### matchsig

フィールドの文字列値が指定されたパターングループに含まれているかを確認し、その結果を出力します。

#### 構文

matchsig [invert=BOOL] [verify=BOOL] guid=SIG\_GUID field=TARGET\_FIELD

必須パラメータ

**guid=SIG\_GUID**

パターングループのGUID識別子

**field=TARGET\_FIELD**

対象フィールド名。対象フィールドの値は文字列型である必要があり、それ以外の型の場合は検索失敗と見なされます。

オプションパラメータ

**invert=BOOL**

検索結果の出力形式（デフォルト: f）

* t: 対象フィールドの値がパターングループに含まれていない場合に出力
* f: 対象フィールドの値がパターングループに含まれている場合に出力

**verify=BOOL**

クエリパース段階でパターングループオブジェクトの有効性を検証するかどうか（デフォルト: t）

* t: パターングループオブジェクトの有効性を検証
* f: パターングループオブジェクトの有効性を検証しない※このオプションは、システムがポリシー同期段階で構文エラーを発生させないように設定します。

#### 説明

ログプレッソ・ソナーは、ネットワーク侵入検知システム（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、アホ・コラシック（Aho-Corasick）アルゴリズムを用いて動作します。入力された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、キーワードで抽出さ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 |
| 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、検証式は省略可能です。

1番目のパターン **xp\_cmdshell** では、sp\_addextendedproc および xp\_cmdshell はマイクロソフトSQLサーバー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、これを検出するために利用できます。このパターンは検証式を持たない例です。

2番目のパターン **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 文字列が両方とも含まれているかを確認し、その後 path フィールドの値が lib.php 文字列と一致するかを検証します。