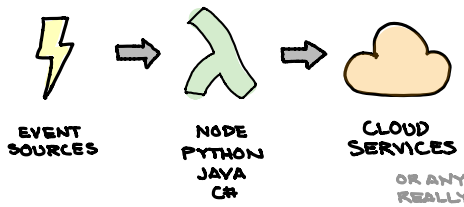
AWS 2017 RE:INVENT — USING AWS LAMBDA AS A SECURITY TEAM — SID301

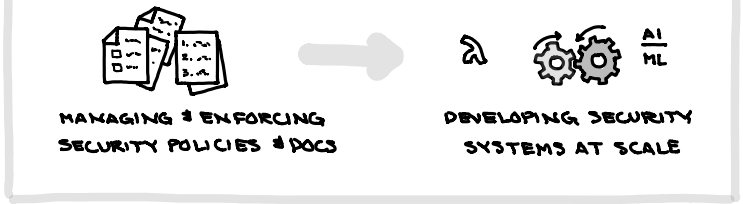
@awsgeek — jerry.hargrove

LAMBDA
- NO INFRA TO MANAGE
- COST EFFECTIVE/EFFICIENT
- BYO-CODE

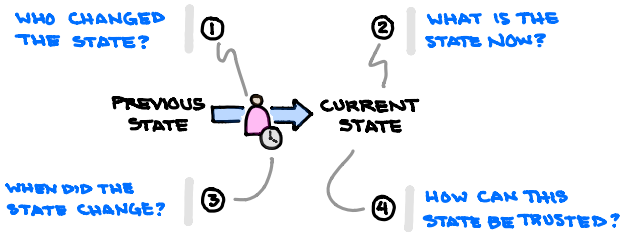
REDUCE OPERATIONAL BURDEN
IMPROVE WORK/LIFE BALANCE



EVOLUTION OF SECURITY ENGINEERING

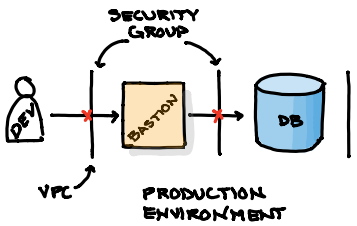


AUDIT



FAMOUS LAST WORDS:

"DON'T WORRY, I'LL CHANGE IT BACK WHEN I'M DONE"



AUDITING GOALS, USING
LOGS, CMDB, CHANGE REVIEW BOARD
ACCESS CONTROL

GOOD AUDIT LOGS ARE:
- IMMUTABLE
- REALITY BASED, AUTO-GENERATED
- COMPLIANCE FOCUSED, NO CHAFF

CHANGE IS EXPECTED, USE:
- AWS CLOUDTRAIL
- AMAZON CLOUDWATCH LOGS
- AWS CONFIG & AWS CONFIG RULES
- AWS LAMBDA

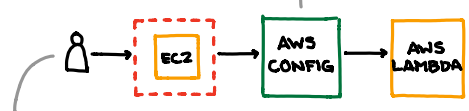
MONITOR

AMAZON CLOUDWATCH ... EVENTS & LOGS
AWS CLOUDTRAIL ..... AUDIT LOGS
VPC FLOW LOGS ..... ENI TRAFFIC
AMAZON MACIE ..... ML/DATA CLASSIFY

AWS LAMBDA
FILTER/ ANNOTATE/ AGGREGATE

YOUR SOC APPS & TOOLS

MONITOR CHANGES TO SECURITY GROUPS



USER CHANGES SECURITY GROUP

FLAG CHANGE AS NON-COMPLIANT
—AND/OR—
SEND NOTIFICATIONS
—AND/OR—
UNDO CHANGES

REMEDIATE

SCALE
COST
SPEED

MANUAL REMEDIATION

ALSO: EC2 RUN COMMAND
AWS STEP FUNCTIONS