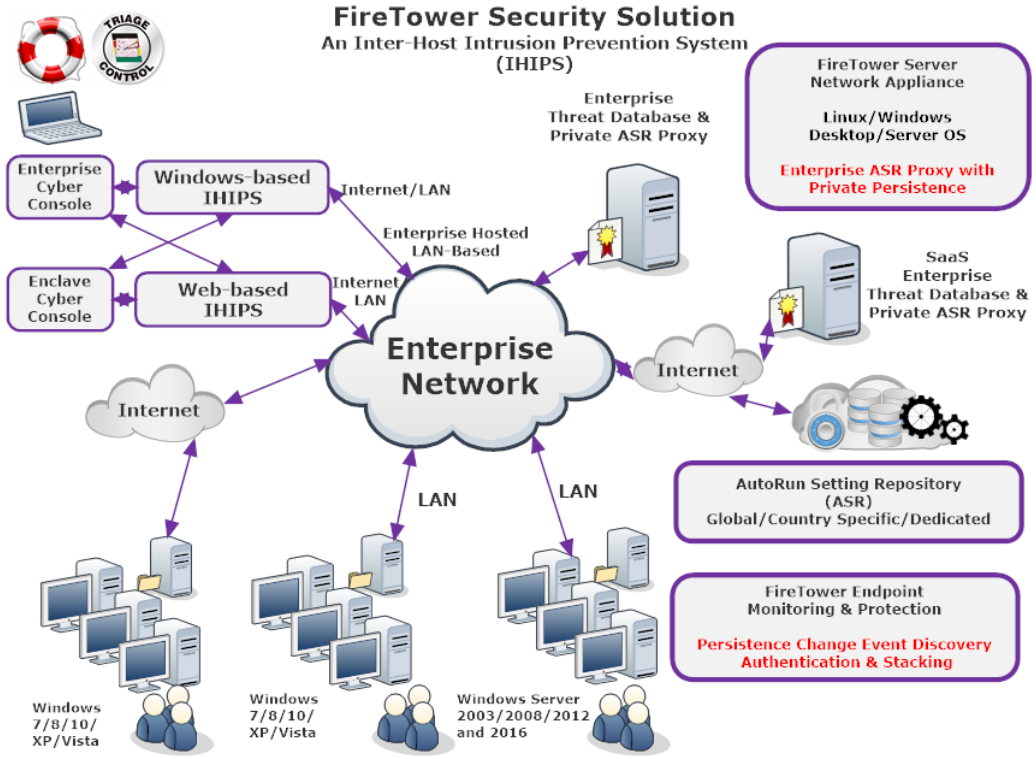
イントロダクション

FireTower は、エンドポイント上のセキュリティーを守るための EDR ツールです。<EDR ツール：エンドポイント（Endpoint）、検出（Detection）対応（Response）＞ FireTower は、ゼロデイ アタックマルウェアに対するオートマティックでリアルタイムな保護を提供し、インシデント対応・調査のためのフォレンジック分析データを生成するための エンドポイント プロテクターです。

FireTower は、エンドポイントコンピュータ内で発生する重要な変更イベントを検出し、その安全性を認証します。 また認証後各エンドポイントのセキュリティーデータを FireTower サーバー サービスにより集中管理する、エンタープライズ脅威データベースへ合成します。FireTower は、この脅威データベースを通じて、組み込まれている分析機能を備えたインタラクティブな脅威分析インターフェイスを使用し、侵害の兆候を探り、包括的なエンドポイントの可視化を実現し、悪質なソフトウエアの活動の検出と封じ込めを強化する機能を提供します。

FireTower セキュリティソリューションは、セキュリティ オペレーション センターとして継続的な監視を実施し、脅威と進行中の攻撃のインジケータを捜すためのライブ フォレンジック調査を提供するための強力なセキュリティー システムです。

1. FireTower のアークティクチャーとそのコンポーネント



2. FireTower セキュリティー ソリューションコンポーネント

FireTower セキュリティソリューションは、以下のサブシステムで構成されています。

1. **FireTower ASR データベース** (Autorun Setting Repository)
2. **FireTower サーバー**
3. **FireTower クライアント**
4. **FireTower サイバーコンソール**
    a. Windows 版 サイバーコンソール
    b. ブラウザ版 サイバーコンソール

3. FireTower ASR (Autorun Setting Repository)

ASR データベースは、システム内に仕掛けられた、何らかのトグルによって、自動的に実行可能なメカニズムの認証に使用されます。 ASR は、Autorun エントリの安全を評価するため、内容を検出スキームに提供します。検査データは既知で安全、既知で危険、または未知で（ゼロデイ）等の結果を導き出します。

ASR によって、まず最初に、サポート担当者やデジタルフォレンジックの調査に関して、システム内に仕掛けられた大部分である安全な自動実行エントリをすばやく調査対象から外す（無視）ことができます。そしてすぐに悪意のある、または疑わしい、おそらく悪意のあるエントリであるだろう等、わずかしかなく、発見が難しい部分に瞬時に焦点を当てることができます。

ASR は Sampan Security、Inc.のセキュリティ脅威調査チームによって管理されています。ASR 内のすべての脅威（パーシスタンスメカニズム）に関するセキュリティーデータは FIreTower サーバー内に存在し、各企業用に個別に修正・調整することができます。これは FireTower サーバー機能である、個別企業のための固有の FireTower ASR プロキシサービスによって実行され、内容を変更・追加でき、認証処理が実行されます。 パブリック ASR の更新処理は自動的かつ定期的にインポートおよび同期されます。 個別に作成されたプライベートな個別 ASR はファイアータワー サーバー内に保管されており外部に公開されることはありません。

FireTower サーバー

FireTower サーバーは、すべてのエンドポイントコンピュータから収集されたセキュリティーデータを脅威データベースへ保存します。継続的な脅威監視とリアルタイム なインシデント対応型の調査機能を備え、エンタープライズセキュリティの状況を確認・認識のためのインタラクティブな脅威分析インターフェイスを提供します。 これはサイバーコンソール（Cyber Console）というコンポーネントで、WinCyCon.exe（x86 および x64）と呼ばれる Windows ベースのものと、ブラウザーインターフェースから使用できる物の 2 種類を用意しています。

FireTower サーバーは個別に構築するオンプレミスタイプと、クラウドサービスを使用して社外のサーバー内に構築する 2 通りをご用意しています。

4. FireTower クライアント

FireTower クライアントソフトウェアは、保護対象であるすべてのエンドポイントコンピュータにインストールします。 FireTower クライアントソフトウェアは、各エンドポイントコンピュータ上にインストールされている現在のアプリケーションと外部から入ってくるアプリケーションの動作を監視することにより、悪意のあるソフトウェアを識別します。 これにより、悪意のあるソフトウエアが事前にデータベースに登録されていなくても FireTower はマルウェアを検出して停止させます。

5. FireTower サイバーコンソール for Windows

サイバーコンソールは、脅威侵入の兆候を探り、包括的なエンドポイントの可視化を提供し、悪意のある活動の検出と封じ込めを強化するために、組み込まれた分析機能を備えた対話型の脅威探索インターフェースです。 FireTower の脅威データベースは、ログイン/パスワードを使用して CyCon からアクセスします。 CyCon は FireTower で保護されたすべてのクライアントコンピュータの情報にアクセスできます。 CyCon は、必須のクライアント PC 情報、自動実行（オートラン）エントリー情報、アラート情報、その他の重要なシステム情報をレポートします。 CyCon は、管理者が疑わしい自動実行エントリの検疫・隔離や削除、ホスト間のフォレンジック分析などの高度な機能を実行することも併せてサポートします。

サイバーコンソール for Windows は、任意の Windows PC にプログラムを単純にコピーして実行することができます。 これは対象の FireTower Windows サーバー エンタープライズネットワークと同一のネットワーク内にある Windows クライアント、またはエンタープライズネットワークと接続可能なリモートサイトの Windows PC が含まれます。（この場合、FireTower サーバーはルーティング可能な IP アドレスまたは DNS 経由によりアクセスされます。）

6. FireTower セキュリティー テクノロジー

エンドポイント プロテクション プラットフォーム
EPP (Endpoint Protection Platform)

ガートナーのレポートによると、エンドポイント保護プラットフォームは、他の多くのエンドポイントセキュリティ機能とともにマルウェア対策スキャンを提供するための企業ツールの基盤となっています。 EPP は、エンドポイントのマルウェアスキャンを実行し、シグネチャベースの検出方法（アンチウイルス（AV）ソフトウェアとも呼ばれます）に大きく依存する予防ツールです。 しかし現在の、EPP エンドポイントセキュリティソリューションは、ゼロデイ攻撃に対するいかなるレベルの保護をも提供できません。

エンドポイント ペリメタ（Perimeter）ディフェンスと防御 ：

従来の AV セキュリティソリューションは、保護のために PC 上に架空の境界線を設定していました。 その主な機能は、マルウェアがこの「境界」を通過して侵入するのをスキャンして、著名（シグネチャ）ベースの検出方法を使用して実行を防止します。 保護されていない施設の入口にいる警備員のように、ブラックリストに登録されている人は「歓迎されていないゲスト」として侵入を完璧に防御します。しかし知られていない署名のマルウェアに対しては（ゼロデイアタック）がこの境界線内に侵入しようとした場合、それを防御することはできません。 悪質なペイロードは、登録がないので（悪意のあるゲストリストにはない）悪意のあるペイロードは正常に実行されてしまいます。

エンタープライズセキュリティ保護は、著名（シグネチャ）ベースの検出方法と防止を備えた EPP ソリューションによって支配されています。 ゼロデイ攻撃が絶え間なく増加する中で、EPP ソリューションは、ホワイトリスト、スキャン、サンドボックスなどの技術によって強化されました。 しかし、これらの解決法は、依然として境界線上（入口/出口対策）の検出および防止に基づいています。 また、ゼロデイマルウェアが一度境界内に侵入すると、エンドポイントコンピュータの可視化や分析機能ような有効な機能は提供されません。

エンドポイント内の検出と対応・対策
EDR (Endpoint Detection and Response)：

最新のセキュリティアーキテクチャ には、大企業、中小企業、およびパーソナルコンピュータデバイスに対する脅威が増大するという課題に対応するため、ゼロデイの脅威に対処する EDR（Endpoint Detection and Response）ツールが新たに追加されました。 EDR は、EPP のような他のエンドポイントセキュリティソリューションの代替物ではありませんが、包括的なサイバー防衛システムにとって不可欠なコンポーネントであることが認識されています。

EDR ツールは、エンドポイントコンピュータ（PC およびサーバー）上のアクティビティを積極的に継続的に監視および記録します。 EPP ソリューションによって提供される境界防御に常に侵入しているゼロデイアタックに対処するため、企業は EDR ツールを使用して包括的なエンドポイントの可視化を実現し、悪意のあるアクティビティを検出し、セキュリティインシデント対応を簡素化できます。

EDR ツールは、AV ソフトウェアの予防措置に、さらにエンドポイントコンピュータでより現実的でリアルな検出とインシデント対応の対処・対策を追加します。 EDR ツールは次のタスクを実行する必要があります。
1. エンドポイントデータの収集
2. データの一元化
3. データの後処理、データマイニング

これらの EDR 要件は、収集し、集中化し、分析する必要のあるエンドポイント内の様々な種類のデータを包括的に収集・分析する必要があります。 FireTower セキュリティソリューションは、これらのタスクを効率的にリアルタイムに実行します。

EDR ツールに必要なエンドポイントデータは、様々な内容を想定する必要があります。例えば、ネットーワーク内に複数のコンピュータが感染している典型的で流行的な感染/インシデントや、各コンピュータに複数の悪意ある脅威が存在し、それぞれ複数の攻撃ステージにいること等、様々なケースを考慮する必要があります

ガートナーの報告によると、セキュリティソリューションには、悪意のある意図を示すパターンや行動の追跡を継続的に監視する必要があることが示唆されています。 しかし、企業では、継続的な監視は、CPU消費やインシデント対応の調査を妨げないように、測定された方法でのみ実行できます。 FireTowerセキュリティソリューションは、永続性なメカニズムを使用してゼロデイアタックを検出できるような測定手法を採用しています。

ゼロデイアタック 感染・被害の拡大
Zero-day Attacks: Exploits and Payloads

EDR は既知のマルウェア侵入を検出することもできますが、FireTower ソリューションはゼロデイ攻撃の検出と対応を中心機能としています。

サイバー攻撃の事件は、通常、ソフトウェア脆弱性を利用し、ターゲットシステムに対して悪意のあるソフトウェア（ペイロード）を配信・実行する構成となっています。ソフトウェア（悪用）で開始されます。 ソフトウェアベンダーがこの脆弱性を修正するためのパッチを作成する機会やセキュリティベンダーがこの攻撃のための署名を作成する機会を得る前に、ソフトウェアの脆弱性が悪用され、攻撃者がペイロードをリリースすると、その時点でゼロデイ攻撃が発生した事となります。 ゼロデイ攻撃はペリメタ ディフェンスに検出の機会を提供しない

ため、EDR ツールは、ペリメタ ディフェンスを超えて入ってくるマルウェアを検出し攻撃の実行を防御する必要があります。

サイバーアタックのライフサイクルと特性:

以下はAPT（Advanced Persistent Threat）攻撃と標的攻撃のライフサイクルを段階的に示した次のものです。

マルウエア キル チェーン（The Kill Chain）

ほとんどのサイバー侵害事件は、複数の攻撃段階（感染、偵察移動、データ奪取、データ持出等）から構成され、異なるコンピュータでは、各攻撃段階は複数の俳優によって（ペイロード）様々に構成されます。 著名（シグネチャー）を持つ既知のマルウェアとは異なり、ゼロデイ攻撃の著名は存在しないため、EDRツールは侵入を検出して格納し、修復段階ですべてのペイロードを識別する必要があります。

EDRツールのゴール:

EDRツールの設計目標は、悪意のあるペイロードの実行を自動検出して隔離し、必要に応じて自動修復を行いながら、使用できるコンピューティングリソースの要件・条件を低減でき、ITサポートスタッフに対する様々な種類のセキュリティーに関連するトレーニングを最小限に抑えられるようできる限り処理を自動化できることです。

ゼロデイ攻撃の検出と対応のために抜け落ちている パーシステンス メカニズム：

FireTower セキュリティー ソリューションは、Windows PC の自動実行セッティング等のパーシステンス メカニズムを分析して、未知の（ゼロデイ）、おそらく悪意のあるソフトウェアの挿入を識別することで、ゼロデイ攻撃から防御する独自の方法を提供します。この方法論は、クラウド内のアプリケーションおよびデータベースコンポーネントと連携して動作するエンドポイント PC 上で実行されるソフトウェアに依存しています。パーシステンス メカニズムは、Windows のクラッシュ、不安定性、パフォーマンスの低下、不要なプログラムの調査、およびウイルスのインシデントの診断とそれらの解決のために、サポート担当者によって長く使用されてきました。 パーシスタンスメカニズムベースの EDR ツールは、既存の企業の Windows IT 担当者が最小限の追加トレーニングで操作することができます。

パーシステンス 、メカニズム:

近年のオペレーティングシステムでは、システムをリブートした後、または指定されたスケジュールに基づいてアプリケーションを自動的に起動できるように、またはそれ以外によりパーシステンス メカニズムが使用されています。 たとえば、Microsoft Windows オペレーティングシステムでは、これを実行するために「自動実行」(Autorun) を使用します。 一般的な自動実行設定は、Windows コンピュータシステムごとに 300～600 個程度のエントリで構成されます。自動実行の設定はパーシステンス メカニズムの 1 つに過ぎず、FireTower クライアントソフトウェアはゼロデイ攻撃の検出に関連する他のパーシステンス メカニズムも併せて監視します。マルウェアとゼロデイ攻撃は、一般に、オペレーティングシステムに組み込まれたパーシステンス メカニズムを悪用して、PC の境界線（ペリメータ）ディフェンスの隙間を通りぬけて侵入した後に PC に悪意のあるパーシステンス メカニズムを作成します。

マルウエア は事実上、常に継続的に実行されます。:

パーシステンス メカニズムは、マルウェアキルチェーンの重要で典型的なマーカーイベントであり、先進的で継続的な脅威を探し出すために、指標として使用されています。 事後分析では、最近のゼロデイサイバーセキュリティ攻撃の大部分が注入または変更されたパーシステンス メカニズムを使用していること明らかにされているため、マルウェアは事実上継続的に実行されています。パーシステンス メカニズムの検出スキームは、用意された複数段階のシナリオの中の 1 つの段階であり、殆どのゼロデイアタックによる情報漏洩はここから始まり、継続的に実行されます。

悪意のあるパーシステンス メカニズムは、通常、マルウエアキルチェインの早い段階でゼロデイ攻撃のペイロードによって展開されます。 セキュリティ違反をインシデントタイムラインの早い段階で発見して認証することができれば、（悪意のあるパーシステンス・メカニズムが検

出できれば）このパーシスタンス・メカニズムとドロッパー・ソフトウェアの両方を容易に強制終了することで攻撃を未然に防ぐことができます。

7. ファイアータワー セキュリティー オペレーション

ウイルス ソフトウエアとの共存によるメリット

エンタープライズ内に AV ソフトウェアが導入されている場合、AV マルウェアの著名（シグネチャー）データベースが最新であることを前提に、インストールされている AV ソフトウェアによって既知（すでに AV ベンダーによって認知されているもの）のマルウェアや悪用されているプログラムが停止される可能性があります。 FireTower は、既知のマルウェアが既に AV ソフトウェアによって停止および隔離される場合、何も実行せず通常の待機状態になっています。

ファイアータワーのパーシステンス メカニズムの検出と認証

パーシステンス メカニズム（Windows オペレーティングシステム内で定義された、ユーザーが知らないうちに、自動的に実行される設定）は、オペレーティングシステムの起動時、ユーザーのログイン時、またはアプリケーションの起動時、その他に、Windows によって自動的に開始されるプログラムです。 ファイアータワーの検出タスクは、ターゲットバイナリファイルの関連メタデータ、デジタル証明書、ハッシュ値（MD5、SHA-1、および SHA-256）を含む既存のすべての「パーシステンス メカニズム」を記録します。 その後も外部から入ってくる脅威からシステムを守るため、リアルタイムで、パーシステンス メカニズムの監視を継続し、それらの追加や変更に対する自動的な認証を開始します。

ASR （オートラン セッティング レポジトリー - Autorun Setting Repository）

ファイアータワー サーバー内に格納される ASR（オートラン セッティング リポジトリ）は、パーシステンス メカニズムの認証（レーティング）するためリアルタイムに使用されます。ASR は Autorun エントリを、既知の脅威、既知の安全、または未知数（ゼロデイ）等のように認証し、それらの情報を検出のためのスキームに提供します；。認証結果は以下のように分かり易く色別にレポートされます。

緑: ファイアータワーの認証によって安全が確認されたエントリー
赤: ファイアータワー および 60 種類以上のウイルスデータベース等により
危険と評価されたエントリー
橙: ファイアータワーによって疑わしいと評価されたゼロデイ エントリー
黄: ファイアータワーによって疑わしい振る舞いは無い（安全）と
評価されたゼロデイ エントリー

パーシステンス メカニズムのソース（調査内容）

1. Windows Update（マイクロソフトによるデジタル署名）
2. ユーザーがインストールしたアプリケーションソフトウェア。
3. マルウェアペイロード実行の結果
4. その他

ファイアータワー エンタープライズ プロテクション プロファイル

エンドポイントを保護するためのプロファイル設定:

A. OFF（オフ）: 監視・レポートのみ、ガード機能無し
B. NORMAL（普通）:黄色および緑色の定格のパーシステンス メカニズムの追加・変更イベントを許可（ホームオフィスの小規模ビジネスコンピュータなど）
C. ESCALATED（昇級）緑色のパーシステンス メカニズムのイベントによる変更のみを許可（例えば、中小企業のコンピュータ）
D. LOCKDOWN（ロックダウン）確実に安全である事が確認された緑色のエントリーによる変更のみを許可

Profile/Rating	緑色	黄色	橙色	赤色
モニタリング	パス	パス	パス	パス
Normal（普通）	パス	パス	ストップ	ストップ
Escalated（昇級）	パス システム/アプリケーション	ストップ	ストップ	ストップ
Lockdown（ロックダウン）	パス システムのみ、およびマイクロソフトによる正規著名のあるもの	ストップ	ストップ	ストップ

企業内で設定する独自のパーシステンス メカニズム：

ファイアータワー セキュリティソリューションは、各企業に対して的確にチューニングされた（ソフトウエアの使用/非使用に関する企業ポリシーまで包含した）ASR（オートラン セッティング レポジトリー）を介して、エンドポイントコンピュータ内で発生するクリティカルな変更イベントに対するリアルタイム認証機能をご提供します。 企業独自でチューニングを加えた独自のデータはもちろん全て非公開に保管できます。

ファイアータワー サーバーに格納される、パブリックの ASR に対するすべての更新は、各企業で登録・変更したアプリケーションの使用に関するポリシーを含むプライベート ASR プロキシサービスと自動的かつ定期的に同期されます。 すべての脅威データは、社内のファイアータワー サーバー データベースに格納され、外部に公開されることはありません。

エンタープライズクライアント（デスクトップ/サーバー）のセキュリティー管理

ファイアータワー セキュリティー ソリューションを使用すると、企業はクライアントコンピュータを場所、建物、部門、コンピュータの種類、ネットワーク環境等の企業内の様々情報別にグループ化する事により管理・構成できます。各クライアントコンピュータは、複数のグループに関連付けることができます。 ファイアータワー セキュリティー ソリューションを使用すると、ルート管理者はグループ管理者に指定されたグループの監視と管理を割り当てることができます。これらのグループ管理者の権限は、割り当てられたそれぞれのグループにのみ適用されます。

8. ファイアータワー エンタープライズ プロテクション タスク

ファイアータワー セキュリティー ソリューションによって提供される次の保護タスクは、企業のセキュリティ要件のあらゆる範囲をカバーします。

1, ゼロデイアタック検知と封じ込め

エンドポイントプロテクション プロファイルを Normal（普通）、Escalated（昇級）、または Lockdown（ロックダウン）に設定すると、ファイアータワー クライアント ソフトウェアは、グループ固有のセキュリティー設定に基づいて、ゼロデイ攻撃の悪意のあるソフトウェアをリアルタイムで検出して検疫・格納することができます。

2. セキュリティー オペレーション センターの継続的な監視

ファイアータワーは、サイバーコンソール（CyCon）ダッシュボードを使用して、エンタープライズセキュリティの状況認識と IHIPS（Inter-Host Intrusion Prevention System）アクティビティ タブで継続的なフォレンジック監視機能を提供します。
IHIPS は、企業内の全体の脅威をデータベースへ継続的に蓄積しいつでも検索する事ができます。脅威を特定し企業内のエンドポイントで進行中の攻撃やマルウェアの横方向（感染）の動きを早期に特定できます。
OODA（Observe、Orient、Decide and Act）ループによる決定サイクルに基づいて、ファイアータワー サイバー コンソールが提供するインタラクティブな脅威分析インターフェースを使用して継続的に監視を OODA ループにより実現できます。

Observe（観察）： ファイアータワー サイバーコンソールダッシュボードと IHIPS アクティビティを使用した企業の脅威状況認識を容易に確認

Orient（対応）： ファイアータワー サイバー コンソール IHIPS アクティビティを使用し、GUI で使用できるソーティング機能やフィルタリング機能等による疑わしい脅威イベントを便利に検索し対応

Decide（決定）： 疑わしい脅威イベントまたは悪意のある脅威イベントが ASR 認証レーティングに基づいて検証されている場合、FireTower Cyber Console IHIPS アクティビティを使用して確認し対応方法を決定

Act（実行）： ファイアータワー サイバー コンソールから IHIPS 機能による、Quarantine All（全て検疫）コマンドを使用し、すべてのリスクのあるエンドポイント システムに対して一斉に隔離コマンドを発行

IHIPS アクティビティビューには、すべてのエンドポイント上のパーシステンス メカニズムの変更イベントが時系列で表示されます。これは、どのエンドポイントに対して、いつパーシステンス メカニズムの変更イベントが実行されたのか示し、下部の表示は、企業内全体で同じパーシステンス メカニズムを持つすべてのエンドポイントを表示します。 各ホスト間でパーシステンス メカニズムの変更イベントの時間的分析は、異なるエンドポイントから同一のイベントがエンタープライズ全体の潜在的なマルウェアの横方向（感染）への動きの可能性がある同じパーシステンス メカニズムによる変更イベントを持つかどうかを判断するための警告として表示されます。

3. インシデント対応とフォレンジック調査

パーシステンス メカニズムに焦点を当てることは、インシデント対応とフォレンジック調査のための業界標準となっています。ほとんどのフォレンジック調査は、マルウェアインシデントを評価し、エラーやマルウェアを発見するための迅速かつ効果的な方法となるため、パーシスタンス メカニズムを調べることによってインシデント対応プロセスを実行します。
ファイアータワーは、パーシステンス メカニズムの変更イベントを継続的に監視することにより、フォレンジックなサポートを提供します。 違反が疑われるとすぐにインシデント対応を実施し、効果的な調査を実行することにより、外部の専門調査員の調査の遅延や莫大な調査・復旧費用を節約することができます。

Sampan Security, Inc.

FireTower セキュリティー ソリューション オーバービュー

＜本ドキュメントは 2017 年 6 月作成＞

U.S. GOVERNMENT RESTRICTED RIGHTS. The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Sampan Security, Inc. as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

COMPLIANCE WITH US EXPORT CONTROL. The Licensed Software is subject to export controls under the U.S. Export Administration Regulations with Export Control Classification Number (ECCN) 5D992. The license type for this ECCN is no export license is required (NLR) and there is no Commodity Classification Automated Tracking System (CCATS) number required. The Software may not be exported or re-exported to entities within, or residents or citizens of, embargoed countries or countries subject to applicable trade sanctions, nor to prohibited or denied persons or entities without proper government licenses. Information about such restrictions can be found at the following websites: http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm and http://www.treas.gov/offices/enforcement/ofac/.
You are responsible for any violation of the US export control laws related to your copy of Sampan Security product. By accepting this Agreement, you confirm that you are not a resident or citizen of any country currently embargoed by the U.S. and that you are not otherwise prohibited from receiving the Software.

Sampan Security, Inc. Nashua, New Hampshire, U.S.A.
http://www.sampansecurity.com and http://firetower.net