Security in
DIGITAL BANKING

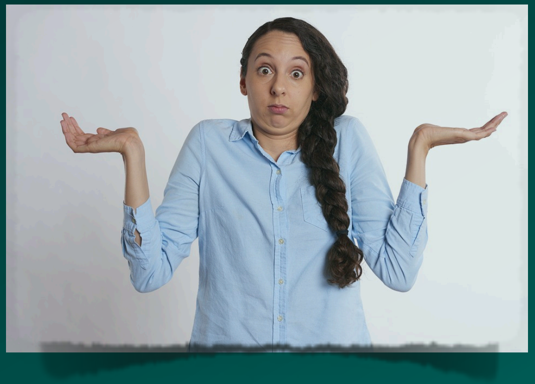
SFAGSD

TL:DR

★ Company 'X' wants build a full service digital bank…

- Security considered paramount and needs to be *world class*
- Extremely short timeframes to satisfy regulator, investor and partners
- Mismatch against audited frameworks adds complexity
- No dedicated cyber staff and limited budget (security managed through ops team)
- Foundation relatively good but little consideration for security in build due to time constraints (build > security)
- Poor security hygiene across the board

Where do we start?



- What DO we have, what WILL we have, what do we need and what do we want (cmdb!, cmdb!, cmdb!)
- Review current architecture, data flows, in/egress points, firewall rules (and configs and all the things)
- Review all cloud connectivity
- Separate the good from the bad
- SOE everyone and everything
- User access review to create UAM for PAM

Where do we start?

- Dump disparate and unmanageable tech (declutter)
- Fix stuff we know works while we monitor traffic
- Bring Dev and Ops together to automate workflows and infrastructure
- Separate test, dev, pre-prod, prod ENVs
- Start dumping tin and migrate to cloud (new dev ENVs must also be SOE)
- Restrict access to cloud ENV + assess security (S3, VPCs, A2A etc)
- Deploy EDR, ISE, Rogue AP detection

Meanwhile…

- We got hit (batten down the hatches)
- Incident response needed a wake up call, procedure reworked and tested
- Start rolling out 2FA, federate devices, split domains and ISE the rest
- Shift responsibility to AMS
- Time based access through security groups to restricted areas

continued...

- Development of use cases specific to bank through high level threat modelling exercise
- Preparation for PCI assessment, int audit and ext audit
- Basic attack path mapping
- Pentest pentest pentest