バイヤーズガイド

ネットワークの検出と応答（NDR）

NDRは、他のネットワークセキュリティツールにない疑わしいイベントを検出します

STELLAR CYBER®

NDRとは何ですか？

*NDR*はネットワークセキュリティから発展しました

今日のネットワーク検出および応答（NDR）には長い歴史があり、ネットワークセキュリティおよびネットワークトラフィック分析（NTA）から発展しています。ネットワークセキュリティの歴史的な定義は、境界ファイアウォールと侵入防止システムを使用してネットワークに着信するトラフィックをスクリーニングすることですが、ITとセキュリティ技術が進化するにつれて、より複雑なアプローチを活用する最新の攻撃により、定義ははるかに広くなりました。

今日、ネットワークセキュリティは、企業がネットワークとそれに接続されているすべてのセキュリティを確保するために行うすべてのことです。 これには、ネットワーク、クラウド（または複数のクラウド）、エンドポイント、サーバー、IoT、ユーザー、およびアプリケーションが含まれます。ネットワークセキュリティ製品は、物理的および仮想的な予防策を使用して、ネットワークとその資産を不正アクセス、変更、破壊、および誤用から保護しようとしています。

これらのセキュリティ製品は通常、ネットワークの特定の側面を対象としています。

- **ユーザーエンティティおよび行動分析（UEBA):** ユーザーおよび/またはエンティティのアクティビティ、ベースラインの通常の動作を監視し、通常のアクティビティから逸脱したアクティビティについてアラートを出します。
- **侵入防止/検出システム（IPS / IDS):** ファイアウォールを通過する許可されたトラフィックの既知の攻撃を監視してブロックします。
- **PCAPデバイス:** コンピューターネットワーク上を移動する生のパケットをキャプチャし、フォレンジック分析や攻撃の再生のために保存します。
- **ネットワークトラフィック分析（NTA):** 内部および外部の利用可能なすべてのソースからトラフィックメタデータを収集し、異常、リスク、および脅威を分析します。
- **ファイアウォール:** トラフィックを許可または拒否することにより、ネットワークへの不正アクセスを防止します。.
- **サンドボックスおよびアンチウイルス/マルウェアソフトウェア:** ネットワーク、エンドポイント、およびサーバーが、ファイルの破損、機密データのエクスポート、またはその他の悪意のあるアクティビティを実行する可能性のある有害なソフトウェアに感染するのを防ぎます。
- **アプリケーションセキュリティ:** アプリケーションソフトウェアの脆弱性を探してブロックします
- **クラウドセキュリティ:** クラウド内のリソースとアプ

ネットワークセキュリティの傘下に入る製品はたくさんあり、それらを総合的に管理してネットワーク上のリスクや脅威を検出して対応することは困難です。そこでNDRが登場します。**テクノロジーカテゴリとしてのNDRは、最初にNTA、IDS、UEBA、TIPを単一のスーパーセットプラットフォームに統合して検出と応答の両方を実現し、次にNTAをはるかに超えて、機械学習と自己相関を通じて他のすべてのネットワークセキュリティ製品の背後にある頭脳として機能することを目指しています。**

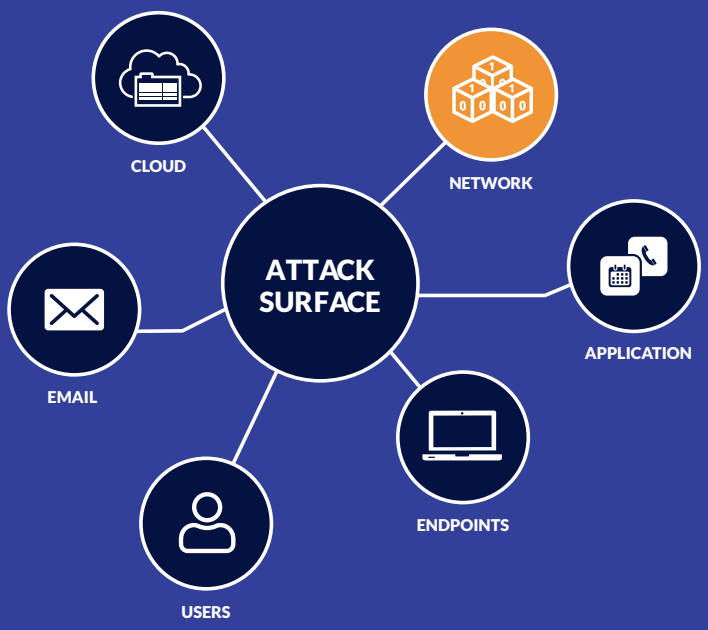
今日のNDRは、最新の攻撃を迅速に発見するために必要な可視性を確保するためのセキュリティ運用のコア機能として、ガートナーによって提案されています。NDRは、SIEMまたはNG-SIEMを完全に補完して、ログを超えた可視性を実現します。

NDRが必要な理由

*NDR*は完全な可視性を保証し、ゼロトラストを検証します

エンドポイントデータとセキュリティツールのログを分析するだけでは、今日の攻撃を阻止するのに十分ではありません。**ネットワークトラフィックについて知っておくべき重要なことが1つあるとすれば、それは嘘ではないということです。**そのため、NDRは、エンドポイントデータ用のEDRおよびセキュリティツールログ用のSIEMとともに、組織のXDRへのデータジャーニーを完了します。 具体的には、NDRは、エンドポイントやその他のログには表示されないもの（ネットワーク全体、デバイス、SaaSアプリケーション、ユーザーの動作）を確認し、高品質のグラウンドトゥルースデータセットとして機能し、リアルタイムの応答を可能にします。

ゼロトラストが採用され続けるにつれて、ネットワークはセキュリティの基礎を改善するさまざまなセグメンテーションを受けます。 他の複雑なシステムと同様に、信頼はあるが検証のアプローチを採用する必要があり、NDRは検証の相手としてゼロトラストを完全に補完します。 **NDRを使用すると、組織は自信を持ってゼロトラストを採用し、その実施を検証できます。**



最新のNDRアーキテクチャ

攻撃対象領域を完全にカバーするための適応アプローチ

NDRソリューションは、非署名ベースの手法を使用します（たとえば、機械学習またはその他の分析技術）品質シグネチャベースの技術（たとえば、アラート用にインラインで融合された脅威インテリジェンス）とともに、疑わしいトラフィックまたはアクティビティを検出します。NDRは、専用センサー、ファイアウォール、IPS / IDS、メタデータ（NetFlow）、またはその他のネットワークデータソースからデータを取り込むことができます。 柔軟な展開アーキテクチャにより、すべての物理環境と仮想環境のトラフィックに加えて、北/南のトラフィックと東/西のトラフィックの両方を監視できます。すべてのデータは、強力なAIエンジンを備えた一元化されたスケーラブルなデータレイクに送信され、疑わしいトラフィックパターンや異常な動作を検出して、忠実度の高いアラートを生成します。特定のソリューションに応じて、最高のNDRベンダーのAIエンジンには、EDRやログなどの他の多くのセキュリティツールからの関連アラートをグループ化してアラートをより効率的かつ正確に表示する高度な自己相関機能がある場合があります。

応答は、セキュリティ運用へのパフォーマンスの高いネットワークベースのアプローチを可能にする検出の重要な対応物であり、NDRの基本です。 疑わしいトラフィックをドロップするためのファイアウォールや影響を受けるエンドポイントを隔離するためのEDRツールへのコマンドの送信などの自動応答、または脅威ハンティングやインシデント調査ツールの提供などの手動応答は、NDRの一般的な要素です。

NDRバイヤーチェックリスト

以下の表を使用して、ベンダーの短いリストを作成します。

以下にリストされている機能は、ソリューションが提供できるようにするものです。

- NDRの最新の定義 – すべてのネットワークセキュリティ製品の頭脳として機能するスーパーセットプラットフォーム
- 完全な可視性とゼロトラスト検証 – すべてのネットワークセキュリティデータを利用できる機能
- アダプティブアーキテクチャ – 柔軟で普及した展開モデル

機能	説明
任意のネットワークソースからの360Oデータ収集	• 仮想インフラストラクチャと物理インフラストラクチャの両方から、専用のネットワークセンサーによる取り込み時にメタデータを抽出します • ファイアウォールトラフィックログ、IDSイベント、NetFlowおよびクラウドフローログを収集します • トラフィックからファイルを組み立てる
データの正規化とコンテキストの作成	• データを一般的な人間が読める形式と検索可能な形式に正規化しますt • 脅威インテリジェンス、ジオロケーション、資産情報、ユーザー情報などのコンテキストでデータを充実させる • IDSイベントなどのセキュリティツール間のデータを、ネットワークセンサーからの豊富なネットワークメタデータと相関させます
AIとアラートの自動グループ化による忠実度の高い検出	• 機械学習による事前構成済みネットワーク検出の完全なスイート：教師なし、教師あり、またはグラフML • 機械学習または高度な分析によるユーザーとエンティティの行動分析 • さまざまなセキュリティツールからの関連するアラートの高レベルのインシデントへの自動相関
自動応答	• 手動および自動の脅威ハンティング • 自動応答プレイブック • ADでのユーザーの無効化やファイアウォールでのトラフィックのブロックなど、迅速な対応アクションを実行するための他の多くのツールとの幅広い統合
追加ツールの緊密に統合されたスイート	• 既知の攻撃検出用のML-IDS、ゼロデイマルウェア分析用のサンドボックス • 資産の包括的かつ自動在庫のための資産管理 • コンプライアンスレポート

購入者への推奨事項

セキュリティを向上させ、疑わしいネットワークトラフィックと異常なユーザーの動作を検出するには、セキュリティとリスク管理のリーダーは次のことを行う必要があります。

- 複雑なネットワークセキュリティスタックを管理する必要をなくし、最高のパフォーマンスを確保するために、スーパーセットプラットフォームとしてNDRを提供するソリューションを実装します。
- ネットワークトラフィックからの既知の攻撃と未知の攻撃の両方を包括的に検出するために、AIベースの両方の検出ツールとシグニチャベースの両方を組み合わせたソリューションを実装します。
- 評価プロセスの早い段階で、評価中のソリューションに適切な自動応答機能があるか、他のセキュリティ製品と直接統合された手動応答機能があるかを決定します。シームレスな統合は、滞留時間を短縮するために重要です。

STELLAR CYBERが包括的なNDRを提供

*Stellar Cyberのオープン*XDR*には*NDR*が含まれており、ネットワークデータをすべてのデータと関連付けます*

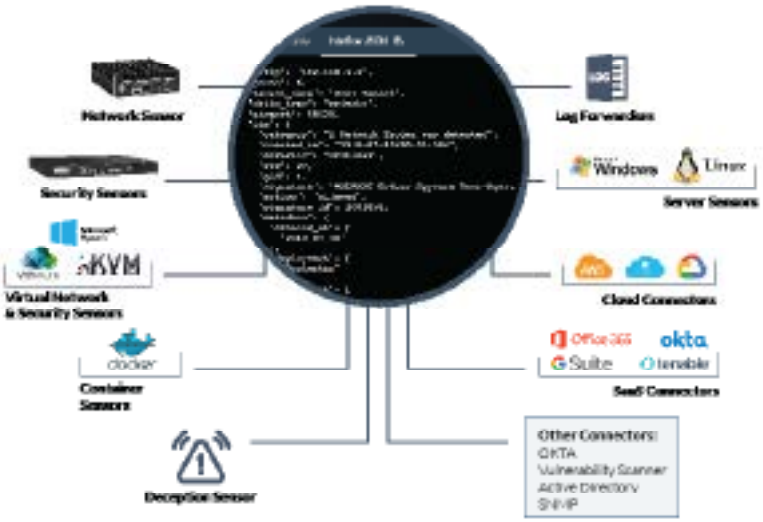
ログを超えて、ネットワークのすべての側面を完全に可視化できます。あなたのネットワークがどこにあるか。 Stellar CyberのオープンXDRプラットフォームには、業界をリードするNDR機能が組み込まれています。ネットワークテレメトリを収集するために分散されたセンサーファミリ、既知の攻撃用のML-IDSエンジン、ゼロデイマルウェア分析用のAV/サンドボックス、データの正規化とコンテキスト作成用の高度なプロセッサエンジンがあります。一元化されたデータレイクストアのコンテキスト化されたネットワークテレメトリ、TIフィード用の脅威インテリジェンスプラットフォーム（TIP）、検出と相関のための強力なAIエンジン、およびさまざまな統合による自動応答。 これらの機能はすべて、箱から出してすぐに機能します。 数日でNDRを起動して実行し、以前は隠されていた脅威を確認します。

- 専用のネットワークセンサーまたは既存のファイアウォールまたはトラフィックフロー（NetFlow）からのトラフィックログを介して、強力なディープパケットインスペクション（DPI）エンジンを使用して、生のネットワークパケットトラフィックを分析し、メタデータをリアルタイムで抽出します。
- 北/南のトラフィック（境界を横切るとき）、および東/西のトラフィック（ネットワーク全体を横方向に移動するとき）を監視および分析します。
- 通常のネットワークトラフィックとユーザーの動作をモデル化し、通常の範囲外の疑わしいトラフィックまたはユーザーの動作を強調表示します。
- ネットワークの異常を検出する機械学習や高度な分析などの行動手法（署名に基づかない検出）を使用します。
- 疑わしいネットワークトラフィックまたはユーザーの動作の検出に対応するための自動または手動の応答機能を提供します。
- DGAやDNSトンネリングなどの回避攻撃には、ディープラーニングなどの高度な機械学習を使用します。

STELLAR CYBERはNDRデータの問題を解決します

Stellar CyberのInterflow – 正規化され、強化された、実用的なデータ

業界は、NetFlowよりも豊富（少なすぎる）、PCAPよりも大幅に軽量（大きすぎる）、ホスト名、ユーザー情報、脅威インテリジェンス、ジオロケーションなどのコンテキスト（ちょうどいい）と融合したデータセットを出力するために、ネットワークパケット、ファイル、ログをキャプチャすることで、サイバーセキュリティのGoldilocksジレンマを解決するという課題に直面しています。



STELLAR CYBER

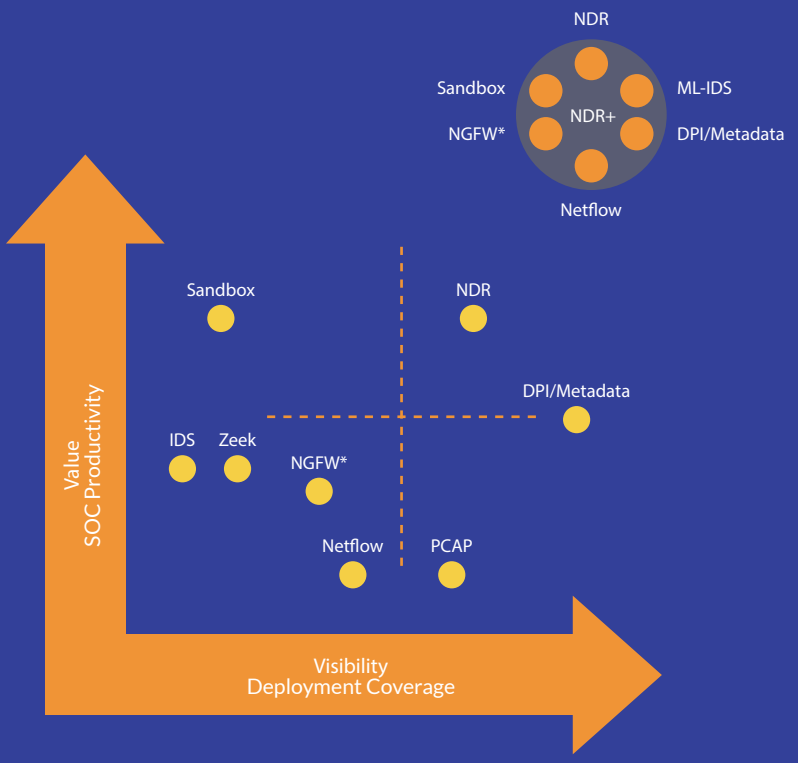
https://jp.stellarcyber.ai

Interflowは、Stellar CyberオープンXDRプラットフォームの不可欠な部分です。パケットからテレメトリを抽出する強力なDPI機能を備えたデータ抽出エンジンと、テレメトリの価値を自動的に高めるフュージョンエンジンです。 これは正規化された強化されたデータモデルであり、ITツールとセキュリティツールが同じ言語を話すことができるため、あらゆる脅威を検出して対応できます。Interflowは、ネットワークセキュリティ専用に構築されたモデルを使用してネットワークセキュリティの問題を解決します。Stellar Cyberの豊富なセンサーセットは、文字通り、どこからでも、どこからでもすべてのテレメトリを収集します。

*Interflow*を使用すると、セキュリティが向上します

1. 手動によるデータ変更の停止– Interflowを使用すると、コンテキストが自動的に作成されます
2. データ量の削減 – PCAPからInterflowへのデータ削減は最大2桁になります
3. 一見無関係に見えるイベント間での相関 – 標準のキー値により相関が容易になります
4. 高度に解釈可能 – わかりやすいデータにより、アナリストのトレーニング時間を短縮します。

STELLAR CYBERのINTERFLOW(インターフロー)は価値と可視性を提供します



PCAP:	保存するデータが多すぎて分析が難しいです
Netflow:	スイッチ/ルーターによって制限されている間、有用であるために十分なデータがありません
IDS:	スケーラブルではありません。うるさすぎて高すぎます
NGFW*:	データが不十分で規模が限られています
Sandbox:	ファイルベースのマルウェアのみで非常に高価です
DPI/ Metadata:	忠実度とコストのバランスが取れています。 展開が簡単です
NDR/NTA:	多くの場合、騒々しくて高価です

ガートナーマーケットガイド：ネットワークの検出と対応：2020年6月

Stellar Cyberだけが12のNDR基準すべてを実現します

	基準	詳細	STELLAR CYBER
1	**データタイプ**	生のパケット、NGFW / IDSログ、NetFlow / IPFix	✓
2	**データソース**	物理または仮想スイッチ、コンテナー、サーバー、IaaS-（Azure、AWS、Google Cloud、プラットフォーム、Oracle Cloud Infrastructure）	✓
3	**トラフィックコンテンツ**	3000以上の識別されたアプリケーション、10,000以上のL2-L7メタデータ、トラフィックフローからのファイルを備えた強力なDPI	✓
4	**データ削減**	パケット重複、データフィルタリング、データ圧縮	✓
5	**暗号化されたトラフィック**	行動分析、証明書検査、JA3	✓
6	**データエンリッチメント**	脅威インテリジェンス、IPジオロケーション、IPからホスト名、IPからユーザー名、IPアドレスタイプ	✓
7	**データ保持**	コンプライアンスのための構成可能なホットストレージと外部コールドストレージ	✓
8	**データの可用性**	データバッファリング、データレプリカ、HA、ディザスタリカバリ	✓
9	**検出**	教師あり学習と教師なし学習、深く適応的な学習、MLを使用したIDS、サンドボックス、UEBA	✓
10	**相関**	IDSイベント、脆弱性、EDR、サンドボックス間の自己相関	✓
11	**応答**	トラフィックのドロップ、ユーザーの無効化、エンドポイントの封じ込め、脆弱性スキャンのトリガー、スクリプトの呼び出し、APIの呼び出し、アラート、レポート	✓
12	**展開**	物理アプライアンスまたは仮想アプライアンス、サーバー、IaaS-（AWS、Azure、GCP、OCI）のIaaSオールインワンまたは分散	✓

今すぐデモをリクエストしてください！

jp.stellarcyber.ai.

Stellar CyberのオープンXDRプラットフォームは、すべてのツールからデータを取り込み、攻撃対象領域全体でインシ デントを相互に関連付け、忠実度の高い検出を提供し、AIと機械学習を通じて脅威に自動的に対応することで、すべて の検出と対応を実現します。当社のインテリジェントな次世代セキュリティ運用プラットフォームは、コストを削減し、 既存のツールへの投資を維持し、アナリストの生産性を向上させながら、すべての攻撃活動を早期かつ正確に特定して修 正することで、企業のリスクを大幅に軽減します。 通常、当社のプラットフォームは平均検出時間(MTTD)で20倍、平 均復旧時間(MTTR)で8倍の改善を実現します。同社はシリコンバレーを拠点としています。

https://jp.stellarcyber.ai