i-Sprint NDR powered by SecAI

HAS High Availability Systems

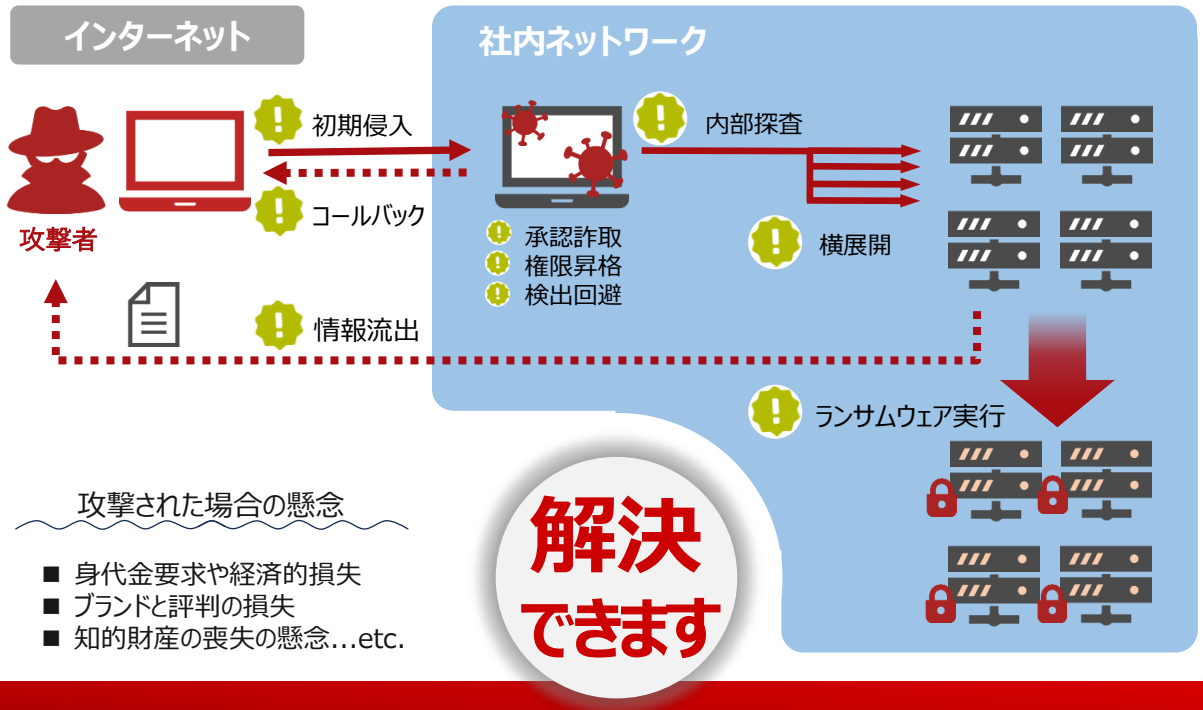
NETWORK BASED THREAT DETECTION and RESPONSE PLATFORM

ネットワーク型 サイバー脅威検出・応答 プラットフォーム

TI(Threat Intelligence)搭載 i-Sprint NDR でサイバー脅威を検出・応答

i-Sprint NDR は、複雑な脅威を自動的に検出し、分析、ノイズ除去、対応できる脅威インテリジェンス（TI）を内蔵したネットワーク検出・応答プラットフォームです。セキュリティオペレーションチームにオールインワンのネットワーク・セキュリティ・ソリューションを提供します。

標準型ランサムウェア攻撃のステップ



攻撃された場合の懸念

- 身代金要求や経済的損失
- ブランドと評判の損失
- 知的財産の喪失の懸念…etc.

解決できます

脅威検出の課題とは？

0day attacksを防ぐのは難しい
0day攻撃の検出は非常に難しい傾向にあります。

アラートを監視するのは無意味
1%のリアルアラートは99%の誤検知で埋もれてしまいます。

資産全体のリスクは特定困難
サイバー攻撃に使用される潜在的なリスクの大部分は事前に認識されていません。

攻撃はますます自動化されている
一方で攻撃への対処は依然として手動で行われています。

i-Sprint Trust without Boundaries

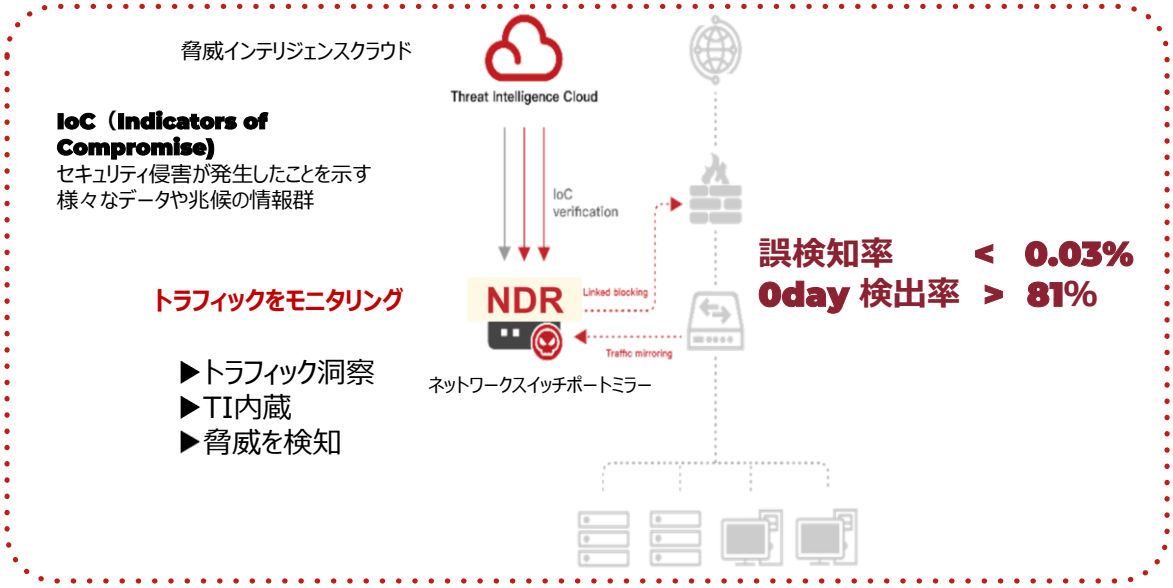
解決できます

i-Sprint NDR

HAS High Availability Systems

– Threat Detection Platform –

トラフィックを洞察 | TIを内蔵
脅威に対してフォーカス | オールインワンのソリューション



IoC（Indicators of Compromise)
セキュリティ侵害が発生したことを示す様々なデータや兆候の情報群

トラフィックをモニタリング

▶トラフィック洞察
▶TI内蔵
▶脅威を検知

誤検知率 < 0.03%
0day 検出率 > 81%

すべての資産とサービスを継続的に検出、プロファイリング
ポート、サービス、アプリケーション、バージョンを調査。また資産に対応するドメインとサブドメインの特定、非暗号化状態の機密情報や、ファイルのアップロードおよびダウンロードを検出します。

攻撃対象の削減
アプリが新規に起動され、パブリックネットワーク経由でアクセス可能かどうかをスマートに判断し、ログインポータルを識別します。 APIリスクを検出し、管理ポリシーの整理と検証をサポート。攻撃対象領域を絞り込みます。

カスタマイズ可能な資産リスクの挙動・ふるまい
さまざまなセキュリティポリシーに基づいて、必要に応じて資産リスク監視アラートを設定し、セキュリティチームが適応的なリスク監視を実現できるようにします。

攻撃経路分析
さまざまな視点からイベントを分析し、外部からの攻撃の情報を多次元的に収集します。また、イベントをタイムラインに集約して、攻撃経路と攻撃プロセスを詳細に分析します。

脅威モニタ
サイバー脅威の状況を視覚的に分析できます。

0day 検出エンジン
セマンティック分析エンジンとAIエンジンが組み合わさることで、0day検知が可能になります。これには、パブリックチャレンジプログラムから収集された高価値な0dayインテリジェンスや、セキュリティ専門家によって収集・分析された情報が活用されています。

正確なインテリジェンスに基づく検出
SecAIインテリジェンスに基づいて、侵害されたホストとAPT攻撃を正確に特定します。既知の脅威に対応して、IOCで侵害されたホストを正確に特定。
キルチェーン上の攻撃手法を包括的・網羅的に検出できます。

大規模なアラート誤検知低減
インテリジェンスベースの検出アルゴリズムを使用してアラートの相関分析を行い、攻撃アラートの精度を保証します。
誤検知の減少により攻撃状況を正確に判断できます。

攻撃の自動調査
完全なフルパッケージ分析に基づいて、攻撃が成功するか失敗するかを自動的に決定します。

組み込みのTCPリセットブロッキング
TCPプロトコルメカニズムを使用して、リセットパケットを攻撃者IPと被害者ホストに同時に送信し、接続をブロックします。

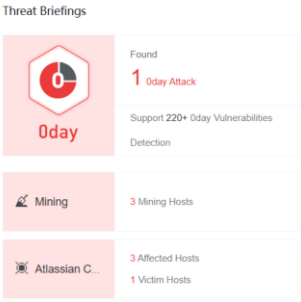
ファイアウォールと統合
ブロッキングIPを生成してファイアウォールにプッシュします。i-Sprint NDRを通してリアルタイムにファイアウォールブロックポリシーを更新します。

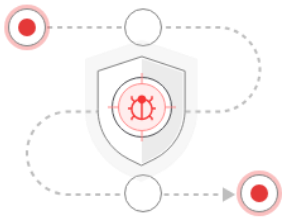
i-Sprint
Trust without Boundaries

なぜ i-Sprint NDR が選ばれるのか？

正確で高精度な検知

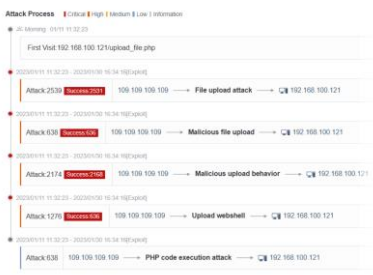
信頼性の高いインテリジェンスサポート
により脅威を検知します。
誤検知率 <0.03%





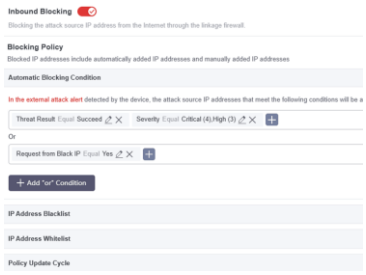
リアルワールド
コンバット-オリエンテッド

攻撃者の視点に立ったリスク分析。攻撃者の情報をインテリジェントに集約し、攻撃プロセスを完全に復元。クラウドサンドボックスで未知の脅威を発見します。



自動応答

自動でTCPリセットブロック、効果は最大99%。数十のブランドのファイアウォールと互換性。



ネットワーク接続をブロックし、顧客拠点での対応を自動化

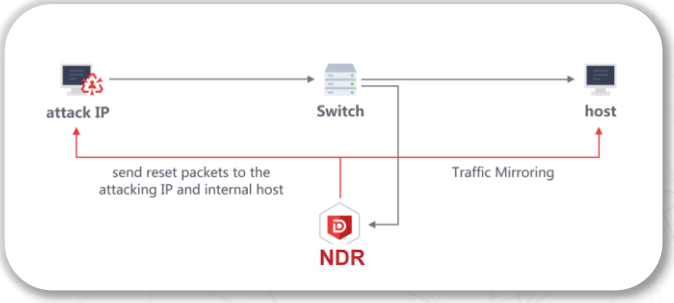
バイパスブロッキング(別名TCPキャノン)

TCPセッションの仕組みを利用し、攻撃IPと内部ホストに同時にリセットパケットを送信することで、ブロッキングの回避を実現。

❶ ブロック用IPの手動入力をサポート

❷ 自動ブロックポリシーの設定をサポート

❸ ブロッキング・ネットワーク・カードの設定をサポート



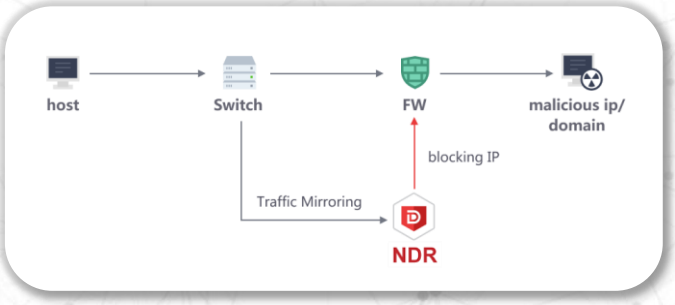
ファイアウォール・ブロッキング

i-Sprint NDRでファイアウォールを設定し、リンケージブロッキングでポリシーを設定し、ブロッキングIPを生成し、ブロッキングのためにファイアウォールにプッシュ。

❶ i-Sprint NDRがブロッキングIPリストを生成

❷ 3rdパーティのファイアウォールの連携をサポート(10+)

❸ ファイアウォールへのブロックキングIP送信をサポート



i-Sprint NDR Trust without Boundaries powered by SecAI

価格、提供形態

Here we go !

HAS High Availability Systems

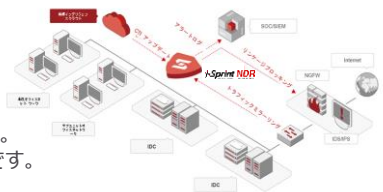
製　品	費　用	契約単位
i-Sprint NDR Powered by SecAI	**最大トラフィック：1Gbps** **¥29,800,000-/年**	**1セット年間サブスクリプション** **最低1年契約、複数年契約は応相談**

サブスクリプション・パックには以下のものが含まれます。(*は導入時のみ)

アプライアンスサーバ	i-Sprint NDR(SW)とHW本体が含まれます。※別途サーバをご用意いただく必要はございません。
ユーザ使用権	1つのi-Sprint　NDRソフトウェアの使用権(ライセンス)が含まれています。 ※複数台サーバが必要になる場合は別途見積もりとなります。
ヘルプデスクサポート SW/HW	i-Sprint NDRに関するお問い合わせについては、電話、またはEメールにてサポートいたします。 平日9時～17時、土日祝祭日年末年始(12月30日～1月4日)を除きます。
新バージョンの提供	i-Sprint NDR関連ソフトウェアの更新版を無償で提供いたします。 バージョンアップ作業は別途有償で対応いたします。
ユーザマニュアルの提供*	製品付属のマニュアル、日本語利用者・管理者ガイド(汎用)を電子ファイルにてご提供いたします。
導入支援*	設定シート(パラメータシート)に基づいたサーバ構築を弊社エンジニアが実装します。 ※ネットワーク機器（L2スイッチなど)の設定（ミラーリング等)の協力をお願いいたします。
トレーニング*	汎用のトレーニングガイドをもとに技術移管トレーニングを実施します。（オンサイト半日程度）
HW交換対応	HWの通常保守(5年)を経過した後のHW交換作業、および、HW本体代が含まれます。

特記事項

1. 導入先となるHW,OSの製品・構築費用を含みます。
2. HWは1U（ユニット）でご用意いたします。サーバラックの空きをご確認ください。
   電源は2口ご用意ください。
3. HWの機器故障時は翌営業日オンサイト対応です。
4. NW機器のミラーリング設定を実施するためコマンド実行権限等を依頼することがございます。
5. ダッシュボード確認の為のクライアントPC/サポートブラウザはWindows10、Windows11です。
   サポートブラウザはMS EdgeとChromeです。
   ＊機能改修は、新バージョンに含まれます。お客様環境によってはご提供できない場合がございます。



NDR製品の利点と強み

NDRは、ネットワーク全体のトラフィックを監視し、異常な通信や行動を検出して対応するため、ネットワーク全体の視点から脅威を捉える能力が強みです。NDRソリューションの導入は、EDRやIPS/IDS より有利になるケースが多くあります。

1.ネットワーク全体の可視性向上:
NDRは、エンドポイントに依存せず、ネットワーク全体のトラフィックをリアルタイムでモニタリングします。ネットワーク内の全てのデバイスやトラフィックの動きが可視化され、エンドポイントに限定されない広範な脅威検知が可能です。これは、EDRやIPS/IDSがエンドポイントや特定のパケットに依存することに対する大きな利点です。

2. 高度でステルス性の高い脅威の検出
NDRは、機械学習を利用して未知の脅威やゼロデイ攻撃を検出する能力があり、シグネチャベースのIDSやIPSより新しい脅威に強いケースが多くあります。

3.エンドポイント回避技術の影響の軽減
ネットワーク内部で攻撃者が横移動（Lateral Movement）する際、エンドポイントを回避して活動する場合があります。NDRは、ネットワークトラフィックに基づいて攻撃者の動きを検知できるため、EDRが見逃す可能性のある内部の攻撃に対して強みを発揮します。

4.ネットワークミラートラフィックによる導入とメンテナンスの容易さ
ネットワークミラーリングによって非侵入型の監視を実現し、導入やメンテナンスコストが比較的低いのが利点です。既存のネットワークインフラに大きな変更を加えることなくトラフィックを監視できるため、大規模なネットワークや拡張性のある環境で特に効果的です。また、AIや機械学習による自動分析機能により、メンテナンスの負担も軽減されます。

株式会社ハイ・アベイラビリティ・システムズ
プラットフォームソリューション事業部

HAS High Availability Systems

お問合せ

〒105-0023
東京都港区芝浦1-2-3　シーバンスS 4F
TEL 03-5730-8850　FAX 03-5730-8700
E-mail : inquiry_desk@ha-sys.co.jp
URL：https://pod-guardians.com