CORRELOG®

Case Study

カスタマー： 相互保険会社

ソリューション： CorreLog SIEM Agent for IBM z/OS

業界： 金融・保険

相互保険会社の IT 環境

この大手自動車相互保険会社は、500 台の Windows と UNIX サーバーおよび 1 台の IBM z/OS メインフレームの混在している独立したデータセンターを所有しています。この保険会社は現在、セキュリティー情報およびイベント管理 (SEIM) のために世界規模のネットワーク管理ソフトウェア・ベンダーとマネージド・サービス・セキュリティー・プロバイダー (MSSP) を使用しています。

導入前の課題

U.S. 東部でサービスしているこの大手相互保険会社は、大手の MSSP および世界規模のネットワーク管理ソフトウェア・ベンダーとの提携を通じて、SIEM ソリューションの 3 分の 2 を既に所有していましたが、これらのシステムのどちらもカスタマーのメインフレームからリアル・タイムにセキュリティー・イベント・メッセージを受け取ることができませんでした。

この相互保険会社は、提携することが容易なだけでなく、非常に迅速にソリューションを導入し設定できるメインフレームのセキュリティー・プロバイダーと一緒に、SIEM ソリューションを完成する必要がありました。

CorreLog が何故選ばれたのか

CorreLog は、30 年以上に遡るメインフレーム技術の分野の中で専門知識を持つメインフレームの SIEM 業界のリーダーとしての位置にいます。この相互保険会社はメインフレームの SIEM コンポーネントについて、柔軟性のあるそして使いやすいソリューションを必要としました、そして CorreLog が選ばれたソリューション・ベンダーでした。この相互保険会社はまた、複雑で異機種環境のあるデータセンターの範囲内での既存技術を使って、仕事をしている経験が豊富なベンダーと提携することが必要でした。CorreLog は、IBM QRadar、HP ArcSight および RSA Security Analytics との統合を認定されています、それらはまた説得力のあるさらに良いことでした。

SIEM Agent for z/OS を使って、CorreLog は、この会社の SIEM の難問を、下記によって解決することができました：

1. メインフレーム・データを保護することに関連する RACF、ACF2、Top Secret、DB2 アクセス、および重要なユーザーの活動が提供しているリアル･タイムなメインフレーム・メッセージを、クラウドベースのシステムに提供すること。

2. 2 ~ 3 時間以内に、この相互保険会社が彼らのセキュリティー・オペレーション・センター (SOC) でイベント・ログを見ることができたこと。これは競合するソリューションと全く対照的です。その競合するソリューションはデータの配信を始めるために数日または数週間掛かる可能性があります。

3. 既に配置済みの既存のシステムと通信してデータを交換すること。同時に、3 つのシステムがリアル・タイムの可視性をこの相互保険会社に提供するために、ユーザーとシステムの活動についてのすべての情報を使用することができます、それはデータ・ロスのリスクを最少化するために必要です。

4. メインフレーム・データのすべてを集約し、完全な監査証跡を作成すること。命令順守を満たすために必要な仕事量を単純化すること。メインフレーム・データのすべては一元的に置かれそして検索することが容易です。

CorreLog を使用する前とその後：他のシステムと協力して機能すること

CorreLog SIEM Agent for z/OS は、規範の順守を満たすリアル・タイムな監視と監査証跡を提供することにより、既存の SIEM 戦略を強固にすることができました。そのMSSP は既にファイアウォール管理サービスと 24x7 監視を提供していました。それはログをネットワーク管理ソフトウェア・ベンダーのクラウドベースの SOC へ送信します、そしてその SOC はまたメインフレームを含むデータセンター全体にわたり 24x7 のネットワーク監視を提供しています。CorreLog SIEM Agent for z/OS は、SIEM ソリューションのパズルで欠けている部分、リアル・タイムなメインフレームのセキュリティー・ログ管理を提供し、そして集約したメインフレーム・イベントをクラウドのログ管理システムに送信します。

このシステムを実装する前は、SIEM のデータ・プールは多種多様な保存場所の数 100 万のイベント・ログで構成されていました。現在は、CorreLog SIEM Agent for z/OS を使用することにより、データはフィルタリング機能を備えて、すべて一元的に置かれています。イベント・フィルターは、情報セキュリティーの意思決定支援のために SIEM へ関連するデータのみを送信することによって、処理能力が最適化されるように支援します。その保険会社のセキュリティー・リソースは、今では、膨大な量のデータを調べる無数の時間を無駄にする必要がありませんーその会社は、セキュリティーとコンプライアンスのために再調査と管理する必要がある適切なデータに気を付けているだけです。

(次項に続く)

(前項からの続き)

このことは、IT 部門のかなりの時間を節約し、IT 管理者が他の喫緊の課題により多くの時間を配分できるようにします。

3 つのシステムを一緒に統合することは、もう一つの大きな恩恵をもたらします：ファイルのすべてを集約することによって、その相互保険会社が監査人に問われたときに規範順守を立証することがより簡単になっています。現在は、たった一人のセキュリティー管理者が、MSSP のダッシュボードに 24x7 の間投入している生きたメインフレーム・データを含む、すべてのデータを検索し検査することができます。そして、さらに重要なことは、彼らはメインフレーム上の異常挙動のアラートを、夜間または週次のバッチ・レポートからではなく、それらのイベントが発生しているときに受け取ります。

この保険会社 の今後

この相互保険会社は現在、データセンター内のハードウェアのいくつかを更新する暫定的な計画と共に、CorreLog、MSSP およびネットワーク管理ベンダーを使った運用モデルのコースを継続する計画です。現在では、より少ない人員でセキュリティー・イベント管理を実施するため、この相互保険会社は IT スタッフをより良く活用することができます。データセンターでの生活はより円滑になり、そしてこの相互保険会社は IT サポートに専念する他のエリアに、より多くのリソースを向けることができます。

CorreLog 社について

CorreLog 社は、クロス・プラットフォームの IT セキュリティー・ログ管理とイベント・ログ相関についての有力な独立ソフトウェア・ベンダーです。次は CorreLog ソリューション・スイートの主力製品です：

- CorreLog SIEM Agent for IBM z/OS™
- CorreLog Visualizer for IBM z/OS™
- CorreLog SIEM Correlation Server™
- The Windows® Toolset Syslog Converter

CorreLog SIEM Correlation Server は、その分野で最高のイベント相関エンジンを使って企業のログ管理を提供します。CorreLog SIEM Server は Windows、UNIX、および Linux プラットホームにわたって稼動し、そしてユーザー活動のログとシステム･イベント・データの収集と関連付けによって、異常挙動とセキュリティー・ポリシー違反を識別することを支援します。これらの CorreLog ソリューションのそれぞれは、PCI DSS、HIPAA、IRS Pub. 1075、SOX、GLBA、FISMA、NERC および多くの他の規制当局による規準によって明記された基準を順守するためにデザインされています。

SIEM Agent for IBM z/OS は、メインフレームの LPAR に常駐し、リアル・タイムに、RACF、ACF2、Top Secret および DB2 アクセスのようなメインフレーム・セキュリティー・イベントを、企業向け SIEM システムのために、分散型の Syslog 形式に変換します。拡張されたメインフレームの可視性を必要とする企業のために、企業向け SIEM を利用できないユーザーのために、CorreLog は Visualizer for z/OS を提案します。そしてそれはあらゆる標準的なウェブ・ブラウザーを通して生きたメインフレームのセキュリティー・ダッシュボードを提供します。

株式会社 ブロード
東京 ：〒100-0014　東京都千代田区永田町 1-11-30
　　Tel 03-6205-7463　（代表）
大阪 ：〒531-0071　大阪市北区豊崎 3-4-13 ｼｮｰﾚｲﾋﾞﾙ 6F
　　Tel 06-6375-3775　（代表）
Email: broad@broad-corp.co.jp
URL　: http://www.broad-corp.co.jp