Suricata - Bug #5177

detect/engine-analyzer: rule analyzer warns about http buffers usage/replacement even when using new keyword

03/07/2022 05:43 PM - Juliana Fajardini Reichow

Status: New
Priority: Normal
Assignee: Juliana Fajardini Reichow
Category:
Target version: 7.0rc1
Affected Versions:
Effort:

Description
Currently, a rule like:

"alert http any any -> any any (http.request_line; content:"GET /index.html HTTP/1.0"; sid:61;)"

Will still generate the warning that should be used only when outdated HTTP keywords are used:

"pattern looks like it inspects HTTP, use http.request_line or http.method and http.uri instead for improved performance"

Expected behavior:
The warning should only be triggered if the rule still uses the corresponding legacy content modifier.