ACCESS '23

> Humans do not have or need access to production cloud accounts

ACCESS '23

> By default, ALL cloud access is privileged access

ACCESS '23

Set Your Identity Baseline

Business Objective: "Enable secure cloud access to facilitate innovation"

Treat ALL cloud users as Privileged Access

- Require multi-factor authentication
- Use temporary credentials
- Log all access

Map your internal identities to the cloud

- Centralize Identity and Access management
- Set up single sign-on
- Apply cloud managed identity policies

Recognize all identities

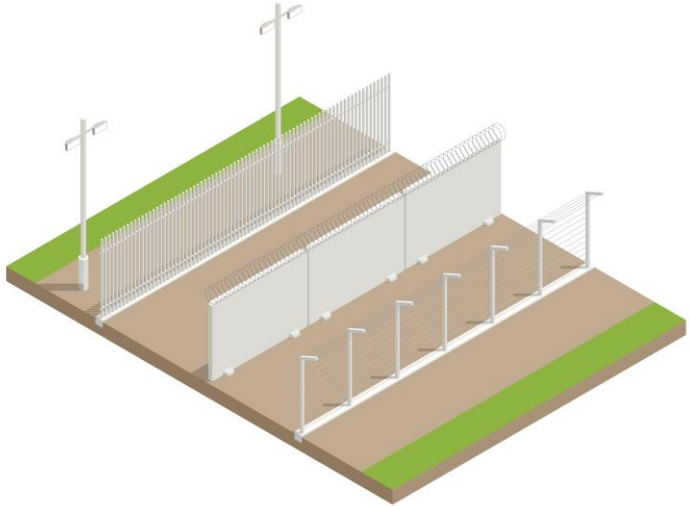
- Cloud Users
- Application Users
- Service Accounts
- Account Owners
- Root Users

Temp Cred Lab

Account Owners

ACCESS '23

Create layers that enable and protect the business



ACCESS '23

Build Your Identity Defenses

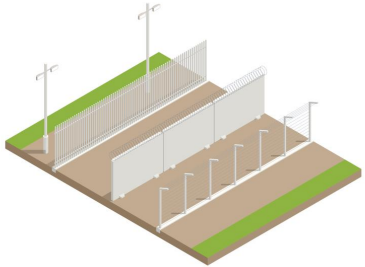
Business Objective: "Enhance security while enabling rapid resource provisioning for faster development"

Build the fences, gates, and guardrails

- Create guardrails permissions for organization
- Create fences with permissions boundaries in accounts
- Create gates with conditions to limit users and roles

Automation pipeline

- Deploy Infrastructure as Code (IaC)
- Deploy identity as code



Secure high risk identities

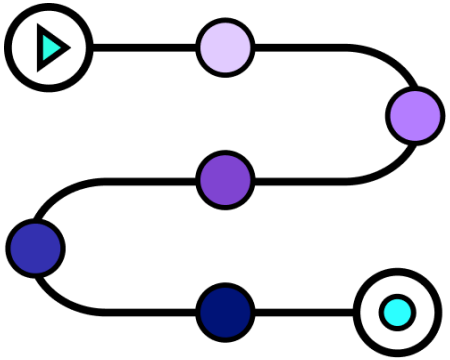
- Root Users
  - Lock away
  - Build break glass
- Service Accounts
  - User keys to roles
  - Secrets management
  - Rotated keys

Break Glass

Boundaries

ACCESS '23

> Nobody wants to buy least privilege



ACCESS '23

Tune Your Identity Access

Business Objective: "Enable a robust least privilege access control framework that streamlines operations, simplifies compliance, minimizes human error and disruption, enhances security processes, while facilitating seamless scalability. "

IAM Analyzer

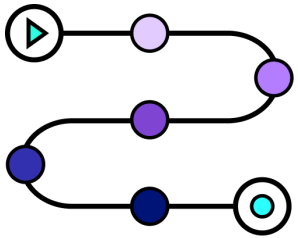
Sonrai Demo

Drive down risk

- Focus on Business Objectives
- Work backwards from data impact

Use automated tools to identify high risk

- Role chaining
- Cross account access
- Unintended public access



Move toward least privilege

- Focus on Business Objectives
- Customize identity policies
- Use automated tools to baseline use
- Secure users and resources
- Look for opportunities to simplify

ACCESS '23

> You do not know,
> what you do not know

ACCESS '23

Monitor Your Identity Access

Business Objective: "Enable instant provisioning for users and environments to maximize efficiency and minimize risk while expediting the delivery of products, features, and services to market, optimizing efficiency, time-to-market, and operational agility."

Honeytoken

IAM Vulnerable

IAM Analysis

Pipelines

- Inspection
- Enforcement

Detect

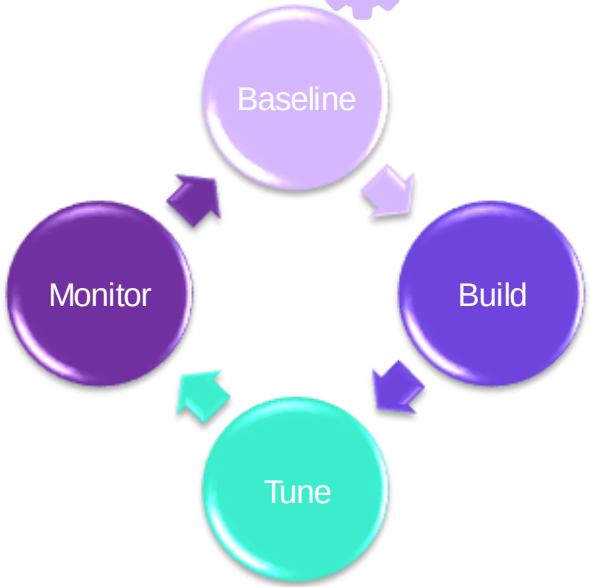
- Honeytokens
- Changed identities/roles
- Key or root usage

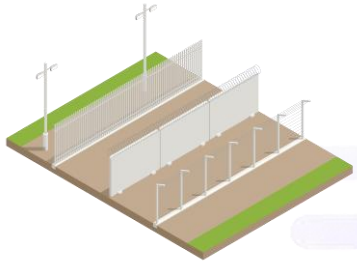
Monitor and Maintain

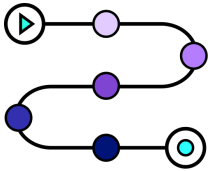
- Unused identities/roles
- Stale identities/roles
- Overly permissive roles
- Unused permissions in roles

Respond

- Red/Blue Team
- Pen Test
- Tabletop Playbooks


Baseline
Build
Tune
Monitor





ACCESS '23

Thank You
and godspeed on your cloud journey!

Appendix

Set Your Identity Baseline

ACCESS '23

- MFA

  https://aws.amazon.com/iam/features/mfa/

- SSO/Identity Center

  https://aws.amazon.com/iam/identity-center/

- Account Owners

  https://aws.amazon.com/blogs/mt/manage-aws-account-alternate-contacts-with-terraform/

- Temporary Credential Lab

  https://www.wellarchitectedlabs.com/security/quests/quest_100_simplest_security_steps/

Build Your Identity Defenses

- Guardrails permissions for organization

  https://aws.amazon.com/blogs/security/when-and-where-to-use-iam-permissions-boundaries/

- Permissions boundaries in accounts

  https://docs.aws.amazon.com/prescriptive-guidance/latest/transitioning-to-multiple-aws-accounts/creating-a-permissions-boundary.html

- User conditions

  https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-use-conditions.html

- Cross account policy logic

  https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic-cross-account.html

- Break Glass

  https://github.com/aws-samples/aws-cross-account-break-glass-example

  https://github.com/awslabs/aws-break-glass-role

Tune Your Identity Access

- Role-Chaining

  https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_control-access_monitor.html

- Simplify with ABAC

  https://aws.amazon.com/identity/attribute-based-access-control/

  https://aws.amazon.com/blogs/security/control-access-to-amazon-elastic-container-service-resources-by-using-abac-policies/

  https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_attribute-based-access-control.html

- Automation Examples

  https://sonraisecurity.com/recorded-demo/

  https://aws.amazon.com/iam/features/analyze-access/

Monitor your Identities

ACCESS '23

- HoneyTokens

  https://blog.gitguardian.com/creating-a-honeypot-token-tutorial/

  https://aws.amazon.com/blogs/security/how-to-detect-suspicious-activity-in-your-aws-account-by-using-private-decoy-resources/

- Privilege Escalation

  https://bishopfox.com/blog/privilege-escalation-in-aws

  https://github.com/BishopFox/iam-vulnerable

- Monitoring

  https://aws.amazon.com/blogs/security/continuously-monitor-unused-iam-roles-aws-config/

- Testing and Response

  https://aws.amazon.com/blogs/security/analyze-and-understand-iam-role-usage-with-amazon-detective/