Group 4: Cyber Guardians

Alexander Echols
Dericus Horner
Dylan Dempsey
Geneva Knott
Anthony Wall

Project Prep 3: MVP

IAM Implementation:

We will configure IAM best practices for the root account, including strong password policies, enabling multi-factor authentication (MFA).

We also will need to implement IAM Roles and policies

- Privilege of least principle

Server Hardening and data protection:

This will be achieved by deploying a Windows Server Domain Controller instance on a private subnet of a VPC accessible only via VPN tunneling.

We will enable encryption at rest using AWS key management services or aws s3 server-side encryption for the DC and other relevant data resources.

Establish VPN connectivity using AWS VPN service to securely access the private subnet.

CIS-Compliant Data Server by:

Achieved by;
Deploying a linux server instance containing PII and PCI data
Enable encryption at rest using Linux native encryption mechanisms.
Configure secure access controls and firewall rules to restrict access to the server utilizing the CIS Benchmarks.

SIEM/Log Aggregation System:

We will deploy the SIEM/log aggregation system in the form of CloudWatch.

We will configure CloudWatch to ingest real-time event logs from key assets (EC2 instance)
We will ensure that the security-relevant logs and sysmon generated logs are collected and analyzed by CloudWatch.

Attack TTP and Event Ingestion:

We will develop a python script utilizing a dictionary and hydra to simulate a brute force attack that will attempt a ransomware attack.
AWS Lambda can be employed to run the function when triggered, these functions could consist of alerts, mitigation, or escalation.
We will implement security measures (triggers or alarms) to detect and generate events for the simulated attack, ensuring the events are seen by CloudWatch

Cloud Monitoring:

We are going to accomplish by;

Enabling VPC Flow Logs to capture traffic and monitor suspicious or malicious activity.
We will also utilize AWS Lambda functions to trigger relevant responses or notifications in case of detected threats

Threat monitoring will be accomplished by monitoring the security logs, and setting up alert mechanisms to id and respond to potential threat activity.

Novelty:
AutoGPT to monitor AWS
LUKS to FDE the Linux server

Project Management

We will utilize github organizations and Trello to work as our project management tools

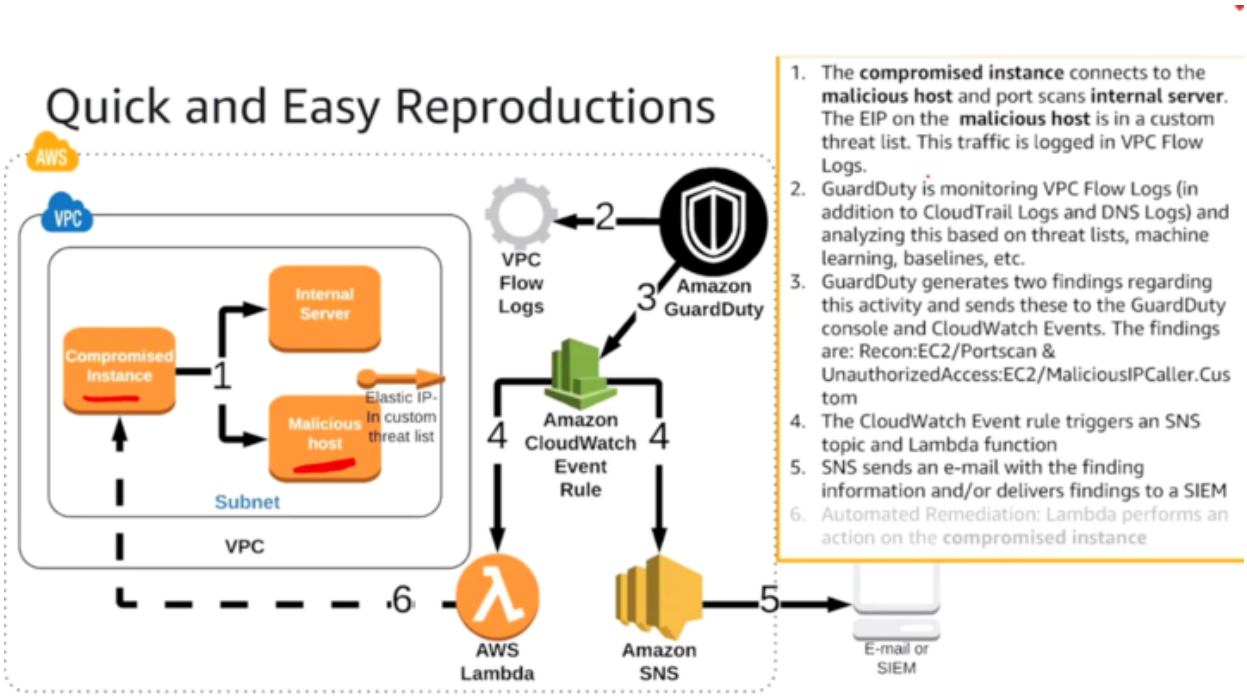
- We will utilize Trello to help with core team activities.
    - https://trello.com/invite/b/BipghZcm/ATTI082defa96011b42ea1eaef8c6c8c393f27C38804/cyber-guardian
- Github will be used to hold any code we utilized.
    - https://github.com/Cyber-Guardians

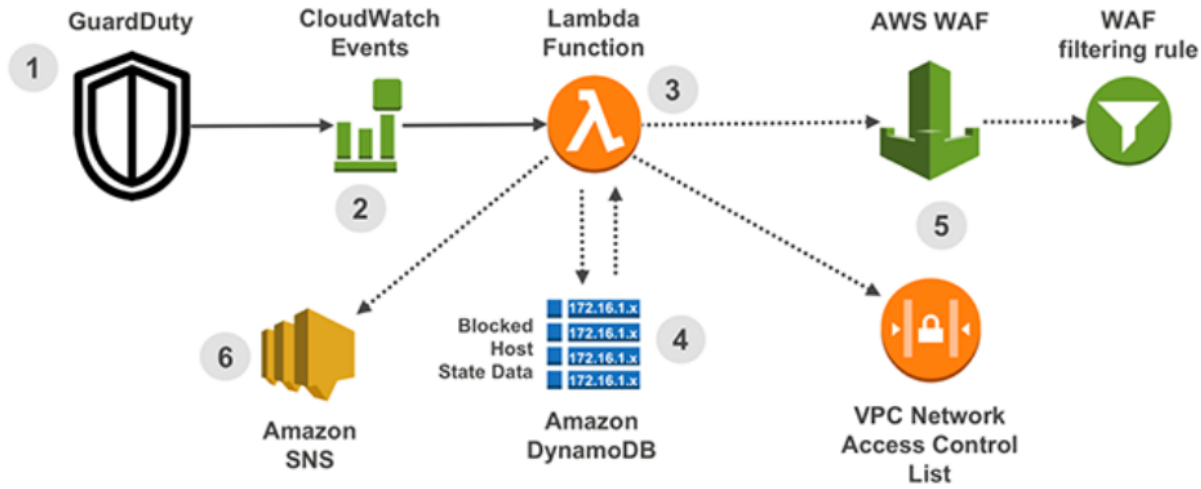
System Diagrams

Create some initial diagrams of any aspects of your solution that you can plan at this stage. Examples include topologies, network diagrams and process flow charts.

Link these assets in your GitHub Documentation repo for review during daily stand-ups.

IN PROGRESS……





SOPs

Fill in your PM Tool with SOPs that need to be written, then evenly distribute the SOPS to different team members to complete.

- For each SOP included in your MSP SOW deliverable, attribute authorship to the team member.
- SOPs will be Google Docs:
    - **Security Incident Plan**
        - **The test plan should include detailed testing procedures of security controls and monitoring solutions along with expected outcomes.**
        - **Include a diagram of the expected events when an attack triggers your monitoring tools.**
    - **Compliance Documentation**
        - **Compliance documentation should be developed to demonstrate that the system meets any relevant regulatory requirements.**
        - **This may include documentation showing compliance with PCI, GDPR, or other industry-specific regulations. (Pick one compliance framework)**