infoblox

活用事例

Askari Bank、Infoblox Threat Defense Advanced でサイバーセキュリティ体制を近代化・強化

概要

Askari Bank は 1992 年 4 月に開業し、パキスタンの大手金融機関の一つに成長しました。

Askari Bank は、個人および法人向けの銀行サービス、ATM、モバイルバンキング、クレジットカード、デビットカードなど幅広いサービスを提供しており、パキスタン全土に 537 の支店を展開しています。同銀行は設立以来、サービス品質の向上、技術と人材への投資、イスラム金融や農業銀行を含む広範な支店ネットワークの活用を通じて成長に注力してきました。Askari Bank のビジョンは、顧客の成功を熱心にサポートし、サービスの品質で顧客を喜ばせることです。このサービスに尽力する上での重要な要素は、銀行の顧客のプライバシーとセキュリティを絶対的に最高のレベルに維持することです。

「さまざまなシナリオを想定して PoC を実施した結果、データの侵入や流出に成功した事例は 1 件もありませんでした。BloxOne Threat Defense が自社の環境で悪意のある活動をブロックする様子を実際に見て、Infoblox ソリューションへの信頼は大幅に高まりました」

Jawad Khalid Mirza
CISO、Askari Bank

課題

新たに出現する脅威に対抗するための、セキュリティ体制強化

世界中のすべての金融機関と同様に、パキスタンの Askari Bank は悪意のあるサイバー攻撃の人気の標的です。強固なセキュリティ体制の維持は長年にわたり Askari IT チームの最優先事項であり、同行はこれまでに、セキュリティオーケストレーション、自動化、対応（SOAR）ソリューションや、長年にわたり信頼してきた Cisco DNS セキュリティ製品を含む、複数のサイバーセキュリティソリューションを導入してきました。Secure Networks 社のコンサルタントと協力する中で、Askari Bank のチームは、DNS 層の脅威が時間の経過とともに進化していることを理解し、DNS テクノロジーの他のオプションを検討することで銀行全体のセキュリティを強化できると考えました。

askaribank LIMITED

「周知のとおり、DNS はセキュリティの観点から設計されていません」と Askari Bank の最高情報セキュリティ責任者である Jawad Khalid Mirza 氏は説明しました。「DNS のオープンアーキテクチャは、DNS が攻撃者の主要な標的となる要因です。金融分野では、こうした脅威は企業からデータを盗み出したり侵入したりしようとする試みとして現れることが最も多くなっています。」

「従来のセキュリティソリューションは、DNS クエリをブロックすることで脅威に対抗するように設計されています」と、PoC の実施に協力した Secure Networks 社の CEO、Asad Effendi 氏は説明しました。「しかし、現在のマルウェア攻撃シナリオでは、不審なトラフィックを単にブロックすることだけで最善のアプローチが成り立つとは限りません」

解決策

BloxOne Threat Defense を活用した高度な DNS セキュリティ

Askari Bank のデータセンターに BloxOne Threat Defense のテストバージョンをインストールし、チームは DNS Messenger とファストフラックス攻撃の特徴を持つ最新のデータ侵入および持ち出し技術を使用して、一連のネットワークトラフィックシナリオを実行しました。「さまざまなシナリオを想定して PoC を実施した結果、データへの侵入や持ち出しに成功した事例は 1 件もありませんでした」と、Khalid Mirza 氏は述べています。「BloxOne Threat Defense が自社の環境で悪意のある活動をブロックする様子を実際に見て、Infoblox ソリューションへの信頼は大幅に高まりました」

BloxOne Threat Defense は、DNS レベルで動作して、他のソリューションでは見逃されるような脅威を検知・表出化し、脅威ライフサイクルの早い段階で攻撃を阻止します。広範な自動化とエコシステムの統合を通じて、SecOps の効率を向上させ、既存のセキュリティスタックの有効性を向上させます。セキュリティ業務全体の管理を SOAR ソリューションに頼っている Askari チームにとって、これらの機能は説得力のある 2 つ目の考慮事項でした。BloxOne Threat Defense の機能と利点の全容が Askari チームに対して明らかになったため、完全な本番環境への展開を進めることが決定されました。

顧客：Askari Bank
業種：金融サービス
場所：パキスタン

取り組み：

- DNS ベースのデータ持ち出し、DGA、DNS Messenger、ファストフラックス攻撃など、分析と機械学習により、データ侵入と持ち出しの手口を防止
- エクスプロイト、フィッシング、ランサムウェア、その他の最新のマルウェアを検出してブロック
- 東西トラフィック監視を通じて、マルウェアの拡散と水平移動を検出
- 特定のウェブコンテンツカテゴリへのユーザーのアクセスを制限し、活動を追跡
- 最も価値の高いインターネット資産に類似ドメイン監視を行うことで、ブランドを保護
- DoH 使用の増加によるリスクを制御：DoH（DNS over HTTPS）ドメインアクセスをブロックし、DoH リクエストを既存の信頼できる DNS に適切に戻す

導入の効果

脅威の検出を迅速化し、インシデント対応時間を短縮

「BloxOne Threat Defense により、当社のセキュリティスタック全体がより効果的になります」と、Askari Bank のセキュリティ・オペレーション・センターユニットの責任者である Umair Shakil 氏は説明しました。「Infoblox ソリューションを既存の SOAR プラットフォームに統合することで、セキュリティスタック内のすべてのツールがリアルタイムのネットワークおよび threat intelligence にアクセスできるようになりました現在、すべてが連携して機能し、広範な自動化を通じて脅威をより適切に特定し、修復できるようになっています」

BloxOne Threat Defense 独自のハイブリッドセキュリティ設計では、クラウドの力を利用して広範な脅威を検出しつつ、オンプレミスのエコシステムとも緊密に統合します。クラウド単独ソリューションに欠けている回復力と冗長性も兼ね備えています。所在地にかかわらず、Askari のチームは、IoT などのデバイス、アプリ、仮想マシン、スイッチポートを、共通コンソールから一元的かつ自動的に保護できます。BloxOne Threat Defense により、Askari チームは、強力で既に利用可能な DNS サーバーを防御の第一線に転換することで、ファイアウォール、IPS、Web プロキシなどの負担がかかっている境界セキュリティデバイスの負担を軽減することができました。チームは、脅威と攻撃者の情報を共有することにより、セキュリティスタックからより多くの価値を引き出し、脅威アナリストとセキュリティ管理者の生産性を向上させることを期待しています。

「BloxOne Threat Defense により、当社の SOC アナリストは、非常に正確なコンテキスト情報に基づいて迅速な意思決定が可能となり、全体的な分析時間が改善されます」と、Secure Networks 社の主任テクニカルエンジニアである Hasan Imam 氏は述べています。「DNS は近年、より顕著な攻撃ベクトルとなっているため、このギャップを埋めるための Askari Bank による積極的な対策と専門性は非常に賞賛されるべきものであり、業界内でセキュリティにおいて先行する方法としての模範を示しています」

「私にとって、Infoblox の BloxOne Threat Defense と同等のレベルの DNS セキュリティを提供しているソリューションベンダーは他にはありません」と Khalid Mirza 氏は結論付けました。「Infoblox との提携により、Askari Bank は DNS インフラストラクチャに必要な保護を確保し、パキスタン全土で同行をご利用されるお客様に安全なサービスを提供するという目標を達成できるようになりました」

Infoblox 株式会社
〒 107-0062 東京都港区南青山 2-26-37
VORT 外苑前 I
3F

03-5772-7211
www.infoblox.com