**re:Invent 2019**

**ARC319**

**Security Vulnerability Identification and Remediation**

**Facilitator Notes**

**Introduction (Prerequisites)**

* Welcome Everyone
* Introduce yourself
* Recap the session number and title “ARC319 – Security Vulnerability Identification and Remediation”
* 300 level workshop, it is expected that you have experience working in the AWS console, if not don’t worry; detailed instructions and we’re here to help
* Mention pre-provisioned account (Provide Links)
* Provide Bit.ly for lab guide (bit.ly/awsarc319)

**Problem Statement**

* Provide Overview of problem statement (devsecops engineer, mergers/acquisitions, bought blogging platform, IaC deployment)
* Overview of lab (read below)
  + This workshop focuses on integrating the new web platform and ensuring a proper security posture is maintained. The lab will involve learning how to monitor, alert, and remediate security events in your AWS environments; primarily focusing on [AWS Config](https://aws.amazon.com/config/) and [AWS Security Hub](https://aws.amazon.com/security-hub/).
  + How else could you use this? Evaluating 3rd party software? Taking hackathon projects to production? Just getting started with a foreign AWS environment?
* Read Disclaimer and ask for confirmation from attendees that they understand
  + **\*\*\*ARC319 will provide scripts and templates that intentionally create security holes, to be remediated. These templates should ONLY be deployed into temporary/sandbox AWS accounts and not into your corporate environment or anywhere with sensitive data.**

**Solution Overview**

* Talk through architecture diagram and AWS services in scope
* Company has strict security posture
* Need to deploy this stack in a sandbox to validate security posture prior to deploying into production accounts
* Knows of some AWS services but new to AWS; mention services briefly but not that the lab focuses on Config and Security Hub as you have a defined list of rules you want to deploy in the sandbox.
* Ask how the architecture might be improved to be better, well architected
  + Route 53 for globally available DNS
  + Cloudfront distribution for S3
  + Caching solution for database reads
  + Additional Availability zones for resiliency

**Task 1**

* Have attendees enable AWS Config and walk through the steps in task 1
* Discuss what Config is
  + AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.
  + Config fits perfectly into a layered security model, always start with preventative controls and use services like Config for detective controls and ongoing compliance validation
  + Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.
  + This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.
  + We will be using Config today for identification and remediation of security configurations
* Have attendees enable AWS Security Hub and walk through the steps in task 1
* Discuss what Security Hub is
  + Requires config
  + AWS Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts.
  + With all the different security tools available oftentimes this leaves your team switching back-and-forth between these tools to deal with hundreds, and sometimes thousands, of security alerts every day
  + With Security Hub, you now have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions.

**Task 2**

* Have attendees deploy config.yaml in task 4 by clicking hyperlink (validating they are in eu-central-1)
* Mention parameters and need to add in an email address that they have access to. Not for marketing or anything like that, just for notifications in this lab.
* Once deployed remind them to capture the ‘Output’ value for ‘IAMRoleArn’ – they will need this later
* Also have them check the email address they entered and confirm their SNS subscription

**Task 3**

* Reiterate disclaimer
* Have users click the hyperlink to deploy their stack (reminding them to be in US-East-1)
* Have them right click the hyperlink and save the target to view the code locally
* Discuss vulnerabilities they see in the code, queue them in to lines mentioned in the lab guide

**Task 4**

* Have the attendees open a new tab for the Security Hub service
* Discuss how you are starting to see certain findings and entries, based on CIS (Center for Internet Security) hardening guidelines
* Briefly discuss the CIS items that are populated in the ‘findings’ section; mention it helps you to know what you don’t know
* Click on the integrations section and discuss various integration options
  + GaurdDuty – Machine learning backed solution to identify common behavior and flag/alert when things are out of the norm
  + Inspector – Vulnerability assessment service with two different options (network based/agentless) and (host based/with Agent)
  + Macie – Machine learning backed service that identifies and notifies you of sensitive data in S3 and learns user behavior as it relates to S3.
  + 3rd party options (currently 22 different 3rd party solutions)
* Look at ‘Findings’
* Click on the name of a rule, take note of the remediation option…. But it’s manual. Discuss how you can do automated remediation (hint… hint… AWS Config)
* Go to findings and filter on ‘AwsS3Bucket’
  + Mention the lack of a rule for bucket encryption, not there but it is a company policy
* Discuss how you could add a rule for encrypting S3 buckets and also leverage automated remediation (Config)

**Task 5**

* Have attendees work through creating their own config rule
* Answer questions as necessary
* Note that it could take some time for the rule to evaluate

**Task 6**

* Have attendees navigate to the AWS Config service in the console
* Direct them to the ‘S3\_Bucket\_Public\_Read\_Prohibited’ rule
  + Click the name
  + Click edit and view the remediation actions
  + Close the edit screen and view the buckets it found (if not populated click re-evaluate, if not remediated, click remediate)
    - If you don’t see resources, move on to the next step and come back later
  + Next Open the Config rule for ‘REQUIRED\_TAGS’
    - Click Edit and note the remediation, pushing to an SNS topic vs. remediating
    - Using a Lambda for remediation
    - Have attendees open Lambda console in another tab and find/review the lambda function with name including ‘requiredtags’ in the name
  + Go back to the config rule
    - Click on the resource name and talk through the configuration timeline (changes in configuration) and Compliance Timeline (changes in compliance status)
    - Validate resource has had tags updated (click on name out of rule screen)

**Task 7**

* Based on time remaining encourage attendees to view existing config rules and create resources that will be remediated with those rules. (S3 bucket w/ public access and enforced tags is the easiest)
* Have them validate resources were remediated

**Task 9**

* Briefly discuss cleanup that is done if lab is not completed in a pre-provisioned account.
* Note that they don’t have to worry about it here as accounts will be decommissioned once lab is finished

**Task 10**

* Discuss the further reading section and encourage attendees to ‘dive deep’