CASE STUDY

カスタマー

Rechenzentrum Region Stuttgart GmbH (RZRS)
シュツットガルト地区コンピューター・センター

ソリューション

CorreLog Correlation Server
CorreLog Agent for IBM z/OS

業界

ドイツ連邦共和国の公共/政府機関向け IT サービス・プロバイダー

RZRS の IT 環境

- IBM System z メインフレーム・シリーズ
- 約 400 台の UNIX と Linux サーバー
- 約 400 台 Windows サーバー
- 複数のデータベースおよびアプリケーション・サーバー
- RZRS は、Windows, UNIX およびメインフレーム・エージェントを使って 2 台の CorreLog サーバーを稼動しています。

導入前の課題

ドイツ政府は 2012 年にすべての国民に ID カードの発行を開始しました。RZRS は、この重要な IT 業務を支援するように要請されました。 ドイツ政府は RZRS がパフォーマンスや可用性に関する SLA を着実に実行することと同時に、政府機関の厳しい要求の順守に対処することを命じました。

RZRS は CorreLog に問合せました。配備のためのその他の要件は、次の通りでした：

- RZRS は、z/OS と分散環境の全域で、安全な一元化されたログ管理ソリューションを提供する必要がありました。
- RZRS は、ネットワーク、データベース、メインフレーム、UNIX/Linux システムから最重要なパフォーマンスと可用性のログを提供する必要がありました。彼らはすべてのデータをセキュリティー・オペレーション・センターに振り向けることは必要ではありませんでした。従って、パフォーマンスの許容レベルでネットワークの処理能力を維持するために、意味のあるデータのみを相関し送信する能力が重要でした。
- RZRS が導入するシステムは、緊急の解決措置のために、サービスデスク・ソリューションへのヘルプデスク・チケットを発行する機能が必要でした。

CorreLog が何故選ばれたのか

RZRS の導入は、Allen Systems Group (ASG)と CorreLog 社間の共同プロジェクトでした。ASG は、別の IBM メインフレーム製品－ASG T-MON と呼ばれる遠隔監視システムーを使って RZRS のニーズを満たしていました。

ASG の担当者が顧客訪問をした際に、RZRS はログ管理とセキュリティー情報およびイベント管理（SIEM）のプロジェクトへの支援を求めました。ASG は RZRS に対して ASG と CorreLog の関係を知らせ、初期の顧客エンゲージメントが開始しました。ほんの数週間のうちに、RZRS はドイツ政府から要請された SIEM プロジェクトのために、CorreLog Correlation Server と CorreLog AGENT for IBM z/OS を選択しました。

KDRS
RZRS

*“**CorreLog** は、私たちがデータセンターのセキュリティーを管理するために使用していたリソースを大幅に削減することができました。*
***CorreLog** 導入前は、多くのシステムのいたる所にデータを書き込んでいる多くのリソースを所有していました、そしてリアルタイムでメインフレーム・データへのアクセスはありませんでした。”*

***-RZRS** 最高技術責任者*

CORRELOG®

CorreLog が満たした要件

データ（国民の身元証明）の重大な特性のために、RZRS は単に脅威の検出のためだけでなく、国家によって定められた政府機関の法令順守のためにも、一元化されたログ管理システムを必要としていました。とても広範囲の業務を管理する SIEM システムはまた、非常に高速でログ・データを収集するという高負荷にも対処する必要がありました。

CorreLog Server と CorreLog AGENT for IBM z/OS は、この作業負荷に対処するための機能を提供しました。

CorreLog の導入結果

- 迅速な配備と比類のない機能性 ー CorreLog AGENT for IBM z/OS を備えた CorreLog Server は、数週間足らずで導入されました。他の競合製品は、リアルタイムの z/OS のログ・データを提供できませんでした、そして彼らは配備のために数ヶ月を見積もっていました。
- 一元化されたログ管理システム ー CorreLog 導入前は、RZRS は、複数のシステムのいたる所に数千のログ・メッセージを書き込んでいる複数の IT リソースを所有していたので、これは成功への鍵でした。CorreLog 導入後は、1 つの IT リソースで 1 つのシステムを管理することができました。
- 自動化されたヘルプデスク・チケットの作成 ー メッセージのグループが、潜在的な侵害に対するシステム警告を示すために関連付けられている場合、CorreLog は、迅速に調査するためにセキュリティー管理者へ、自動的にヘルプデスク・チケットを発行することができます。
- CorreLog AGENT for IBM z/OS は、z/OS システムからそのまま RZRS のセキュリティー・オペレーション・センターへ、Syslog メッセージを配信するために、業界唯一のリアルタイムの SMF メッセージ・コンバーターを提供しました。
- CorreLog AGENT for IBM z/OS は、ユーザやシステムの挙動に関連した次のイベントタイプを「監視」することができます：RACF、TSO ログオン、プロダクション・ジョブの異常終了、TCP/IP 接続、FTP ファイル転送、さらに ACF2 および DB2 データベース・アクセスなど。
- CorreLog AGENT for IBM z/OS はまた、CorreLog の dbDefender™ 製品の DB2 監視を提供しました。dbDefender は、データセンターのセキュリティー違反を示すこともあり得る、DB2 に関連している特権ユーザの活動およびその他の活動に関して、DB2 を監査します。
- 高速インデックス機能 ー CorreLog Server は、1 秒以内で 1 テラバイトのデータを検索することができる独占所有権のある Google タイプの高速インデックス方式を使用しています。
- CorreLog の高速メッセージ受付機能は、1 秒間に 10,000 メッセージ以上の集中的なトラフィックを処理することができます。

CorreLog 社について

CorreLog 社は、優れた相関機能を兼ね備えたセキュリティー情報およびイベントの管理（SIEM）ソリューションを提供しています。CorreLog の主要製品、CorreLog Correlation Server は、ログ管理、自動学習機能、ニューラル・ネットワーク技術、独占所有権のある意味相関技術および高度に相互運用可能なチケット発行とレポーティング機能を、固有のセキュリティー・ソリューションにまとめたものです。CorreLog は、セキュリティー脅威を指摘するためにユーザの活動とイベント・データを収集し、索引化しそして関連付けすることで、ネットワーク攻撃、不審な行為およびポリシー侵害を自動的に識別しそして対応します。そしてそれは、組織が規範順守違反、ポリシー違反、サイバー攻撃および内部脅威に迅速に対応できるようにします。

RZRS 社について

RZRS は、シュツットガルト地域に重点を置いた IT サービス企業です、そして同社のそこでの市場占有率はほぼ 100%です。40 年以上の経験を持つ同社は、地方自治体の部門の特殊要求を熟知しています、そして専門的サポートを提供します。IT の問題を中心にした総合的なケアは、コストがかからない利用を可能にし、そして同時に、円滑な運用および一貫した効率的な体制を確保します。

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