Press Release

2022 年 7 月 6 日
丸紅 IT ソリューションズ株式会社

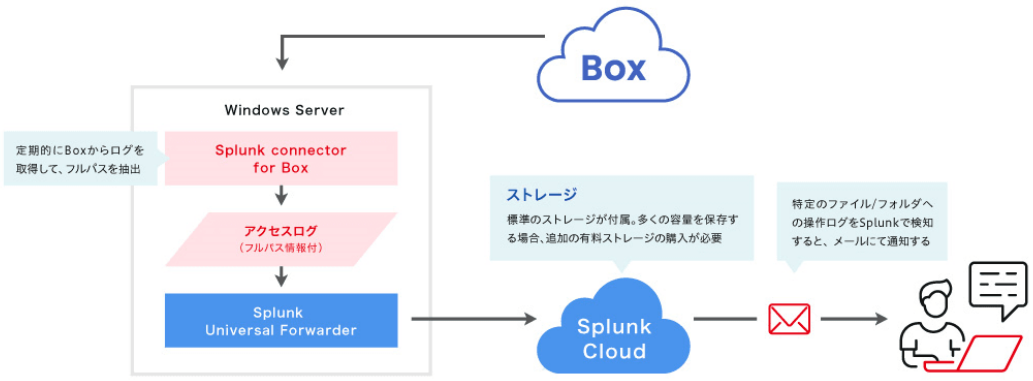
Box ログをフルパスで抽出し、特定操作のログを検知する
「Splunk connector for Box」販売開始

丸紅 IT ソリューションズ株式会社（本社：東京都台東区、代表取締役社長：徳田 幸次 以下、丸紅 IT ソリューションズ）は、エンタープライズ・コンテンツ・マネジメント・プラットフォーム「Box」と連携するエコソリューションとして、「Splunk connector for Box」の提供を開始しました。

丸紅 IT ソリューションズは Box の一次代理店として多数のエコソリューションを開発・販売し、Box のライセンスや導入支援とともにお客様に提供しています。そのなかで、情報セキュリティの脅威に直面している多くの企業からの声を受け、2021 年に通信・セキュリティログの監視・管理ツール「Splunk」の代理店契約を締結しました。Splunk は、ゼロトラストを構成するアーキテクチャの中で監視やログ収集・分析といった SIEM の役割を担うソリューションです。企業に眠るマシンデータを活用し、可視化および検索を実現します。Splunk のアドオン機能を利用することで、Box や Okta などクラウドサービスのログを収集して活用することが可能になります。

「Splunk connector for Box」は、Splunk に転送する Box ログ情報を出力するためのエコソリューションです。
Box のログを Splunk に連携し、たとえば外部共有アクションをリアルタイムで検知する仕組みを構成する場合、通常、ログには当該ファイル名と直下のフォルダ名のみが出力され、ネストされているフォルダ名が表示されません。そのため、同一の名前のファイルが存在する場合、どのフォルダで行われた操作なのか特定することが不可能という課題が生じます。

そこで開発したのが、Box のフルパス情報を抽出する「Splunk connector for Box」です。
Box テナントより 75 分前～60 分前の Box ログ情報を 15 分間隔でフルパスにて抽出して CSV 出力し、Splunk に連携します。これにより特定のファイル・フォルダへの操作ログを Splunk で検知させ、Splunk の標準機能であるアラート設定を利用してメール通知する運用が実現します。



Box の仕様上、Box アクティビティログの記録が最大で 1 日程度遅れることがあります。連携遅延が生じて 15 分間隔処理で取得できず Splunk へ転送ができなかった場合は Box ログを翌日に検査・抽出・転送するための処理が実装されています。
外部共有アクションの他、大量ダウンロードの検知や、特定のフォルダでのイベントログの生成などのユースケースでも利用可能です。

「Splunk connector for Box」の価格や詳細については、紹介サイトのお問い合わせ窓口よりお問い合わせください。

■本サービスに関する詳しい情報は、クラウドベースのコンテンツ管理プラットフォーム Box の紹介サイトおよび「Splunk connector for Box」の紹介サイトをご覧ください。
https://www.misol-box.com/solution/splunkconnectorforbox/

【丸紅 IT ソリューションズ株式会社について】
丸紅 IT ソリューションズは、丸紅グループ向けならびにエンタープライズ向けに、IT コンサルティング、業務システムやセキュリティ基盤の構築、システムの運用設計、各種クラウドサービスなどの事業を展開しています。確実なプロジェクト管理力と IT 基盤構築力、運用設計力で、開発プロジェクトを成功に導き、お客様のビジネス革新を実現します。

以上

<お客様のお問い合わせ先>
丸紅 IT ソリューションズ株式会社
ソリューション事業本部 ソリューション営業部 電話：03-4512-3333
ホームページ: https://www.misol-box.com/