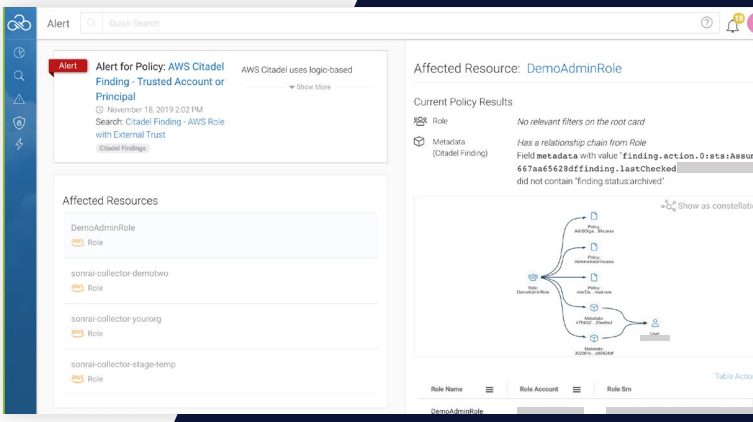
sonraí SECURITY

Integration with AWS

Who Can and Has Accessed AWS Resident Data, Resources, and Infrastructure?

Organizations building applications on AWS quickly discover how important identity and access management (IAM) is to securing data resident in public cloud. A poor IAM configuration can expose corporate data to potential breaches by an external actor or an over-permissioned insider. Sonrai Dig, our identity and data governance platform, helps organizations understand and monitor IAM, configuration helping to eliminate weak or accidental configurations that if left unchecked, will inevitably lead to a disaster.



Increased Visibility Into AWS Workloads

- Cross-account configuration checks for possible data exposure from poor usage of configuration and trust relationships.
- Automated alerts for overprivileged IAM users or compute.
- Timely notification of high risk IAM, network, and resource configurations.

Assess AWS Policy Change Risk

- Continually monitor configuration drift against an approved baseline
- Integrated use of AWS resource tags to align risk with workload classifications
- Strong audit capabilities of changes to configuration and data access

Answer Important AWS Questions

- Who has accessed AWS resources and data?
- Who can access AWS workload data and their components?
- Does the AWS IAM configuration properly protect data if a credential is stolen or misused?

Supports for 189 AWS Services

- Data stores including S3, RDS, DynamoDB, and more
- Compute including EC2, Lambda, and more
- Other services including key management, networks, load balancers, and more

Ready to graph, identify, and monitor identities and data inside your AWS? Request a demo today.

sonraísecurity.com | info@sonraísecurity.com | 646.389.2262

sonraí SECURITY