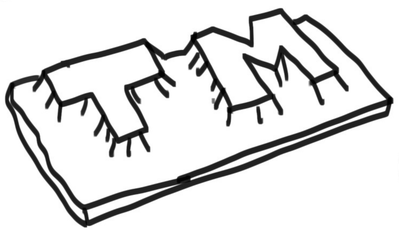
EVOLVING THREAT MODELING FOR AGILITY + BUSINESS VALUE WITH DevSecOps

PANEL TALK

- LANDSCAPE OF TM
- CURRENT TM CHALLENGES
- EVOLVING TM.



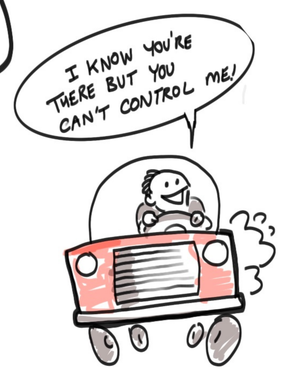
DEPENDS ON THE SCENARIO

WHICH APPROACH IS BEST?

METHODS
STRIDE
- PASTA
- ATTACK TREES

APROACHES
- ATTACKER CENTRIC
- ASSET "
- DEVELOPER "

OUTCOME ORIENTED



CAR EXAMPLE:
WE DON'T CARE IF THE HACKER GETS ENGINE DATA — WE DO CARE THAT THEY DON'T TAKE CONTROL OF THE CAR!

CHECKLISTS ARE FINE — BUT DO YOU KNOW **WHY** YOU'RE DOING THAT??

"IF YOU DON'T ANALYZE THE ENTIRE SYSTEM — IT'S LIKE / TRYING TO SCAN A ROOM LOOKING THROUGH THE KEYHOLE!!"

THREAT MODELING EVOLVES TO BE MORE COLLABORATIVE — SECURITY IS BUILT IN.

EFFECTIVE THREAT MODELING REQUIRES A VARIETY OF PEOPLE —
- DIFFERENT COMPETENCIES
- DIFFERENT VISIONS OF SYSTEM

BIGGEST PAIN POINT
- TOTALLY RELIANT ON AUTOMATED TOOLS
- SILOED APPROACH
- DEPENDANCE ON INSUFFICIENT DIAGRAMS
- STATIC PROCESSES
- OVERTHINK AT START/ NOT INCREMENTALLY
- CHECKLIST DISCOVER KNOWN THREATS

WHAT IS YOUR APPROACH TO RISK?

APPLICATION SPACE HAS EVOLVED

& HAD AN IMPACT ON THE THREAT-MODELING KNOWLEDGE BASE

FROM WEB TO CYBER-PHYSICAL*
* TRAFFIC LIGHTS

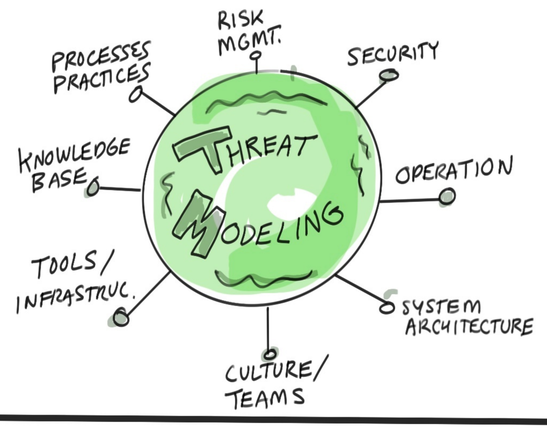
CURRENT DEMANDS
- UBIQUITOUS AGILE + DEVOPS DEVELOPMENT
- ADVANCED SOLUTION FOR EMERGING TECH + PLATFORMS
- FASTER PRODUCT BUILDING
- DEVSECOPS PRINCIPLES CODIFY SECURITY CONTROLS
- STAKEHOLDERS/LEADERSHIP MORE INTERESTED IN THREAT MODELS

HOW MUCH SECURITY IS ENOUGH?

USE YOUR BRAINS!!

THREAT MODELING CAN CHANGE HOW WE THINK ABOUT ATTACKS!

INTEGRATED THREAT MODEL APPROACH



EFFECTIVE THREAT MODELING
- LAYERED: FROM EXPERT + NON-EXPERTS
- INTEGRATED: WITH OVERALL PROCESS
- ACTIONABLE OUTCOME: NEED EFFECTIVE CONTROLS
- CONTINUOUS ACTIVITY: MAKE NEW MODULES
- PROVIDE VALUE TO STAKEHOLDERS: MAXIMIZE VALUE