Written Explanations

AWS IAM:
In our technical demo, we have integrated AWS Identity and Access Management (IAM) to enforce proper access controls and permissions. We followed IAM best practices to set up individual user accounts for each team member, ensuring that they have the least privilege necessary to perform their tasks. We implemented multi-factor authentication (MFA) for added security and regularly rotate access keys. By leveraging IAM, we demonstrate how granular access control is achieved, reducing the risk of unauthorized access and data breaches.

AWS CloudTrail:
As part of our technical demo, we have integrated AWS CloudTrail to provide comprehensive visibility into API activity and changes within our AWS environment. We have enabled CloudTrail logging and configured it to capture all API calls made by users, services, and resources. By analyzing the CloudTrail logs, we can track and audit changes to IAM policies, security groups, and other critical resources. This demonstrates how CloudTrail enhances security and assists in troubleshooting and compliance auditing.

Amazon GuardDuty:
In our technical demo, we have incorporated Amazon GuardDuty as a threat detection service. GuardDuty continuously monitors our AWS environment, analyzing network traffic, DNS logs, and AWS CloudTrail events to identify suspicious and malicious activities. We have configured GuardDuty to generate alerts for various types of threats, including unauthorized access attempts, compromised instances, and known attack patterns. By showcasing GuardDuty, we demonstrate how it proactively detects potential security threats and helps mitigate risks in real-time.