While trying to build 6.0.5 on Debian's s390x port, we noticed that tests segfault in the new version (see https://ci.debian.net/data/autopkgtest/testing/s390x/s/suricata/21160408/log.gz). Tracking this down, it seems that CIDRFromMask() returns -1 when trying to determine a network prefix length for a given netmask (e.g. 24 for 255.255.255.0). This causes DetectAddressParseSingle() to return NULL and hence the test to try and dereference a null pointer, causing the segfault.

I compared values passed into CIDRFromMask() via gdb on amd64 and s390x and found that they are different:

```
amd64
...
Test AddressTestCutIPv401 :  
Breakpoint 1, CIDRFromMask (netmask=16777215) at util-cidr.c:34  
...

s390x
...
Test AddressTestCutIPv401 :  
Breakpoint 1, CIDRFromMask (netmask=4294967040) at util-cidr.c:34  
...
```

My patch at https://gist.github.com/satta/7406fe735d8b449a4c9af73822d2bc9a fixes the code for both architectures.
#5 - 05/31/2022 01:43 PM - Jeff Lucovsky
- Status changed from In Progress to In Review

https://github.com/OISF/suricata/pull/7449

#6 - 06/01/2022 12:44 PM - Jeff Lucovsky
- Status changed from In Review to Closed

Merged in https://github.com/OISF/suricata/pull/7453