障害発生率が限りなくゼロの セキュリティ監視サービスを提供

「包括的な脅威の検出と可視化」&「セキュリティ運用」を最大限に効率化するサポート&セキュリティサービスの安定したインフラをOne Identity SSBで実現

お客様：
テクマトリックス株式会社

業 種：
ソリューション販売、IT サービス提供

国：
日本

従業員数：
1,086名（連結・2019年3月末現在）

Webサイト：
www.techmatrix.co.jp/

チャレンジ

日々巧妙化、高度化するサイバー攻撃に対するセキュリティサービスの高品質化と需要拡大に応えるため、従来のセキュリティ監視サービスを刷新し、新たなマネージドセキュリティサービスを構築。

ソリューション

テクマトリックスでは、「包括的な脅威の検出と可視化」&「セキュリティ運用」を最大限に効率化するサポート&セキュリティサービス「TechMatrix Premium Support powered by TRINITY」（以下、TPS）を新たに提供。「イベントログ（Syslogを含む）の超高速&大量処理と、高いコストパフォーマンス」という開発テーマを実現するために、One Identityの高速・高信頼ログ管理アプライアンス「syslog-ng Store Box（SSB）」を採用した。

利 点

- セキュリティ関連のイベントログを確実に収集し、SIEMに超高速で転送。
- データベースクエリによりイベントログが取得可能で、分析やフィルタリングまでを実行可能な、マネージドセキュリティ機能を提供。
- きわめて高い可用性と信頼性のサービスを、省コストで実現。
- 高度なセキュリティ対策を担保する仕組みを提供。

「サービスインして以来、
障害の発生率がゼロに保たれています。
これほどアプライアンスが
安定しているのは驚きでした。
また、現在最大で約２万イベント／秒の
トラフィックを処理していますが、
まったく遅延などがなく余裕のある
パフォーマンスを発揮しています」

テクマトリックス株式会社
セキュリティ研究所 所長
佐山 享史 氏

世界の最先端ソリューションや自社開発のIT サービスを提供しているテクマトリックス株式会社(以下、テクマトリックス)。同社のTPSの特長は、セキュリティ製品の販売から構築、保守サポートと合わせ、機器運用やセキュリティ監視までをトータルにワンストップで提供することだ。この中心となっているのが、高機能アプライアンス「One Identity SSB(syslog-ng™ Store Box)」。パワフルかつ大容量のSyslog取得・転送機能が、可用性と信頼性に優れたマネージドセキュリティサービスを可能にしている。

ニーズに応えた監視サービスを立ち上げ

マネージドセキュリティサービス(以下、MSS)分野で、大きな実績を持つテクマトリックス。同社 セキュリティ研究所 所長 佐山享史氏は、セキュリティ監視サービスの需要の拡がりとあわせて、高い品質が求められる傾向が強まっていると指摘する。「そこで新たに立ち上げたのが、TPSです。複数のセキュリティ製品の相関分析による統合監視と最適化した機器運用を低コストで提供しますので、セキュリティ強化のみならず、セキュリティ運用の効率化とコストダウンが実現できます」。

加えて、EDR製品を活用したインシデントへの初動調査と初動対応までをオプションサービスで提供している点も特長だ。

採用の決め手は「超高速」「大量処理」そして「高いコストパフォーマンス」

TPSの開発では、「高スループットで、クラスタによる冗長化が実現可能」がテーマになった。MSSの需要拡大につれて企業のデータ活用も活発化していく。膨大なイベントログを確実に取得し超高速で処理する上で、高可用性・耐障害性は必須の要件だ。「中でも、セキュリティ関連のイベントログ(Syslog)を確実に取得できること。そのログをSIEMに高速に転送できることの2つに挑戦しました。この要件を満たすソリューションが、One Identity SSBだったのです」。

採用の最大の決め手は、イベントログ取得から転送のプロセスを、大幅に効率化・簡素化できる点だ。「ファイアウォールから生成されるトラフィックログは膨大ですが、One Identity SSBのタグ付け機能を使えば、リアルタイムな分析が必要なログと不要なログを仕分けられるので、処理工程やデータベース構成をシンプルに効率化できるのです」。

余裕の高速トラフィック処理能力と、限りなくゼロに近いトラブル発生率を実現

One Identity SSBの最大のメリットは、障害の発生率がほぼゼロな点だ。佐山氏は、「これほどアプライアンスが安定しているとは、私自身の経験に照らしても予想以上でした」と語る。高トラフィック時の処理能力も期待通りだった。現在、最大で約2万イベント/秒のトラフィックがあるが、遅延などはまったく発生していない。イベントログの仕分けやタグ付け処理によるレイテンシーもない。One Identity SSBのインデックスエンジンは、最大で毎秒10万メッセージまで持続的に収集・インデックス化が可能だ。加えて、ハードウェアによるクラスタ構成が組めることも機器運用を行う上で非常にメリットがあると語る。「障害が起きにくい機器でも、必ず不具合が発生します。SSBではハードウェアでクラスタ構成を組めるため、障害発生時のリスクと負荷を減らすことができていると考えています」。

イベントログの収集・転送の際にフィルターをかけて、お客様の特性にカスタマイズしたログ分析が行えるのもOne Identity SSB ならではの特長だ。「syslog-ngサーバーで、こうしたフィルタリング機能を備えている製品は非常に珍しい。お客様本位のサービスを実現する上でOne Identity SSBは最適の選択でした」。

マネージドセキュリティサービスの未来を先取りする取り組みを推進

テクマトリックスでは今後、現在のTPSのサービス規模のさらなる拡大を検討中だ。ユーザーの増加に合わせて、クラスタ構成台数の追加も含めたシステム拡張と、サービス内容の強化・充実を図っていきたいと佐山氏は語る。「もう一つの目標は、EDRの運用の自動化です。迅速な対応が求められるEDR運用の最適化においてもOne Identity SSBを活用していきたいと考えています」。

近い将来、IoT機器の普及などでログ量は爆発的に増大し、この領域のセキュリティ監視が非常に重要な課題になるのは確実だ。「当社も、そうした時代の要求に先駆けたMSSをいち早く提供していきたい」と意気込む佐山氏。テクマトリックスの目指す「一歩先のマネージドセキュリティサービス」を、One Identity SSBが支えていく。

One Identityについて

クエストソフトウェア社の提供するOne Identityは、ログ管理および特権アクセス管理(PAM)のソリューションです。この製品を利用することによって、組織の中にアイデンティティ中心のセキュリティ戦略を導入することが可能になります。その導入形態も、オンプレミス、クラウド、両者のハイブリッドなど環境を選びません。アカウント管理、IDガバナンスと管理、特権アクセス管理などの機能によって、ユーザーやシステム、データを選ばない、セキュアなアクセス環境を実現できます。

© 2020 One Identity LLC ALL RIGHTS RESERVED. One Identity、および One Identity ロゴは、米国およびその他の国における One Identity LLC の商標および登録商標です。One Identity の商標の完全なリストについては、当社の Web サイト(www.oneidentity.com/legal)にアクセスしてください。その他すべての商標、サービスマーク、登録商標および登録サービスマークは各所有者に帰属します。