MICRO FOCUS | VERTICA

お客様事例

Verticaデータ分析プラットフォーム
ArcSight Enterprise Security Manager

Finansbank

Micro Focus® ArcSightとVerticaを利用することで、トルコの銀行大手Finansbankは異常検知を迅速化し、より強固なセキュリティと詐欺防止プロセスを実現しています。

課題

銀行にとっては信用がすべてです。銀行は、金融サービスを利用する消費者や企業といった顧客の信頼を獲得して維持する必要があります。

強固なサイバーセキュリティを確保することは、銀行のビジネスに求められる最優先事項の1つです。

Finansbankにとって、セキュリティの確保は命題となっています。1987に設立されたFinansbankは、トルコの国家機関の1つであり、同国の市民や企業が必要とする金融サービスを提供することで、人々の日常を支える役割を担っています。

Finansbankは、同行のシステムをサイバー犯罪や詐欺から守るため、Micro Focus ArcSight Enterprise Security Manager (ESM) を同行のセキュリティ情報およびイベント管理 (SIEM) ソリューションとして導入したのです。さらに、Finansbankは、サイバーセキュリティ能力を一層強化するために、一歩進んだ施策を講じています。それは、ビッグデータ分析機能を最大限に活用することです。

「Verticaを通じてビッグデータの威力を利用することで、セキュリティ機能を改善できます。」

Finansbank
コンサルティングセキュリティデザイナー
Erdem Alasehir氏

ソリューション

20 ～ 40億行のデータ

FinansbankのIT部門は、Micro Focus Softwareのビジネスプロセス管理ソリューションを複数採用しています。Micro Focus Asset Manager、Service Management、Universal Configuration Management Database、Business Availability Center、Operations Manager、Data Center Automation、Business Service Managementソフトウェアなどです。

Finansbankのセキュリティ組織には異なるニーズがあります。同行のバンキングソフトウェアを人々が使用すると、ArcSight ESMが、約15,000のデータソースから、1日あたり120ギガバイトのデータを収集します。その情報の総量は、20 ～ 40億行に達します。Hadoopに保存されるこのデータは宝の山であり、その活用が同行にとって重要な課題になっていました。Finansbankが望んでいたのは、高度なSQL分析を実行することで、サービスを利用する人々の行動を理解し、無害な行動と、異常値、悪質な可能性がある行動を迅速に判定できるようにすることでした。

FINANSBANK

概要

■ 業界

銀行/金融サービス

■ 所在地

トルコ共和国

■ 課題

銀行のサイバーセキュリティ機能を強化する。

■ 解決策

ビッグデータ分析ソフトウェアを実装し、ユーザー行動のベースライン作成とプロファイリングを高速化する。

■ 成果

+ 15,000のデータソースから1日あたり120ギガバイト以上のデータを収集
+ 20 ～ 40億行のデータに対するクエリを実行
+ レポート作成の改善
+ セキュリティチームによる迅速な異常検出の実現

「Verticaの実装により、コンプライアンスレポートや監査レポートの作成が容易になりました。以前には、大量のレポートの作成に時間と人手がかかっていました。今ではほんの数分で完了します。」

Finansbank
コンサルティングセキュリティデザイナー
Erdem Alasehir 氏

www.microfocus.com

「われわれは、ArcSight ESMを補完する強力な分析ソリューションを探し始めました」と語るのは、Finansbankのコンサルティングセキュリティデザイナーの Erdem Alasehir氏です。「最初はオープンソースのソフトウェアを検討しましたが、オープンソースはあまり使いやすくないことがわかりました。その後で、Verticaデータ分析プラットフォームを紹介されました。」

成果

Micro FocusとFinansbankのセキュリティチームは、Verticaが同行のニーズを満たすかどうかを検証するための概念実証 (PoC) を開始しました。すなわち、Hadoopと統合して、同行のArcSightログファイルに対するクエリを高速化できるかどうかです。PoCは成功でした。「レポートの作成には、ごく短時間しかかかりませんでした」とAlasehir氏は語ります。同氏によれば、概念実証期間中にチームが収集したデータは10億行に及びました。「データトラフィックとプロファイルのベースライン作成を即座に実行できました。これは、Verticaの実装前には不可能だったことです。」

また、チームはVerticaのインストールとメンテナンスが容易であることも高く評価しました。「セキュリティ部門は、データベースアナリストの助けを借りずに、自分たちだけでVerticaを使用することができました」とAlasehir氏は説明します。

複雑なクエリを数分以内に実行

PoCの成功を見たFinansbankは、Verticaの実稼動インスタンスを導入しました。「以前には、当行のセキュリティソフトウェアから収集される大量のデータを処理する方法がありませんでした」とAlasehir氏は語ります。「しかし、Verticaなら容易に処理できます。そして、Verticaは高速です。複雑なSQLクエリの実行に2 ～ 3分しかかからないのです。また、Pythonミドルウェアを開発して、レポート作成を自動化したり、計算を行ってほぼリアルタイムのプロファイルテーブルをVerticaで維持したりしています。この組み合わせは、完璧に機能しています。」

Vertciaの高速性は、きわめて重要な役割を果たしています。それによって、同行は悪意のある行動や詐欺を示す可能性がある異常により早く対処できるからです。これにより、同行はサイバーセキュリティの戦いをきわめて有利に進めることができます。サイバー脅威は常に進化しています。企業が既存のサイバー攻撃手段を無効化しようとしている間に、ハッカーや詐欺師たちは利用できる新しい脆弱性を探しているのです。Finansbankは、複雑なモデリングを迅速に実行する機能を通じて、このような脆弱性にいち早く対処するための手段を手にしました。

「高速で堅牢なデータベースがあれば、制約はもはや想像力の限界だけになります」とAlasehir氏は語っています。「Verticaによるサイバーセキュリティ機能の向上には、本当に満足しています。性能面だけでなく、ユースケースの統合と作成の容易さに関してもです。」

Micro Focus
英国本社
United Kingdom
+44 (0) 1635 565200

米国本社
Rockville, Maryland
+1 301 838 5000
+1 877 772 4450

www.microfocus.com

マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com

www.microfocus-enterprise.co.jp

詳細情報: **Vertica.com**

VERTICA | MICRO FOCUS