Options for Securing Within the Cloud

Demo

Instructor: In this demonstration we're going to set up a couple of AWS S3 buckets and look at some options for securing them. So first things first. We'll create a bucket and provide a name. We'll leave it as the default region that we have set up right now of US East. We're not going to turn on versioning, but when we check the box for logging our requests, we can target a specific S3 bucket. We could send it to ourselves, but there's a warning there. Essentially you re logging your access request to that drive and it could get fairly big. We'll use the default encryption option and we're also going to check the option to enable CloudWatch. The default is to block all public access to your S3

bucket. You can override that here or you can do it later as well.

And now that it's been created, let's go ahead and create one more. So that one is going to be private. Let's make a public one available, and the only thing we're going to do different here is we're not going to enable the default encryption. We want it to be public, so we'll uncheck the block called Public Access Options. We do need to acknowledge that this is a security risk. We'll have to go through something similar a few more times just to make sure we can make it completely publicly available, and this would be an example if you were going to store static web content that would be publicly available to the world.

So we're going to upload first a file to our public bucket. I just have a video file that is being uploaded. Pretty easy, drag and drop, and we're going to make that option available to the public. So we do want to grant public read access. Again, we get another warning, and we click Next, and then we have to choose a storage class. We're going to use Standard, but you can see some other options there, and then we'll go ahead and upload, and our status is starting there at the bottom.

Well, let's go ahead and look at our other bucket, our one that we want to be private, and we're just going to do a similar test where we're going to upload a file. So add a file. Pick a file name. We're not going to change

any information in here. Public access is blocked, so we're just going to accept the defaults, and again, use Standard for our storage class, and we'll go ahead and upload.

Now that they're both uploaded, kind of skipped ahead a bit. Let's take a look at some of the settings for these. You look here on the right, we do have no encryption set up for our public test bucket, so the file that we put up there is not encrypted, and if we go to access that file, you see our video loads no problem. We're opening that up in a different browser, not the one that we're logged into currently.

So let's take a look at our other file, which is in a private bucket or a non-public bucket. We'll just look at the options there. You can see that it is encrypted based off of our default encryption for that bucket. If we try to copy that link and open it in our other browser, we see we get an error message. So we have successfully created two buckets, one that is publicly accessible for our static web content, and one that is not publicly available. Amazon has a feature called Access Analyzer for S3. It needs to be enabled at the per region level, so every bucket within that region would be able to have Access Analyzer run against it. So we'll enable it for our region where our buckets are and after about 30 minutes or so or every 30 minutes it updates with its findings. As you see as we switch regions, we might not have any findings in one region

whereas we do have findings in the region where we have our bucket. We could take a remediation action and block all public access right here from this interface if we want to. We Don't want to. But we can also drill into the findings, look at the finding ID, and you have additional information there and then, of course, you can do your remediations as well, to archive that bucket or to block that.

We'll just go back and just review our permissions real quick, and again, you see we have two buckets, one that's publicly available, and one that is not, and in this alternative S3 bucket viewer, we can also see that this bucket here is public.