Security in the cloud means more than you think

For public sector customers, ensuring compliance and security is vital. AWS provides these organizations with a broad set of cloud-based services to build world-class solutions. In this session, we go over native logging tools in AWS such as AWS CloudTrail, Amazon CloudWatch Alarms, Amazon CloudWatch Logs, and Amazon GuardDuty. We also cover automated remediation of compliance events, alerting tools, and other…

Prework:

Create new account for each workshop.

Apply Lambda function for delete IGW Attach

Create Trail to prewarm separate LogGroup – log file delivery can take a few min.

Pre-warm logs for VPC events (create VPC, create IGW, attach) to circumvent 5 min delay.

1. Intro (2 min)
   1. Address compliance challenges
   2. Nod to NIST/CIS/SRG
2. Intro services (7m)
   1. CloudTrail (2m)
   2. CloudWatch Alarms/Logs (3m)
   3. GuardDuty (2m)
3. Scenario 1 (15 min)
   1. Intro – Compliance rules dictate the tracking of/management of remote accesses via managed network access control points (AC-17(3), CIS Networking 4.4)
   2. Demonstrate new account CloudTrail settings
      1. Create Trail (ReinforceTrail)
         1. Apply to all regions, all read/write events, Do not select all S3 buckets for logging (discuss each point)
         2. S3 create a new s3 bucket (reinforcecloudtrailbucket-date)
            1. Discuss going and locking down this bucket
         3. Show S3 bucket options, discuss retention in S3, using separate account to host log bucket
         4. Encrypt log files with SSE-KMS (AU-9, CIS Logging 2.7)
         5. Create new KMS key (ReinforceKMSKey)
            1. Discuss looking at Key Policy, IAM policy for access to log key
         6. Enable log file validation (digest/hash of each log file published hourly, ensure no tampering)
      2. Configure new CloudWatch Logs Group (ReinforceLogGroup)
      3. Demo creation of new IAM role (may fail, retry worked fine. Try on baked account)
   3. Create CloudWatch Alarm
      1. Click into Log group, start looking at stuff
      2. Create new VPC, create IGW, attach IGW (Reinforcevpc, reinforceigw)
      3. Review events
      4. Create alarm for ATTACH