# AWSRaid

Hashim Alkhateeb

December 2025

CyberDefenders AWSRaid Lab

## 1 Scenario

Your organization utilizes AWS to host critical data and applications. An incident has been reported that involves unauthorized access to data and potential exfiltration. The security team has detected unusual activities and needs to investigate the incident to determine the scope of the attack.

**Question 1:** Knowing which user account was compromised is essential for understanding the attacker's initial entry point into the environment. What is the username of the compromised user?

To find the compromised account name, I went to check the login failures and successes to see if suspicious activity was going on. I used the filters:

```
eventName=consolelogin responseElements.ConsoleLogin=Failure}
eventName=consolelogin responseElements.ConsoleLogin=Success
```

Based off these results, the user **helpdesk.luke** has the most failed login attempts with 10, followed immediately by a successful login event from the same IP address. This pattern confirms the account was successfully brute-forced.

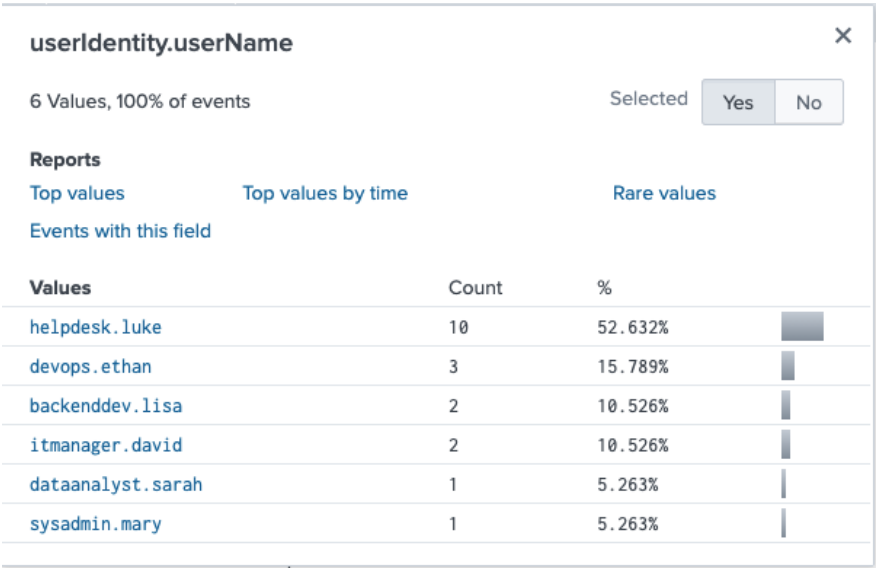


Figure 1: **helpdesk.luke** with most login failure attempts

**Question 2:** We must investigate the events following the initial compromise to understand the attacker's motives. What is the timestamp for the first access to an S3 object by the attacker?

The event name for accessing an S3 object is "GetObject". In addition, "reverse" lists the events in chronological order. Knowing that and the user the attacker is using, I used the filter:

```
eventName="GetObject" userIdentity.userName="helpdesk.luke" | reverse
```

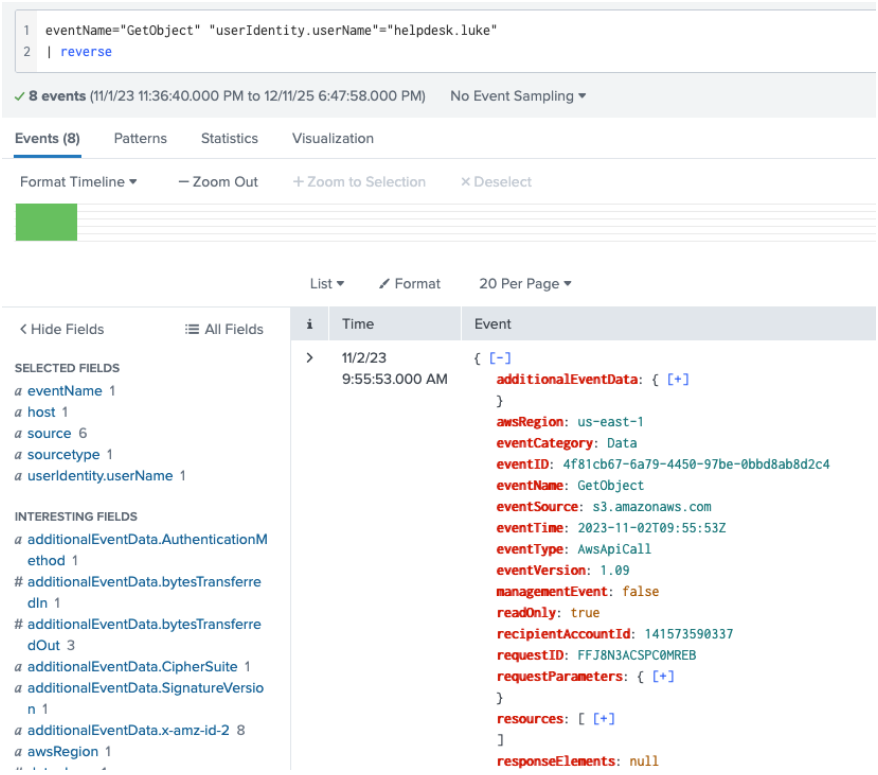


Figure 2: **2023-11-02 09:55**

**Question 3:** Among the S3 buckets accessed by the attacker, one contains a DWG file. What is the name of this bucket?

For this question, I simply added to the previous filter: `requestParameters.key="*.dwg"`. Now the results display buckets accessed by the compromised user with a file extension of .dwg.

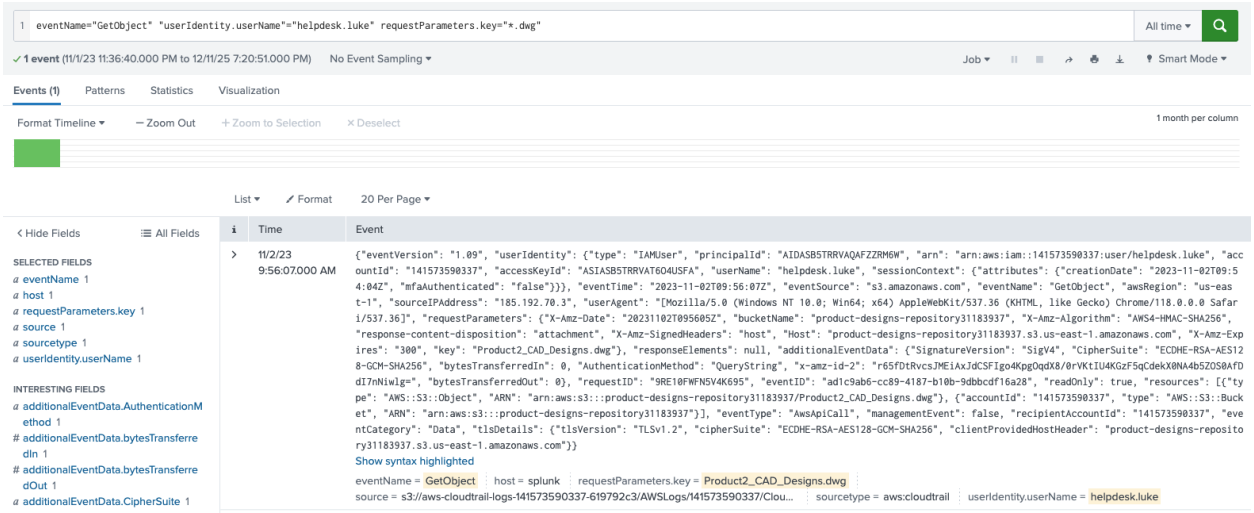


Figure 3: The file is within the **product-designs-repository31183937** bucket

**Question 4:** We've identified changes to a bucket's configuration that allowed public access, a significant security concern. What is the name of this particular S3 bucket?

After searching up what eventName is used for configuring access to a bucket, I found "PutBucketPolicy". I searched through the event names the compromised account has triggered and didn't find that but I found `PutBucketPublicAccessBlock`. This can be used to either block public access. However, after looking through the requestParameters field, I found the attacker disable the block by setting its parameters to false.

```
userIdentity.userName="helpdesk.luke" eventName="putBucket*"
```

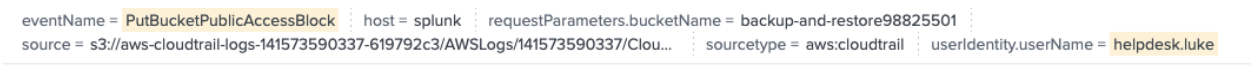


Figure 4: **backup-and-restore98825501** changed to public


Figure 5: Attacker setting parameters to false, therefore, making the bucket public.

**Question 5:** Creating a new user account is a common tactic attackers use to establish persistence in a compromised environment. What is the username of the account created by the attacker?

I used the filter:

```
userIdentity.userName="helpdesk.luke" eventName="create*"
```

I didn't know the exact eventName but made an educated guess that it would start with "create". Two events showed with eventName "CreateLoginProfile" and "CreateUser", each targeting the user **marketing.mark**.


Figure 6: **marketing.mark** account created.

**Question 6:** Following account creation, the attacker added the account to a specific group. What is the name of the group to which the account was added?

I first filtered for events triggered by the compromised user "helpdesk.luke" using the filter `userIdentity.userName="helpdesk.luke"`. From here, I selected the field "eventName" and navigated through its top values. From here, I found the event "AddUserToGroup" which does the action the question describes.

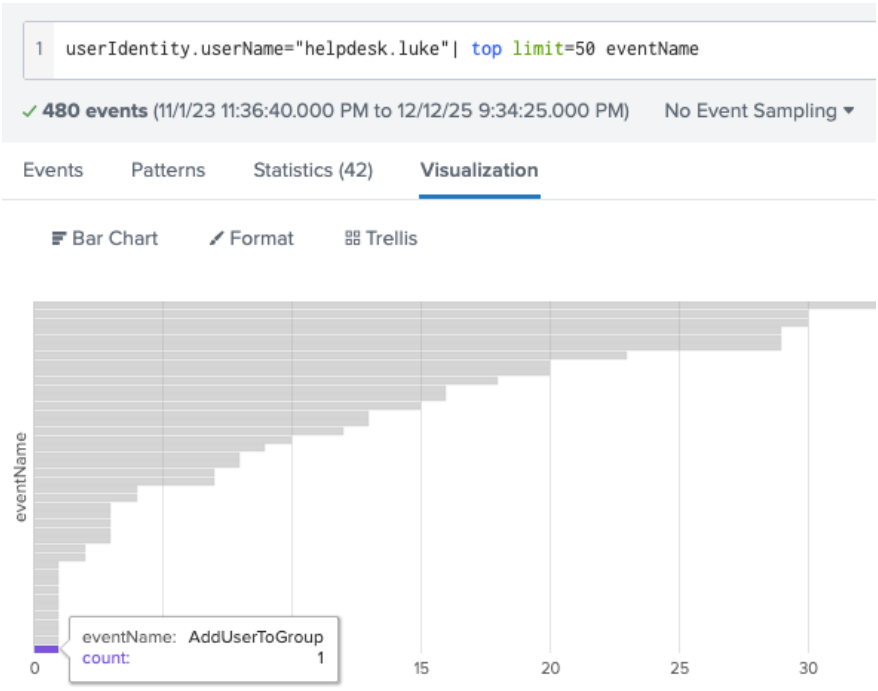


Figure 7: Located the eventName

Afterward, I simply added it to the filter and found which group marketing.mark was added to.

```
userIdentity.userName="helpdesk.luke" eventName="AddUserToGroup"
```


Figure 8: marketing.mark added to **Admins** group