

SIEM INTERVENTION PANEL



SIEM & Tactical Analytics

SUMMIT & 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

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...

Sooooo 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

A silhouette of a person stands on a dark, rocky outcrop, their arms raised in a gesture of triumph or celebration. The background is a dramatic sky at sunset or sunrise, with a bright yellow and orange glow near the horizon transitioning into a deep blue at the top. Scattered clouds are illuminated from below, creating a mix of orange, red, and purple hues. The word "VICTORY" is written in large, white, distressed, block letters across the upper right portion of the image, appearing as if painted or stenciled onto the sky.

VICTORY