Tianna Farrow
Dominique Bruso
Zachariah Woodbridge
Bryanna Fox
Heraldo Morales
Deqa Hussein

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:

1. How does it fit into your scenario's requirements?
2. What problem or pain point does it solve? In other words, what value does this add to your client?
    - Keep it high level without going into too much detail, 3-4 sentences is enough.
3. Minimum Viable Product (MVP) definition.

Tianna Farrow
Dominique Bruso
Zachariah Woodbridge
Bryanna Fox
Heraldo Morales
Deqa Hussein

- What is the **minimum** required for you to present on your demo day?
    i. **CIS-compliant Windows Server DC**
    ii. **Private VPC Subnet only accessible through VPN tunneling**
    iii. **Data encrypted at rest and at transite**
    iv. **CIS-Compliant Data Server**
    v. **Log Aggregation**
    vi. **Cloud Monitoring**

MINIMUM Project Requirements

For this project, your client has requested a demonstration of how you'll be able to protect their cloud infrastructure. You'll need to implement the following in AWS Cloud to demonstrate how you'll secure the AWS environment:

- IAM
    - Proper IAM best practices must be implemented for the root account
    - Proper IAM for all team members must be implemented using AWS best practices
- Server Hardening and Data Protection
    - CIS-compliant Windows Server DC hosted on a private subnet of a VPC and accessible only via VPN tunneling
        - Data needs to be encrypted at rest and encrypted in transit
        - Deploy Sysmon to generate security-relevant system logs
    - CIS-compliant Data Server
        - Linux server instance containing PII and PCI data
        - Data needs to be encrypted at rest and in transit
- SIEM / Log aggregation system
    - Splunk, CloudWatch, Elastic Stack
    - Configured to ingest event logs in real time from key assets including EC2 instances
    - Show an attack TTP, attack must incorporate a Python script using a new library you have not worked with yet.
    - The attack should trigger an event that gets ingested by the SIEM solution
- Cloud Monitoring
    - Capture traffic for the client to demonstrate how the attack TTPs would be detected in the AWS Cloud using VPC Flow Logs and any additional automation necessary
    - An AWS Lambda function triggering a relevant response to a detected threat (this fulfills the requirement for a shell script)

Tianna Farrow
Dominique Bruso
Zachariah Woodbridge
Bryanna Fox
Heraldo Morales
Deqa Hussein

    - Monitor for threat activity in your AWS environment
    - Monitor Security Logs for failed SSH attempts on your instances
- Novelty
    - Challenge yourselves to implement a novel tool, system, or technique that was not demonstrated or performed during lab time in term 1 of your Ops 401 class.

MINIMUM Presentation (55%)

Components of the presentation must include:

- A. Team members individually introduce themselves using their own professional pitch. (3 min, explain why they are making the career change)
- B. Topical overview (2 min)
    - B1. As the "Problem Domain", describe the project scenario you were assigned and the overall client requirements.
        - B1a. Compliance requirements
        - B1b. Security systems requirements
- C. Technical demonstrations of solutions (12 min)
    - C1. Introduce the cloud architecture diagram of your environment
    - C2. Demonstrate your solution(s) to the problem domain here
- D. Final thoughts on how the project went (3 min)
    - D1. Each team member should share some final thoughts on the project. Some topics you could discuss here include:
        - D1a. The team's approach to planning and communication throughout the project
        - D1b. A technical obstacle or two and how those obstacles were overcome
        - D1c. A portion of the outcome you are particularly proud of achieving
- E. Q&A (5 min)

MINIMUM Deliverables (45%)

Submit to instructor a single link to your Github Org. All team members are to contribute an equal share to documentation corresponding to the components they worked on and should clearly indicate which components each contributed to in their individual project submission notes.

- GitHub Repository (10%)
    - A repo under an appropriately name Github "Organization"

Tianna Farrow
Dominique Bruso
Zachariah Woodbridge
Bryanna Fox
Heraldo Morales
Deqa Hussein

    - Sufficient documentation in the top level README to explain to a stranger who you are, what this project was about, and how all of the material in the repo pertains to it.
        - This README should be:
            - Attractively formatted
            - Include links to relevant files in the repo
            - Include links to each of your own Github accounts AND LinkedIn accounts
    - All other deliverables should be included as files in this repo
    - Deployment scripts: Scripts used to automate the deployment process of the project, which includes provisioning the required AWS resources, deploying the code, and configuring the services.
- Presentation Material (5%)
    - Slide deck, as a PDF
    - A link to the video of your presentation (when it becomes available)
- Cloud Architecture design (20%)
    - AWS infrastructure components, their interactions, and how they fit together.
        - This diagram should be comprehensive and understandable to all stakeholders involved in the project.
    - All components must be labeled, and diagram must be presentable (straight lines) and free of defects/typographical issues. Take your time to create a quality diagram; do not rush!
    - Clearly indicate AWS instances, networks, tools and services.
    - A clear, written explanation and justification of your cloud architecture design.
    - Add descriptions of how you incorporated these systems into your technical demo:
        - AWS IAM
        - AWS CloudTrail
        - Amazon GuardDuty
    - Include a table or chart of network infrastructure and configuration details (yes, this will overlap with your topology -- you must document your network in both ways):
        - Subnets and their uses
        - Include Subnet Masks, CIDR addresses, etc.
        - Security Group rules
- SOP and Policy Documentation (10%)
    - Security Incident Plan
        - The test plan should include detailed testing procedures of security controls and monitoring solutions along with expected outcomes.

Tianna Farrow
Dominique Bruso
Zachariah Woodbridge
Bryanna Fox
Heraldo Morales
Deqa Hussein

        - 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)

*Pulled from: project-guidlines.md

https://github.com/codefellows/seattle-cybersecurity-401d10/blob/main/class-20/project-guidelines.md

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.