Omar Ardid omar.ardid.817@gmail.com
Steve Cherewaty scherewaty@gmail.com
Gilbert Collado gilbertcolladoxd@gmail.com

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 scenario. 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:

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?

- IAM - Management of AWS resources access & permissions
- VPC - Amazon Virtual Private Cloud within which EC2 instances operate.
- VPC Flow Logs - Monitors IP traffic in and out of the VPC.
- CloudWatch - Within AWS, takes in VPC Flow Logs and organizes events.
- EC2 - Virtual machines within the VPC, acting as operating endpoints.
- Python - Automated tools used by Troll Trace are developed in python.
- Splunk - Platform for searching mass log data.

What problem or pain point does it solve? In other words, what value does this add to your client?

Each of these components acts as a painkiller, but all of them combined provide at least partially automated solutions to monitoring individual machines and the network at large. This allows a small team (if not a single individual) to parse massive amounts of data, set up alarms and take actions on hacking attempts.

Minimum Viable Product (MVP) definition.

What is the minimum required for you to present on your demo day?

- IAM - user and group management, least privilege, IAM policies.
- VPC - Allows for maximum flexibility and scalability.
- VPC Flow Logs -log format & storage.
- CloudWatch - logs, alarms and events.
- EC2 - Linux & Microsoft instances.
- Python - Various tool scripts
- Splunk - Log aggregator for search, indexing, correlating and reporting.

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.