Creating and Deploying the System and Performing the Specified Tasks

The final project of MIS420 consisted of creating and deploying an EC2 instance of OpenVPN services using Amazon Web Services(AWS) as well as implementing security measures to secure the instance. In launching the EC2 instance, the overall functionality was tested in viewing the IP address before connecting to the OpenVPN and the IP address after connecting to the VPN. The purpose of the application was to successfully launch an application using AWS and securing the EC2 instance and S3 backup by setting alarms for any unusual activity, monitoring/logging system, Identity access management, vulnerability scanners, and encrypting a S3 bucket.

To minimize the attack surface and secure the application, there were different security measures implemented which all relate back to the principles of information security. The first security implementation was configuring AWS CloudWatch Alarms to monitor network traffic. Configuring AWS CloudWatch Alarms allows for performance monitoring in terms of network utilizations and security monitoring to create an alert if there are any deviations from the baseline of network traffic.

After configuring the monitoring/logging system, a S3 bucket was created to hold backups for the EC2 instance. Having backups of the EC2 instance for system versioning which allows a user to restore from a backup should a security incident happen. The backup process was also set up to be automated by creating a lifecycle run. With backups being automated this is reducing the risk of data loss if a security event takes place. Overall automated and scheduled backups are part of risk mitigation strategy, business continuity, and disaster recovery.

Furthering implementing security measures, Identity and access management configuration were set separating users access to different areas of the application such as the EC2 instance, S3 buckets, and backup/vulnerability scanner. When creating users to access these resources, permissions are given to each user limiting access to other areas of the application. Identity and access management relates back to the principle of least privilege, while in turn is minimizing the attack surface. In addition to access permissions, Policies were also set in place to limit what a user can do based on their attached policies.

Configuring CloudWatch alarms is used to send an alert to the system administrations if there is activity that is taking place such as unauthorized access or high capacity data transfers. When combining CloudWatch and CloudTrails, logging is tracking/monitoring all activity that is

taking place. CloudTrail also has a feature that enables log file validation, ensuring the integrity of log files. Having log file validations is important if there is an audit on processes. Logging an S3 bucket that contains backup files of the EC2 instance is important because the bucket contains the entire system's data. Using CloudTrail to log activities gives insight about access requests, who and when was the bucket accessed and what actions were taken.

With some risk mitigation implemented, A vulnerability assessment was conducted using AWS Inspector to access the security of the S3 bucket and the Ec2 Instance. Inspector scans specified targets, detects vulnerabilities, and creates the results of the assessment. Conducting a vulnerability assessment is crucial to security operations as the process is able to detect and address potential vulnerabilities before they are exploited. Proactively conducting a vulnerability scan helps with compliance of security standards. After the initial assessment, implementing scheduled regular assessments is best practice to refine security configurations based off of newly identified vulnerabilites.

To further secure the S3 bucket that contains backups for the system, Server-side encryption with Amazon S3 managed keys was enabled and configured. With encryption enabled, this security measure ensures that the backups and logging information is confidential and maintains integrity of data at rest and in transit. With encryption setup, this security measure prevents unauthorized modifications to the S3 bucket which also adds another layer of security.

Having this application setup on cloud allows for redundancy of data across different data servers across the region. If a security incident were to happen, disaster recovery/business continuity shouldn't be a problem due to the cloud's data redundancy. As opposed to on-premises systems, this may be a single point of failure vulnerability if an organization only had one location of operation. There are also overhead costs associated with on-premises due to the need for administrators to set up, maintain, and update their systems infrastructure. Security is continuous meaning, monitoring and patching is a requirement. Hosting an application on the cloud is a solution because of the automation services such as security monitoring, resource monitoring, and backups. Depending on deployment of cloud services, there are some risks such as data breaches with multi-tenancy, service outages/downtime which affects availability of data, and too much reliance on cloud service may result in vendor lock-in.

Using S3 buckets is convenient to users because of scalability allowing users to store large amounts of data and ensures availability. Cost of a S3 may be seen as both a pro and con as

the charge is based on usage rather than estimating how much resource you are going to need. The con of using S3 bucket is not accounting for excess usage of resources which could result in high costs. Along with S3 usage there are automation services such as versioning and lifecycle policies. Versioning allows for administrators to store, retrieve, and archive different versions of objects in a bucket which could be useful when developing new applications or deploying patches and updates. Data lifecycle management is also an automated service that transitions data that is rarely accessed into AWS glaciers to free up resources as it mainly consists of older large data files. Some other cons to S3 bucket usage is not having the proper access permissions and configurations that could lead to unauthorized access and actions.

The log and alert monitoring system that was set up was “network packets out” to monitor the activity and packets being sent to the EC2 instance. Monitoring the amount of outbound packets being sent could be an identification of a botnet attack or a denial of service attack.

Further Securing the System

To further enhance the security system, more layers of defense can be implemented such as: Developing a baseline, continuous monitoring, multi-factor authentication, systems hardening, and role based access controls.

Developing a baseline is the first step to be done in order to determine “normal” operations of the EC2 instance. This can be done by analyzing the CloudTrails and CloudWatch logging information. If there are any deviations from the baseline that takes place, documentation and analysis is the next step to address the reasons for deviations. Another layer to add is to conduct continuous monitoring and audits which includes performing penetration tests to determine any weakness and vulnerability of the system. In addition to that, continue monitoring the current state of the system and testing it against the determined baseline. Implementing multi factor authentication is done through the IAM management console for each user. There are different ways of going about implementation such as: software authenticators, hardware authentications, and SMS authentication. The next layer to implement is to harden a system using vendor guidance. Using OpenVPN’s recommendation to improve security consists of securing root users for servers on virtual machines, securing the administrative user, and hardenting the web server cipher suite string. Hardening of the web server encrypts data in transit as web interfaces are not susceptible to man in the middle attacks or plain text communication. Other factors of hardening include: regular updates and patches to new vulnerabilities discovered, deploying Intrusion detection services and intrusion prevention services to detect and prevent the possibility of a cyber attack. Role-based access control is another layer of defense to add as this relates to the principle of least privilege. In the application there are different roles from handling the S3 bucket, the EC2 instance, and vulnerability. Each of the roles are given permissions as to what actions they are allowed to perform. For example, an administrator may have access to all roles while a developer may not need to have access to backups and log information in the S3 backup. Scheduling routine checks on these roles for the duration of their responsibilities should be implemented as assignments change based on completion of responsibilities.

3 Months Support Plan

To maintain the application for the next three months, the process of this would be: installing patches and updates, log monitoring, and security system monitoring.
The system administrator should be responsible for installing new patches and updates to the system. The system administrator is also responsible for checking for patches published by AWS for the OpenVPN server. When there is an available update or patch, it is critical for the patches to be installed during non-peak usage times. Scheduling updates to take place during non-peak hours minimize business operations and server disruptions. While installing patches, the system administrator must also ensure that the current system configuration is interoperating with new updates/patches. Checking for updates and patches should be done twice a month as the landscape of security is ever changing.

The next step to keep the system running is log monitoring. With CloudTrails automated, it is critical to review log information for any unusual or suspicious activity. Some suspicious activity include failed login attempts and different location logins.The person in charge of this task would be the security analyst. Log analysis should be done on a weekly basis. In addition to that review the CloudWatch alarms that have been set up to modify the alarms based against new baselines if needed.

The next step to keep the system running would be reviewing the automatic system security configurations. This would include identity access management reviews ensuring that users do not have access to roles they no longer need because of the changes in roles and responsibilities, the frequency of this check should be monthly as projects have a specified time period. In addition to that, ensure that the CloudWatch Alarm is functioning properly and make any adjustments based on new baselines or security landscape changes, this should be done weekly by the cloud administrator. Performing monthly security audits through AWS inspector is crucial to keeping the system running as Inspector provides assessments results of available vulnerabilities. Reviewing inspector assessments also allows the security analyst to address security weaknesses if any are found.

Overall, installing patches and updates, reviewing log information, and security system configurations would be the actions needed in order to keep the instance running for the next three months.

Incident Response Plan

The information at risk in the EC2 instance and the VPN are going to be information about the devices that connected to the EC2 instance, VPN and EC2 configuration credentials, as well as access to the S3 bucket which holds the most sensitive information. If an eavesdropper gains access to the management console, could lead to unauthorized access to all AWS services being used to host and protect the instance as well as modify configurations across the entire AWS environment to gain full control.

In response to an infected instance, the first action to take is to isolate the EC2 instance by temporarily shutting the insurance down or configuring security groups to limit incoming and outgoing traffic. Once the instance is shut down, Review any unauthorized active sessions to terminate the session. The next action is to determine which user credentials were compromised and suspend the account. These actions are to be done using AWS systems manager and start gaining control. Once the system is isolated and users are suspended, an assessment of the system is to be conducted.

The investigation of the system consists of using Inspector to conduct a vulnerability assessment of the EC2 instance and S3 bucket. Once assessment is done, cross reference the vulnerabilities by using the Security Technical Implementation Guide(STIG) to also address other weaknesses and vulnerabilities. Also reviewing CloudWatch logs to discover the initial point of unauthorized access.

Depending on the severity of the unauthorized access, completely starting from scratch would be the best choice while addressing the newly identified vulnerability. If the compromised system did not result in severe damages, then restoring from a snapshot that is safe would be the best course of action. Prior to fully backing up a system, system administrators should sandbox the backups to identify whether or not a backup has been compromised.

Documenting the series of events after an cyber incident and recovery is important as well to update the response plan. Once recovered, the system admin is to develop a new baseline for the system and reconfigure the thresholds for CloudWatch Alarms to alert. While recovering to normal operations systems security testing should be changed to weekly to ensure risk mitigation measures are in place to prevent future incidents.

Scap Failure

The implementation of the Security Content Automation Protocol(SCAP) and STIG was unable to work on the system because the ubuntu terminal was unable to locate the package for the SCAP security guide, despite trying to get the update files and upgrade the system. Other efforts include trying to download and unzip the package in the terminal from a git repository but the terminal system failed and was forced to reboot. Also trying to run SCAP on OpenSCAP was not working. Running SCAP and STIGS would be able to cross reference an Inspector assessment to determine if there were any other vulnerabilities. While Inspector is specifically made for AWS services, SCAP is a standardized security policy that is applicable across different systems. Other security testing could be a manual audit going through the entire system. In addition to that penetration testing to possibly exploit vulnerabilities to a system.