CYBERARK

DATA SHEET

DISCOVER SHADOW ADMIN RISKS AND PROTECT CLOUD PRIVILEGED ENTITIES WITH CYBERARK SKYARK

INTRODUCTION

As business cloud adoption increases, so do the security risks associated with Cloud Shadow Admins – entities that appear to have limited permissions, but effectively are full admins. Shadow Admins have specific sensitive permissions that grant them the ability to escalate privileges in the cloud. These entities, which often arise naturally from misconfigurations, can be targeted by attackers and manipulated to put cloud environments at risk. CyberArk SkyArk is an open source tool that scans both AWS and Azure platforms to discover the most privileged entities (users, groups and roles) in a given cloud environment. Developed by the CyberArk Threat Research Labs team, the SkyArk tool helps security teams identify and secure both straightforward privileged accounts and stealthy Shadow Admins that pose security risks.

HIGHLIGHTS

- Discover, assess, and secure cloud privileged entities
- Protect cloud environments from the growing threat of hidden Shadow Admin users
- Scan both AWS and Azure environments to support blue and red teams
- Easy to run and only requires read-only permissions
- Available as a free open source solution.

Shadow Admins and the Needed Paradigm Shift

While organizations may have a grasp of their legitimate admin accounts, Shadow Admins in cloud environments can be more difficult to discover. Thousands of permissions can exist in the cloud. As a result, there are many cases through which Shadow Admins can be created, all of which vary from one organization to another. The risks to all organizations, however, are the same; despite the appearance of limited permissions, Shadow Admins with only one permission could potentially have the equivalent power of legitimate admins. Additionally, Shadow Admins can in effect have unrestricted control over existing legitimate cloud admins.

The following scenarios provide examples of both how Shadow Admins can be created and the risks they pose:

- A user with only one permission, but a permission granting the ability to change passwords for other full admin users.
- A user with a single permission to manage other groups' members. If an attacker gains control of this type of user, they can modify the members of an existing admins group and add compromised users, in effect creating new full admins.
- Applications responsible for recovering users' passwords. These applications have permission to reset passwords; therefore, if compromised, these applications could enable attackers to reset an existing admin's password and take control of their account. In this scenario, an attacker could perform any malicious actions they wanted.
- AWS users with permissions to run new EC2 VM instances and attach IAM role identities. If compromised, these users could run a new VM instance with an admin role identity attached to it. Attackers could then connect to this EC2 VM instance to gain full admin control and assume the attached privileged role.
- Azure applications registered in the Azure Active Directory. These applications can be granted sensitive Azure permissions. Therefore, if a user owns a sensitive application, a potential attacker could compromise this user, then take control over the application and perform privileged actions through it. In this case, the attacker gains admin

privileges through the sensitive application even if the compromised user wasn't an Azure admin to begin with.

SkyArk is the most comprehensive scanning tool for discovering the most privileged entities throughout an organization's cloud environments, including entities with the permissions above.

Securing Shadow Admins

Following the discovery of admin users, including Shadow Admins, organizations should take three critical steps:

1. Check the discovered entities to ensure they're recognized. Unrecognized accounts have a higher probability of being malicious accounts and should therefore be analyzed to determine their validity. Attackers may already have created their own Shadow Admins to build persistence in the target cloud.
2. Eliminate unnecessary admins. Some admins discovered by SkyArk might be unintended admins. Organizations should remove the sensitive permissions from unintended admins discovered by SkyArk and convert them to non-privileged users.
3. Secure the remaining list of proper privileged entities. Admins need end-to-end protection: strong passwords with frequent rotation, session monitoring, multi-factor authentication (MFA), audit trail of activities, and other security best practices are essential.

Customization

SkyArk also includes customizable sub-modules that security teams can use to gain additional insights regarding their organizations' cloud environments, including AWStrace, which helps investigate sensitive actions within AWS environments including those involving AWS Access Keys. More details and full explanations could be found on the SkyArk GitHub page.

Execution Options

For scanning AWS:

1. Read-only permissions over the IAM service.
2. AWS PowerShell module (download link can be found in the tool's GitHub page).

For scanning Azure:

1. Read-only permissions over the Azure Active Directory and subscription's IAM.
2. Azure PowerShell module locally available or run the scan directly from the Azure Portal using Azure CloudShell.

TAKE THE NEXT STEP

Businesses can only protect themselves from the risks they are aware of. CyberArk SkyArk is a complimentary, open source cloud security tool to help your organization expose cloud Shadow Admins and protect cloud privileged entities. The tool can enable Security and Red teams with the complex mission of identifying Shadow Admins that could escalate their privileges to put full cloud environments at risk, underscoring the business need for a privileged access security program. Get started today by contacting your local CyberArk Customer Success Representative, or by accessing the SkyArk Quick Start Guide on GitHub.