

# ACCESS<sup>'23</sup>

The Cloud Identity, Access, and Permissions Summit

## Securing the Inevitable: Disarming Identity and Permissions Risks in Your Cloud

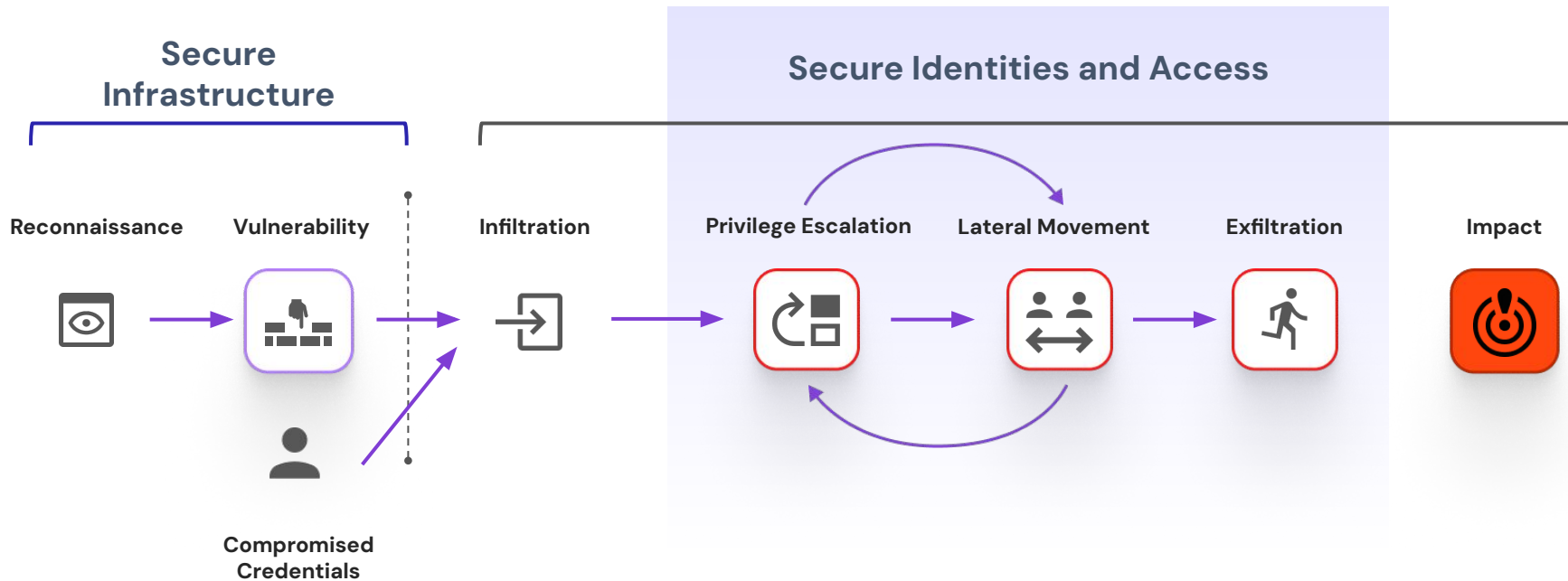
Sandy Bird, Co-Founder and CTO



sonrai  
security

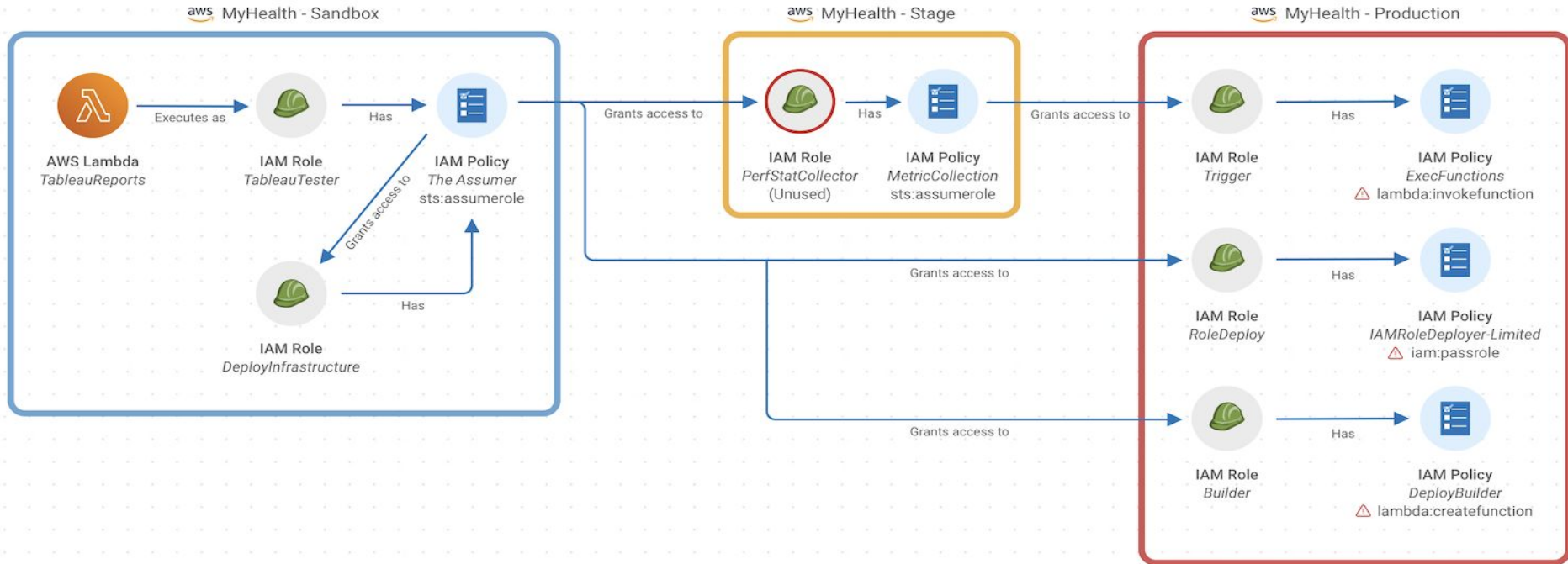


# Securing Identities Stops Intruder Advancement

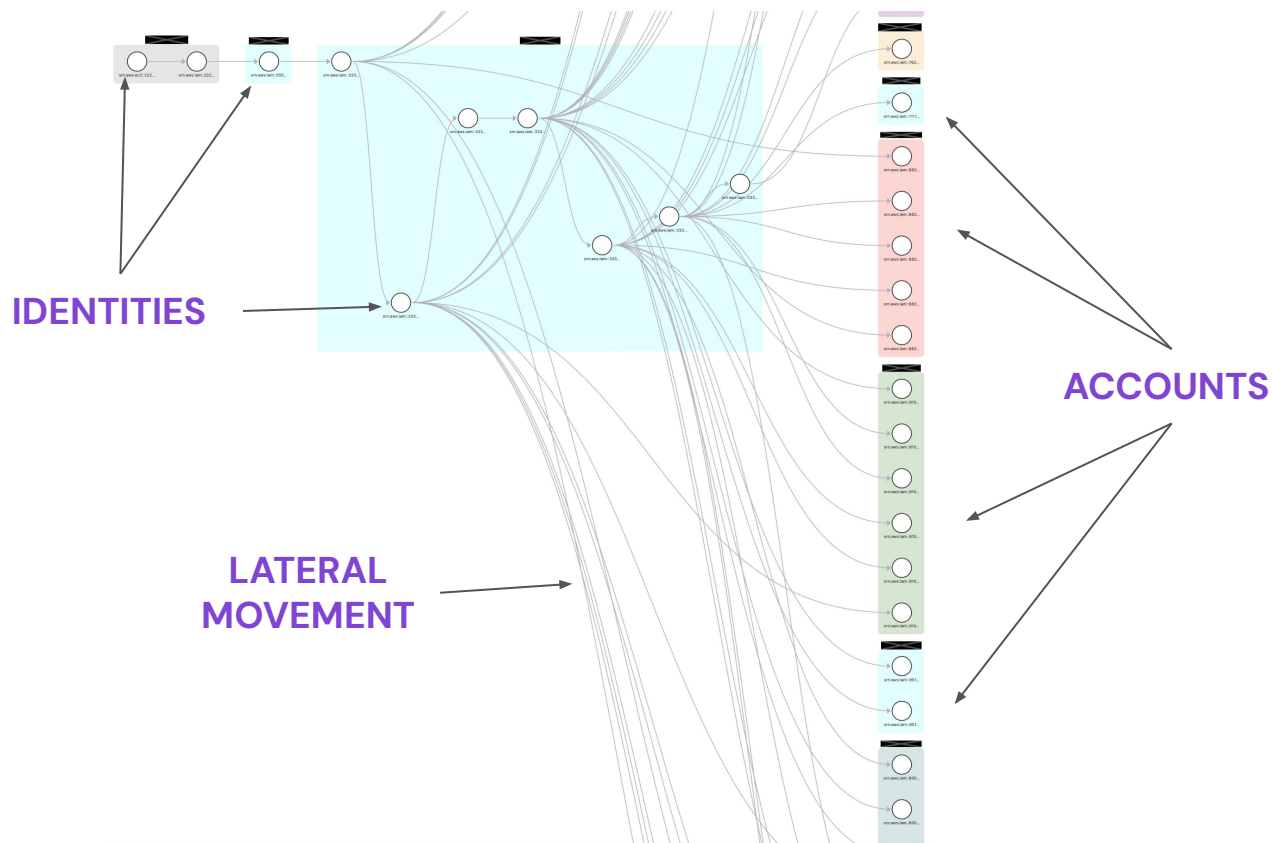


**Intruders find points of access.  
Securing identities is an effective way to stop their advancement.**

# Lateral Movement Through Escalation and Pivoting



# Lateral Movement through Access to Access

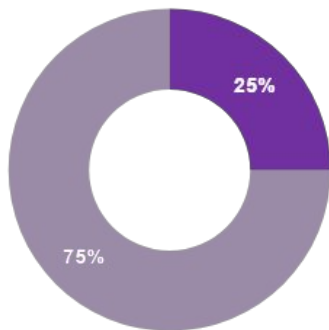


# Removing Unused Identities Is Important

## CUSTOMER EXAMPLE

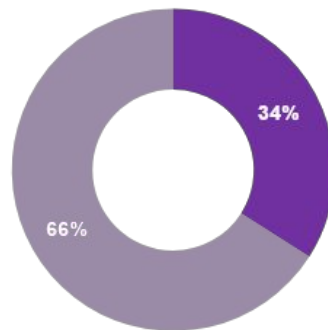
### Total identity

■ Fixed ■ Remaining



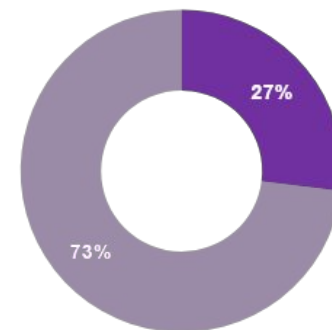
### Third-party trust

■ Fixed ■ Remaining



### LATERAL MOVEMENT

■ Fixed ■ Remaining



# What to Do in Your Own Cloud Environment

1



## Certify all critical accounts:

break glass roles,  
infrequent  
automation roles,  
and highly  
privileged roles

2



## Delete all:

never-used  
identities  
(IAM users, roles)

3

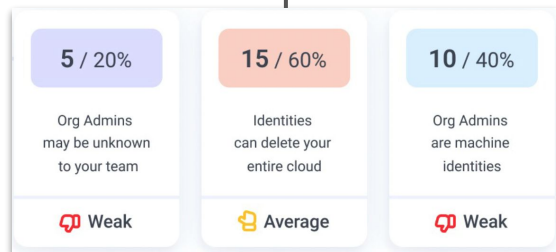
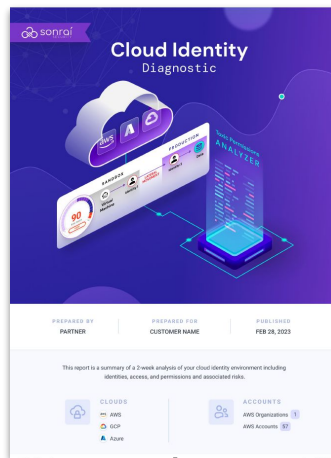


## Deny or remove:

STS AssumeRole  
and PassRole from  
every identity that  
doesn't use the  
permission

# The Cloud Identity Diagnostic

- Fast Answers
- Immediate Actionability
- Clear Strategy



## Output Includes:

- Overall Identity Risk Summary
- Full Summary of Privileged Identity Usage

## Comprehensive coverage across 6 core identity domains

- Access Key Hygiene
- Identity Fundamentals
- Unused Identities
- Trust
- Overprivileged Identities
- Lateral Movement Risk

# Q&A