Suricata - Task #5181

detect/engine-analyzer: add rule analyzer warnings about rules that could use the frame keyword/semantics/feature

03/07/2022 06:07 PM - Juliana Fajardini Reichow

Status: New
Priority: Normal
Assignee: Juliana Fajardini Reichow
Category: 
Target version: TBD
Effort: 
Difficulty: 
Label: 

Description
With the addition of frame support, the rule analyzer could now also check for rules with patterns like:
- For SMB traffic: check for content "\xFF" or "\xFE" (especially with "startswith")
- For TLS traffic: check for contents "\x16 03 03" (especially with "startswith")
- ... similar patterns for other protocols
And issue warnings that those can be converted to the new frame semantics.

This task must wait on the definition of the frame keyword/semantics syntax.

Related issues:
Related to Task #5050: rules/frames: settle on rule syntax

History
#1 - 03/07/2022 06:08 PM - Juliana Fajardini Reichow
- Related to Task #5050: rules/frames: settle on rule syntax added