Non-People Identities
The New Battleground in Cloud Security
Our Speakers

**Kelvin Coleman**
Executive Director
National Cyber Security Alliance

**Eric Kedrosky**
Director of Cloud Security
Research & CISO
Sonrai Security

**Dave Shackleford**
Founder & Principal
Voodoo Security
What we’d like to talk about

- What exactly do you mean by “Non-People Identities?”
- What problems do Non-People Identities cause?
- What are some best practices for managing these types of Identities?
- Steps you can take today and strategies for continuous protection
Non-People Identities Defined

Types of Non-People Identities

Compute Processes
Virtual Machines, EC2 instances, Serverless functions, etc.

IT Administration
Shared accounts, service accounts, technical accounts

Automation
Deployment role, Infra as Code, Bots, etc.

Cloud Services
AWS Config, Azure Advisor, etc.

“Non-person identities are pieces of compute, digital identities, that have access rights and control over other identities or pieces of compute in your public cloud.”
Non-People Identities Are Everywhere In Your Cloud

Global Restrictions and Resources Policies
Unfortunately, It Happens Everywhere
Patterns of Escalation in Public Cloud

Direct Self Escalation
Identity can modify its own rights to make itself an administrator

Indirect Escalation
Identity can modify another identity’s credentials to impersonate it

Unintended Inheritance
Cloud IAM or RBAC permission gives access at a level not intended

Confused Deputy
Identity with a low level of permissions gets access to a resource or service with a higher level of permissions and directs it to perform actions on its behalf

Resource Permissions Escalation
Identity has permission to change the configuration settings on a resource to allow the identity to perform unintended actions on that resource
Good news: Non-People Identities Can Be Managed

Best Practices to Consider

- Carefully create and manage “break glass” Identities
- Have a team or process responsible to certify Identities regularly
- Avoid over-permissioning: develop an approach to get to and maintain least privilege.
- Kill dormant identities
- Continuously monitor your identities for behavior and/or permissions changes
- Continuously monitor for Privilege Escalation risks.
What Sonrai Focuses On in Cloud Security

Identity Governance
- Eliminate all identity risks.
- Get to Least Privilege and stay there.
- Continuously monitor for deviations.

Data Governance
- What Non-Human Identities can access your data?
- How can they access it?
- What are they doing with it?

Platform Governance
- Build cross-cloud platform security with Intelligent CSPM.
- Build in your cloud controls.
- Alert on deviations.

Governance Automation
- Governance Automation Engine helps companies to shift left and integrate teams.
See into your cloud. Find Your Risks. Prioritize your Alerts.

**Infrastructure Overview**

<table>
<thead>
<tr>
<th>All Infrastructure</th>
<th>Compute</th>
<th>Images</th>
<th>Network Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>☁️ 4586</td>
<td>⚡️ 964</td>
<td>☑️ 1897</td>
<td>⚑ 34</td>
</tr>
</tbody>
</table>

**Top Identity Risks Identified**

See under the hood of your public cloud identity performance. Stop guessing and find out exactly where you risk lies. Here is a breakdown of your identity risks that need attention.

**Top Data Risks Identified**

Most organizations worry about data breaches caused by cybercriminals. However, risk from carelessness around securing people and non-people identities are often overlooked. Here is a breakdown of your data risks.

- Encryption not Enabled on Data Containers - Buckets: 49 Findings
- AWS Compute - S3 Permission to Discover all Buckets and Read all Data: 19 Findings
- Public access to data (Object): 7 Findings
Thank You!

Sonraí Security Headquarters
261 Madison Ave, 9th floor, NY, NY 10017
P: (646) 389-2262 E: info@sonraisecurity.com