## Description

While updating some older TLS sigs in the ET Ruleset which do not make use of existing suricata buffers, I came across a rule (2023476) which uses pcre capture groups to ensure the detected CN value from either the subject or issuer certificate is found at least twice in the content. The rule does not make use of any static values to detect the malicious certificates and relies on a pretty gnarly regex.

When attempting to covert this rule to tls buffers, I did not have a generic way to ensure that the issuer and subject certificates were the same, indicating a self signed certificate.

This issue was discussed in [https://redmine.openinfosecfoundation.org/issues/1356](https://redmine.openinfosecfoundation.org/issues/1356), however the solution depends on Lua, which is not required by default, and therefore not an option in this specific effort of updating existing rules.

I propose the creation of a new keyword tls.self_signed which acts similar to that of tls_cert_expired and tls_cert_valid and matches when the subject and issuer are the same.