securonix

データシート

NXLog Management

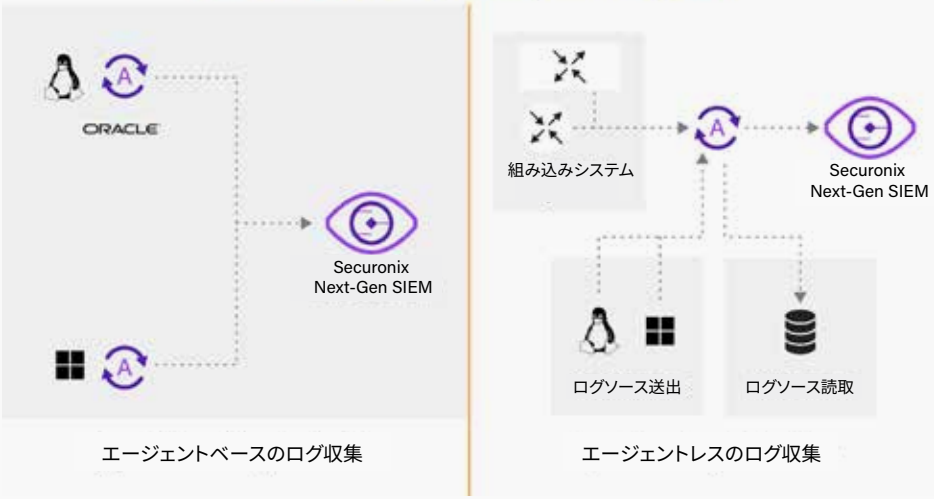
究極のログ収集と一元化されたログ管理

一元化されたログ収集による脅威の検知と対応の強化

組織は、SIEM ソリューションに投資して、セキュリティ運用の改善、リスク管理、インシデント対応の迅速化、テジタルフォレンジックを行っています。しかし、ログ収集が不十分であることが原因で、SIEM が適切な相関処理や分析をできなければ、組織は SIEM への投資を有効活用できません。

Securonix と NXLog のインテグレーションは、高い柔軟性と信頼性がある、ログ収集および転送を行うソリューションを提供します。NXLog はスケーラブルなログ管理システムであり、効率的、安全、かつ信頼性の高い方法で口グ収集を行います。また、データの構造化、フォーマット、フィルタリングを行います。ほとんどのオペレーティングシステムに対応し、他のツールでは取り扱わないデータソースに対応できるため、組織内のあらゆるシステムの可視性が向上します。

マルチプラットフォーム環境におけるログ管理サポート



NXLog による高性能なログ収集の真価

NXLog は、データを一元的に取り込み、フィルタリング、分類、変換、正規化をより簡単に行い、ログ管理を合理化する高性能なログ収集システムです。

IT セキュリティの運用を自動化

複数のログソースからデータを収集し、複数の宛先に転送する機能を持つ単一の製品であるため、ログ収集を容易にします。Securonix はホストレベルでのイベントログ解析を行うため、ログ収集時の転送と管理のコストを削減できます。

転送中のログのリスクを低減

Securonix と NXLog のインテグレーションを行うことにより、Securonix Next-Gen SIEM へのログ転送を、安全かつ確実にします。

データに対するコンプライアンスを維持

ファイルの整合性監視は、重要なファイルやフォルダへの変更監視と検知を行うことで、コンプライアンスを支援します。

NXLogを使用したログの収集

マルチシステム環境でデータを収集できる、スケーラブルなログシステムを実現します。

一元化されたログ収集管理

柔軟なログ収集

単一のテクノロジーで、多種多様なログソースからのデータの取り込みをシンプルに実現できます。

エージェントベースのログ収集：NXLog は、Windows イベントログ、Linux カーネルログ、Android ログ、各種システムのローカルシステムログなど、プラットフォーム固有のデータソースに対応し、エージェントとして機能します。

エージェントレスのログ収集：エージェントのインストールをサポートしていない組み込みシステムやレガシーシステム（ルーターやスイッチなど）の場合、それらシステムのネイティブプロトコルを使用して、NXLog インスタンスにログデータを送信します。

ログの集約：NXLog は、組織全体のログ収集とフローを管理します。ログ取集の一元化により、ログ収集とフロー管理が効率化され、ログデータの一貫性が保たれます。

コンプライアンス要件の遵守

セキュリティ対策における検知とコンプライアンス

必要なログメッセージを Securonix Next-Gen SIEM に取り込むことで、コンプライアンスと標準にかかる要件を遵守できます。

コンプライアンス：収集した監査ログの監視を行い、Windows レジストリを含む、サポート対象のすべてのプラットフォーム上のファイルとディレクトリへの変更を検知します。

ファイルの整合性監視：NXLog のファイル整合性監視は、潜在的な不正な変更など、アセットに対するアクティビティに関するアラートを上げます。Securonix Next-Gen SIEM によるセキュリティ監視において、NXLog のイベントログを取り込むことにより、重要アセットでのマルウェア発生やマルウェアによる悪意のある変更といった、インシデントへの対応を支援します。

リスクの低減

転送するログのリスクを低減

単一のソリューションで多数のデバイスからログを収集し、整合性を失うことなくログを転送できます。リスクを低減するため、このソリューションでは、圧縮、プロトコルレベルで ACK を使用した応答、バッチ処理による信頼性の高い転送を行います。

SSL/TLS データ暗号化：攻撃者によって転送中のログデータが変更または閲覧されるのを防止するため、転送するログデータを暗号化します。NXLog は、SSL/TLS によるデータ暗号化、多くの入出力モジュールのサポート、強力な認証、メッセージの整合性と機密性を提供します。

データセキュリティ：特別な権限を設定し、ログ転送をセキュアにします。

NXLogで動作するSecuronixログコレクターマネージャー

NXLogを搭載したSecuronix Nex-Gen SIEMの詳細については、
www.securonix.com/request-a-demo でお申し込みの上、デモをご覧下さい。