概要

業界

- エネルギー

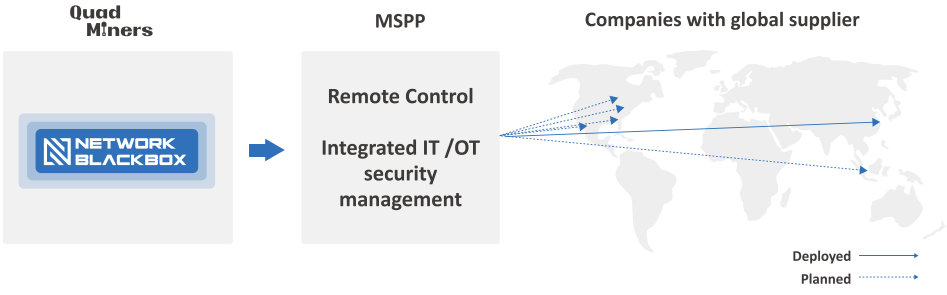
課題

- SOCから検出されたセキュリティ脅威を直接分析することができない
- 脅威の特定と対応時間の遅れ
- 各拠点でのITとOTの可視性の制限
- 脅威に対する一貫性のない監視と対応
- セキュリティ脅威の管理を行うITスタッフの不足

導入効果

- フルパケットに基づく決定的な証拠によるMTTDおよびMTTRの削減
- 少数のセキュリティ担当者との連携で運営可能な、効率的で一貫性のある脅威対応を確立
- ITとOTの両方の領域を可視化

エネルギー企業におけるQuad Minersの Full-Packet NDR Solution



背景

Quad　Minersは最近、世界のバッテリー業界をリードするエネルギー企業にNetwork Detection and Response（NDR）ソリューションを導入しました。生産設備のグローバル化を推進しており、海外と韓国国内の両方に事業を展開している同社は、重要なインフラと運用のセキュリティを確保するために、国内のManaged Security Provider（MSP）企業を頼りに、海外の生産施設にSecurity Operation Center（SOC）サービスを実装しています。
しかし、サイバーセキュリティの脅威の複雑化と高度化に伴い、Industrial Automation and Control Systems（IACS）のセキュリティを強化するためにさまざまなソリューションを検討していました。これは単なるオプションとしてではなく、ゼロトラストアーキテクチャの観点から、Information Technology（IT）領域とOperation Technology （OT）領域の両方に一貫したサイバーセキュリティインフラを実装するための戦略が必要でした。なぜなら、IACSネットワーキングの主流はテクノロジー、特にIACS　OTとITの融合であるためです。Quad　MinersのNDRソリューションは、ネットワーク上に発生した事象のリアルタイムでの可視化、脅威検出機能を備えているとともに、インシデント対応機能ではITとOTの両方の領域をカバーし、サイバーセキュリティ体制の強化と重要なインフラを保護できることから、推奨されるソリューションとして選ばれました。

課題

世界のバッテリー業界をリードする同社は、セキュリティ業務に関するいくつかの課題に直面していました。一つ目は、これまで韓国国内のManaged Security Provider（MSP）企業に依存し、海外の生産施設にSecurity Operation Center（SOC）サービスを提供していたことです。これにより、検出された脅威をSOCから直接分析することができず、脅威の特定と対応時間に遅れが生じ、潜在的なセキュリティインシデントの発生リスクが高い状況にありました。

２つ目は、各拠点のITチームとOTチームの可視性が制限されているため、脅威を常に監視し対応することが困難で、かつ、脅威管理を行うITスタッフの不足によりセキュリティ運用を効率的に管理することができていなかったことです。
これらの課題により、同社はセキュリティサービスの強化と重要なインフラの保護を実現するため、ネットワーク上に発生した事象のリアルタイムでの可視性、脅威検出、インシデントの対応機能を提供できるソリューションを探すようになりました。

ソリューション

Quad　MinersのNDRソリューションは、世界のバッテリー業界のセキュリティ課題の中で、同社にとって理想的なソリューションであることが明らかとなりました。Quad　MinersのNDRソリューションの実装により、同社はネットワーク内のすべての脅威をSOCから直接検出・分析することが可能となり、これまでより速く潜在的な脅威を特定し、対応することが可能となりました。また、フルパケットベースのNDRを導入することで、ITドメインとOTドメインの両方でネットワークを可視化し、脅威への対応時間を短縮、全体的なセキュリティ体制を強化しました。
Quad　Minersは、ModbusなどのICS業界標準プロトコルを特定しました。これはフルパケットデータの分析後、カスタマイズと開発を通じて大手エネルギー企業で使用されるプロトコルが含まれます。さらに、Quad　MinersのNDRソリューションは、脅威の決定的な証拠とシンプルな分析画面を提供し、脅威への対応時間を短縮、日々のセキュリティ運用を効率化しました。重要なインフラを保護するためのリアルタイムでの可視性、脅威検出、インシデント対応機能を提供することで、同社のセキュリティ課題に対処しセキュリティ運用の強化に貢献しました。

導入効果

Quad MinersのNDRソリューションの実装により、世界のバッテリー業界をリードするエネルギー企業のサイバーセキュリティ体制が大幅に改善されました。フルパケットに基づく決定的な証拠により、潜在的な脅威に対する平均検出時間（MTTD）と平均対応時間（MTTR）を短縮することができました。またこのソリューションは、少数のセキュリティ担当者とともに運用できるグローバルな生産施設に対して、効率的かつ一貫性のある脅威対応プロセスの確立にも役立ちました。フルパケットベースのNDR の導入により、ITとOTの両方の領域のネットワークの可視性が向上し、死角が最小限に抑えられ、脅威への対応時間が短縮されました。Quad MinersのNDRソリューションを導入したことで、同社はセキュリティインシデントを迅速に検出して対応できるようになり、全体的なセキュリティ体制が強化され、重要なインフラを保護することが可能となりました。その結果、セキュリティリスクが減少し、運用効率が向上しました。
脅威を迅速かつ効果的に検出し対応することができるQuad Minersのソリューションは、同社のセキュリティニーズに対して効果的かつ効率的であることが証明されました。

なぜエネルギー企業にNDRを導入したのか？

エネルギー企業は、複雑で複数の場所にまたがる重要なインフラをITネットワークに依存して運用しているため、潜在的な脅威を特定し、インシデントに対応することが困難になっています。ネットワークを脅威から保護し、規定に準拠し、アクティビティをリアルタイムで包括的に可視化し、ネットワークパフォーマンスを最適化し、インシデントに迅速かつ効率的に対応することを可能にするNDRソリューションは、同社にとって必要不可欠です。

Quad Miners

Quad Minersは、世界中に高度な脅威検出および対応機能の提供をリードするNDRベンダーです。当社の独自のセールスポイントは、フルパケットキャプチャ機能です。これにより、管理者はペイロードからネットワークトラフィックの詳細を確認し、セキュリティをより強化することができます。他のセキュリティソリューションでは検出されない可能性のある脅威を検出でき、脅威の決定的な証拠を提供し、クライアントの迅速かつ効率的な対応を実現します。Quad MinersのNDRソリューションは、ITおよびOT環境全体でのネットワークの可視性も提供し、死角を最小限に抑え、脅威への対応時間短縮に貢献します。

Quad Minersは、イノベーションと顧客満足度への強いコミットにより、ネットワークセキュリティの強化を目指すクライアントにとって信頼できるパートナーとしての地位を確立しています。Quad Miners のNetwork Blackboxは検出を行うだけではなく、既存のセキュリティインフラとプロセスを活用して高度化するための理想的な地位を確立しています。

NETWORK BLACKBOX

Quad Minersの次世代ネットワークセキュリティソリューションであるNetwork Blackboxは、事故記録全体を分析する航空機ブラックボックスのように、ネットワークトラフィックからすべてのパケット原本を保存し、これを加工することでハッキングなどの攻撃前後をすべて把握し、素早く検知して対応することができます。

Quad Miners

Contact Us

sales_jp@quadminers.com

+81-3-3500-3221