Reflection on AWS Cloud Security Lab

IAM

What permission were granted:
iam:GetAccountSummary

iam:ListAccountAliases

iam:ListMFADevices

iam:ListAccessKeys

By granting Read-Only privileges to user Student A, prevents the student from changing security status or modifying anything without the administrator knowing. Reducing risk is the first step in attack prevention. It prevents unverified new users from being created and passwords from being changed.

How this demonstrates least privilege compared to using the root account:

My IAM user ('StudentA') has IAMReadOnlyAccess so they cant change passwords or delete resources. My Root account is unrestricted and permanent access to every service.

S3

How blocking public access and using bucket policies help prevent S3 data leaks like in the Capital One case.

Blocking public access prevents accidental data leakage at the core level. Bucket policies allow specified access to s3 storage sources. This JSON document determines access and operations that can be done on the bucket.

EC2

The logic behind creating a security group with restricting to My IP is if an attacker gets access, they still can't get to your network. Its purpose is to keep all of the internet out and only allowing just enough access to complete your work.

How limiting inbound rules and using IMDSv2 / instance roles relate to the SSRF path used in the Capital One breach.

In the Capital One breach, if the SSRF patch happened and IMDSv2 had been used it could've prevented the attack. V2 needs a session token to authenticate and requires a PUT token request.

Logging, Monitoring and Billing Awareness

CloudTrail
-CloudTrail console's Event History shows account activity that can be used to fix IAM permission errors. The purpose is to create a trail which helps tracks potential breaches that might happen.

AWS Config
-Config's purpose is to track relationships and connections of resources. If any configurations were changed, this would record it to change back to a more secure state.

Why relying only on periodic audits (instead of continuous monitoring) creates a “window of opportunity” for attackers, as discussed in the case study.

That "window of opportunity" is when security breaches happen due to lapse in surveillance. It allows attackers to go undetected during which they can install backdoors and steal data. CloudTrail records API calls, Billing shows any costs that may have been charged and Config keeps track of any changes in resource use.