Ops 401 Midterm

Our Team

1. Brad Baack
2. Gilbert Collado
3. Ethan Pham

Brad Baack

- United States Marine
- Cyber Security Engineer
- Traveler

LinkedIn

Gilbert Collado

- Cyber Security Professional.
- US NAVY veteran, 9 years as an Electronics Technician.
- Skilled in Hardware,windows, linux and MacOS troubleshooting
- Expertise in Repair of CCA’s, soldering components and building PC Systems.

Ethan Pham

- Cyber security professional
- Skilled in Windows, Linux, and MacOS troubleshooting
- Skilled in bash, powershell, and python3 coding
- Very new to cybersecurity

LinkedIn

Client Needs

- Implement Strong Access Controls
- Server Hardening and Compliance
- Continuous Monitoring and Detection
- Automated Threat Response

IAM POLICES
☑ Ildentity and Access Manageent
☑ Ddonity Allless Managent
☑ henhity and Access
☑ In Inenten ulament
☑
☑ Va
☑ iddn nogent
☑

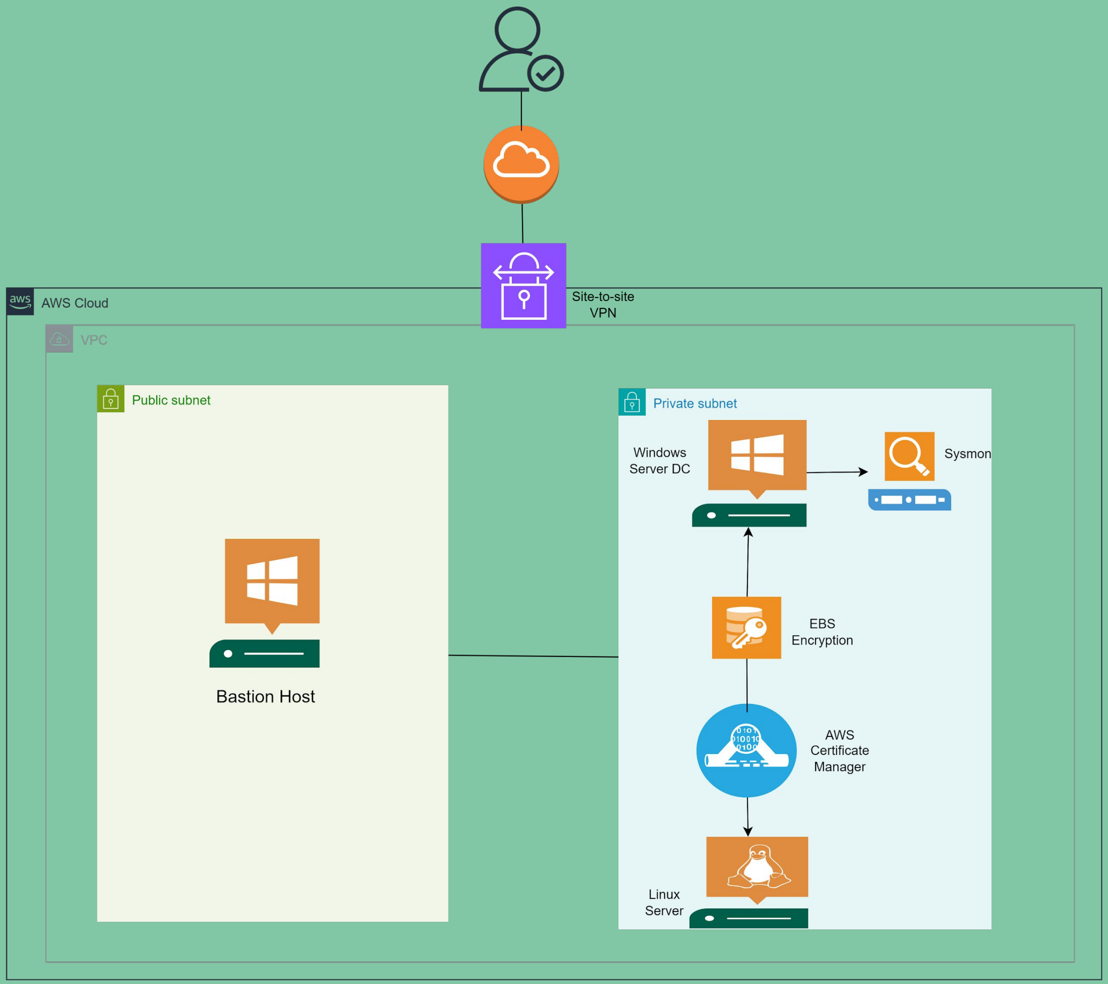
Identity and Access Management

- **Enhanced Security**
- **Compliance**
- **User Management.**

MITRE
ATT&CK™

- **Initial Access (T1078):** Brute force attack using valid accounts.
- **Execution (T1059):** Command and Scripting Interpreter, potentially used if the attacker gains access.
- **Persistence (T1098):** Account Manipulation to maintain access.
- **Privilege Escalation (T1078):** Using stolen credentials to gain higher privileges.
- **Defense Evasion (T1070):** Indicator Removal on Host to avoid detection.
- **Credential Access (T1110):** Continued brute force attempts for additional credentials.
- **Lateral Movement (T1021):** Remote Services like SSH to move between systems.
- **Collection (T1119):** Automated Collection of sensitive information.
- **Exfiltration (T1041):** Exfiltration Over C2 Channel to transfer data out of the network.

SERVER HARDENING
AND DATA PROTECTION


Site-to-site
VPN
AWS Cloud
VPC
Public subnet
Bastion Host
Private subnet
Windows
Server DC
Sysmon
EBS
Encryption
AWS
Certificate
Manager
Linux
Server

Server Hardening and Data Protection

- **Objective: Enhance security of cloud infrastructure**
- **Measures: Apply CIS benchmarks**
- **Encryption: Data at rest and in transit**

Access via Bastion Host and VPN

- **Bastion Host: Secure access point in public subnet**
- **VPN: Site-to-site connection for secure access**

Windows Server DC

- **Compliance: CIS benchmarks for security**
- **Access: RDP via Bastion Host**
- **Logging: Deploy Sysmon for logging**

Linux Data Server

- **Compliance: CIS benchmarks for security**
- **Access: SSH via Bastion Host**
- **Data Types: PII and PCI data**

Protecting Sensitive Data

- **Encryption: Comprehensive encryption strategies**
  a. **Data at Rest: EBS encryption**
  b. **Data in Transit: AWS Certificate Manager**
- **Monitoring: CloudWatch for centralized logging**

Log Aggregation and Cloud Monitoring

Logging and Cloud Monitoring

CloudTrail:

- **Records and monitors API events**
- **Records and monitors user activity**

CloudWatch:

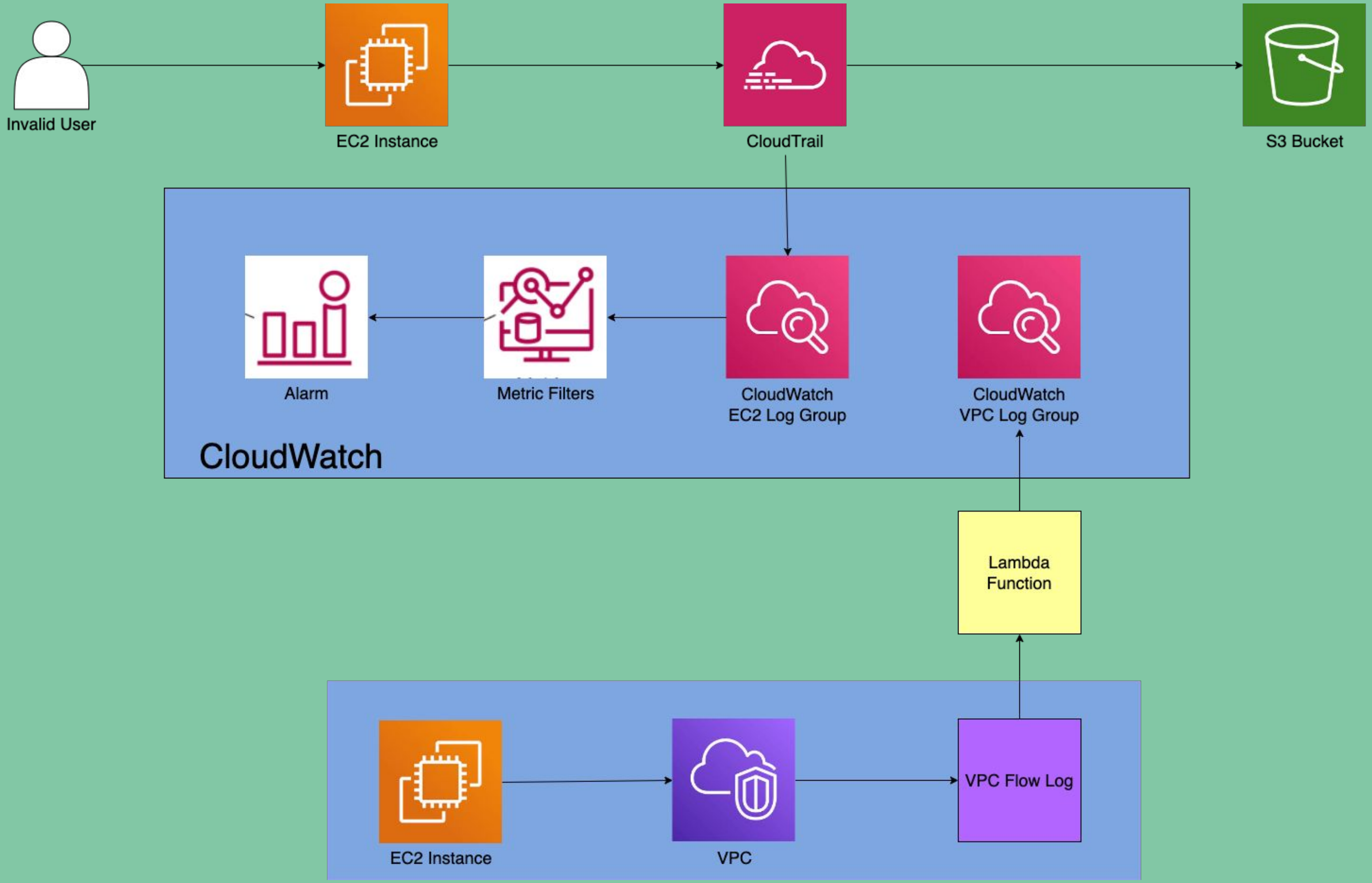
- **Records logs, metrics, and events**
- **Filter metrics and alert of events**

VPC Flow Logs

- **Records traffic over VPC**

Lambda Function

- **Executes code for performing services**


Invalid User
EC2 Instance
CloudTrail
S3 Bucket
Alarm
Metric Filters
CloudWatch EC2 Log Group
CloudWatch VPC Log Group
CloudWatch
Lambda Function
EC2 Instance
VPC
VPC Flow Log

ec2
instuce
SSH Brutt force attack
as sescr ance ((aB))
(scirll) incsotss it)

Mitre Attack Follow up

- **Initial Access (T1078)**: Brute force attack using valid accounts to gain initial access to specific servers.

- **Credential Access (T1110)**: Continued brute force attempts to obtain additional credentials.

- **Lateral Movement (T1021)**: Using SSH to move between systems within the network.

Resources and Thanks

- Tools Utilized
  - Amazon Web Services (AWS)
  - Github
  - Visual Studio Code (Vscode)
  - Python 3
  - ChatGPT
- Special Thanks
  - Ethan Denny
  - Zachary Derrick

SCAN ME

Questions?