RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HT-R04

SNEAK YOUR WAY TO CLOUD PERSISTENCE - SHADOW ADMINS ARE HERE TO STAY

Asaf Hecht

Security Researcher
CyberArk
@Hechtov

Lavi Lazarovitz

Labs Team Leader
CyberArk
@LaviLazarovitz

AWS Shadow Admins

- A video frame -

The videos are available in the “Cloud Shadow Admins” blog post:
https://www.cyberark.com/threat-research-blog/


AWS Shadow Admins
• Combinations of Permissions Create a Tier 0 Account
• Control Other Privileged Entities
• Hidden in Masses of Permissions and Accounts

AWS Entities

ROOT ACCOUNT

IAM

USERS

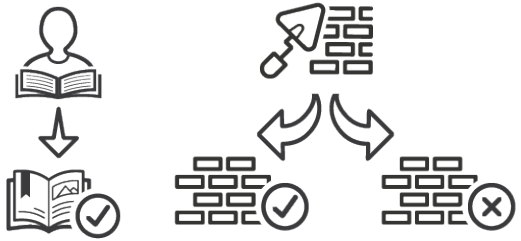
GROUPS

ROLES

AWS Permissions Policies

EFFECT

ACTION



RESOURCES

AWS Permissions Policies

Example for full “Administrator” policy:

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

or “Deny”

or any other actions from thousands of options

or any other available AWS resources

Policy 2 - also Full Admin - Shadow Admin


```
    "Statement": [
        {
            "Sid": "ShadowPolicy",
            "Effect": "Allow",
            "Action": [
                "iam:CreateInstanceProfile",
                "iam:PassRole",
                "iam:AddRoleToInstanceProfile",
                "ec2:AssociateIamInstanceProfile"
            ],
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/*",
                "arn:aws:ec2:*:*:instance/*"
            ]
        }
```

SNEAKY PERSISTENCE AND ESCALATION VECTORS

10 Sets of Permissions You Should Search and Control

IAM Sensitive Permissions to Follow

IAM -> Sensitive API Permission Categories

Groups

Credentials

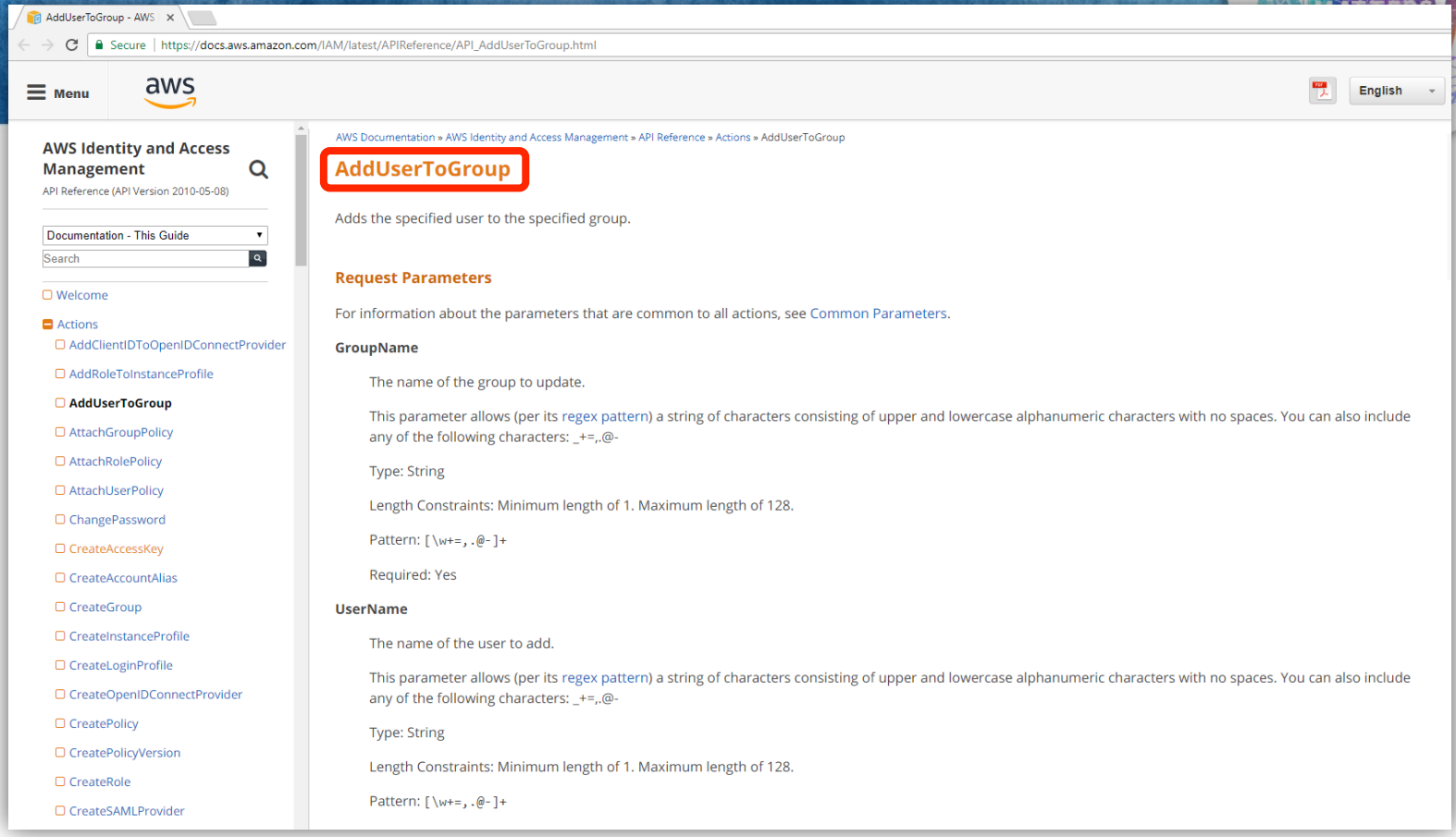
Permission Policies

Roles

(1) Permission to: AddUserToGroup

Malicious User

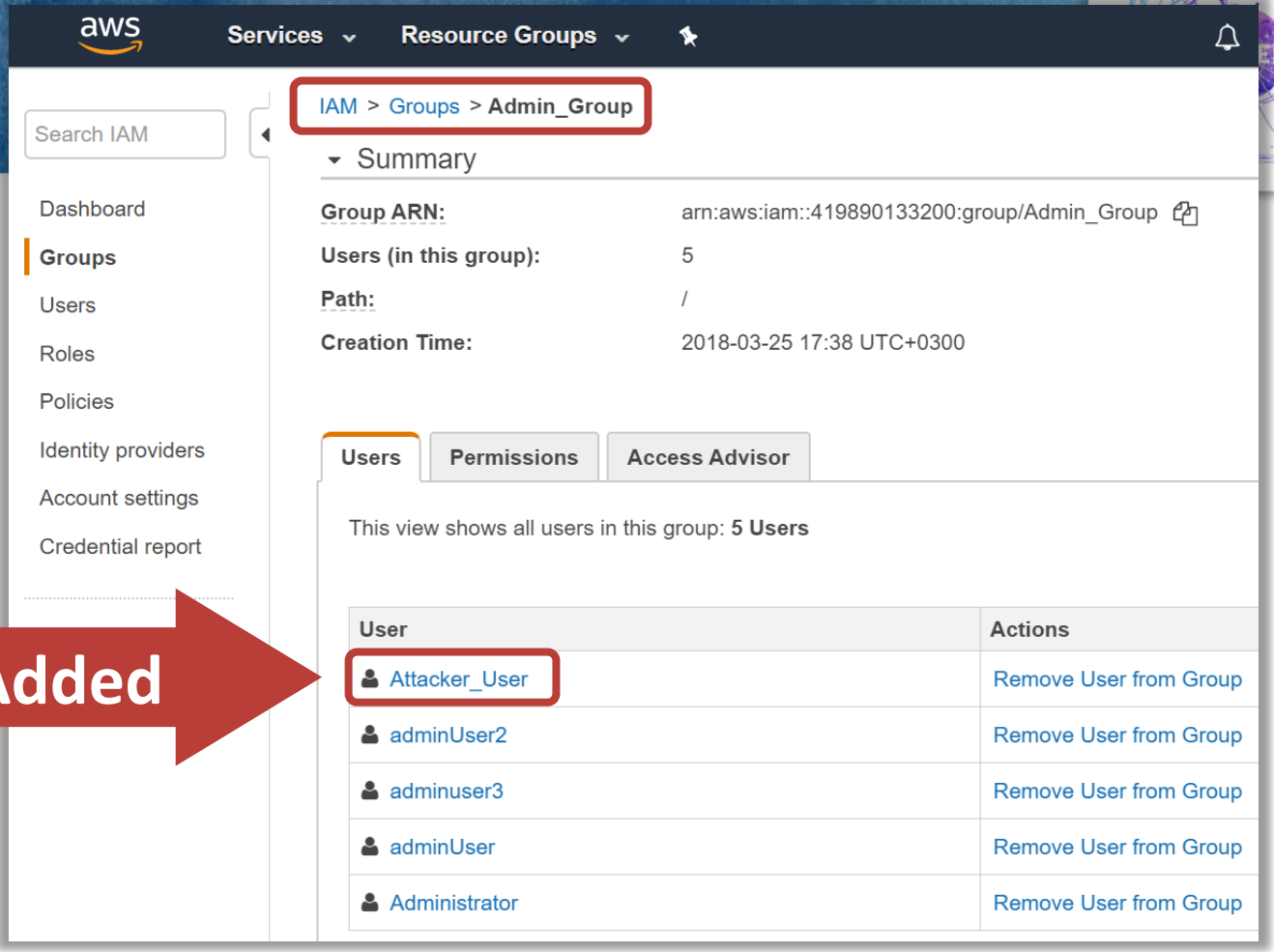
Admin Group


AddUserToGroup - AWS
Secure | https://docs.aws.amazon.com/IAM/latest/APIReference/API_AddUserToGroup.html
Menu
aws
English
AWS Identity and Access Management
API Reference (API Version 2010-05-08)
Documentation - This Guide
Search
Welcome
Actions
AddClientIDToOpenIDConnectProvider
AddRoleToInstanceProfile
AddUserToGroup
AttachGroupPolicy
AttachRolePolicy
AttachUserPolicy
ChangePassword
CreateAccessKey
CreateAccountAlias
CreateGroup
CreateInstanceProfile
CreateLoginProfile
CreateOpenIDConnectProvider
CreatePolicy
CreatePolicyVersion
CreateRole
CreateSAMLProvider
AWS Documentation » AWS Identity and Access Management » API Reference » Actions » AddUserToGroup
AddUserToGroup
Adds the specified user to the specified group.
Request Parameters
For information about the parameters that are common to all actions, see Common Parameters.
GroupName
The name of the group to update.
This parameter allows (per its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-
Type: String
Length Constraints: Minimum length of 1. Maximum length of 128.
Pattern: [\w+=,.@-]+
Required: Yes
UserName
The name of the user to add.
This parameter allows (per its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-
Type: String
Length Constraints: Minimum length of 1. Maximum length of 128.
Pattern: [\w+=,.@-]+

AddUserToGroup API Call

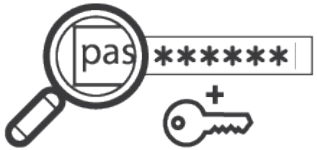
AWS CLI

```
>aws iam add-user-to-group --group-name Admin_Group --username Attacker_User
```


aws
Services
Resource Groups
Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
IAM > Groups > Admin_Group
Summary
Group ARN: arn:aws:iam::419890133200:group/Admin_Group
Users (in this group): 5
Path: /
Creation Time: 2018-03-25 17:38 UTC+0300
Users
Permissions
Access Advisor
This view shows all users in this group: 5 Users
User
Actions
Attacker_User
Remove User from Group
adminUser2
Remove User from Group
adminuser3
Remove User from Group
adminUser
Remove User from Group
Administrator
Remove User from Group

Newly Added

Jumping Forward to the Credentials Category



Credentials

Web Login

Password

Programmatically

Access Key

(2) Permission to: CreateAccessKey

- A video frame -

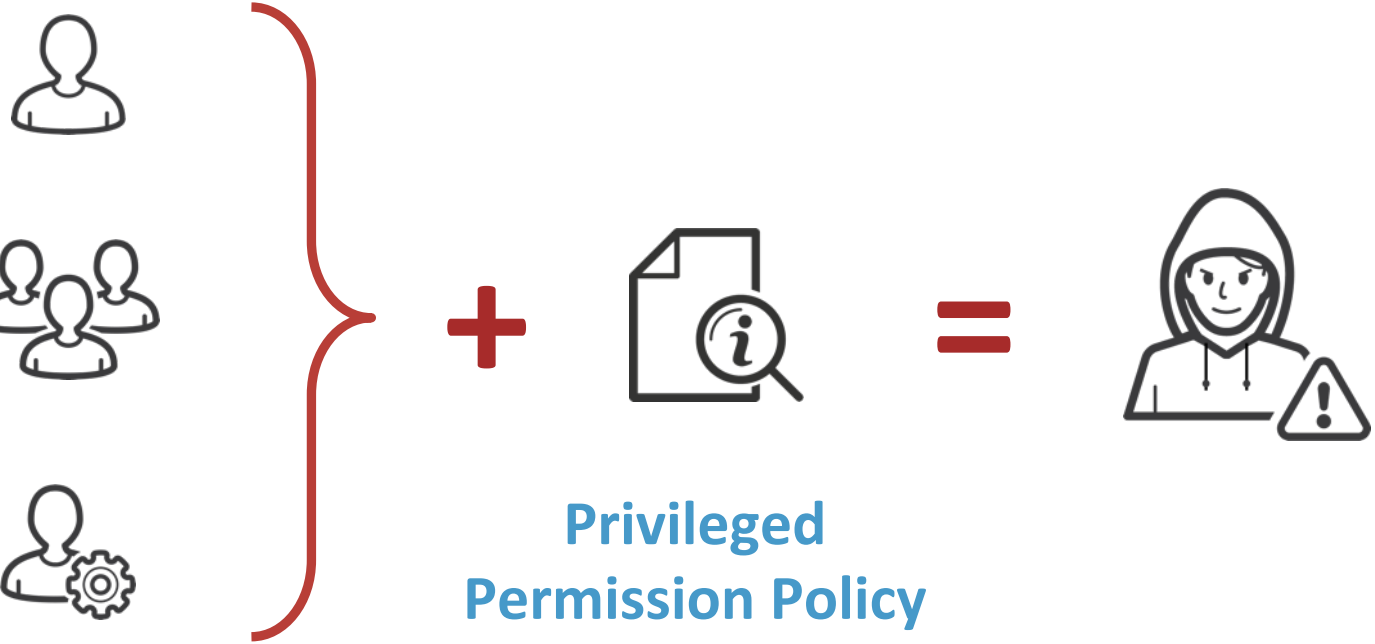
The videos are available in the “Cloud Shadow Admins” blog post:
https://www.cyberark.com/threat-research-blog/

(3) Permissions to: Attach*Policy

Users

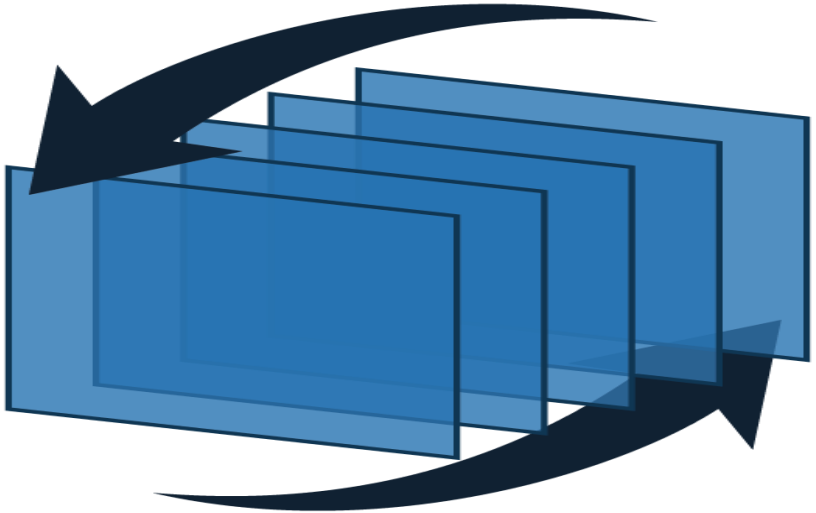
Groups

Roles



Privileged
Permission Policy

(4) Permissions to: *PolicyVersion



Modifying Policy Versions

- A video frame -

The videos are available in the “Cloud Shadow Admins” blog post:
https://www.cyberark.com/threat-research-blog/

Modifying Policy Versions


```
>aws iam create-policy-version --policy-arn [Policy-name] --policy-document [Path-to-the-new-policy-version]
```

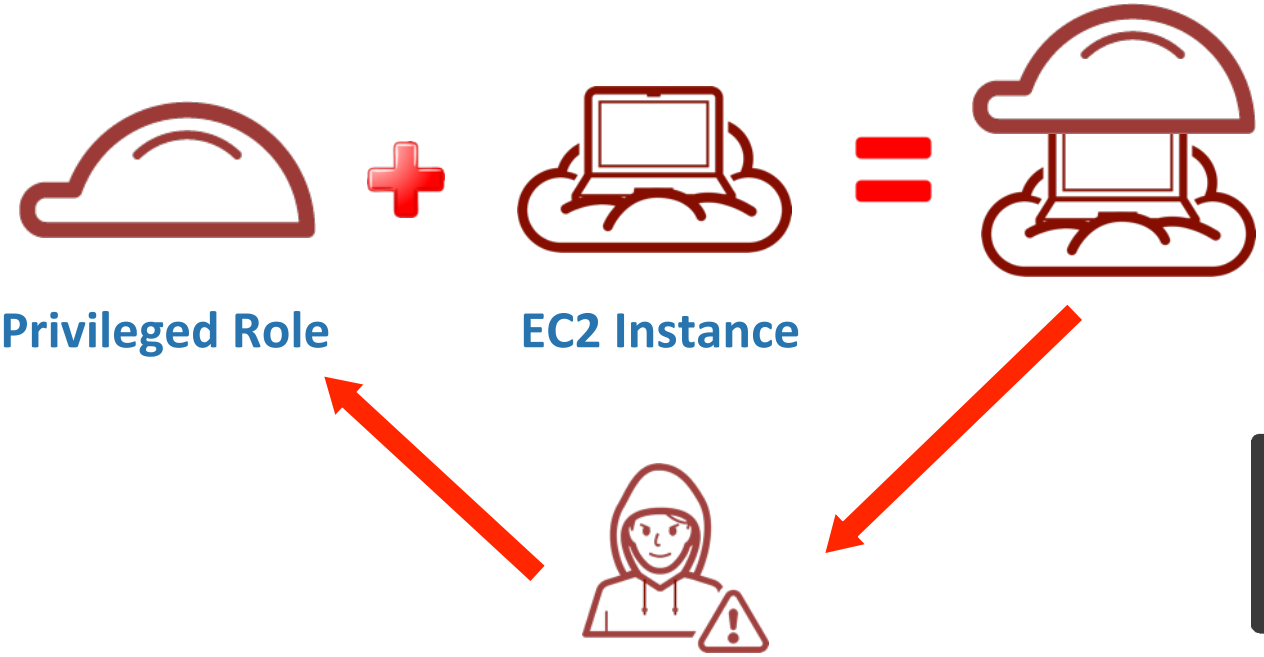
The Target Policy Name

The New Permissions

```
>aws iam set-default-policy-version --policy-arn [Policy-name] --version-id v3
```

The New Version

(5) Permissions to: *InstanceProfile



IAM Sensitive Permissions to Follow

Category	API specific permissions
Groups	(1) AddUserToGroup
Credentials	(2) CreateAccessKey (3) CreateLoginProfile (4) UpdateLoginProfile
Permission policies	(5) AttachUserPolicy AttachGroupPolicy AttachRolePolicy (6) PutUserPolicy PutGroupPolicy PutRolePolicy (7) CreatePolicy (8) CreatePolicyVersion SetDefaultPolicyVersion
Roles	(9) PassRole CreateInstanceProfile AddRoleToInstanceProfile (10) UpdateAssumeRolePolicy

Hiding The Shadow Admins

- Use benign names: “readOnly”
- Attach permissions to legitimate group
- Deny read access to account

AWS Shadow Admins

Detection & Mitigation

Detection & Mitigation

SKYARK

GitHub

AWStealth

Identify Existing Shadow Admins

AWStrace

Identify Shadow Admins Activity

Remove Shadow Admins Privileges

Secure Shadow Admins Credentials / MFA

SkyArk: Free Cloud Security Project

Publish - Today

→ AWStealth Module

Scans AWS entities **Needs Read Only Access** **Discovers Shadow Admins**

https://github.com/cyberark/SkyArk

SkyArk \ AWStealth - Demo

Discovering AWS Shadow Admins

SkyArk: Free Cloud Security Project

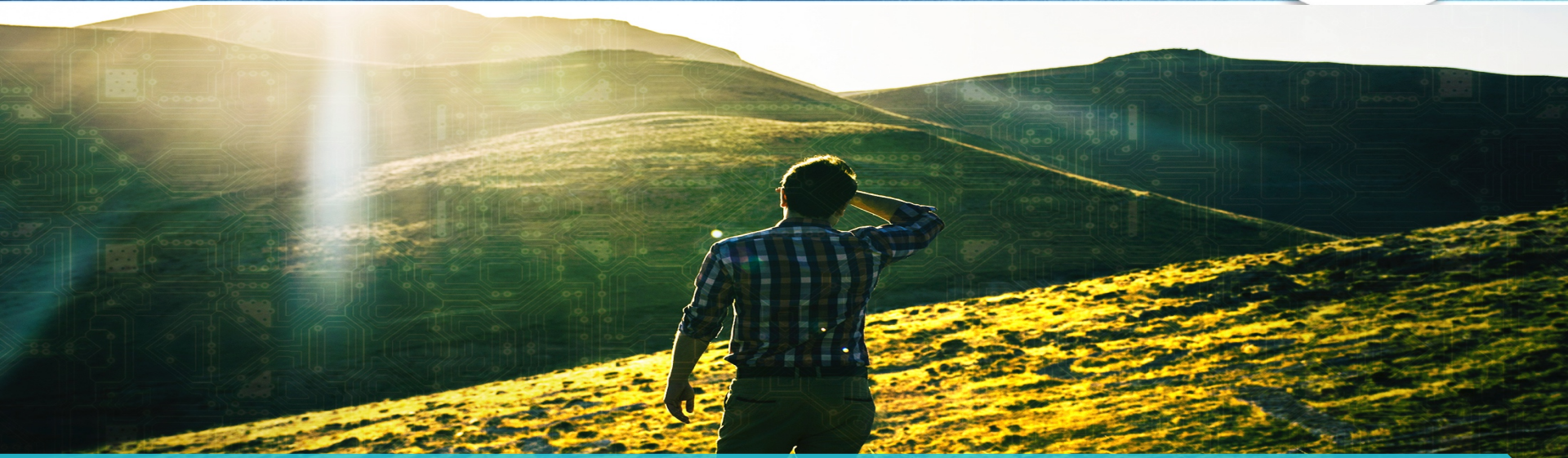
SKYARK → AWS*trace* Module

Scans AWS logs

Needs Read Only Access

Identifies Sensitive Activities

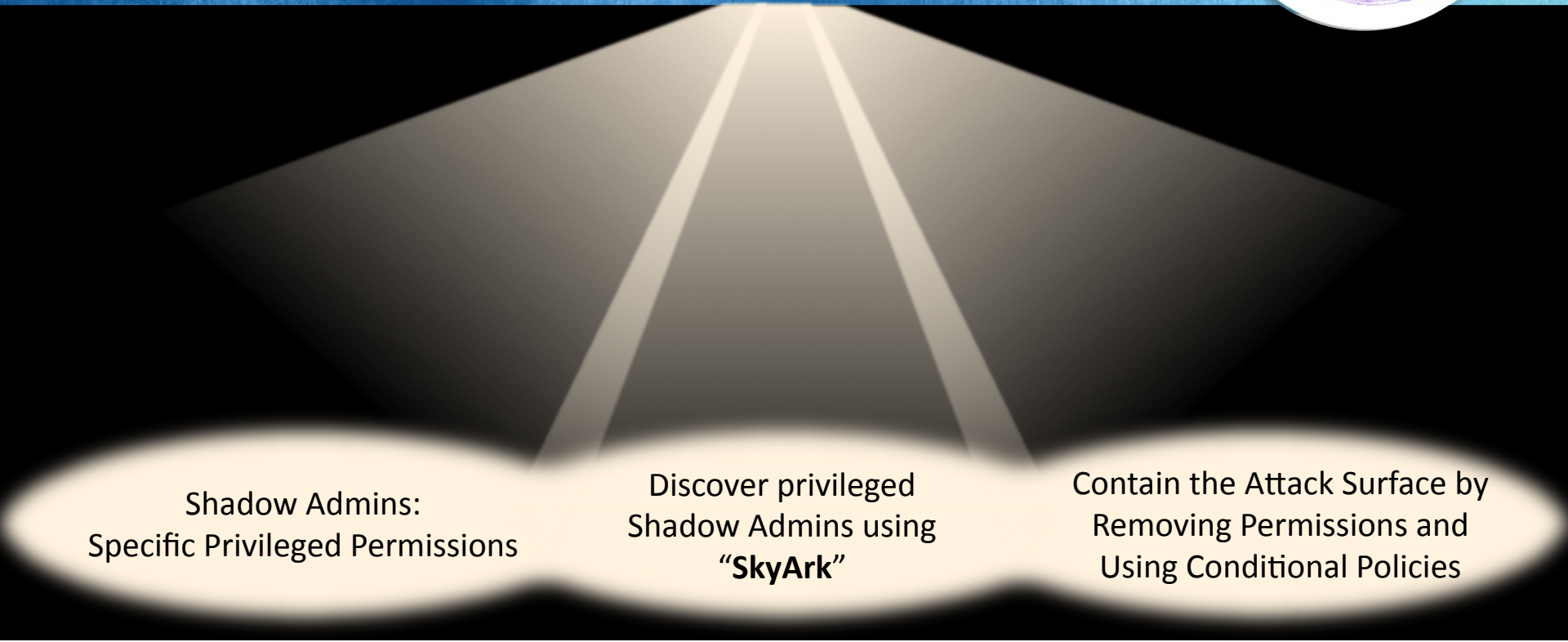
https://github.com/cyberark/SkyArk



SkyArk \ AWStrace - Demo

Analyzing AWS CloudTrail Logs

GuideLights



Actionable Takeaways

1. Scan your environments for AWS Shadow Admins:
    - SkyArk\AWStealth
2. Monitor for sensitive permission actions:
    - SkyArk\AWStrace
    - Configure automatic alerts on permission changes
3. Remove Shadow Admins sensitive permissions where possible
4. Secure Cloud Admin accounts:
    - MFA
    - Credentials management

References

- **SkyArk - free mitigation tool, available in GitHub:**

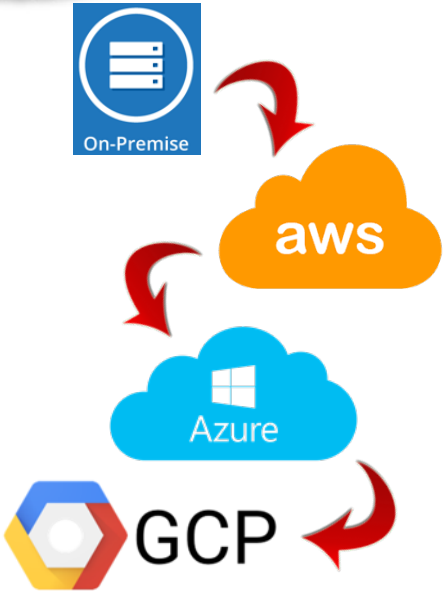
  https://github.com/cyberark/SkyArk

- **AWS Shadow Admins - Blogpost:**

  https://www.cyberark.com/threat-research-blog/

- **AWS Official links:**
  - AWS Security Center:
    https://aws.amazon.com/security/
  - AWS IAM User Guide:
    https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html
  - AWS IAM API References:
    https://docs.aws.amazon.com/IAM/latest/APIReference/Welcome.html
  - AWS CloudTrail User Guide:
    https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

GREAT… ANY Q? WE WILL TRY TO A



Also, follow us for more updates and fun:

Lavi.Lazarovitz@cyberark.com, **@LaviLazarovitz**

Asaf.Hecht@cyberark.com, **@Hechtov**