### matchsig()

対象式を評価した文字列に対して、指定されたパターングループのいずれかのパターンがマッチした場合は true、マッチしない場合は false を返します。

#### 構文

matchsig(STR\_GUID, STR\_EXPR)

**STR\_GUID**

パターングループの GUID。GUID 文字列は有効なパターングループ識別子でなければなりません。無効なパターングループ GUID を指定した場合、クエリは失敗します。

**STR\_EXPR**

検索対象の文字列表現式。評価結果は文字列である必要があります。式を評価できない場合や無効な値の場合は false を返します。

#### 説明

ログプレッソ・ソナーは、ネットワーク侵入防止システム（IPS: Intrusion Prevention System）と同様に、数千件以上のキーワードを同時に検出できるよう、Aho-Corasick アルゴリズムを用いて動作します。入力文字列をパターングループに属するすべてのキーワードと一括で照合し、その後、キーワードで絞り込まれたパターンの検証式を順次実行することで、最終的にパターンと一致するイベントを検出できます。

パターン例

|  |  |  |  |
| --- | --- | --- | --- |
| # | パターン名 | パターン（必須）：一次高速検出 | 検証式（任意）：二次フィルター |
| 1 | xp\_cmdshell | "sp\_addextendedproc" and "xp\_cmdshell" |  |
| 2 | zb\_now\_connect | "REMOTE\_ADDR" and ("fputs" or "fwrite") | path == "lib.php" |

パターンは文字列パターンとブール検証式で構成されており、検証式は省略可能です。

1番のパターン **xp\_cmdshell** では、sp\_addextendedproc と xp\_cmdshell は Microsoft SQL Server で頻繁に使用されるコマンドです。攻撃者が SQL インジェクション等を利用して sp\_addextendedproc を用いて xp\_cmdshell コマンドを登録し、これを通じてシステムコマンドを実行して悪意のある行為を行うことがあるため、これを検出する用途で利用できます。このパターンは検証式を持たない例です。

2番のパターン **zb\_now\_connect** は、[ZeroBoard 4.1 pl7 - 'now\_connect()' Remote Code Execution](https://www.exploit-db.com/exploits/9590) を利用し、リモートから任意のコード lib.php を実行する攻撃を検出する例です。このパターンでは、入力フィールドに fputs または fwrite のいずれかの文字列と REMOTE\_ADDR 文字列が両方とも検出されるかを確認し、その後 path フィールドの値が lib.php 文字列と一致するかどうかを検証します。