概要

業界

- 軍事組織

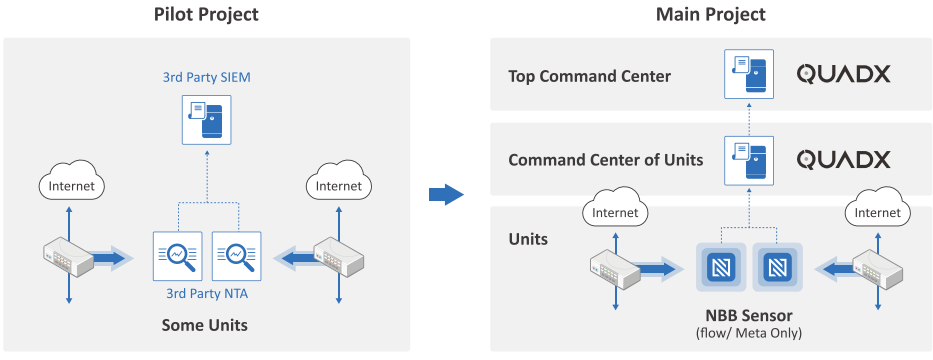
課題

- 全国のセキュリティ製品で検知される脅威イベントを統合
- 全国のセキュリティ製品で検知される脅威イベントを統合
- 陸軍部隊におけるすべての通信内容をロスなく収集
- 既存のセキュリティシステムとの統合に不可欠なデータ分析機能の導入

導入効果

- 軍事システム全体におけるメタベースおよびフローベースのデータ分析の体系化
- 陸軍保安センターにおける交通監視および分析システムの統合
- 全軍へのサイバー戦争対策サポート

軍事組織



今日のデジタル時代において、軍事組織は国家安全保障に重大なリスクをもたらすサイバー脅威の増加に直面しています。 軍がデジタル作戦の戦略的価値を意識するにつれ、サイバー戦争は現代の戦争においてより重視されるようになってきました。 サイバー攻撃は迅速かつ匿名で行われる可能性があり、比較的少ない投資で大きな損害を引き起こすことが多々あります。 これらの脅威に対抗するために、軍事組織はセキュリティインシデントを迅速かつ効果的に検出して対応できる、堅牢で高度なサイバーセキュリティソリューションを必要としています。Network Detection and Response (NDR) ソリューションの大手プロバイダーである Quad Miners は、軍事組織と緊密に協力し、フルパケットフローとメタデータに基づくトラフィック分析システムを確立しています。 このケーススタディでは、軍事組織が直面している課題と、Quad Miners の NDR ソリューションがフルパケットベースのトラフィック 調査を行うことで、どのようにこれらの課題に対処したかを考察します。

背景

近年、特定の軍事ネットワーク (インターネット、イントラネット) で、フローおよびメタデータベースの分析システムが試験的に導入され、一定の効果をあげています。ただし、包括的なセキュリティ体制を確立するには、分散した陸軍ネットワークからすべてのトラフィックを収集して完全に可視化する必要があります。 さらに、既存のセキュリティ インフラとNetwork Traffic Analysis (NTA) ソリューション間の運用上の有効性を検証できる、セキュリティの脅威に対する統合分析システムを構築しなければなりません。

課題

軍は、軍事システム全体にわたってセキュリティの脅威から効果的に保護するための統合分析システムを必要としています。　これには、全国規模のセキュリティソリューションからの脅威イベントと統合分析をまとめる必要があります。　ただし、軍は全国に分散しているため、安定したネットワークトラフィックの収集と、部隊のすべてのネットワーク通信用のトラフィック情報ロスなく収集する必要があります。
さらにNDR ソリューションは、既存のセキュリティシステムを即座にサポートできる重要なデータ分析機能を提供する必要があります。
これには広大な敷地面積を持つ軍事基地全体をカバーするソリューションが必要ですが、すべてのエンドポイントとインフラからネットワークトラフィックを収集して分析することは困難です。
さらに、軍はセキュリティアラートやイベントの詳細な調査に十分な情報を必要としていましたが、既存の NTA 製品ではネットワークの可視化と既知の脅威の検出のみを行っていました。　つまりソリューションは、トラフィックに関連付けられたメタデータを含め、すべてのネットワークトラフィックを分析用にキャプチャし、脅威を完全に可視化できなければなりません。
最後に、軍は急速に進化する脅威に対応できるソリューションも必要としています。これにはNDR ソリューションの継続的な更新と拡張が必要です。　ソリューションは新たに出現する脅威に適応でき、既存のセキュリティインフラと統合できる柔軟性を備えている必要があります。

ソリューション

Quad Miners の NDR ソリューションは、軍が直面する課題に対して包括的なソリューションを提供することができました。 競争力のある PoC を通じて統合管理および分析システムの有効性が検証されています。 Quad Miners は、フルキャプチャされたトラフィックから再構築されたパケット ストリームの分析によってのみ抽出できるメタデータとして豊富なデータセットを使用し情報を強化することで、さまざまな異常や脅威に対する詳細な調査を行える効果的なソリューションであることが証明されました。また、パケットデータの保存は行いません。　このNDRソリューションには、セキュリティソリューションの脅威イベントの解析による統合サポート、各地域のセンサーによるすべての通信トラフィックの収集、軍事特性に合わせた異常、脅威、およびコンテンツの検出機能が含まれています。
Quad　Minersはまた、データアナリストの派遣サポートを提供することにより、全国で最速のセキュリティ分析システムの構築を実現しました。 ディスパッチ サポートにより、セキュリティの脅威に適時に対応できるようになり、分析と対応に要する時間が短縮されました。
総じて、Quad Miners のソリューションは、軍がセキュリティ目標を達成するための包括的かつ効果的な解決策を提供しました。　このソリューションは、既存のセキュリティインフラとシームレスに統合され、既存のセキュリティシステムを即座にサポートするために必要なデータ分析機能を備えています。NDR ソリューションは、軍事基地全体をカバーし、ネットワーク セキュリティへの包括的なアプローチを実現しました。

導入効果

Quad Miners の NDR ソリューションの実装により、軍全体でフローおよびメタデータベースでのデータ分析の体系化が可能となり、統合された脅威検出とデータ分析機能が提供されました。　陸軍セキュリティセンターにトラフィック監視および分析システムを統合することで、セキュリティ脅威の効率的な集中監視および管理が可能になりました。
NDR　ソリューションは、ネットワークトラフィックの可視性を高め、セキュリティ脅威に対して適時の検出と対応を実現することで、軍のサイバー戦争への対策を大幅に改善しました。　さらに、フルパケットキャプチャベースのシステムに移行する必要性が認められ、NDR ソリューションはこのニーズを満たすソリューションを提供しました。
データアナリストの派遣により、全国最速のセキュリティ分析体制を実現し、セキュリティインシデントの分析および対応時間を短縮。 全体を通して、Quad Miners の NDR ソリューションは、軍に包括的で効果的なネットワーク セキュリティソリューションを提供し、サイバーセキュリティ体制を大幅に強化しました。

軍事組織がNDRソリューションを必要とする理由

軍はサイバーセキュリティ体制を強化し、潜在的なサイバー脅威から身を守るために、Network Detection and Response (NDR) ソリューションを必要としています。 軍でのテクノロジーと外部や内部との接続が増加するにつれ、サイバー攻撃と潜在的なデータ侵害のリスクが高まります。 NDR ソリューションはリアルタイムでネットワーク全体の可視化と脅威検出を提供できるため、セキュリティチームはセキュリティインシデントを迅速に特定し対応できます。 さらに、NDR ソリューションはネットワークトラフィックデータを分析して、ネットワークの潜在的な脆弱性を特定するのに役立つ洞察とパターンを軍へ提供します。 総じて、NDR ソリューションは、サイバー脅威を検出、防止、および対応する軍の能力を大幅に向上させることができます。