Security V2 GameDay

Module 1 Inspector with Image Builder **Difficulty Level: 100**

Applications are complicated objects that need to be constantly updated and monitored to ensure they are up to date with versions and security patching. If a server or software package in the application is out of date, then it can become an easy target for nefarious hackers and bad actors. This is particularly important in a compliance environment where application developers must be able to show that they have a mechanism for ensuring their software is up to date. Players will learn how to find if an application is out of date, and how to create an automated pipeline to ensure that the application doesn't fall behind on security patches.

Difficulty Level: 100

Module 2: Event-Driven Security

Through the lens of security, the AWS CAF promotes "automation as an underlying theme for all strategy." In this module players will leverage 1) Guard Duty 2) EventBridge and 3) Lambda for threat-remediation and response.

Module 3: Secrets Manager **Difficulty Level: 200**

According to the Verizon 2019 Data Breach Investigations Report, the top Attack Vector for Web Applications is Stolen Credentials. Intruders are constantly looking for a way to breach their targets. In most scenarios, by the time the victim understands that they have been breached, it is too late to reverse the tragedy. This module will utilize AWS Secrets Manager to secure credentials that are used in Lambda and API Gateway

Module 4: Secure Database **Difficulty Level: 200**

Customers will learn how to encrypt an unencrypted RDS database, develop a notification system to alert security vulnerabilities with AWS Config, AWS Lambda, and Amazon Cloudwatch.

Module 5: IAM Access Analyzer **Difficulty Level: 100**

Leveraging automated reasoning and provable security techniques and services is key to scaling securely. This module enables customer to use AWS IAM Access Analyzer to identify the resources in their account, such as Amazon S3 buckets or IAM roles, that are shared with an external entity. This allows them to identify unintended access to their resources and data, which is a security risk.