



How to Achieve Least Privilege at Cloud Scale with Cloud Infrastructure Entitlements Management (CIEM)

Maya Neelakandhan

Founding engineer, Head of Customer Success



Agenda

◆ CIEM and Cloud Permissions Gap

◆ Introduction to the key hidden risks

◆ Mitigation Strategies

◆ Q & A

◆ Resources

Cloud Infrastructure Entitlements Management



Discover who (identities) has access to what (resources), which permissions across your cloud infrastructure



Manage risk by giving identities just-enough and just-in-time permissions to perform their daily tasks and nothing more



Monitor privilege escalation risks and enforce separation of duties



Monitor identity activity changes and prioritize alerts based on risk level associated with anomalous behavior

By 2023

75%



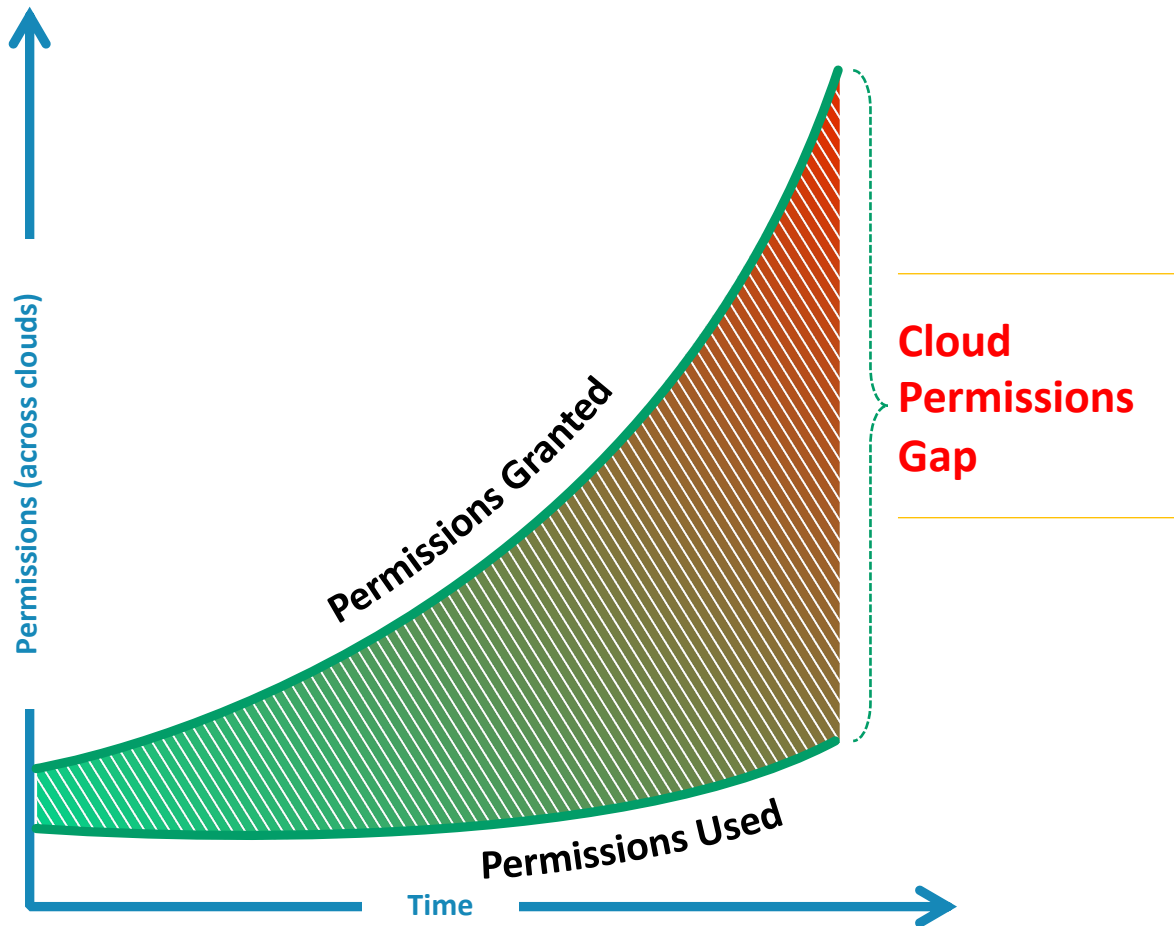
of security failures will result from inadequate management of identities, access, and privileges

up from

50%

in 2020

Permissions Gap = Biggest Risk



Proliferation of permissions, roles, services and resources

Exponential growth of identities, especially non-human

Disparate authorization models and increased automation

Diverse computing environments and workloads

Recent Breach: Attack Chain

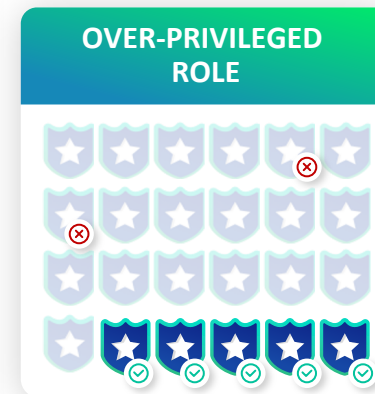


HACKER



EC2 INSTANCE

Hacker assumed an IAM role
attached to ec2 instance



List s3 buckets

Copy s3 buckets



Hacker was able to access
high-risk privileges to
exfiltrate data



“

Even if a customer misconfigures a resource, if the customer properly implements a "**least privilege policy**", there is relatively little an actor has access to once they are authenticated - significantly diminishing the customer's risk.

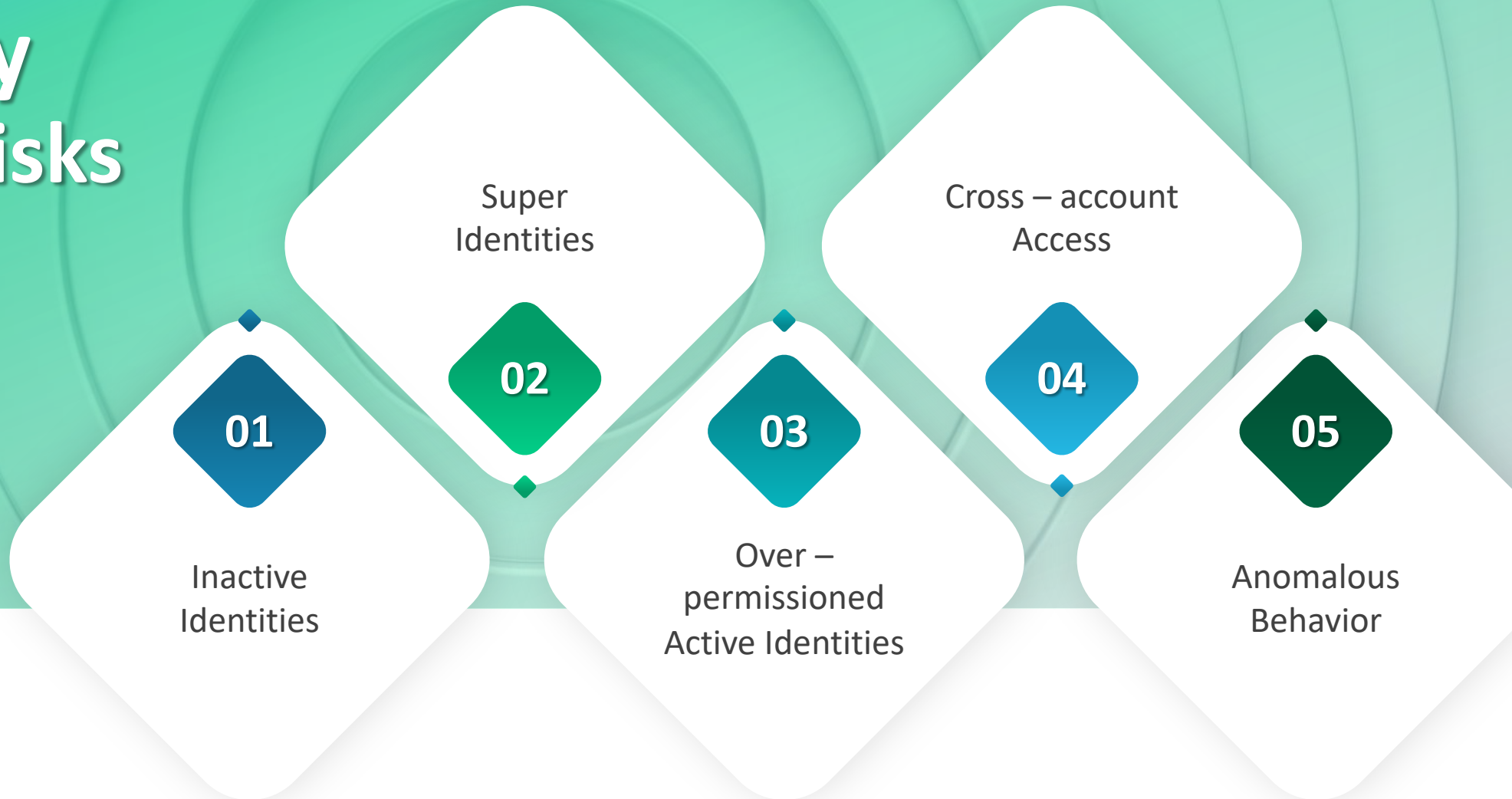
Stephen Schmidt, CISO, AWS

”

Source: Page # 2, second paragraph, line 3

<https://www.wyden.senate.gov/imo/media/doc/081319%20Amazon%20Letter%20to%20Sen%20Wyden%20RE%20Consumer%20Data.pdf>

The 5 key Hidden Risks





Risk

#1

Inactive Identity



Inactive Identity

is a human or non-human user with permissions and access to cloud resources that have not been utilized



Risk

#2

Super Identities

Super Identities

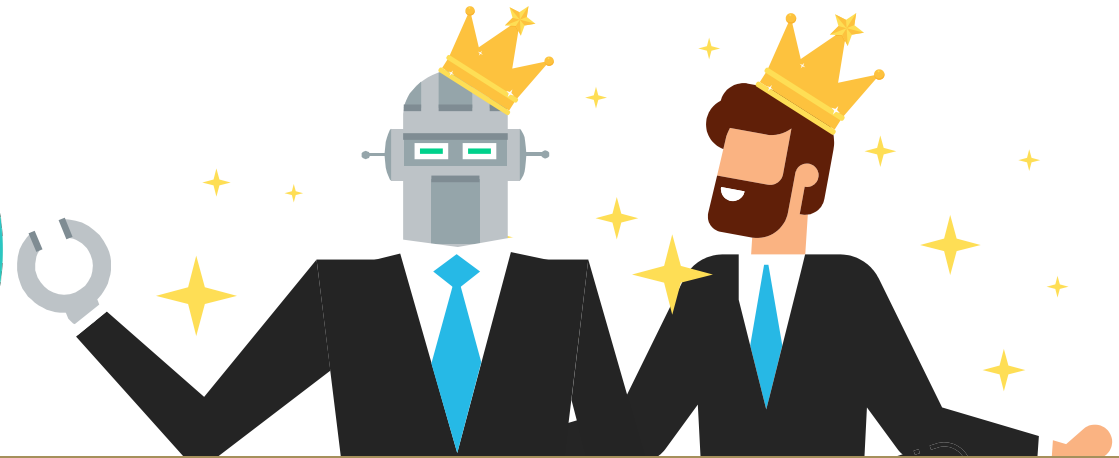
are human and non-human users that have been granted a super-admin role



Risk

#3

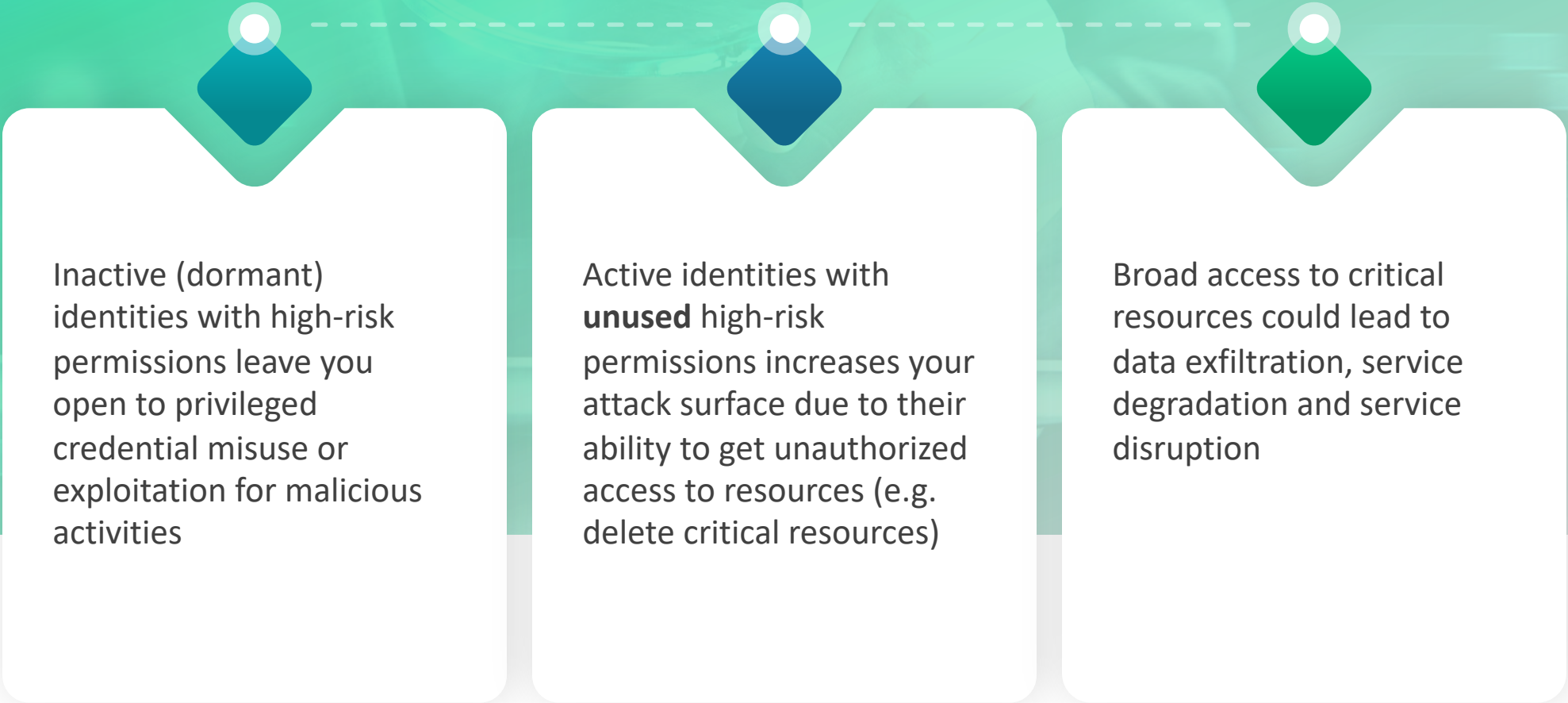
Over-permissioned Active Identities



Over-permissioned Active Identities

are human and non-human users with more permissions than needed to perform their day-to-day tasks

Implications of Over-Provisioning



Inactive (dormant) identities with high-risk permissions leave you open to privileged credential misuse or exploitation for malicious activities

Active identities with **unused** high-risk permissions increases your attack surface due to their ability to get unauthorized access to resources (e.g. delete critical resources)

Broad access to critical resources could lead to data exfiltration, service degradation and service disruption



Risk

#4

Cross Account Access

Cross Account Access

allows an external identity to access an account or an internal identity to access a different environment (e.g., test, staging)

Implications of Cross Account Access



Easy to lose control over who can access your account(s)



Unnecessary lateral movement capabilities



Unauthorized access to critical resources



Leverage role chaining to access accounts without direct access





Risk

#5

Anomalous Behavior




Anomalous Identity Behavior

occurs when a human or non-human identity's access pattern changes in relation to their historical activity


Examples of Anomalous Behavior



Access a critical resource for the first time




Use a permission(s) for the first time



Sign in from a different/multiple IP addresses



Atypical time of day login



Multiple attempts to gain unauthorized access

One Platform To Manage All Permissions Across All Clouds

Visibility

Gain insights into effective **permissions of all identities**, and their **usage**

Remediation

Provision **Just Enough Permissions** along with **On Demand & JIT** with the click of a button

Monitoring

Continuously monitor activity, alert on anomalies and measure sprawl with the **Privilege Creep Index**





RBAC today:
Assumptions based,
static & manual



**Grossly over-permissioned
identities, roles**



Mary uses 5
privileges



Fred uses 3
privileges





New Paradigm:
Data driven, dynamic & automated



Identities only have the permissions they need



Mary uses **5 privileges**



Fred uses **3 privileges**



Mitigation Strategies



Disable inactive identities, groups or convert them to “read-only” status



Remove all high-risk permissions that have not been used over 90 days



Remove access to specific resources (e.g., databases) that have not been accessed over 90 days



Create (customize) least privileged roles/policies



Continuously monitor active identities to prevent permissions creep/sprawl



Allow temporary access to high-risk permissions on demand or just-in-time (resource and time bound)

svai

4

Tasks

Over-provisioned identity using < 1% of permissions granted

Search

All Tasks

UNUSED (531)

USED (25)

▶ ec2	362/363
▶ logs	! 44/44
▼ s3	92/93
s3:AbortMultipartUpload	
s3:BypassGovernanceRetention	
s3:CreateAccessPoint	
s3:CreateBucket	
s3:CreateJob	
s3>DeleteAccessPoint	
s3>DeleteAccessPointPolicy	
s3>DeleteBucket	

▶ ec2	1/363
▶ iam	✓ 20/20
▶ s3	1/93
▼ signin	✓ 2/2
signin:ConsoleLogin	
signin:SwitchRole	
▶ sts	✓ 1/1

Who has access to what

Resource Name	Account	Resource Type	No. Of Times Users Accessed	Tasks		No. Of Users	
				Granted	Used	Access With	Accessed
cloudtrail [redacted]	[redacted]	bucket	189.3K	99	6	29	12
Tasks				Users with Access			
<div><div>Search</div><div>All Tasks</div></div>				<div>NOT ACCESSED (26)</div> <div>arn:aws:iam:: [redacted]</div> <div>arn:aws:iam:: [redacted]</div> <div>In-Group2-Wi [redacted]</div> <div>arn:aws:iam:: [redacted]</div> <div>arn:aws:iam:: [redacted]</div> <div>With-IAMS3F [redacted]</div> <div>arn:aws:iam:: [redacted]</div>			
<div>UNUSED (93)</div> <div>▶ s3 93/99</div>				<div>ACCESSED By Current Users (3)</div> <div>arn:aws:iam:: [redacted]</div> <div>arn:aws:iam:: [redacted]</div> <div>arn:aws:iam:: [redacted]</div>			
<div>USED (6)</div> <div>▼ s3 6/99</div> <div>s3:GetBucketAcl</div> <div>s3:GetBucketLocation</div>							

Create custom activity-based roles and policies

The screenshot shows the 'Details' tab of the CloudKnox interface. At the top, there are three tabs: '1 Details', '2 Tasks', and '3 Preview'. Below the tabs, there are two dropdown menus: 'Authorization System Type' set to 'GCP' and 'Authorization System' set to 'Knox-S...'. A red box highlights the 'Knox-S...' dropdown. Below these, a section titled 'How Would You Like To Create The Role ?' contains five buttons: 'Activity of User(s)', 'Activity of Group(s)', 'Activity of Service Account(s)' (which is highlighted with a blue border), 'From Existing Role', and 'New Role'. Below this section, there is a 'Tasks performed in last' section with radio buttons for '90 Days' (selected), '60 Days', '30 Days', '7 Days', and '1 Day'. At the bottom, there is a 'Search user' field, a dropdown menu set to 'All', and a checkbox labeled 'Collect activity across all GCP Authorization Systems'. Below this, there are two columns: 'Available Service Accounts (55)' and 'Selected Service Accounts (1)'. The 'Available Service Accounts' column contains a list of service accounts, with a red box highlighting one of them. The 'Selected Service Accounts' column contains a list of selected service accounts, including 'Sentry VM Bot' and another account with a red box.

The screenshot shows the 'Tasks' tab of the CloudKnox interface. At the top, there are three tabs: '1 Details', '2 Tasks', and '3 Preview'. Below the tabs, there is a Google Cloud logo, a status indicator 'Online' with a green dot, and 'Controller Enabled'. To the right, there is a 'Role name:' field set to 'CK_ROLE_demd' and an 'Authorization System:' dropdown set to 'Knox-S...'. Below this, there is a 'Tasks' section with a search bar and a dropdown menu set to 'All'. Below the search bar, there are two columns: 'Available Tasks (4145)' and 'Selected Tasks (160)'. The 'Available Tasks' column contains a list of tasks, including 'accessapproval:requests', 'accessapproval:settings', 'actions:agent', 'actions:agentVersions', 'aiplatform:annotations', and 'aiplatform:annotationSpecs'. The 'Selected Tasks' column contains a list of selected tasks, including 'appengine:services', 'bigquery:connections', 'bigquery:jobs', 'bigquery:models', 'bigquery:routines', and 'bigquery:tables'.

Provide high risk permissions with Just in Time access

1 Policies / Tasks 2 Confirmation

Auth System Type AWS Auth System 9674718

User sval

Request Policy(s) Request Task(s)

Select Policies

All

Available Policies (656)	Selected Policies (1)
AccessAnalyzerServiceRolePolicy	AdministratorAccess
AdministratorAccess	
AlexaForBusinessDeviceSetup	
AlexaForBusinessFullAccess	



Create Schedule

Frequency

Date 05/16/2020

Time :

Repeat On

For

Alerts on unauthorized and anomalous activity

INSIDER THREAT CREATE USER

Authorization System Type

AWS

Authorization Systems

cloudknox-staging

Resources

1 Resources

Tasks

1 Tasks

Identities

1 Identities

Activity

Identity Name	Resource Name	Task Name	Date	IP
jo	jo	iam:CreateUser	09 Sep 2020, 7:35 PM	

CLOUDKNOX
SECURITY INC.

Azure

Based on 90 days of data starting from Apr 19, 2020

Outliers detected on Jul 17 2020, 12:00 AM - 11:59 PM UTC

Organization

CloudKnox Security Inc

Authorization System Name

CloudKnox Subscription

1 outlier found involving 1 identity

Identity Name

NewCloudKnoxApp

Identity Domain

CloudKnox SubscriptionLocal

Identity Type

Unusual pattern of action times (UTC)

	Average	Most Similar Day	Yesterday
12AM - 4AM	19%	0%	0%
4AM - 8AM	19%	100%	57%
8AM - 12PM	4%	0%	43%
12PM - 4PM	16%	0%	0%
4PM - 8PM	22%	0%	0%
8PM - 12AM	19%	0%	0%

Top 3 Actions

Name	Count
Microsoft.Authorization/roleAssignments/delete	2
Microsoft.Authorization/roleAssignments/write	2
Microsoft.Authorization/roleDefinitions/delete	2



CloudKnox Demo

Free Risk Assessment

With a no cost, no obligation
cloud permissions risk
assessment



Requires less than **30 minutes** of your time



Get a detailed report
within **24 hours**



You will be able to:



Evaluate where you are today and where you need to be to meet your risk mitigation goals



Identify the areas of greatest risk for mitigation so you know where to focus your resources



Improve your risk posture with actionable insights and prescriptive recommendations



For a copy of the slides,
please email me at:
maya@cloudknox.io

More Info:

<https://www.cloudknox.io/resources/>
Contact: info@cloudknox.io