**1. Security**

* Implement overarching security practices across all areas of your architecture.
* Stay informed on AWS and industry security recommendations and integrate them into your practices.
* Automate security processes, including testing and validation, to scale security operations effectively.
* Centralize security controls and manage them through version-controlled templates.

**2. Identity and Access Management (IAM)**

* Enforce least privilege access and use multi-factor authentication (MFA) for all accounts.
* Manage identities centrally and eliminate reliance on long-term static credentials.
* Use temporary credentials for machine access and ensure strong password policies.
* Implement role-based access control (RBAC) to assign permissions based on roles, not individuals.
* Enable identity federation with existing directory services for seamless access.
* Regularly audit and monitor IAM policies and credentials.

**3. Detection**

* Implement logging and monitoring across all AWS services and applications.
* Use AWS CloudTrail and CloudWatch for monitoring API activity and events.
* Centralize log analysis and automate responses to security incidents.
* Integrate GuardDuty for continuous threat detection and automated alerts.
* Maintain visibility into your environment with configuration tracking via AWS Config.
* Use automated tools to analyze logs and detect potential security incidents.

**4. Infrastructure Protection**

* Apply a defense-in-depth strategy by implementing security controls at every layer of your infrastructure.
* Use security groups, network access control lists (NACLs), and web application firewalls (WAF) for traffic filtering.
* Implement stateful and stateless packet inspection for network protection.
* Enforce encryption for data at rest and in transit across all services.
* Regularly patch and harden your infrastructure, including virtual machines and containers.
* Segment networks using Virtual Private Cloud (VPC) to isolate workloads.

**5. Data Protection**

* Classify data based on sensitivity and apply appropriate protection mechanisms, such as encryption.
* Use AWS Key Management Service (KMS) to manage encryption keys and enable automatic key rotation.
* Ensure data is encrypted both at rest and in transit using AWS-native encryption services.
* Implement data lifecycle management policies, including versioning and archiving, to prevent accidental data loss.
* Control data movement and ensure compliance with regional data regulations.

**6. Incident Response**

* Prepare for incidents by pre-provisioning tools and environments for investigation and forensics.
* Automate incident response actions, such as isolating instances and capturing forensic data.
* Conduct regular incident response simulations to test and improve your response plan.
* Ensure detailed logging and monitoring are in place to facilitate quick detection and investigation.
* Maintain a clean-room environment for secure analysis and recovery from security incidents.
* Document and review incident response procedures regularly to ensure they are up-to-date and effective.