rules: Keyword for determining if the http_host is an ip address

02/20/2020 10:43 PM - Jason Williams

Description
In the ET ruleset in order to express the fact that http communications are going to an IP address rather than a hostname we have to do pcre.

Some variation of this is all over the place, often not properly using the http_host buffer:

```
pcre: "/^?:\d{1,3}\.(\d{1,3}(?::\x3a\d{1,5})?)$/W";
```

If it wouldn't be too taxing, it would be very useful to have a simple statement to express that the hostname in the http_header is an ip address. I don't know that a transform is the right place for it as we're not looking to do anything with the ip, but something like below:

```
http.host; is_ip;
```

Related issues:
Related to Task #4097: Suricon 2020 brainstorm

History
#1 - 02/20/2020 10:45 PM - Jason Williams
I typo'd the pcre from memory, but you know what i mean...
```
pcre: "/^?:\d{1,3}\.(\d{1,3}(?::\x3a\d{1,5})?)$/W";
```

#2 - 11/14/2020 02:25 PM - Jeff Lucovsky
- Related to Task #4097: Suricon 2020 brainstorm added

#3 - 11/24/2020 09:36 AM - Victor Julien
- Subject changed from Keyword for determining if the http_host is an ip address to rules: Keyword for determining if the http_host is an ip address