Palo Alto Summary Logic

# CEF Logs

* Bytes\_Sent is from source to destination
  + CEF: total\_in
* Bytes\_Received is from destination to source
  + CEF: total\_out

# Summaries

## Inbound

* Entity = Destination IP
* Direction = In to destination
* Bytes\_Sent = total\_out
  + Destination sending out to Source
* Bytes\_Received = total\_in
  + Destination receiving from source

## Outbound

* Entity = Source IP
* Direction = Out from source
* Bytes\_Sent = total\_in
  + Source sending out to destination
* Bytes\_Received = total\_out
  + Source receiving from destination

# Functions

## Im\_NetworkSession\_Inbound

* Entity = Destination IP
* Source = 0.0.0.0
* SBytes = Bytes\_Received = total\_in = Destination Receiving from Source
* DBytes = Bytes\_Sent = total\_out = Destination Sending to Source

## Im\_NetworkSession\_Outbound

* Entity = Source IP
* Destination = 0.0.0.0
* SBytes = Bytes\_Sent = total\_in = Source Sending out to Destination
* DBytes = Bytes\_Received = total\_out = Source receiving from destination

# Rule Logic

* Source internal. If bytes received is > 0, it means an internal IP is receiving a response from an Internet IP
  + Outbound
  + Source = Internal
  + DBytes > 0
* Destination internal. If bytes sent is > 0, it means an internal IP is receiving a response from an Internet IP
  + Inbound
  + Destination = internal
  + SBytes > 0