AWS Security Faux Pas

What To Do Before You Get Penetration Tested

Name: Blaise St-Laurent
Title: Architecture & Cloud Lead
Date: Nov 2020

Who am I?

- Architecture & Cloud Lead
- 22 years in the security field
- Came from a network security background
- Cloud agnostic, but primarily AWS and Azure focused; for my sins I've even worked in Oracle Cloud

ZX Security

- Organisation structure:
  - 25 staff
  - 7 years in business
  - 2018 Deloitte Fast 50
  - CREST Certified

ZX Security

- What we do:
  - Web based security testing (API, website etc)
  - Internal and external penetration testing
  - Specialist work (hardware, red team, physical access)
  - Security design and architecture reviews
  - vCISO, SLT security advice and consulting
  - And of course cloud security reviews

ZX Security

- Client Size:
  - 2 seats – 800,000 seats
- Client Location:
  - NZ (Oceanic)
  - North America
  - Europe
  - Asia

ZX SECURITY

ZXSECURITY.CO.NZ

AWS Security – Broad trends

- Mostly from Gov't point of view:
  - People have largely stopped trying to do P2V(cloud)
  - AWS is its own world, not just a handy alternative to VMWare
  - Lots of "failed" first attempts

AWS Security – Broad Trends

- DevOps is driving a lot of excitement
  - The basics aren't necessarily done well though!
- Security is mostly still focused on S3 buckets being secured
- Serverless is sexy but scary, still being digested as a concept

How ZX Assess Cloud Security

- Automated and manual testing:
  - Automated to perform reconnaissance and get the low hanging fruit
  - Manual testing / examinations to confirm and dive deeper
- Also examine any source code, externally facing resources

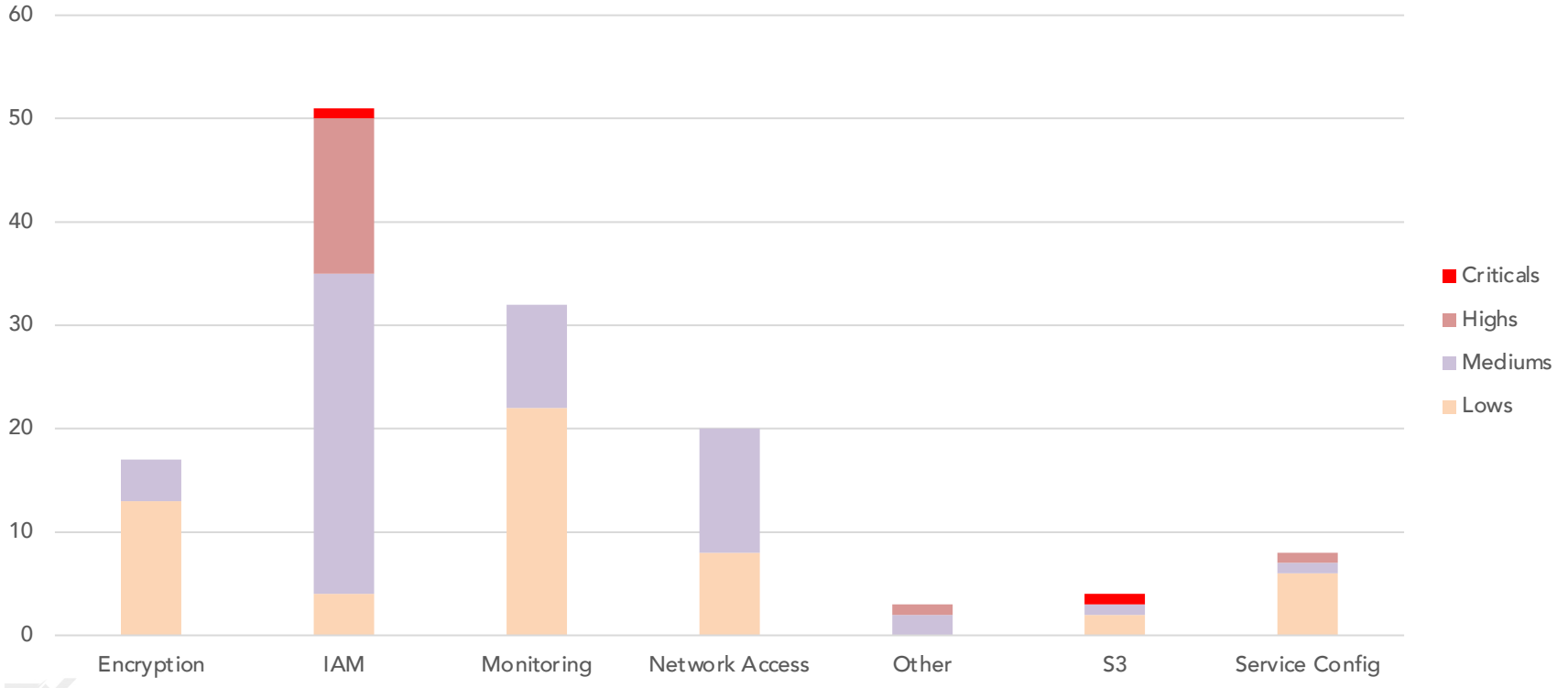
ZX SECURITY

ZXSECURITY.CO.NZ

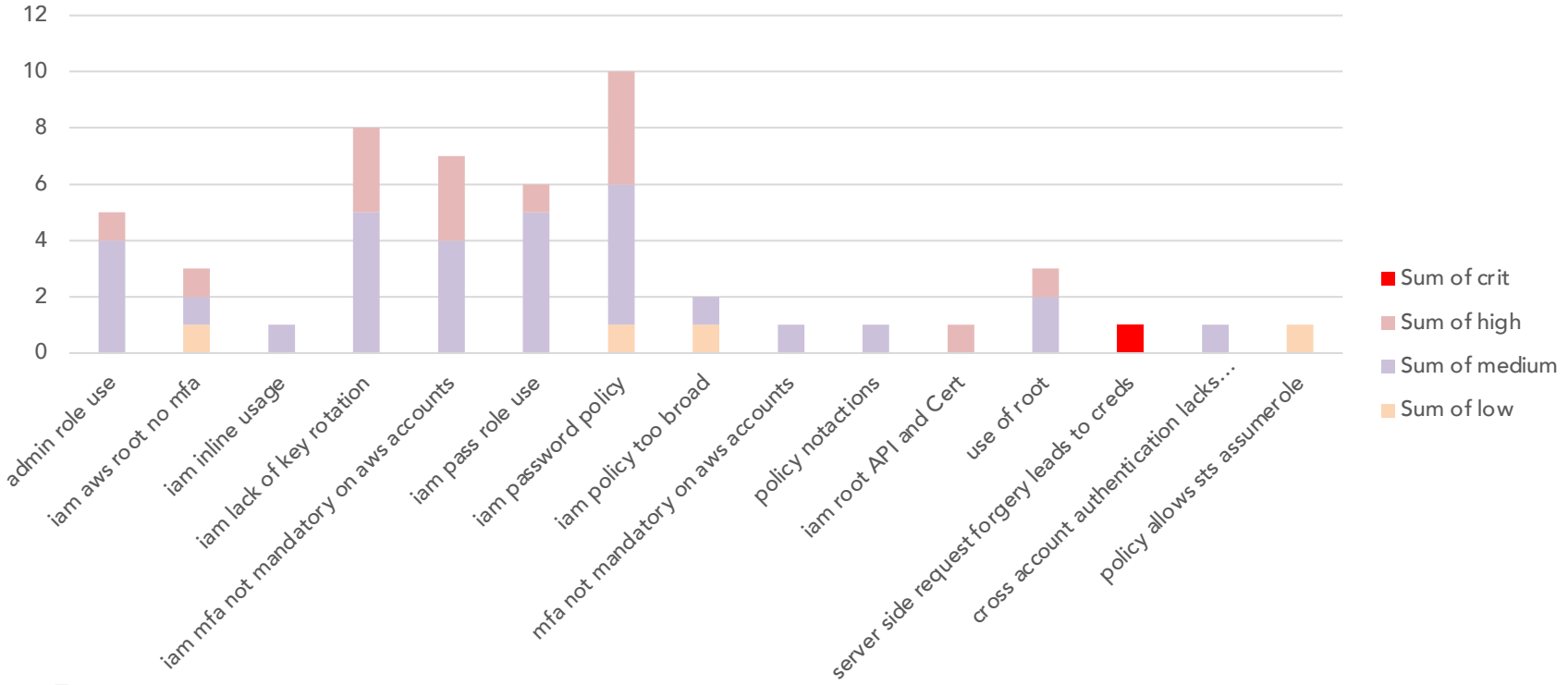
The Data

- Pulled from 20+ reports over the last 24 months
- ZX uses normalized findings for many common issues so we can compare across customers
- Issues' impacts and likelihood change depending on context
- Note we are looking primarily at how common they are, this can be for a few reasons:
  - Easy to pick up programmatically
  - Not a default setting

Broad Trends



IAM Deep Dive



IAM Major Issues

- Password policy
  - Over-represented thanks to NZISM / Audit / Compliance
- Lack of Key Rotation
- Policy Configuration issues:
  - PassRole / AssumeRole (both sts and IAM)
  - NotActions
  - General Sloppiness
- Server-Side Request Forgery!
  - CapitalOne
  - Major Networking Vendor

Monitoring Deep Dive

Summary of Critical and High Findings

- Critical: World writeable bucket
  - Better: it had root creds stored in a file
- Critical: SSRF leads to metadata server in EC2
- Lack of key rotation (especially important on CI/CD)
  - Keys copied into github
- SNS Publishing open to public

Other Important Findings

- Administrator role use abused
  - Spinning up resources unapproved for company use
- No MFA (admins and root)
- Password policy
- PassRole use – iam:* is a terrible idea
- Inspector findings ignored – why have it?
- Logging absent or ignored

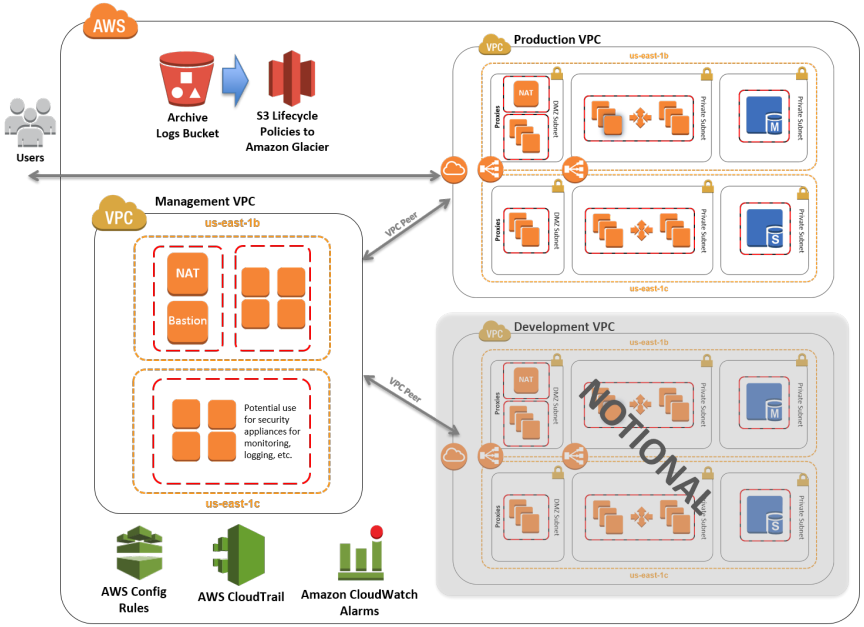
AWS Security Services

- Almost too many of them - https://aws.amazon.com/products/security/
- Critical ones to understand fully:
  - IAM (!!!)
  - CloudTrail / CloudWatch / Config
  - Inspector / GuardDuty
  - AWS Shield and WAF
  - AWS KMS, Cert Mger and Secrets Mger

Free Tools

- Current opensource toolset takes a little effort to get running.
- Cloud Security Suite - https://github.com/SecurityFTW/cs-suite
- ScoutSuite - https://github.com/nccgroup/ScoutSuite
- Prowler - https://github.com/toniblyx/prowler
- Awsume - https://github.com/trek10inc/awsume
  - Manages all the different roles / auth you're likely to do
- AWS-Vault - https://github.com/99designs/aws-vault
- Firefox with Multi-Container plugin (to manage different logins to the console)

What Does Good Look Like?



AWS PCI-DSS - https://aws.amazon.com/compliance/pci-dss-level-1-faqs/
CIS AWS Foundations Benchmark - https://www.cisecurity.org/cis-benchmarks/
NZISM --- lol.

What Does Good Look Like?

- Separate AWS accounts:
  - Management Account – Users, groups, auth.
  - Archive / Security (either in Management, but better in its own account)
  - Separate accounts for each application stack (either prod / pre-prod, or more granular)
- Everything tracked using Config
- Everything logging (EC2 OS, ECS, All of AWS Mgmt) back to a common bucket
- CloudWatch monitoring and notifying on anything suspicious.

What Does Good Look Like?

- Users (humans, automated, etc)
  - MFA ALL THE THINGS! If people use it, MFA
  - All users defined in Management account, assigned to groups
  - Groups assigned to Roles which are allowed to AssumeRole into other Accounts.
  - MFA and External ID required for any role assumption

What Does Good Look Like?

- Roles / Policies:
  - The lifeblood of security in AWS – where most of the mistakes happen
  - Roles used to interact with AWS, component to component!
    - ex: EC2 instance can be granted a role that can allow anyone with a login to the box to create other EC2 instances!
  - AWS provides TONS of appropriate pre-configured policies, use them!

LinkedIn: Blaise St-Laurent
Email: Blaise@zxsecurity.co.nz
Website: zxsecurity.co.nz