SIEM INTERVENTION PANEL

SIEM & Tactical Analytics SUMMMIT & TRAINING

Scottsdale, AZ

SUMMIT: **Nov 28-29**

FOUR COURSES: **Nov 30 – Dec 5**

ACHIEVE ACTIONABLE INTELLIGENCE FOR TACTICAL SECURITY OPERATIONS


Sit down
We need to talk
ICANHASCHEEZBURGER.COM


THE SANS INSTRUCTORS SAID:
"WE NEED TO TALK"
imgflip.com

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.

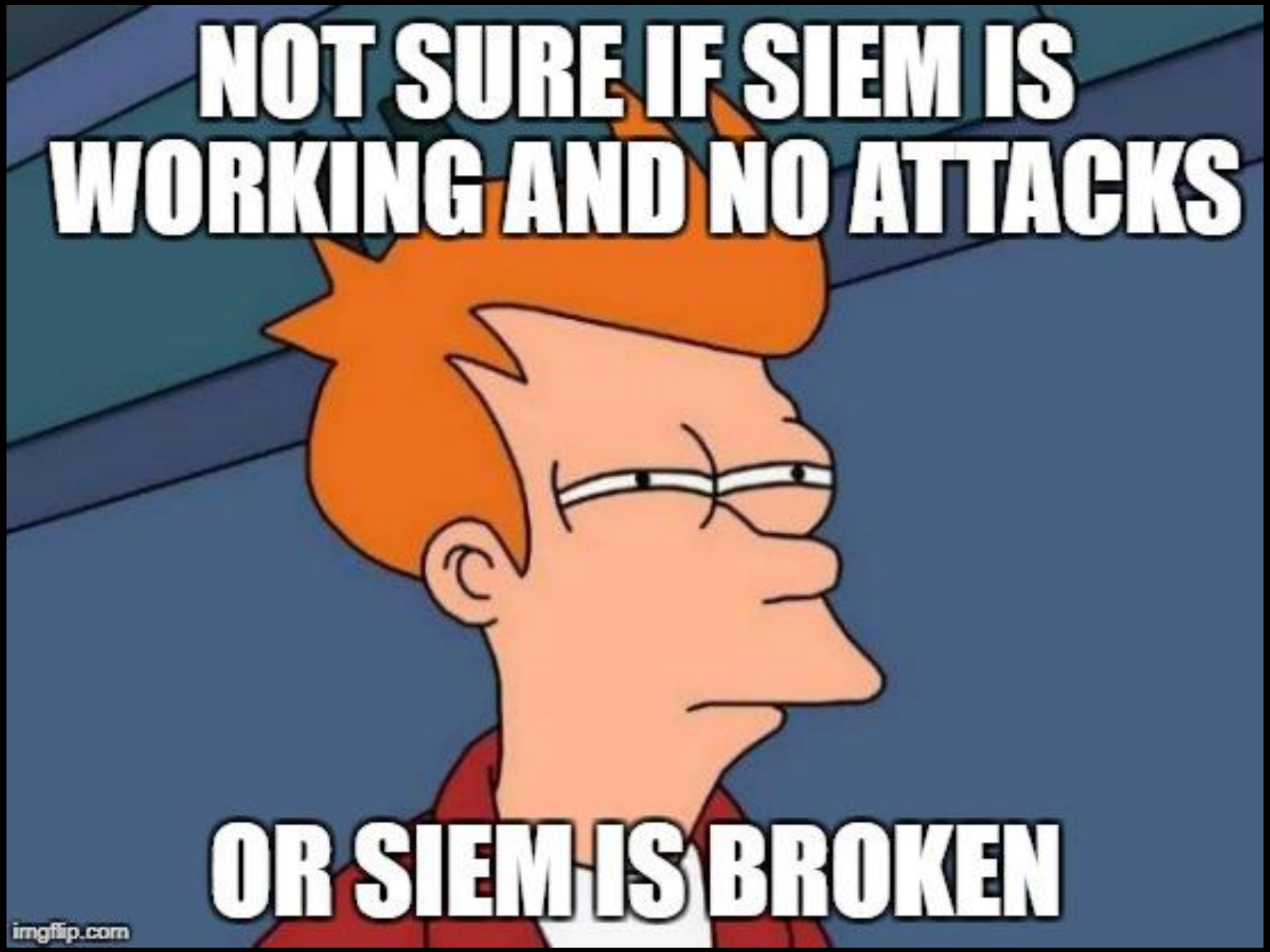
Intervention:

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
imgflip.com

SIEM Care & Feeding


BILLABLE HOURS
BILLABLE HOURS EVERYWHERE
imgflip.com

Automated Response


AUTOMATED SIEM RESPONSE
38
WORKS AS EXPECTED
imgflip.com

Tuning?
Why is it so needed?

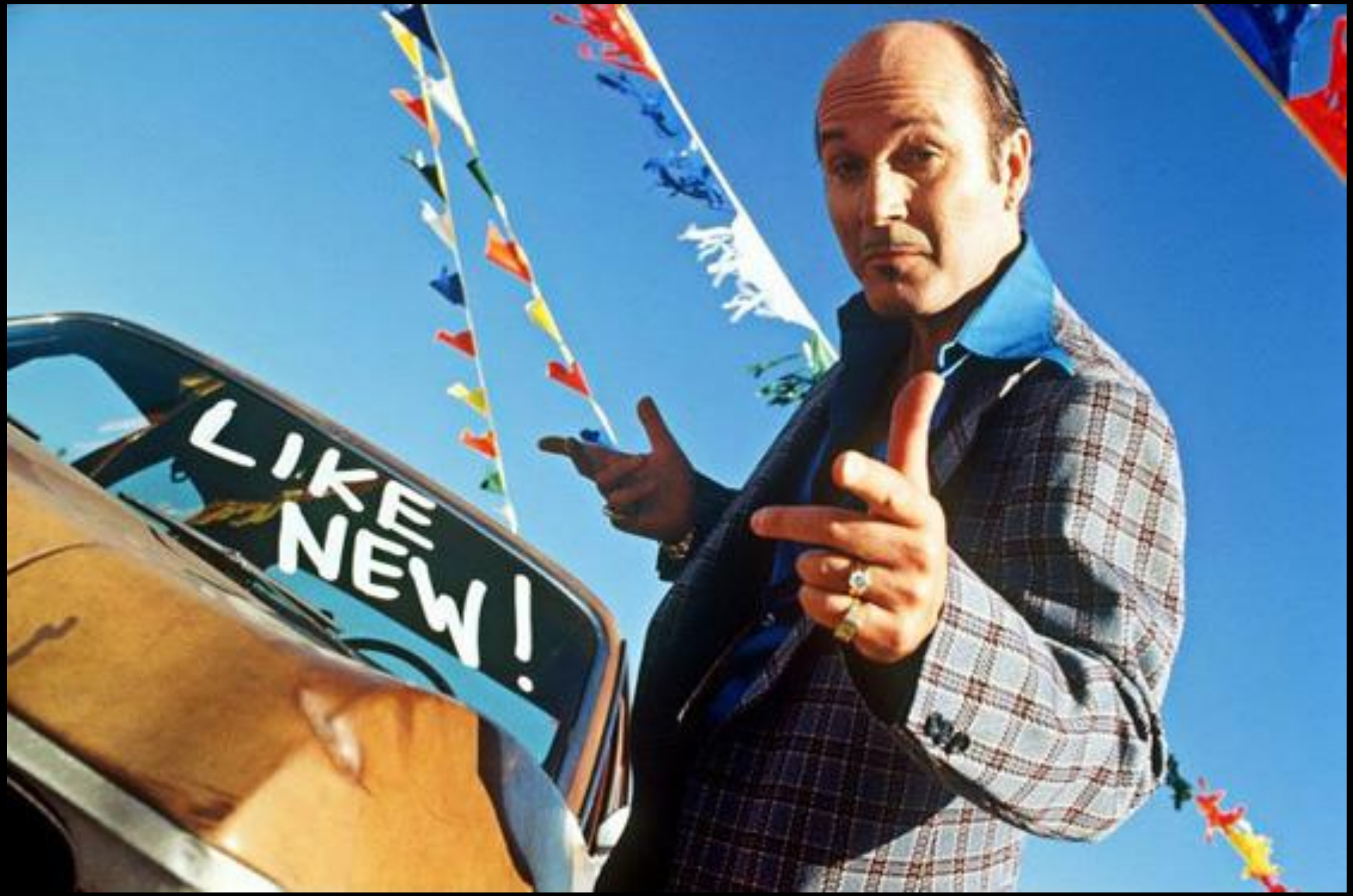

THE AMOUNT OF FALSE POSITIVES
IS TOO DAMN HIGH
imgflip.com

Sizing a SIEM

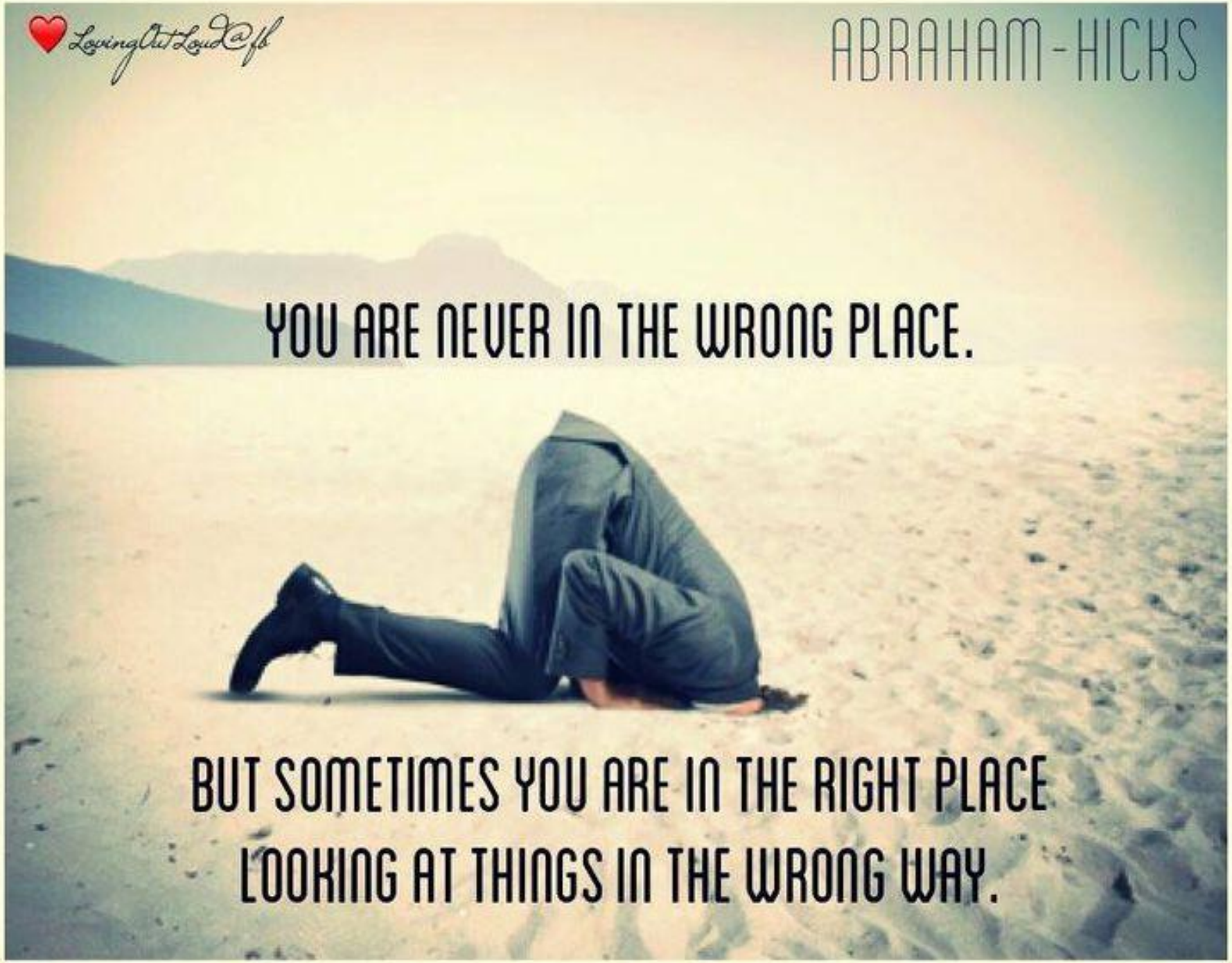

SIEM ISN'T WORKING WELL
SO SIEM VENDOR TELLS ME TO BUY MORE SIEM
imgflip.com

“A refreshing sip of water!”

Machine Learning / AI


LIKE
NEW!

What data are you watching?


LovingOutLoud@fb
ABRAHAM-HICKS
YOU ARE NEVER IN THE WRONG PLACE.
BUT SOMETIMES YOU ARE IN THE RIGHT PLACE
LOOKING AT THINGS IN THE WRONG WAY.

Quick wins


VICTORY