USE CASE

SIEMを最適化する

syslog-ng by Quest

syslog-ng™ Premium Edition

を使えば、企業は自社の IT 環境全体からログメッセージを収集、フィルタリング、標準化、転送、保存することができます。

syslog-ng™ Store Box™ (SSB)

は、syslog-ng Premium Edition の強みを活かした高信頼性ログ管理アプライアンスです。

- syslog-ng Store Box について知る
- 評価版ダウンロード
- お問合せ

SIEM(Security Information and Event Management) ソリューションは多くの企業の IT セキュリティ戦略の核心となっていますが、SIEM を運用して維持をしていくには多額の費用がかかる場合があります。
SIEM を最適化することで経費を削減してパフォーマンスを向上させることができます。

課題

ログデータ収集
ログは、多くの時代遅れなシステムやアプリケーションを含む幅広い種類のデバイスで作成されるため、企業は様々なフォーマットで受信したログデータの意味を解析することに四苦八苦しています。

データの整合性
SIEM ソリューションの多くは、データ解析に特化しています。
そのため、ログデータの見落しに繋がる信頼できるログ収集、転送、保管においては不十分です。

パフォーマンス
巨大なネットワークでは、様々な種類のデバイスとアプリケーションから大量のログが生み出されます。多くの SIEM ソリューションにおいては、データが多すぎて検索に時間がかかるようになります。

拡張性の問題
IT ネットワークでは、ログソースの量もログデータの量も常に増加し、現在のソリューションの拡張は困難で高価なものになります。

高価な TCO
SIEM を購入して導入し、維持していくことは、費用の点からも社内のリソースの点からもしばしば高くつきます。

ソリューション

前処理を分散
syslog-ng Premium Edition のアプリケーションは、中央に格納されるログデータのサイズと複雑さを軽減するために、クライアント上のデータを比類のない速度でフィルタ、解析、再書き込み、分類することができます。また、分析する必要の無い不要なログメッセージをフィルタリングすることで SIEM の負荷を軽減し、処理能力とライセンスコストの両方を節約できます。

信頼性の高いログ転送
syslog-ng Premium Edition および syslog-ng Store Box はクライアントから中央ログサーバーへのデータ転送を次の機能を利用することによりメッセージの損失をゼロにできます。
TCP や高信頼のログ転送プロトコル（RLTP™）によるログ転送、クライアント側のディスクバッファ、およびネットワーク障害時のクライアント側のフェイルオーバー。

集中型コレクション
syslog-ng Premium Edition は、Linux、UNIX、HP、IBM、Microsoft Windows、および Solaris の様々なバリエーションを含む 50 以上のプラットフォームの上にインストールすることができます。

改ざん困難なログ転送とログの保存
syslog-ng PremiumEdition と syslog-ng Store Box は、ログの転送およびログストア（暗号化され、タイムスタンプされたログファイル）のために、SSL/ TLS 暗号化を使用しています。

簡単且つわかりやすいライセンスモデル
syslog-ng PremiumEdition と syslog-ng Store Box のライセンスは、処理されたデータの量ではなくログを送信するホストの数に基づいており、ログデータの総量や速度の増加によってコストが増加することはありません。

メリット

SIEM のより良いパフォーマンス
ログデータのサイズと複雑性を減少させることで、大幅に検索時間を改善します。

より質の高いデータ
改ざん防止されたセキュアなログは、そのままのフォーマットで、法的手続において使用することができます。

SIEM 分析で高まる信頼性
ログが欠落、改ざんされていないことが保証され、調査結果の信頼性を向上させます。

費用対効果の高い拡張性
ログ管理インフラストラクチャを拡張するとき、予測可能なホストベースのライセンスモデルでより容易に計画できます。