Modbus インスペクタ

Modbus インスペクタの概要

タイプ	インスペクタ（サービス）
使用方法	検査
インスタンス タイプ	マルチトン
その他のインスペクタが必要	`stream_tcp`
有効	`false`

Modbus プロトコルは、遠隔監視制御・情報取得（SCADA）システムとプログラマブル自動化コントローラ（PLC）の間でメッセージを交換するための通信規格を定義します。Modbus プロトコルは TCP ポート 502 を使用します。

`modbus` インスペクタは、ネットワークトラフィック内の Modbus メッセージを検出して分析します。有効にすると、Modbus 侵入ルールのオプションを通じて特定の Modbus プロトコル フィールドにアクセスできます。

Modbusインスペクタを設定するためのベストプラクティス

ネットワークに有効になっている Modbus デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーの modbus インスペクタを有効にする必要があります。

Modbus インスペクタのパラメータ

Modbus TCP ポートの設定

binder インスペクタは、Modbus TCP ポートの設定を定義します。詳細については、『バインダインスペクタの概要』を参照してください。

例：

```
[
    {
        "when": {
            "role": "server",
            "proto": "tcp",
            "ports": "502"
        },
        "use": {
            "type": "modbus"
        }
    },
    {
        "when": {
            "role": "any",
            "service:" "modbus"
        },
        "use": {
            "type":"modbus"
        }
    }
]
```

（注） modbus インスペクタはパラメータを提供しません。

Modbus インスペクタのルール

modbus インスペクタ ルールを有効に、イベントを生成し、インライン展開では、違反パケットをドロップします。。

表 *1 : Modbus* インスペクタのルール

GID:SID	ルール メッセージ
144:1	Modbus MBAP ヘッダーの長さが、指定した機能に必要な長さと一致しない（length in Modbus MBAP header does not match the length needed for the given function）
144:2	Modbus プロトコル ID がゼロでない（Modbus protocol ID is non-zero）
144:3	予約済み Modbus 機能コードは使用中になっている（reserved Modbus function code in use）

Modbus インスペクタの侵入ルールのオプション

`modbus` オプションは、単独で使用することも、`content` および `byte_jump` 侵入ルールのオプションと組み合わせて使用することもできます。

modbus_data

データカーソルを Modbus `Data` フィールドの先頭に設定します。

シンタックス：`modbus_data;`

例：`modbus_data;`

modbus_func

Modbus `Function` フィールドが指定した Modbus 機能コードと一致していることを確認します。Modbus 関数コードを表す正の整数または文字列リテラルを設定できます。

型：文字列

シンタックス：`modbus_func: <function>;`

有効な値は、次のとおりです。

表 *2 : Modbus* 関数コード値

コード	文字列
1	`read_coils`
2	`read_discrete_inputs`
3	`read_holding_registers`
4	`read_input_registers`
5	`write_single_coil`
6	`write_single_register`

コード	文字列
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

例：

```
modbus_func: read_coils;
modbus_func: 8;
```

modbus_unit

メッセージ内の Modbus ユニット ID が指定されたユニット ID と一致することを確認します。Modbus ユニット ID を表す数値を設定できます。

型：整数

シンタックス：`modbus_unit: <unit_id>;`

有効な範囲：`0` 〜 `255`

例：

```
modbus_unit: 1;
```

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。