@awsgeek

AWS 2017 RE:INVENT

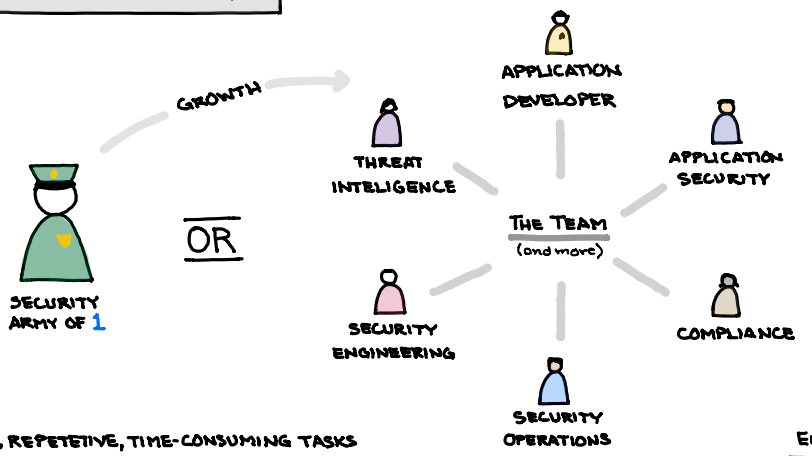
FORCE MULTIPLY YOUR SECURITY TEAM WITH AUTOMATION & ALEXA

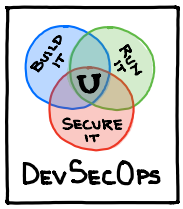
SID302

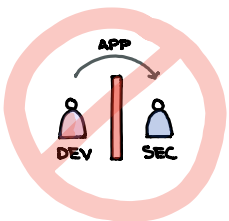
jerry.hargrove

USE AUTOMATION TO EMPOWER INOVATION IN SECURITY

Q WHAT'S YOUR SECURITY AUTOMATION MATURITY LEVEL ?





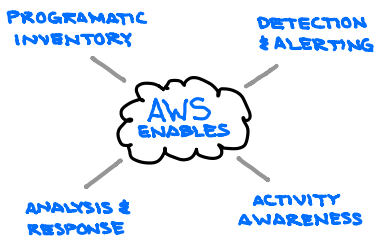


A. MANUAL, REPETETIVE, TIME-CONSUMING TASKS

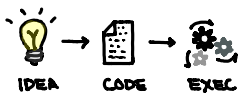
Q. WHAT ARE THINGS THAT MAKE YOU GO 'UGH'?

EMPOWER SECURITY

SAY "HOW?", NOT "NO"



FROM "UGH!" TO "AHA!"



- DESCRIBE OBJECTIVE, SIMPLY
- IS IT BEHAVIOR OR CONFIG?
- WHERE & HOW TO ACCESS DATA?
- HOW QUICKLY MUST IT BE DONE?
- WHAT TOOLS CAN YOU USE?
- WHO CAN WRITE THE CODE?

AMAZON INSPECTOR
SYSTEMS MANAGER
PATCH MANAGER
CLOUD WATCH
CLOUD TRAIL

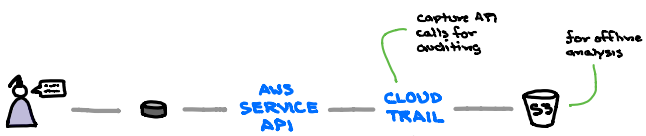
"ALEXA, IDENTIFY INSTANCES RUNNING VULNERABLE SOFTWARE"

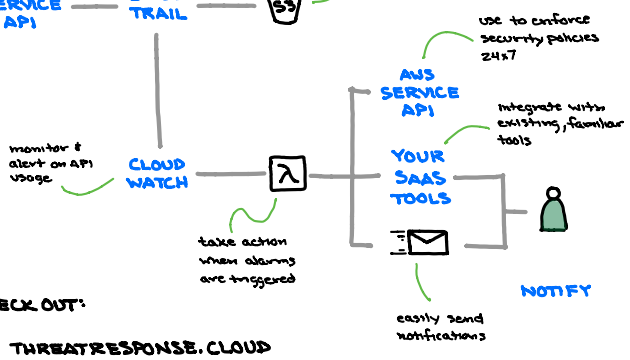
"ALEXA, PATCH VULNERABLE INSTANCES"

"ALEXA, IDENTIFY INSTANCES ACTING ABNORMALLY"

"ALEXA, ISOLATE ABNORMAL INSTANCES"

"ALEXA, RUN FORENSICS ON SUSPICIOUS INSTANCES"





WHAT SHOULD YOU AUTOMATE?

EVERYTHING, STARTING WITH:

COMPLIANCE — AUDIT (SCANNING, INVENTORY, CONFIG CONFIRMATION)

SECOPS — REMEDIATION (PATCHING, REFRESHING)

SECOPS — RESPONSE (ISOLATION, TAGGING, ENFORCEMENT)

THREAT INTEL — ANALYSIS (FORENSICS, LOG DIVING)

REPORTING (SUMMARIES, PIVOTING)

CHECK OUT:

- THREATRESPONSE.CLOUD
- NETFLIX SECURITY MONKEY
- NCC GROUP SCOUT