Sit down

We need to talk
THE SANS INSTRUCTORS SAID:

"WE NEED TO TALK"
Intervention:

An intervention is the act of inserting one thing between others, like a person trying to help. You could be the subject of a school *intervention* if your teachers call your parents about the bad grades you've been hiding.
Intervention:

An intervention is the act of inserting one thing between others, *like a person trying to help*. You could be the subject of a school *intervention* if your teachers call your parents about the bad grades you've been hiding.
There’s lots going well...
Soooo much to improve!
SIEM Complaints
NOT SURE IF SIEM IS WORKING AND NO ATTACKS

OR SIEM IS BROKEN
SIEM Care & Feeding
BILLABLE HOURS

BILLABLE HOURS EVERYWHERE
Automated Response
AUTOMATED SIEM RESPONSE WORKS AS EXPECTED
Tuning? Why is it so needed?
THE AMOUNT OF FALSE POSITIVES IS TOO DAMN HIGH
Sizing a SIEM
SIEM ISN'T WORKING WELL

SO SIEM VENDOR TELLS ME TO BUY MORE SIEM
“A refreshing sip of water!”
Machine Learning / AI
What data are you watching?
You are never in the wrong place.

But sometimes you are in the right place looking at things in the wrong way.
Quick wins