データベースからの検出データの消去

[Discovery Data Purge] ページは、ネットワーク検出イベント データベースとユーザ検出イベント データベースからファイルを消去するために使用できます。データベースを消去すると、該当するプロセスが再起動されることに注意してください。

注意 データベースを消去すると、防御センターから指定したデータが削除されます。削除されたデータは**復元できません**。

ネットワーク検出データベースとユーザ検出データベースを消去するには、以下を行います。

アクセス：Admin/Any Security Analyst

ステップ 1 [System] > [Tools] > [Data Purge] の順に選択します。

[Data Purge] ページが表示されます。

ステップ 2 [Network Discovery] で、次のいずれかまたはすべてを実行します。

- データベースからすべてのネットワーク検出イベントを削除するには、[Network Discovery Events] を選択します。
- データベースからすべてのホストと侵害の痕跡フラグを削除するには、[Hosts] を選択します。
- データベースからすべてのユーザ イベントを削除するには、[User Activity] を選択します。
- データベースからすべてのユーザ ログインとユーザ履歴データを削除するには、[User Identities] を選択します。

ステップ 3 [Connections] で、次のいずれかまたはすべてを実行します。

- データベースからすべての接続データを削除するには、[Connection Events] を選択します。
- データベースからすべての接続の概要データを削除するには、[Connection Summary Events] を選択します。
- データベースからすべてのセキュリティ インテリジェンス データを削除するには、[Security Intelligence Events] を選択します。

（注） [Connection Events] を選択しても、セキュリティ インテリジェンス イベントは削除されません。セキュリティ インテリジェンス データを使用した接続がセキュリティ インテリジェンス イベント ビューアから消去されることはありません。同様に、[Security Intelligence Events] を選択しても、関連したセキュリティ インテリジェンス データを使用した接続イベントは削除されません。

ステップ 4　[Purge Selected Events] をクリックします。

項目が消去され、該当するプロセスが再起動されます。