概要

業界

- 政府機関

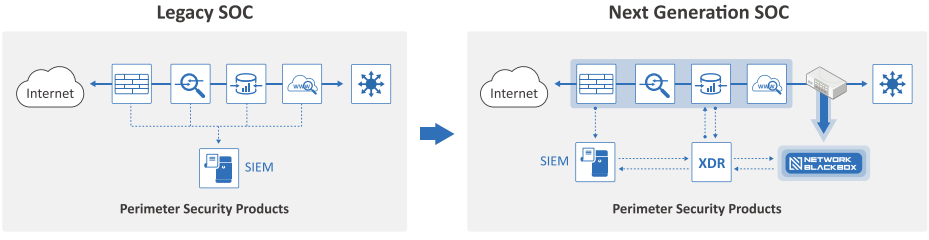
課題

- 検出および生成されたセキュリティイベントの監視のみへの集中
- サイロ化されたセキュリティイベント分析システム
- 検出されたセキュリティイベントのリスクと影響、遅延の発生の判断が困難

導入効果

- セキュリティイベントの高度化
- 証拠に基づいた攻撃のリスクと影響の即時的な判断
- MTTDとMTTRの削減
- 国内の交通セキュリティを強化および二次的なプロジェクトの実施可能性の特定

対応時間の短縮を目的とした高度なセキュリティシステムの導入事例



このケーススタディでは、某政府機関へ高度なセキュリティシステムを導入し、セキュリティ侵害への対応時間を短縮した事例に焦点を当てます。サイバー脅威が絶えず進化し巧妙化しているため、政府機関は機密情報やシステムを保護するための堅牢なセキュリティインフラを構築することが不可欠です。
政府機関はセキュリティインシデントを迅速に検出し対応できる総合的セキュリティソリューションを必要としていました。徹底的な評価を経て、オフィスはセキュリティ体制を強化し応答時間を短縮するために、Quad Miners の Network Detection and Response (NDR) ソリューションを採用しました。
このケーススタディでは、政府機関が直面している課題とQuad Miners によって実装されたソリューションおよび高度なセキュリティシステムの採用によって得られた成果について考察します。

背景

政府機関は、複雑なセキュリティ構成で複数の境界にまたがる統合インターネット網を運用しています。システム、政府機関、部門および職員の多様性が保護されているため、効果的なサイバーセキュリティ対策を確保することが重要です。政府機関はデジタル化の推進に力を入れているため、セキュリティの課題が複雑化し、進化する脅威に対応できる高度なセキュリティシステムが必要になります。その実現のために、政府機関は集中化された統合セキュリティ運用を導入し、包括的なセキュリティカバレッジを提供しています。しかし、セキュリティ侵害の巧妙化と頻度の増加に合わせて応答時間を短縮し、インシデント対応能力を向上させる必要性を感じています。これに対応して、セキュリティ体制を強化し、サイバー脅威のリスクを軽減するためにQuad Miners の NDR ソリューションに注目しました。

課題

政府機関はセキュリティ運用に関していくつかの課題に直面していました。
統合インターネット網には複数の境界にまたがるセキュリティ構成があり、セキュリティイベントの監視と検出が困難でした。さらに、セキュリティイベント分析システムがサイロ化されていたため、検出されたセキュリティイベントが被害者のシステムに及ぼすリスクと影響を判断できない状態でした。政府機関は以前、従来のセキュリティイベント管理システムに依存していました。このシステムではアラートが頻繁に生成されることが多く、セキュリティチームがインシデントに優先順位を付けてタイムリーに対応することが困難でした。これにより応答時間が遅くなり、セキュリティ侵害が発生するリスクが高まりました。
また政府機関はデジタル化の推進を目指していました。つまりセキュリティシステムは機敏で、新しいテクノロジーや脅威に適応できる必要があり、これには複数のセキュリティソリューションを統合し、セキュリティの状況全体を一元的に表示できる、より高度なセキュリティシステムが不可欠でした。

ソリューション

Quad　MinersのNDRソリューションは、包括的で統合されたセキュリティシステムの実装を通じて、政府機関が直面する課題を解決することができました。このソリューションは、セキュリティ侵害に関連する応答時間を短縮し、一元化された統合セキュリティ運用の提供を目的としていました。
まずNDRソリューションは、キャプチャされた全パケットから再構築されたパケットストリームからのみ抽出できる、豊富なデータセットとメタデータを使用して情報を強化することにより、ネットワーク上のセキュリティ侵害の決定的な証拠を収集しました。これにより、ネットワークトラフィックの詳細な分析が可能になり、セキュリティ侵害の原因特定に役立ちました。
次にこのソリューションは、Stellar Cyber(XDR)と既存のSIEMおよびNetwork Blackboxを統合することで分析を自動化しました。これによりセキュリティイベントとそれぞれのリスク、被害者のシステムへの影響をより迅速に特定できました。また複数のセキュリティシステムを統合することで、ネットワークセキュリティの状況をより包括的かつ全体的に把握できるようになりました。
Network BlackboxとStellar CyberはSyslogを通して統合されていました。Network Blackboxは分析で重要となるメタデータを含む詳細なセッション情報を送信します。これによりほかのセキュリティ製品でアラートが発行されたセキュリティイベントの影響および有効性に関する具体的な証拠を得られます。さらに、API統合による生パケットの解析を含むコンテンツやファイルも提供します。
最後に、このソリューションはネットワーク構成の変更を最小限に抑えることを目的としていました。ネットワーク構成の変更は潜在的な脆弱性を生み、セキュリティ侵害のリスクを高める可能性があります。ネットワーク構成の変更を監視および検出できるシステムを実装することにより、政府機関はネットワークセキュリティにリスクをもたらさない、許可された変更のみを確実に行えます。

導入効果

Quad Miners の NDR ソリューションを実装した後、政府機関が得た成果は以下の通りです。

- セキュリティシステムの高度化: NDR ソリューションは、政府機関がセキュリティインシデントをリアルタイムで検出して対応できる、より高度なセキュリティシステムの構築に貢献しました。これにより組織の全体的なセキュリティ体制が改善されました。

- 攻撃のリスクと影響を即座に判断: NDRソリューションにより、政府機関は確保した証拠に基づいて攻撃のリスクと影響を即座に判断できるようになりました。これにより、組織はセキュリティインシデントに迅速に対応し、潜在的な影響を最小限に抑えることに成功しました。

- MTTD と MTTR の短縮: NDR ソリューションにより、政府機関はセキュリティインシデントの平均検出時間 (MTTD) と平均応答時間 (MTTR) を短縮することができました。これはセキュリティインシデントの分析と対応の自動化によって実現されました。遅延が最小限に抑えられ、セキュリティ オペレーション センターの効率が全体的に向上しました。

- 内部トラフィックのセキュリティを強化し、二次プロジェクトを作成する可能性の特定: NDR ソリューションは、政府機関に内部トラフィックセキュリティに関する洞察を提供しました。 これにより組織は改善するべき領域を特定し、二次プロジェクトに優先順位を付け、全体的なセキュリティ体制を強化することに成功しました。

総じて、政府機関は Quad Miners の NDR ソリューションを使用してセキュリティ運用を改善することに成功しました。現在組織は、セキュリティインシデントにリアルタイムで対応できる、より高度で効率的なセキュリティシステムを導入しており、インシデントのリスクと影響を軽減しています。