RESOURCE CENTER

SIEM管理のためにSplunkを使用してBitwardenイベントを監視する

BitwardenとSplunkがどのように統合され、悪意のある攻撃やネットワーク侵害に対する防御のためのセキュリティ情報・イベント管理（SIEM）を提供しているかをご覧ください。

Get the full interactive view at
https://bitwarden.com/ja-jp/resources/monitor-bitwarden-events-using-splunk-for-siem-management/

bitwarden

Splunkは、マルチクラウドやオンプレミス環境で大量のデータを可視化するために使用されるセキュリティおよび観測可能性ツールです。このソリューションは、稼働時間、異常、停止、不審なアクティビティなどの重要なメトリクスに関する洞察を提供します。これらのクラウド観測可能性インサイトにより、Splunk は悪意のあるアクティビティを検出し、データセキュリティイベント発生時に IT、DevOps、SRE チームに通知することができます。

Bitwarden とSplunkは、悪質な攻撃やネットワーク侵害に対する防御のためのセキュリティ情報・イベント管理 (SIEM) を提供するために統合されています。SIEMテクノロジーは、オンライン・アプリケーションに対する潜在的な脅威を特定すると同時に、クラウド・インフラ・データのコンプライアンスとセキュリティ管理をほぼリアルタイムで提供する。これは、さまざまなデータソースで発生する詳細なイベントのコレクションを記録することによって達成される。

BitwardenとSplunkを使用することで、パスワード管理アクティビティ全体のアクティビティに関する詳細な情報を収集し、ビジュアルダッシュボードに表示して簡単に監視することができます。この2つを統合することで、ユーザーのアクティビティ、パスワードの変更、共有パスワードなどの情報を含む、特定のBitwarden組織に関する貴重な洞察を提供します。他のインフラ、アプリ、ネットワークのモニタリングと組み合わせることで、Splunk は企業のセキュリティを全体的に把握することができる。

splunk>®

目次

BitwardenとSplunkを併用するメリットは以下の通りです。

- Bitwardenのログから不審な活動に対するアラートと詳細なレポート
- SIEMの監視対象をウェブサイトとアプリケーションの認証情報に拡大
- ビジュアル・ダッシュボードとイベント検索マクロによる容易なモニタリング
- ユーザーによる特定のクレデンシャル・アクセスの記録
- 企業のセキュリティ・ツールのユーザー導入に関する洞察
- 元従業員がアクセスしたクレデンシャルをリストアップするオフボーディング・レポートにより、より厳重なセキュリティとアクセス・コントロールを実現。

ご存知でしたか？

Bitwardenは60種類以上のイベントを記録し、そのログは永続的に記録され、

分析や既存のセキュリティシステムへの統合のためにSplunkに渡すことができる。

統合の詳細Bitwarden 公式 Splunk アプリ

Bitwarden は、ユーザーインターフェイスで利用可能な公式 Bitwarden Event Logs アプリを通じて、Splunk Enterprise セルフホスト、Splunk Cloud Classic、Splunk Cloud Victoria インストールに簡単に統合できます。アプリのエントリはSplunkbase **にもあります。**Bitwarden ヘルプセンターの Splunk SIEM統合ドキュメント の手順に従ってください。Bitwarden 組織が Splunk に接続されると、3 つのダッシュボードがあらかじめ作成されています：認証イベント」、「Vault アイテムイベント」、「組織イベント」です。このデータを活用するために、他のカスタムダッシュボードを構築することもできる。

または、Bitwarden API統合を使用して、組織からイベントデータをエクスポートしてSIEM機能をセットアップすることもできます。Public APIは、あなたの組織やユーザーに関する情報を提供することができます。Vault Management APIは暗号化されたデータに関する情報へのアクセスを提供し、所有するエンドポイントで`serve` コマンドを使用して Bitwarden CLI クライアント内でホストされます。これら2つのAPIを組み合わせることで、組織と保管庫の全体像を把握することができます。

その他のリソース

- BitwardenでSplunkを使う
- イベントログ
- オンボーディングとサクセッションにおけるイベントログ
- Splunk SIEM
- ビットワーデン公開API
- ビットワーデン保管庫管理API