

# [Feature] Keyword Detection

Network APT (NSM)

Exported on 05/22/2023

## Table of Contents

1 Quá trình detect theo signature keyword.....	3
2 Cách thêm một keyword detect module .....	4

```

graph TD
    subgraph Setup_phase [Setup phase]
        A[Register detect module into sigmatch_table array] --> B[Setup func, Match func, name, ...]
        B --> C[Signature table]
        C --> D[LoadSignatures]
        D --> E[SigLoadSignature]
        E --> F[ProcessSigFile]
        F --> G[SigLoadOut]
        G --> H[SIGMATCHPrepare]
        H --> I[DetectEngineApp/DetectEngineHttp/DetectEngineGraph]
    end

    subgraph Suricata_Main_Loop [Suricata Main Loop]
        J[Incoming packet: Packet "p, uint8_t" *] --> K[Validation: ValidateType/Packet "p, uint8_t" *]
        K --> L[Decoding: Decode/Packet "p, uint8_t" *]
        L --> M[Decodetree: DecodeTree/Packet "p, uint8_t" *]
        M --> N[FlowSetup: Flow/Packet "p"]
        N --> O[DetectRun]
        O --> P[DetectRun/PacketRules -> inspect the rule against the packet]
        P --> Q{app_inspect != NULL}
        Q -- True --> R[DetectRunTx -> inspect app layer transaction]
        R --> S[DetectRunTxInspector -> inspect a rule against a transaction]
        S --> T[Run_app_inspect Callback]
        T --> U[DetectEngineApp/DetectEngineHttp/DetectEngineGraph]
        U --> V[DetectEngineApp/DetectEngineHttp/DetectEngineGraph]
    end

    subgraph Central_Processing [ ]
        W[Parse action, protocol, src address, dst address -> save into corresponding fields in Signature struct]
        X[Parse option]
        Y[SigMatchDetectName -> get detect module from sigmatch_table]
        Z[module Detect -> set option value to corresponding hexword and expand option to rule_data-related]
    end

    C --> W
    C --> X
    C --> Y
    C --> Z
  
```

## 2 Cách thêm một keyword detect module

- Chạy auto-generate script:

```
$ script/setup-simple-detect.sh <keyword>
```

- Ví dụ:

```
→ suricata-suricata-6.0.4 scripts/setup-simple-detect.sh testt
```

Detect module Testt has been set up in tests/detect-testt.c and detect-testt.h and the build system has been updated.

The detect module should now compile cleanly. Try running 'make'.

Next steps are to edit the files to implement the actual detection logic of Testt.