Steven Bo Bekendam
Cyber Architect - AWS Landing Zone Case Study
February 23, 2025

1. *Risk Assessment: Identify top three potential threats to AWS landing zone and suggest mitigation strategies for each*

1) **Data Security** - Identify data content being stored/transmitted and sensitivity levels according to company data labeling policy. Apply appropriate hardening templates/AMI's for each computing resource (Container, VM/EC2, etc) and storage level elements (Database, Disk, etc). Ensure appropriate access controls are defined (muti-Account OU strategy) and enforced for direct/raw or downstream access to the data. Where data is in transit, apply necessary encryption protocols (TLS, SSH, etc) to guard against threats of cleartext exposure of contents.

2) **Edge/Network Security** - Configure access to resources in a fashion which eliminates unnecessary exposure to services or interfaces to unintended audiences. Utilize AWS firewall/WAF for perimeter, an appropriately configured Transit Gateway or DirectConnect with ACLs for network peering/interconnectivity and host/resource based firewalls to restrict unnecessary access/blast-radius of compromise.

3) **Inadvertent Misconfiguration** - Utilize IaC (Infrastructure as Code) where feasible and ensure each change/modification is rigorously tested and stored in an enterprise approved code repository. Terraform/ControlTower can be used to deploy CI/CD for automated test/builds. SAST/DAST and other application/code vulnerability scanners should be utilized during build and test phases - while a post implementation verification needs to be performed to ensure changes meet the expected design in production accounts.

2. *Architecture Design: Outline the key components of a secure architecture for the AWS Landing Zone, focusing on a secure foundation for workload and data deployments.*

Data being utilized for this environment needs to be evaluated against the enterprise's data classification policy. If content is considered confidential, then necessary controls to protect the data shall be enforced. Data at rest controls such as file/disk systems using KMS, or data in transit / SSL certificates managed by AWS Certificate Manager - need to be applied.

For securing workloads, ensure access is limited to the