Omar Ardid omar.ardid.817@gmail.com
Steve Cherewaty scherewaty@gmail.com
Cody Blahnik cody.blahnik@gmail.com
Julian Pena juliancamilopenamanrique@gmail.com

# Scenario and Problem Domain

Your team has been contracted to improve the cybersecurity processes and systems for a client company, focusing on logging, monitoring and detection of adversarial activity on cloud infrastructure.

# 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:

- **IAM/Access Management**

-Access Analyzer

- **Server & Data Protection**

-Sysmon (logging)
-LUKS  (Novel)

- **Cloud Monitoring**

-Cloud Trail (API)
-Cloud Watch (Monitor Apps)
-Guard Duty (Monitor flow logs from EC2's)

- **Lambda**

-Code to take an action (Timeout, close port)

- **Log Aggregation (SIEM)**

-ELK Stack (Novel)

1. **How does it fit into your scenario's requirements?**

   The principle of least privilege and access control ensures that unauthorized users cannot abuse their privileges. Data at rest inside our Windows and Linux Servers are encrypted with custom code.  S3 buckets are also encrypted.  System logs are monitored with sysmon. Most components will be AWS products, including cloud monitoring through CloudTrail, CloudWatch, and GuardDuty. A custom Lambda function will take action on predetermined conditions, and SNS will notify the user(s).

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

The structure we're building will ensure maximum protection against various attack TTPs.  If an intrusion or attack does occur the event will be quickly logged and automated responses will act appropriately.  Additionally, the proper administrators will be notified in real time.

3. **Minimum Viable Product (MVP) definition.**
    - What is the **minimum** required for you to present on your demo day?

Architect an AWS infrastructure for The Company with IAM management, data protection, cloud monitoring, and SIEM solution as a construct to prevent attacks.  A Globex employee accidentally published their password on a GitHub repo. With the leaked password, we will demonstrate a brute-force attack attempt on the Linux public server. The IDS/IPS will log the attempt notify administrators and prevent these attacks using lambda scripts.

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.