Identity Crisis

Multi Cloud IAM
$ whoami - Julian Wiegmann

- if worktime < 7:
  - networking, firewalls, solaris/nix*, web proxies, DNS, waf, network intrusion detection
- elif worktime > 7 and worktime < 15:
  - SOC, I&R, SIEM, EDR, detect & prevent, projects like email security, sandboxes, etc.
  - Managing a great team and managing security *implementation and operations* projects
- if oldandwise ?= true:
  - Cloud Security full time

Love cyber security, love learning & challenge of securing companies
Intro
Multi Cloud Security is Challenging
IAM is key to understand

Look the same but are different
IAM is always relevant
Basics
What is IAM?
Old School Security

- Bad is on the outside (Internet)
- Secure the perimeter
  - Firewall / DMZ
- Flat and “secure” LAN
- Approach moved to inside LAN
  - Control inside with ‘firewalls’ and vlans etc.
    - “what can communicate with what”
- Did not and does not work!
Identity is the new Perimeter

- Cloud is inherently “on the Internet”
- How we work, we want to work and deliver software is
  - “on the Internet / Web”
- Loosely coupled software architectures need to communicate securely in insecure networks
- Everything ‘authS’ and everything has an Identity
- “who can communicate with who”
Cloudy IAM
Cloud IAM

- Each cloud has its own IAM (solutionS) and two basic IAM scopes
  - Control Plane
  - Data Plane
- Cloud providers design and build their services ‘around’ their IAM
- Typically two types of identities
  - Humans & "Infrastructure / Apps / Service” identities
- Granular role-based access control
- “Least privilege” & “Zero Trust” is implementable
- “who can communicate with who” with granular “with which permissions” & sometimes “conditions”
Cloud is Secure

Easy job for me?
No

Biggest threat in cloud security is:

- Misconfiguration (our fault not CSP)
- 61% of cloud breaches are due to credentials/access
- Impact of Incident depends on how well you implemented IAM
- Loads of offensive tools for cloud IAM exists (misconfigurations / features) to find and abuse misconfigurations
- Some bad defaults by CSPs around IAM
Study and Crisis
Need to deep dive / learn IAM

- IAM is king, IAM is key, everything is around IAM
- Of course I get and know IAM generally
  But:
- Primary cloud knowledge = GCP
- Basic understanding of Azure and Azure AD too
- Now also need to understand AWS
and I want to really ‘understand’!
Let's understand AWS Policy evaluation logic.

1. **Decision starts with Deny**
   - Is the principal's account a member of an organization with an applicable SCP?
     - No: Evaluate all applicable policies
     - Yes: Does the requested resource have a resource-based policy?
       - No: Does the principal have an identity-based policy?
         - Yes: Does the principal have a permissions boundary?
           - Yes: Is the principal a session principal?
             - Yes: Final decision: Deny (implicit deny)
             - No: Final decision: Deny (implicit deny)
           - No: Is there a session policy?
             - Yes: Is this a role session?
               - Yes: Final decision: Allow
               - No: Final decision: Deny (implicit deny)
             - No: Final decision: Deny (implicit deny)
       - No: Is there an Allow?
         - Yes: Final decision: Deny (implicit deny)
         - No: Final decision: Deny (explicit deny)
   - Yes: Final decision: Deny (explicit deny)

2. **Deny evaluation**
   - Organizations SCPs
   - Resource-based policies
   - Identity-based policies
   - IAM permissions boundaries

3. **Session policies**
   - Final decision: Allow

---

*A session principal is either a role session or an IAM federated user session.*
But…

**Policies** is the hardening/baseline for the cloud control plane & service in Azure

**Policies** are “Conditional Access Policies” in Azure Active Directory which check “if/when you can authenticate”

IAM **Policies** in GCP define ‘who’ can do ‘what’ depending on the role that is attached to the resource

Why are there so many steps and different ‘**policies**’ in AWS…

What did I do…
Understand how “Deny” authorizations works

- Not generally available in GCP, “transitive” allow policy system
- Not possible in Azure unless you use Azure Blueprints
- But you can have ‘notActions’ (not allowed?) in Azure “Role Definitions”
- There are implicit denies in AWS “permission boundary”, “Organizations SCPs” or “session policies”
- But also explicit denies in the AWS “IAM policies”
Crisis
Approach

- Slow down
- Focus on one (cloud + topic)
- Make notes on
  - key concepts
  - key terminology
- Mind-map / draw how things relate
- Test / try everything in each cloud
Google Cloud IAM Concepts

who (identity) has what access (role) for which resource

- Permissions per API
- IAM permissions (read, write, create, delete)
- Custom Roles
- Predefined Roles
- Organization IAM
- Project IAM
- Service Account IAM
- User IAM

Types
- Users
- Groups
- Service Accounts
- Roles
- Policies
- Conditions

Create & Manage
- IAM
- Resources
- IAM Policy
- Allow Policy

Add & Manage
- IAM
- Resources
- Role Bindings

Remeber:
- IAM Policy: All users have read access to IAM policies.
- Role Bindings: IAM roles are not assigned to users directly; instead, they are assigned to groups, service accounts, or organizations.
- IAM policies can be used to allow or deny access to resources.
- RoleBindings can be used to allow or deny access to resources.

Conditions (Logic Block)

Note: Granting a role is also known as creating a role binding to an allow policy. Lower-level resources inherit the allow policies and role bindings of higher-level resources.
Free to use

Medium: Visualizing Multi Cloud IAM Concepts
Short: shorturl.at/ceorT
Some tips around IAM

- Take it slow, try and test in each cloud what you learned step-by-step
- You cannot defend it if you do not know how the attackers hack it (basics knowledge is enough)
  - Always use ATT&CK, pentesting, red teaming talks/videos/github tools and knowledge sharing to understand how IAM can be hacked/abused/used by malicious actor

Thank you