Hey Team,

I have a quick question when it comes to some of the metadata fields that are extracted from the eve.json logs.

I am looking to analyze network traffic for any abnormal amounts of data leaving the network. I see that some metadata included in Suricata alerts are "flow.pkts_toclient", "flow.pkts_toserver", "flow.bytes_toclient", and "flow.bytes_toserver". My main question is what do the two different categories, "toclient" and "toserver", mean? Does this mean that "flow.pkts_toclient" are the amount of packets that are running through my inline Suricata box to the dest_ip? Or would that be the "flow.pkts_toserver"? Do either the "flow.pkts_toclient", or "flow.pkts_toserver" only correlate to the dest_ip, so if the dest_ip is a public ip, I know that this is the amount of packets leaving my network out to the Internet?

Any clarification would be greatly appreciated!

Best Regards,

Taylor

Flows have a direction. The IP which starts the conversation is considered the client, and the packets it sends are in the 'to server' direction. The other talker is considered the server and the packets it sends are in the 'to client' direction. So in a flow records the 'flow.pkts_toserver' is a count of the number of packets from client to server, 'flow.bytes_toserver' counts the total bytes in the same direction. The 'flow.*_toclient' records are the same, but in the opposing direction.