アラートの概要

アラートサービスの概要

広く展開されているアラートサービスと統合するために、Multicloud Defense は Microsoft Sentinel、PagerDuty、ServiceNow、および Slack と統合して、重要なシステムレベルのアラートを転送します。これにより、クラウド オペレーション チームは、Multicloud Defense Cloud Controller によって検出されたユーザー定義のシステムイベントと重大度レベルについてアラートを受信し、対応することができます。これは、Multicloud Defense Controller 内で、任意の統合に対するアラート サービス プロファイルとアラートルールを使用して実現されます。

サポートされているアラートサービスとの統合を設定するには、**[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[サービス（Services）]**に移動します。

これらのサービスとの統合には、API URL、API キー、またはその両方が必要です。通常、API キーと URL は、これらのサービスを管理する組織の管理者が生成する必要があります。

（注） ServiceNow との統合の場合、ServiceNowが Multicloud Defense Controller からアラートを受信して表示できるように、Webhook を設定する必要があります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。