DocuSign

Datasheet
Monitor

アクティビティをリアルタイムで監視し、機密文書への不正アクセスを検出

不正アクセスやサイバー攻撃から機密情報を保護することは、組織にとって重要な課題です。

ドキュサインは、米国や EU を含む世界中の厳格なセキュリティ基準を満たしていますが、契約書など機密文書の安全性は、各組織におけるクレデンシャル管理および運用の整合性に委ねられています。

DocuSign Monitor

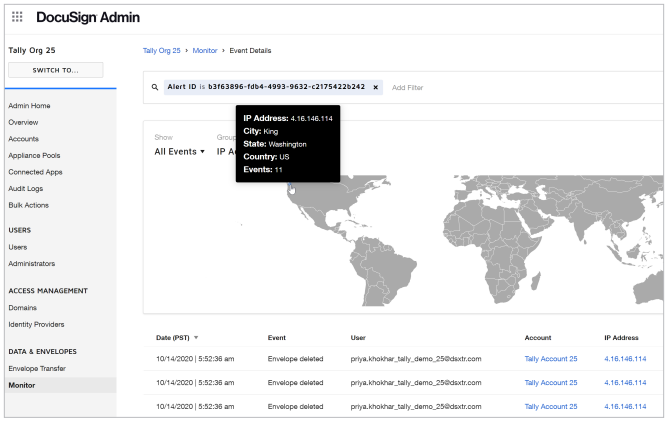
DocuSign Monitor はサイバー攻撃等から合意・契約文書を守るために、高度な分析を用いて DocuSign eSignature に関連するウェブサイト、モバイル、さらには API アカウントのアクティビティを監視し、組織のセキュリティ運用を強化します。

- ルールに基づいた警告で社内外の潜在的な脅威を検出
- 詳細な情報にすぐにアクセスしてインシデントの原因を究明
- サイバー攻撃等の脅威が確認された際に迅速な対応が可能

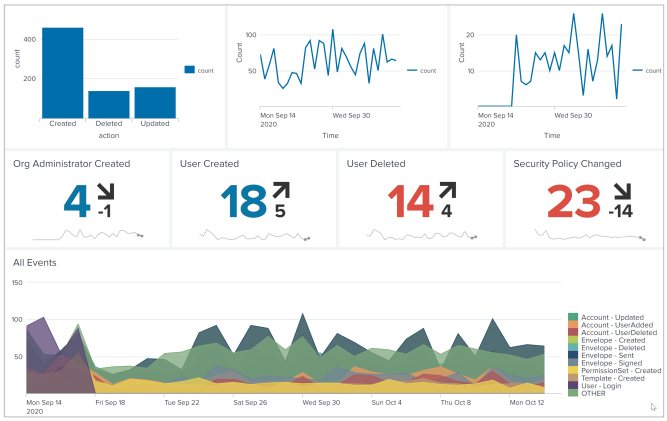
代表的な不正アクティビティを検出する組み込みアラートを使い、40 種類以上のイベントをリアルタイムで監視します。ドキュサインの豊富なテレメトリには、IP アドレス、位置、履歴など詳細な情報が含まれており、インシデントを効果的に調査できます。セキュリティチームや管理者が準リアルタイムの情報を入手することで、重要な文書に攻撃があった場合でも、被害が拡大する前に、脅威を軽減し解決するための対応策を迅速に決定することができます。

Monitor API

DocuSign Monitor API から、既存のセキュリティスタックや、Splunk、Tableau、Power BI などのデータ可視化ツールにアクティビティの情報が直接送信されます。API を活用することで、セキュリティチームはダッシュボードや警告を特定の要件やセキュリティ規制に合わせてカスタマイズできます。



DocuSign Monitor は、DocuSign Admin Center 上にある警告の履歴や詳細のデータを可視化します。



既存のセキュリティスタックにも直接連携することができます。(Splunk 内の表示)

DocuSign Monitor のメリット

不正なアクティビティを早期に検出
ログイン試行やパスワード変更、エンベロープの削除など、40 種類以上のイベントを監視し、内部または外部からの攻撃を早期に検出することができます。

組織ごとのニーズに合わせてアラートをカスタマイズ
事前に組み込まれたアラートだけでなく、特定の要件やセキュリティ規制に合わせてアラートをカスタマイズできます。

詳細な情報で迅速な原因究明を実現
IP アドレス、位置、履歴などの情報にすぐにアクセスでき、セキュリティチームがインシデントに優先順位をつけると共に、迅速に調査を行うことができます。

セキュリティスタックとの統合
Monitor API は、テレメトリデータを Splunk など既存の SIEM（Security Information and Event Management）ソフトウェアに直接送信することができ、セキュリティ運用を簡素化・効率化することができます。

アクティビティに関するデータを最大限に活用
アカウントのアクティビティ全体を可視化し、その傾向を把握することができます。結果は Tableau や Power BI など、普段から利用しているツール上で確認することが可能です。

主な業界
エネルギー
教育
金融
官公庁
ヘルスケア
保険
ライフサイエンス
不動産
通信

アクティビティの一例
ログイン試行
パスワードの変更
メール初期設定
アカウント設定
セキュリティ設定
権限の設定
アカウント招待
アカウントリンク
ユーザーグループの更新
エンベロープの削除
エンベロープの
ダウンロード
エンベロープの転送 等

お問い合わせ

DocuSign Monitor に関する詳しい情報や製品デモは弊社営業担当までお問い合わせください。

ドキュサイン・ジャパン株式会社
東京都港区虎ノ門4-3-1
城山トラストタワー35階

docusign.jp

連絡先
japan.marketing@docusign.com
03-4577-9801