SUP311 rapid detection and noise Reduction w/ Automation

same Problems as us
small sec teams

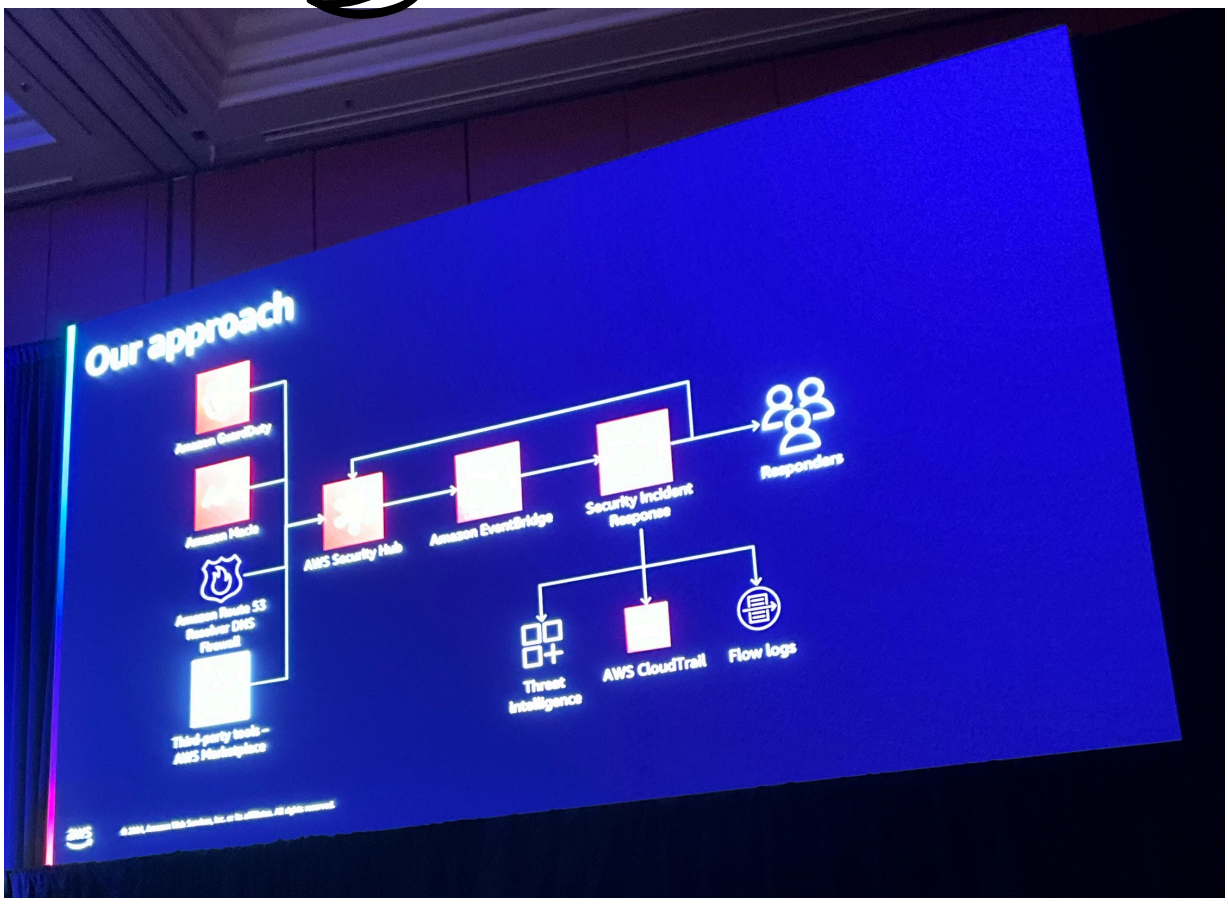
Manual threat triage

work
Fundraise
*Alb logging on by default!

Centeralized logs
automation

Known
good
behavior

Tier 1 all automated



AWS Sec Hub for aggregation

AWS DNS firewall

AWS has managed services

10-12% of findings that could Auct! Investigate