D.E.E.P Impact has been contracted to improve the cybersecurity processes and systems for a client company, focusing on logging, monitoring and detection of insider adversarial activity on cloud infrastructure.- Pending given scenario

William Baur
Hector Cordova
Festus Oguhebe, Jr
David Renteria
Tommy Taylor
Breanna Taylor

Prepare for Projects: Systems Selection Document

This project will require you to demonstrate skills you've learned so far in the course.

Deliverable

Start a new Google Doc, and include the following components in your system selection submission.

- Name the doc "ops-201d# Team# System Selection"
    - Replace "#" with your cohort number and team number/name.
- Add team members to the "People with access" category with "Editor" privileges, using their gmail address.
- Format your Google Doc to be pageless.
    - File > Page Setup > Pageless > OK
    - Click on the margin's bar top/left side
    - Hover over Text Width
    - Select Full
- List all team members' full names at the top of the doc.
- Copy and paste your team's scenario into the doc with a header.

Systems Selection

Review the project guidelines and scenarios. Meet as a team and decide what systems, platforms, or tools you'll be using this project. Each should represent a clear, logical solution to a problem the client company is facing.

Create a high-level list of systems, platforms, or tools you're going to implement for your client. For each, explain: AWS(Cloudtrail,Cloudwatch,IAM,VPC,EC2,),Linux,Microsoft, Python

- How does it fit into your scenario's requirements?
    - CloudWatch - AWS tool used similarly to a SIEM (ie Splunk) to monitor for malicious activity
    - VPC- Flow Logs - Monitors IP traffic at all network interfaces
    - CloudTrail-Records and stores logs of activity in the AWS account.
    - IAM-Management of AWS resources access
    - EC2-Allows for affordable use of virtual servers and application use
    - Python-use of an automated script for a brute force attack
- What problem or pain point does it solve? In other words, what value does this add to your client?
    - CloudWatch-Response to suspected malicious activity after being alert by CloudTrail
    - VPC Flow Logs-Enables CloudWatch to respond to m
    - CloudTrail-The security of AWS with the who,what,when,how,and where.
    - IAM- Controls the access of resources and the actions that want to be performed by an user
    - EC2- server asset to perform as data at rest, store sensitive data on and active directory,domain controller services
    - Python- the use of automate scripting of brute force attacks
- Minimum Viable Product (MVP) definition.
    - What is the **minimum** required for you to present on your demo day?
    - CloudWatch-logs,alarms metric filters, events
    - VPC Flow Logs-log storage,log format
    - CloudTrail-data event, insights
    - IAM-user and group management,least privilege,IAM policies
    - EC2- Linux Instance and Microsoft Instance
    - Python- script that brute force attacks a known user and password, copy a file,extract copied file via SFTP

During your pitch, your instructor will help you scope your project. Some features may become MVP and some may become stretch goals.

Once you are ready, find your instructor and pitch your solution ideas.

Submitting your work

This is a group submission. Only one person must submit for group credit.

Please have everyone's name at the top of the Google Doc.

Share your Google Doc so that "Anyone with the link can comment" in the submission field below.

This step must be completed and approved before proceeding with any project work. Notify your instructor when this is ready for review.