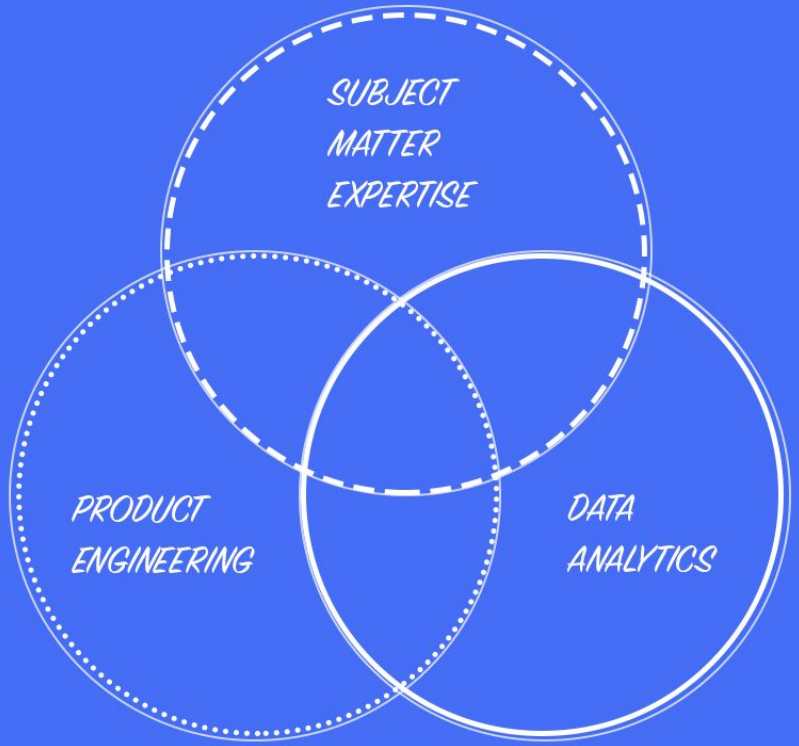
Who am I?

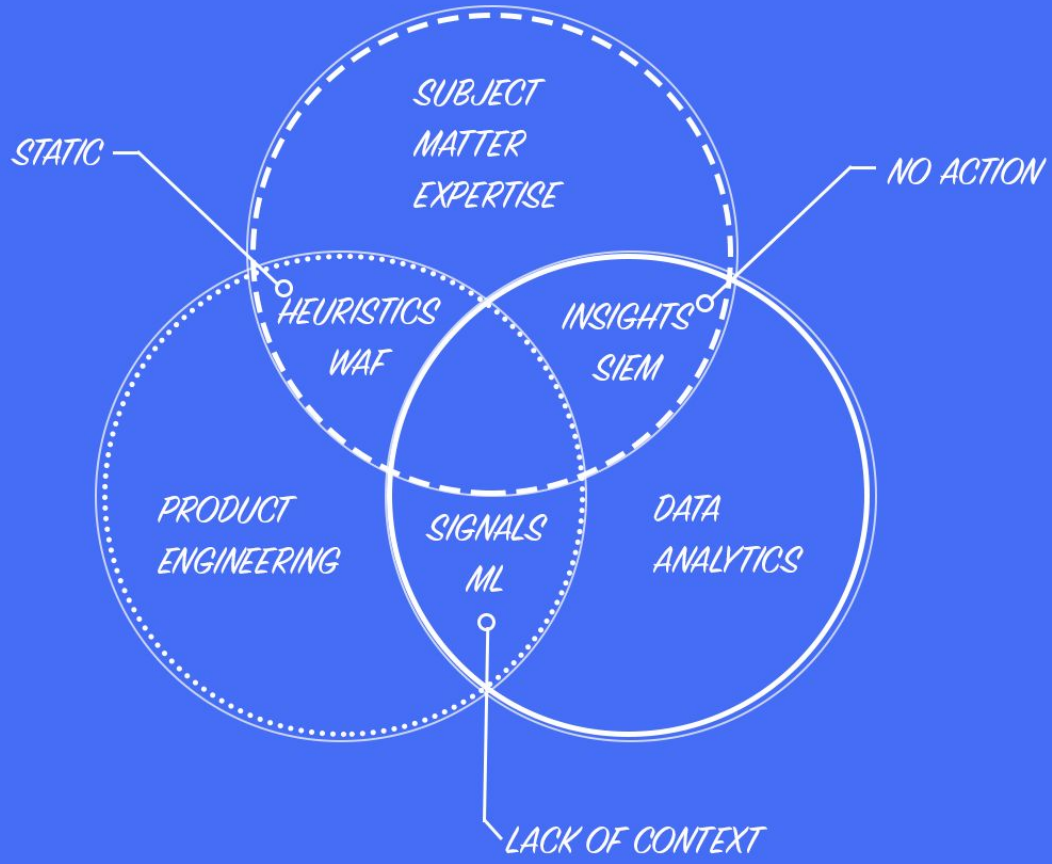
@bubblewire
Arkose Labs
Scandi

Why am I here?

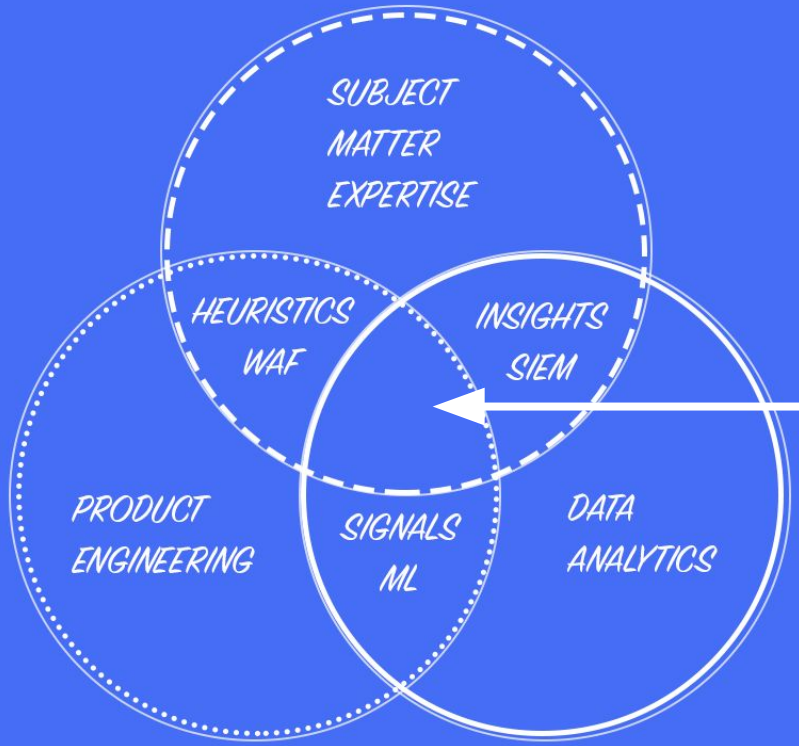


BUILDING *SECURITY* PRODUCTS

ACCURATE,
ACTIONABLE
& SCALABLE
SOLUTIONS



TRADITIONAL DEFENSIVE PRODUCTS



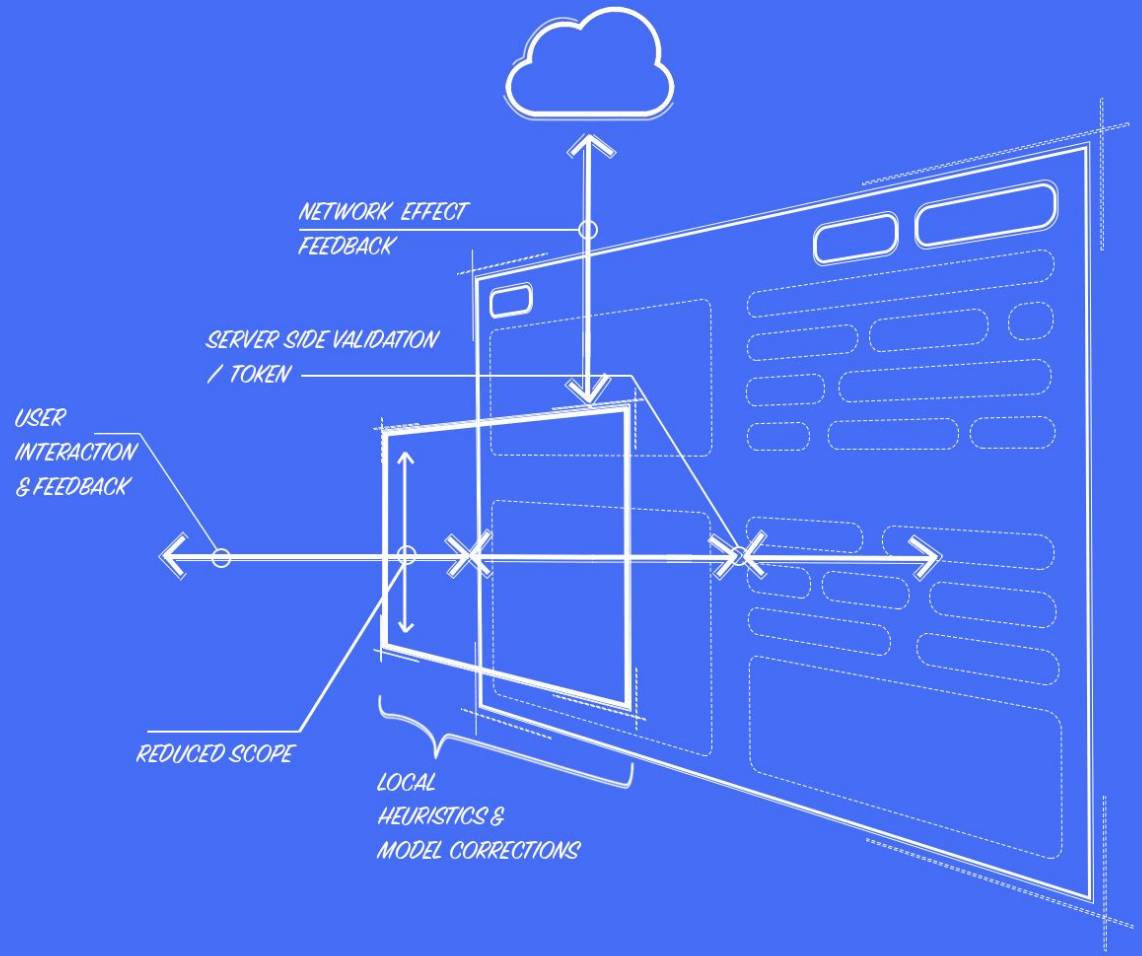
SWEET SPOT

FOR ACCURATE, ACTIONABLE & SCALABLE SOLUTIONS

HOW DO WE

SCALE

ENABLING
AUTOMATION
AND MACHINE
LEARNING
WHILST
AVOIDING
COMMON
PITFALLS



INTERMEDIATE
ATTACK SURFACE

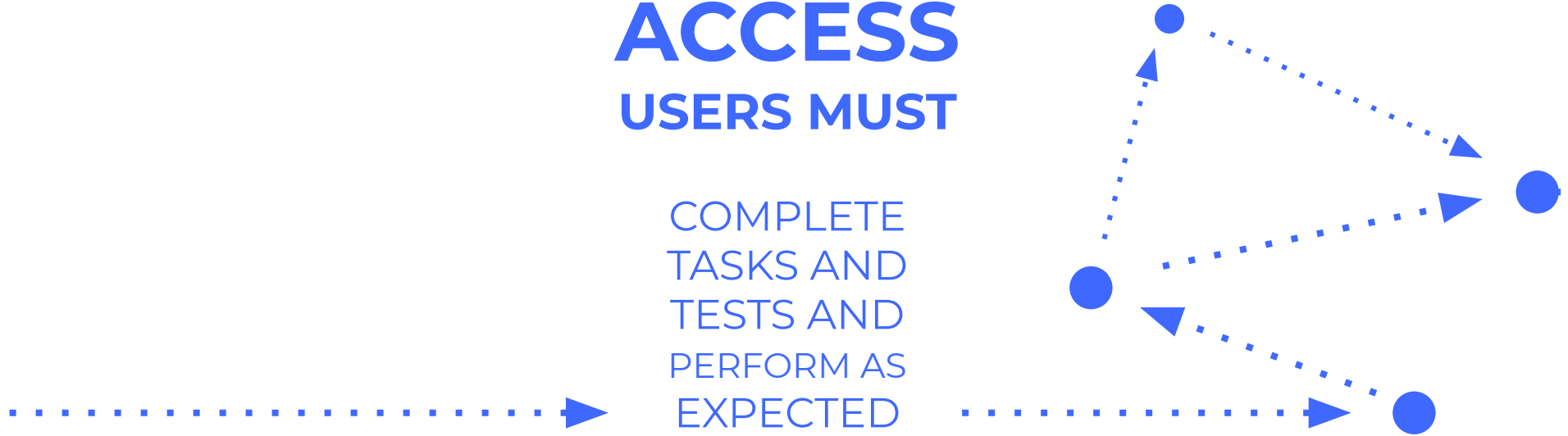
SEPARATED ENVIRONMENT USED TO TEST AND VALIDATE SUSPECT USAGE, ACTION OR BEHAVIOR

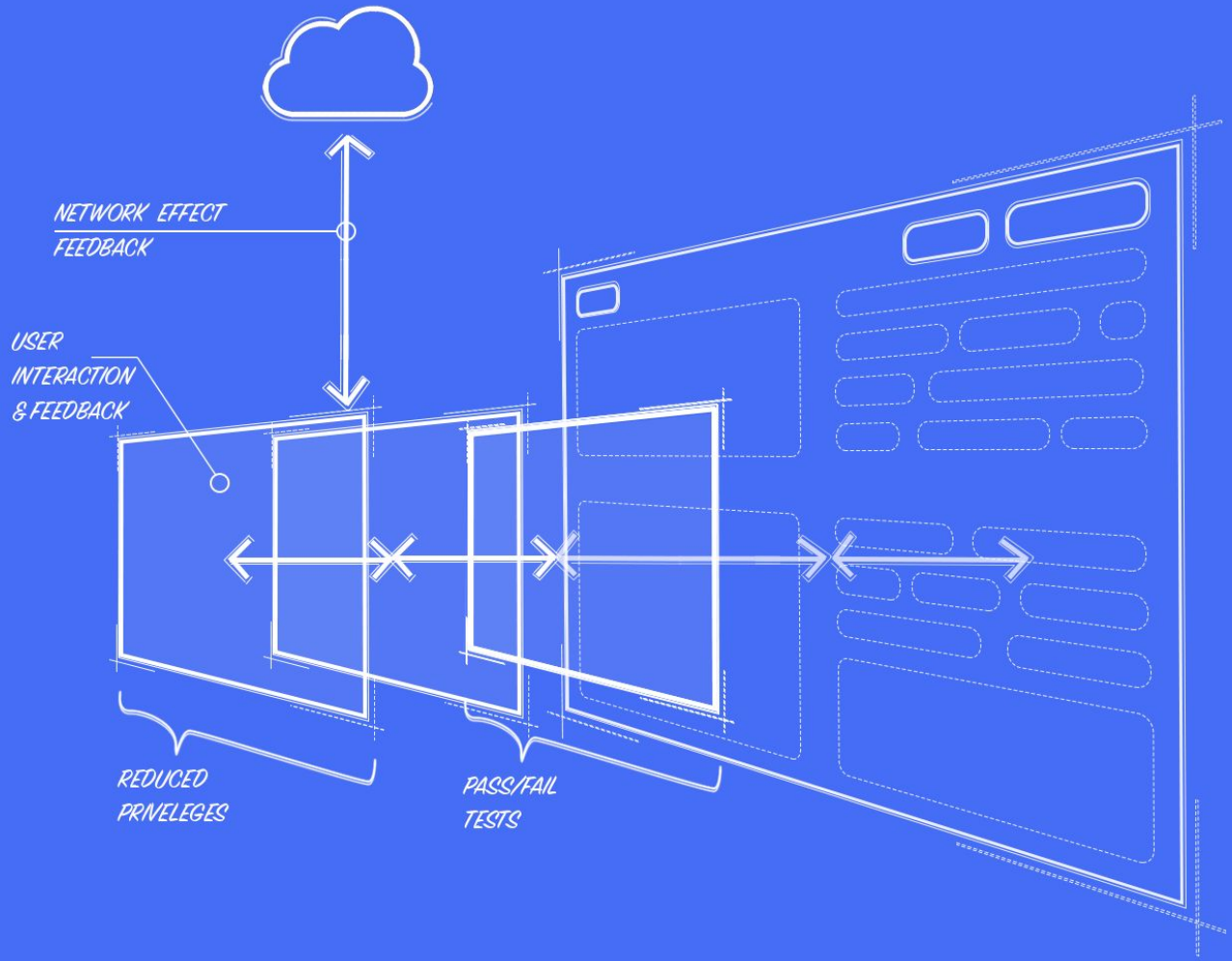
WHERE WE SEE SOME ADJACENT *CONCEPTS*

INTERACTIVE HONEYPOTS, LAYER 7 IDS, ANTI-FRAUD, SPAM, BOT & ATO SOLUTIONS

TO RETAIN ACCESS USERS MUST

COMPLETE TASKS AND TESTS AND PERFORM AS EXPECTED





ESCALATED VALIDATION

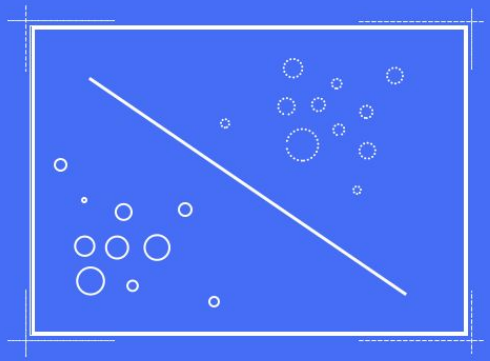
& WHAT WE LEARN FROM HONEYPOTS

BENEFITS OF INTERMEDIATE ATTACK SURFACE

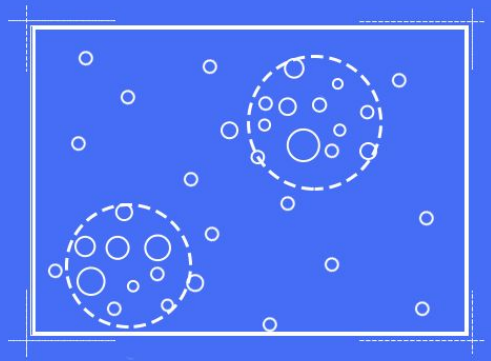
MOVE TARGET FROM YOUR ASSETS, WASTE ATTACKERS TIME AND EXHAUST RESOURCES VALIDATE USERS

BUT WHAT IF IT COULD LEARN?

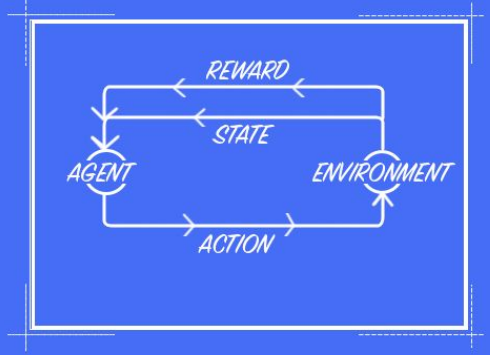
SUPERVISED



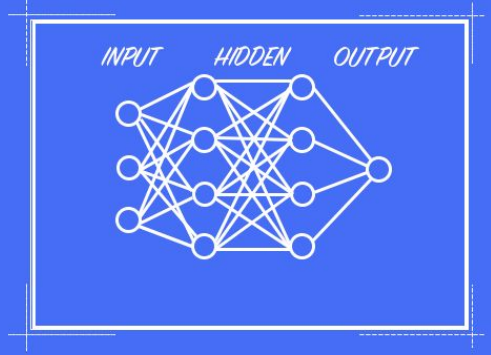
UNSUPERVISED



REINFORCEMENT LEARNING

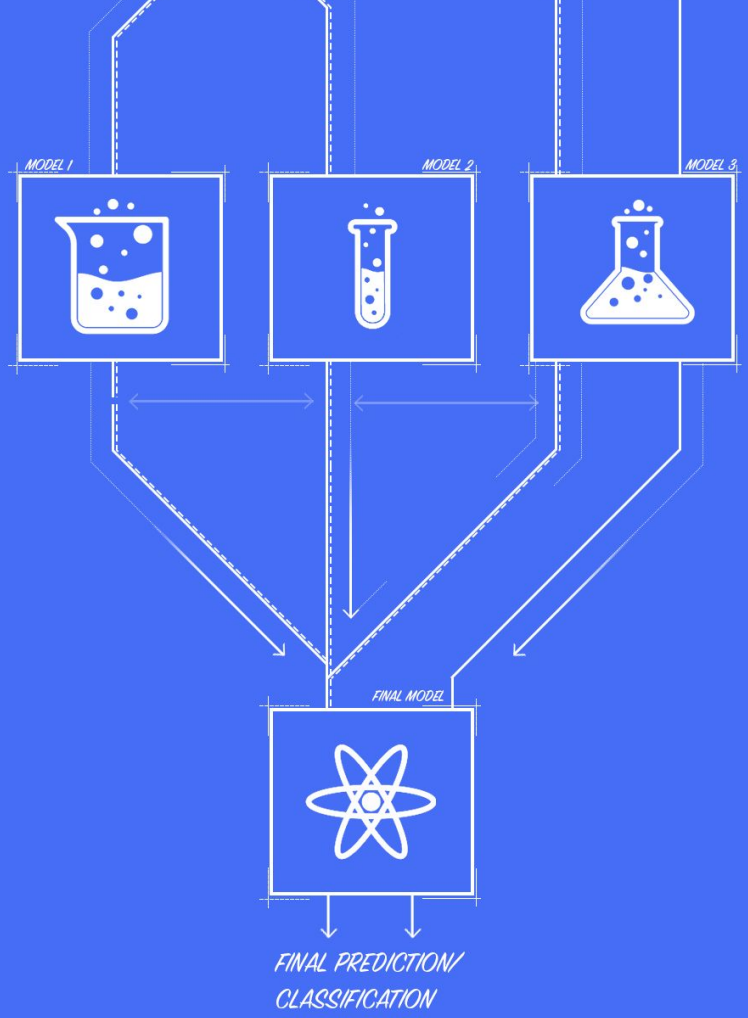


DEEP LEARNING



MACHINE *LEARNING*

DIFFERENT ALGORITHMS FOR DIFFERENT SITUATIONS WITH DIFFERENT REQUIREMENTS



ENSAMBLE *ALGORITHMS*

META ALGORITHMS THAT COMBINE SEVERAL ML MODELS FOR IMPROVED PERFORMANCE

APPLYING MACHINE LEARNING IN SECURITY

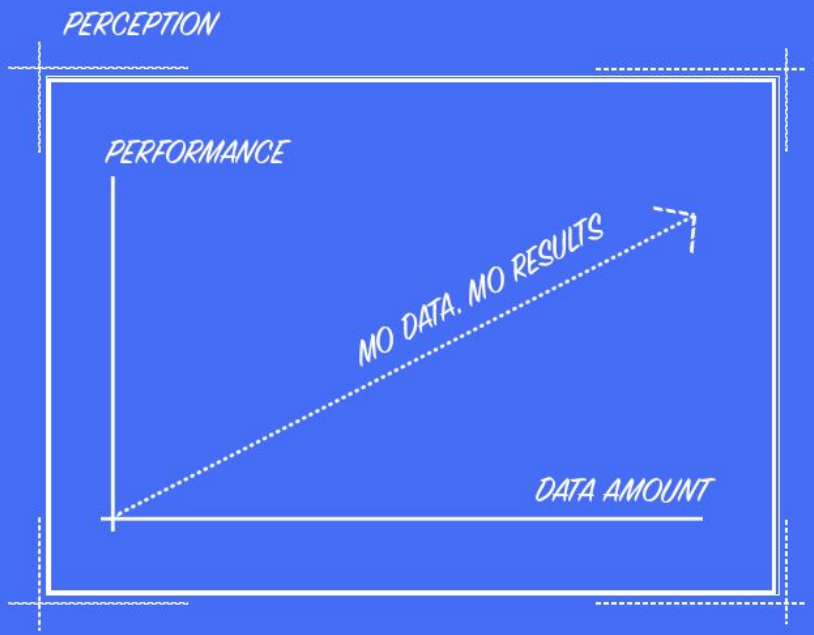
SHOW US THINGS
WE *DON'T KNOW*

DO THINGS *WE DO KNOW* FASTER OR MORE EFFICIENT (AT SCALE)

ISSUES IN MACHINE LEARNING IN SECURITY

SECURITY EXPERTS
ARE ~~NOT~~ RARELY
DATA SCIENTISTS

DATA SCIENTISTS
ARE ~~NOT~~ RARELY
SECURITY EXPERTS



PERCEPTION

MORE DATA

BETTER

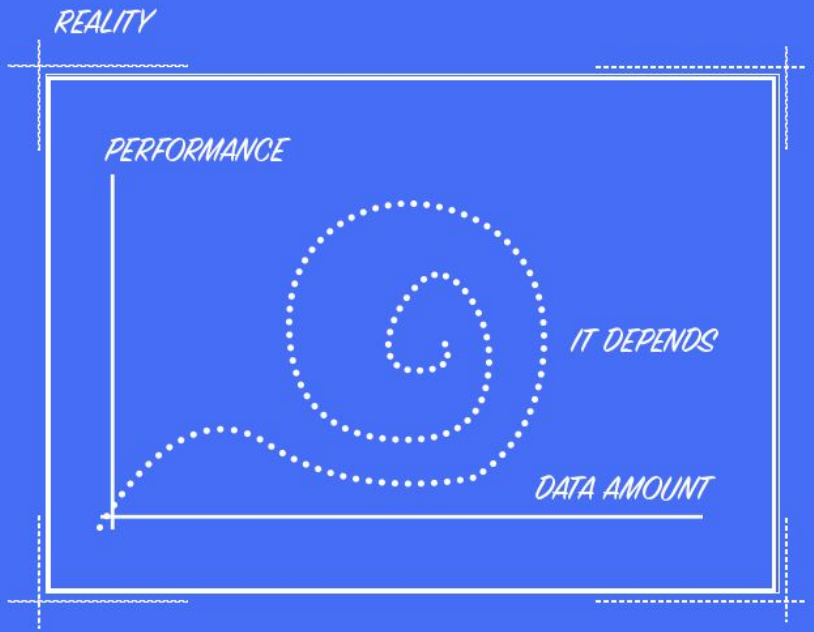
PERFORMANCE

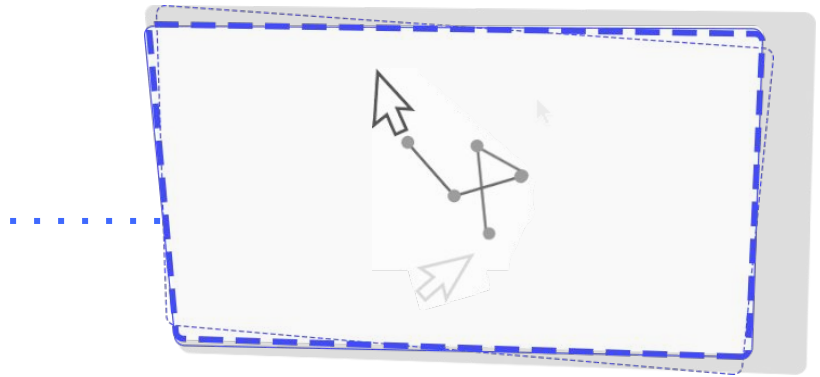
MANY BELIEVE THAT FEEDING MORE DATA TO THE MODEL ALWAYS YIELD BETTER RESULTS

REALITY

SIZE DOESN'T REALLY MATTER

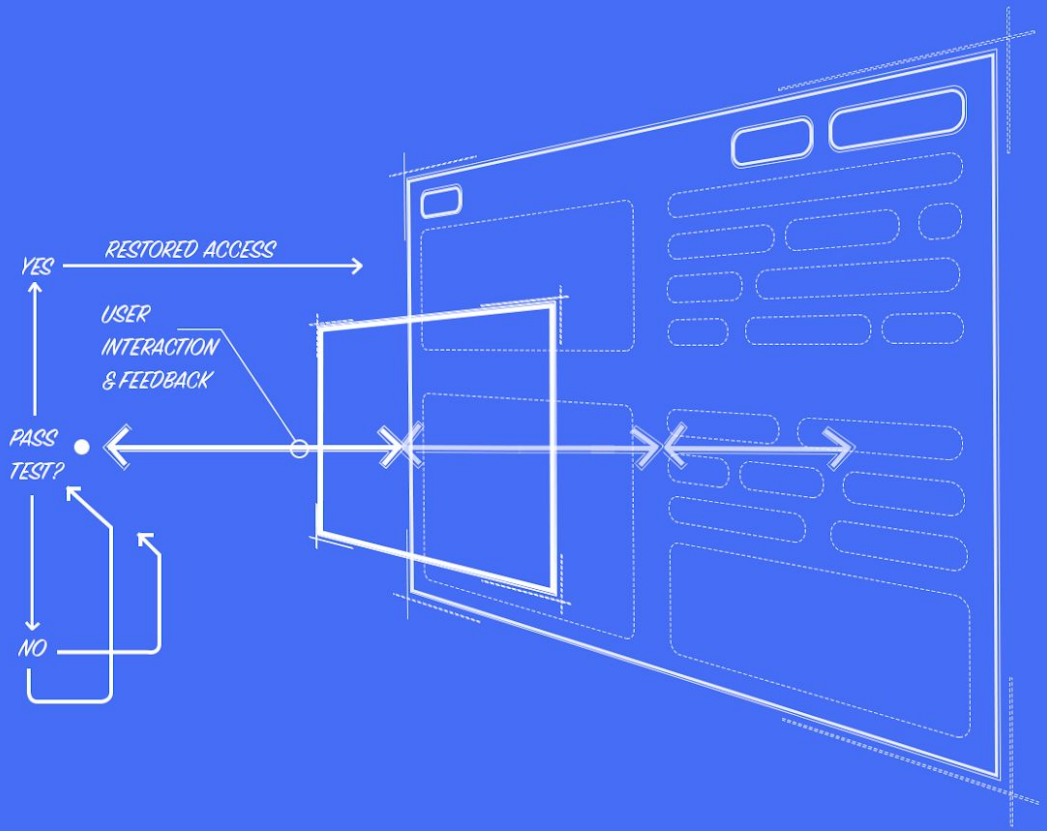
WHAT MATTERS MORE IS A CLEARLY DEFINED PROBLEM STATEMENT





REDUCING SCOPE

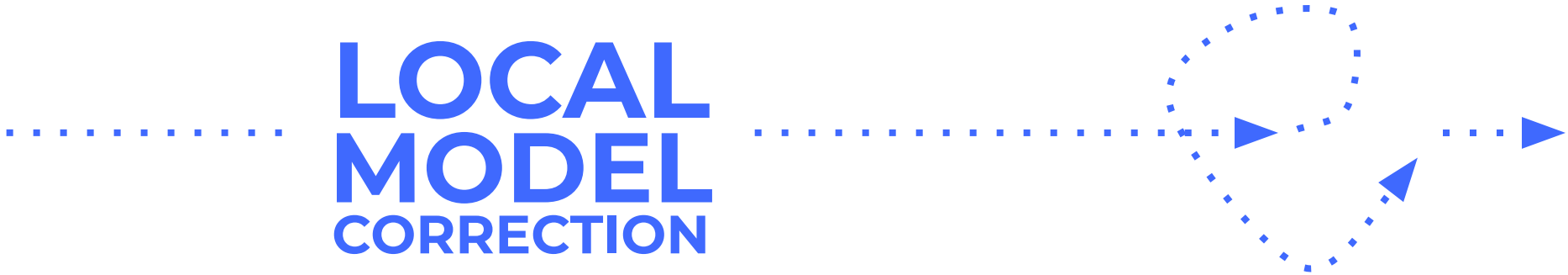
DEFINING EXPECTED BEHAVIOR FOR BETTER RESULTS



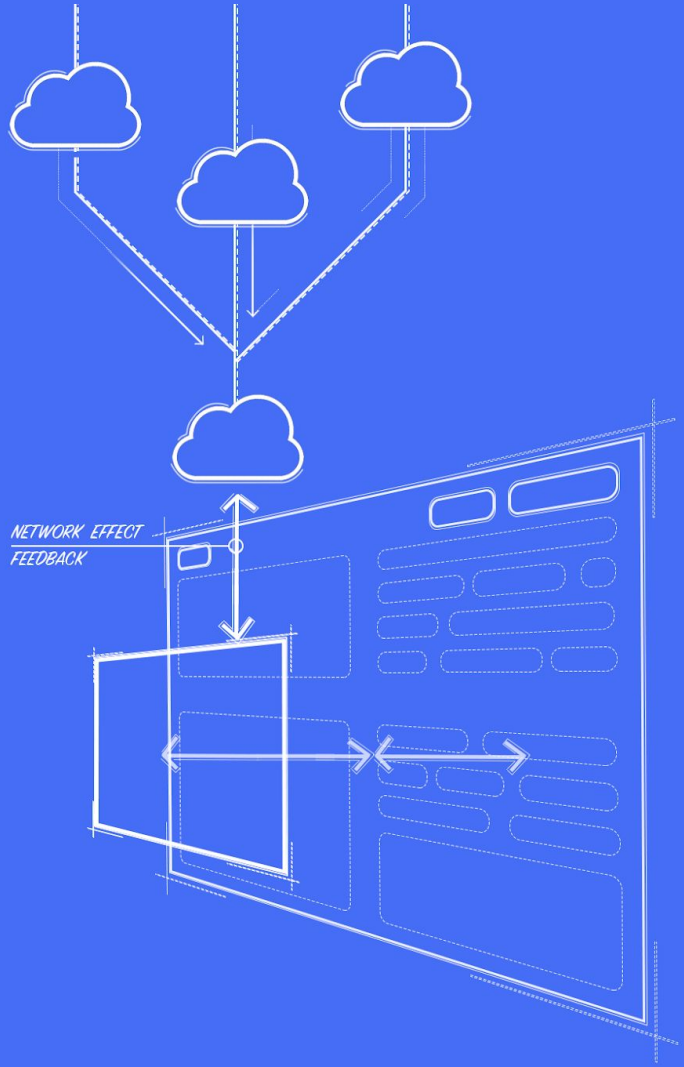
INTERACTIVE REINFORCEMENT

UTILIZING USER INTERACTION AS CONTINUOUS REINFORCEMENT FOR MODELS & HEURISTICS

LOCAL MODEL CORRECTION

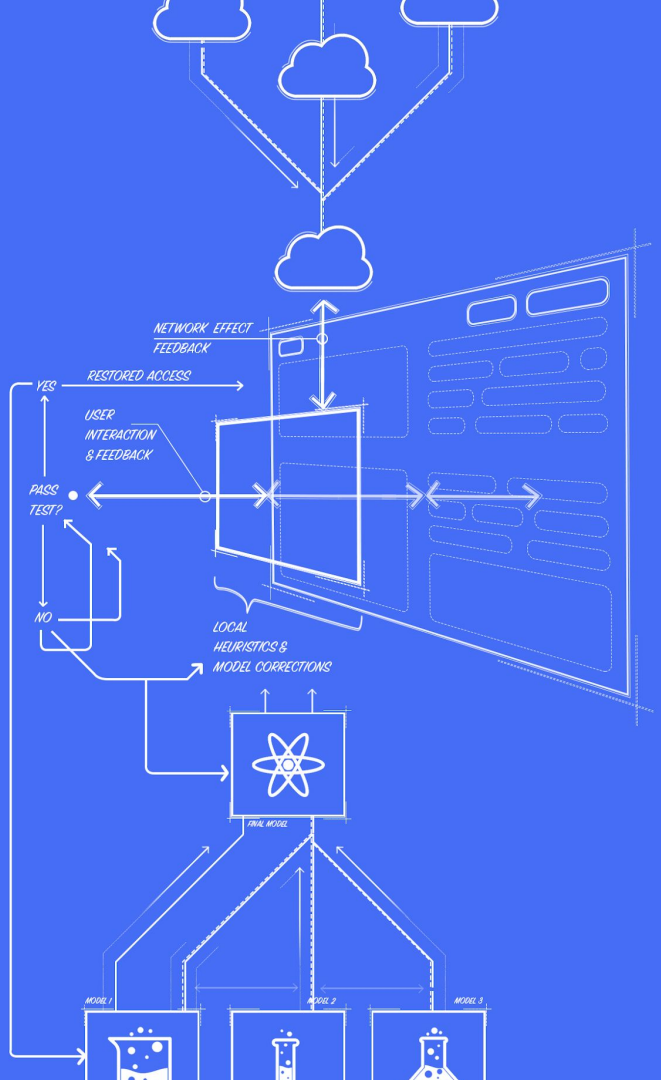


BE SELECTIVE
ABOUT WHAT
TO REINFORCE



GLOBAL *NETWORK* EFFECT

SIMILARITY IN ATTACKS ACROSS MANY TARGETS PROVIDE GLOBAL PERSPECTIVE


NETWORK EFFECT
FEEDBACK
YES
RESTORED ACCESS
USER
INTERACTION
& FEEDBACK
PASS
TEST?
NO
LOCAL
HEURISTICS &
MODEL CORRECTIONS
FINAL MODEL
MODEL 1
MODEL 2
MODEL 3

CONCLUSION

THANK YOU

IM BUILDING
PRODUCTS AT

Arkose Labs

COME SEE OUR
BOOTH #860

Let's connect!

@bubblewire

arkoselabs.com