[Feature] Keyword Detection

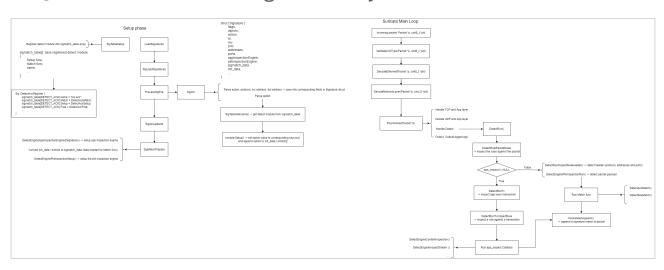
Network APT (NSM)

Exported on 05/22/2023

Table of Contents

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

1 Quá trình detect theo signature keyword



2 Cách thêm một keyword detect module

Chay auto-generate script:

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

Ví du:

→ 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.