

SNP311 rapid detection

and noise reduction w. Automation

same problems as us

Small sec teams manual threat triage

work Fundraise
* All logging on by default

Centralized automation

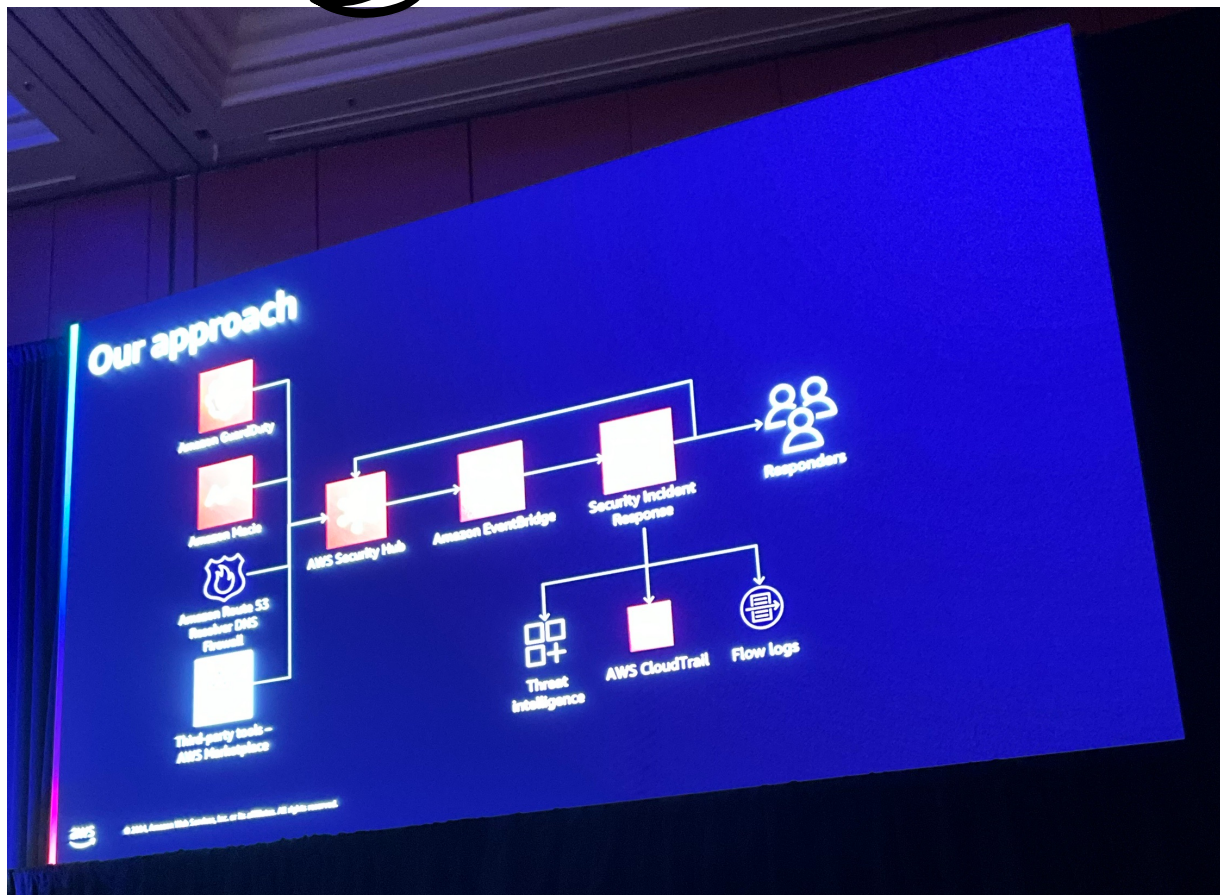
Known good behavior

Our solution

- Aggressive automation
 - We stopped using humans for tier 1 and replaced them with automation
 - Built our automation to identify good, expected activity
 - Data we collect allows us to define a security boundary for individual customers and AWS accounts
 - Encouraged our security engineers to learn Python and contribute to our automation
 - Leveraged data to prioritize development and eliminate repetitive tasks



Tier 1 all automated



AWS Sec Hub for aggregation
AWS DNS firewall
AWS managed services at findings
10-12%
that could
be automated
Actionable