Cybersecurity Plan — Capital One

Zhengtao Wang

ITC 6520 Network Protection & Cloud Security

Capital One Data Breach

- Cybersecurity Data Compromised
- Safe Haven —> UnderScore the Critical Importance
- Date: May 26, 2023
- Cybersecurity incident involving NCB Management Services, Inc., a Capital One vendor —>Suffer Data Brench
- Exposed Critical Customer Information

Cybersecurity Plan Objectives

- **AWS Services -**
  - Identity and Access Management (IAM)
  - CloudTrail
- Logging and Monitoring
  - 1) API Calls 2) Monitor Resource Configuration Change
- Data Backup and Disaster Recovery

Cysecurity Plan Framework (Five Steps):

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

How the policy applies to the organization - 4W

- **Who : which personnel?**
- What : which equipment, networks, or processes?
- When: are there any time or status restrictions?
- **Where : which locations?**

Identify

- Risk Assessment：
  The key is to assess the impact of the risk on the company and individuals and to develop relevant strategies in a timely manner.

- **Computing Asset Management ：**
  Classify and enforce strong access controls, encryption and monitoring of data by sensitivity and develop plans to mitigate damage

Protect

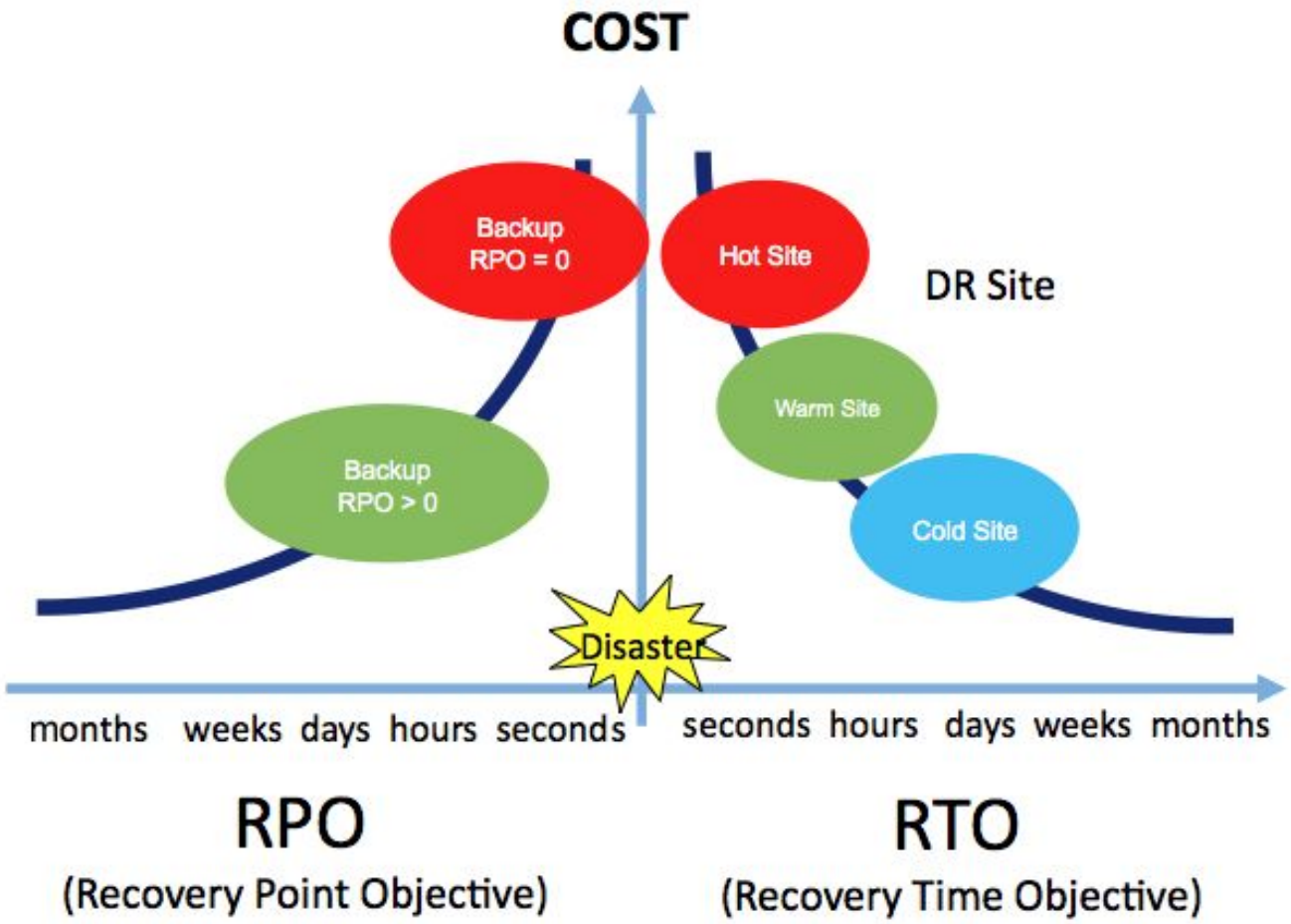
- **Incident Response Plan**
- User Training
- Both worked collaboratively to improve cybersecurity

Detect

- **Vulnerability Management Plan:**
  (VMP) is a strategic framework aimed at cybersecurity challenges.
- **Core Goals:**
  Aims to enhance awareness and reduce cybersecurity vulnerabilities
- **Scope:**
  Defines the boundaries of responsibility

Respond

- Data **cold site** vs. **hot site**
- Data **Availability** and **Operational Resilience**
- Scope:
  Address the cybersecurity challenge of unexpected events with **multi - region capability**


COST
Backup
RPO = 0
Hot Site
DR Site
Warm Site
Backup
RPO > 0
Cold Site
Disaster
months weeks days hours seconds
seconds hours days weeks months
RPO
(Recovery Point Objective)
RTO
(Recovery Time Objective)

Recover

1.Visibility: This clarity ensures that all relevant stakeholders understand their roles and responsibilities during incident recovery.

2.Risk Reduction: It minimizes the potential impact on the organization's operations, data, and reputation.

3.Communication: It ensures that stakeholders are informed and that relevant authorities or parties are notified when necessary.

4.Documentation: This documentation is valuable for post-incident analysis and continuous improvement.

5.Compliance: Executing the plan helps ensure compliance.

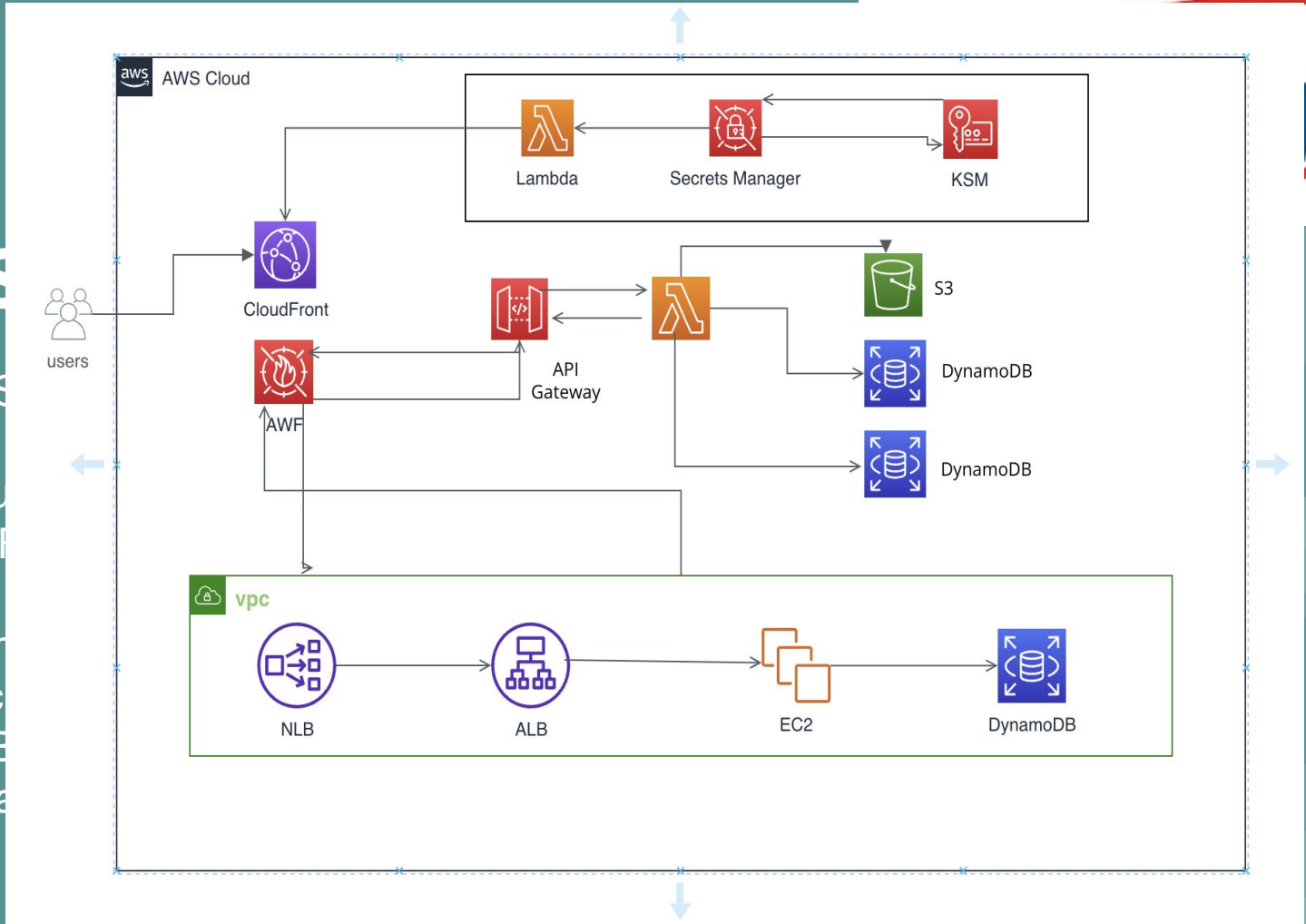
AWS Architecture and Implementation

- AWS High - Level Picture
- AWS Design
- AWS Possible Improvement
- AWS Course Reflection and Learning

AWS

The AWS

- clou
- AWF
- API
- Lam
- Sec
- NLB
- S3 a



AWS Design

Step 1: Create VPC and Internal Resources

Step 2: Create and Configure the API Gateway

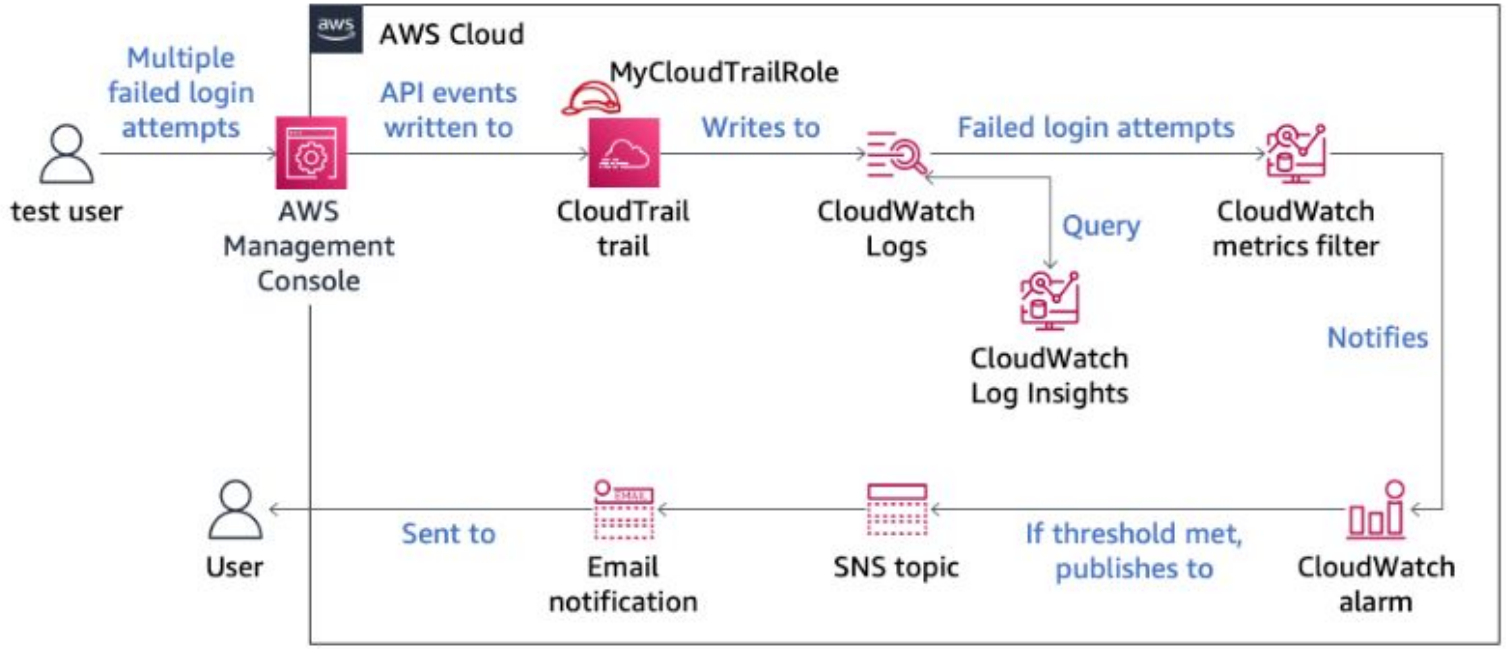
Step 3: Create the Lambda Function

Step 4: Setting Up the API Gateway to Connect to the VPC

Step 5: Deploy the API Gateway

Step 6: Test API Access

Step 7: Monitoring and Security


AWS Cloud
Multiple failed login attempts
API events written to
MyCloudTrailRole
Writes to
Failed login attempts
test user
AWS Management Console
CloudTrail trail
CloudWatch Logs
Query
CloudWatch metrics filter
CloudWatch Log Insights
Notifies
User
Sent to
Email notification
SNS topic
If threshold met, publishes to
CloudWatch alarm

AWS Course Reflection and Learning

- Explore the field of cybersecurity
- Lab1 - Securing VPC Resources by Using Security Groups
- How IAM role gain different access permissions
- Combination of experiment and theory

Future Envision
(What Could Go Wrong in the Future)

- Future Incident Response Plan
  - Adopt a zero-trust model
  - Regular Vulnerability Assesment
  - Foster a Culture of Awareness

References

Mahesh, Boykin, C., ruiz, J., Harris, C., Burbon, R., Hollins, L., Price, R. F., Tonda, Sandra, Harris-Allen, P., Larson, C., Cole, F., Lussier, B., Morgan, D., Wilson, G., caesar, Z., Smith, D., Cooper, L., Hena, … Cortez, S. G. (2023, October 14). Capital one class action settlement, payment date, how to claim it?. RajNeetPG. https://rajneetpg2022.com/capital-one-class-action-settlement/

Big data. (2013). Mary Ann Liebert, Inc. https://therecord.media/capital-one-ncb-management-services-data-breach

Capital one data breach settlement payments have started. Dataconomy. (2023, October 13). https://dataconomy.com/2023/09/29/capital-one-data-breach-settlement/