hack4glarus-2019-winter - Task #7382

Monitoring at a different level (BPF/Suricata/Cilium)

11/29/2019 11:02 PM - Philipp Buehler

Status:	Closed	**Start date:**	11/29/2019
Priority:	Normal	**Due date:**	
Assignee:	Philipp Buehler	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
PM Check date:			

Description

Traditional pull based monitoring (nagios et al) is DEAD>
Push based (partly Prometheus, Riemann) is cooler.

But it's still somewhat superficial requests.. how about monitoring directly "from the wire".

Reasearch on gathering data on an app-level without app-internal instrumentation (eg. haproxy/suricata).

History

#1 - 11/30/2019 01:02 AM - Philipp Buehler

Cilium: https://docs.cilium.io/en/stable/
Suricata: https://suricata-ids.org/docs/
BPF:
http://www.brendangregg.com/blog/2016-03-05/linux-bpf-superpowers.html
https://cilium.io/blog/2018/04/17/why-is-the-kernel-community-replacing-iptables/

#2 - 11/30/2019 01:07 AM - Philipp Buehler

The idea is to tproxy chain haproxy traffic and let suricata "inspect" the traffic.
Pull the eve.json output into ELG or so.

haproxy:
listen inbound
bind public-ip:80
server moni 172.23.42.1:80 send-proxy # lives on a loopback if (e.g. lo1)
frontend monitor-in
bind 172.23.42.1:80 accept-proxy name monitor-in

suricata makes traffic analysis on lo1

#3 - 12/01/2019 11:40 AM - Philipp Buehler

- Status changed from New to Waiting

Time ran out, VM too slow to install all necessary toolchain

#4 - 01/02/2024 12:35 PM - Nico Schottelius

- Status changed from Waiting to Closed