CYBER SHIELD

AGENDA

Team Member Introductions

Scenario

Suggestion

Demo's

Q&A

Joe Gutmann

- Worked at City, State, and Federal Government levels
- Marine and Air Force Vet in the Intel and Logistics fields
- Small Business Owner
- Lived in Japan for several years, and traveled throughout SE Asia/Europe
- Loves art, can't draw stick figures

Yue Moua

I

- US Navy Veteran

- Cybersecurity, Bash, PowerShell, Python

- Disciplined, Detail-oriented, Responsible

- Eager to Contribute to Cybersecurity

Thierry Tran

- US Army Veteran
- Pursuing B.S of Computer Science in SNHU (expected graduation in June)
- Inspired by my friend, pursuing CyberSecurity Professional in Code Fellow
- Hobby: Soccer, Movie, Travel.

Amleset Tesfamariam

- Location: Seattle, Washington
- Previously: worked in healthcare; friend introduced me to cybersecurity field
- Career Ambitions: interested in threat hunting/intrusion detection, purple teaming, and cybersecurity analysis
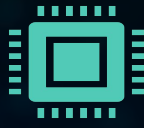- Interesting Fact: Fluent in Tigrinya

SCENARIO

Client Overview:

Desire someone else to improve their cybersecurity processes and systems.

They sell art, and are concerned about their website availability, the confidentiality, and integrity of their proprietary data

Key Focus:

Enhancing cybersecurity posture, especially in cloud infrastructure

Project Objectives:

The primary project objective is to enhance cybersecurity measures within the AWS (Amazon Web Services) environment.

Specific Goals:

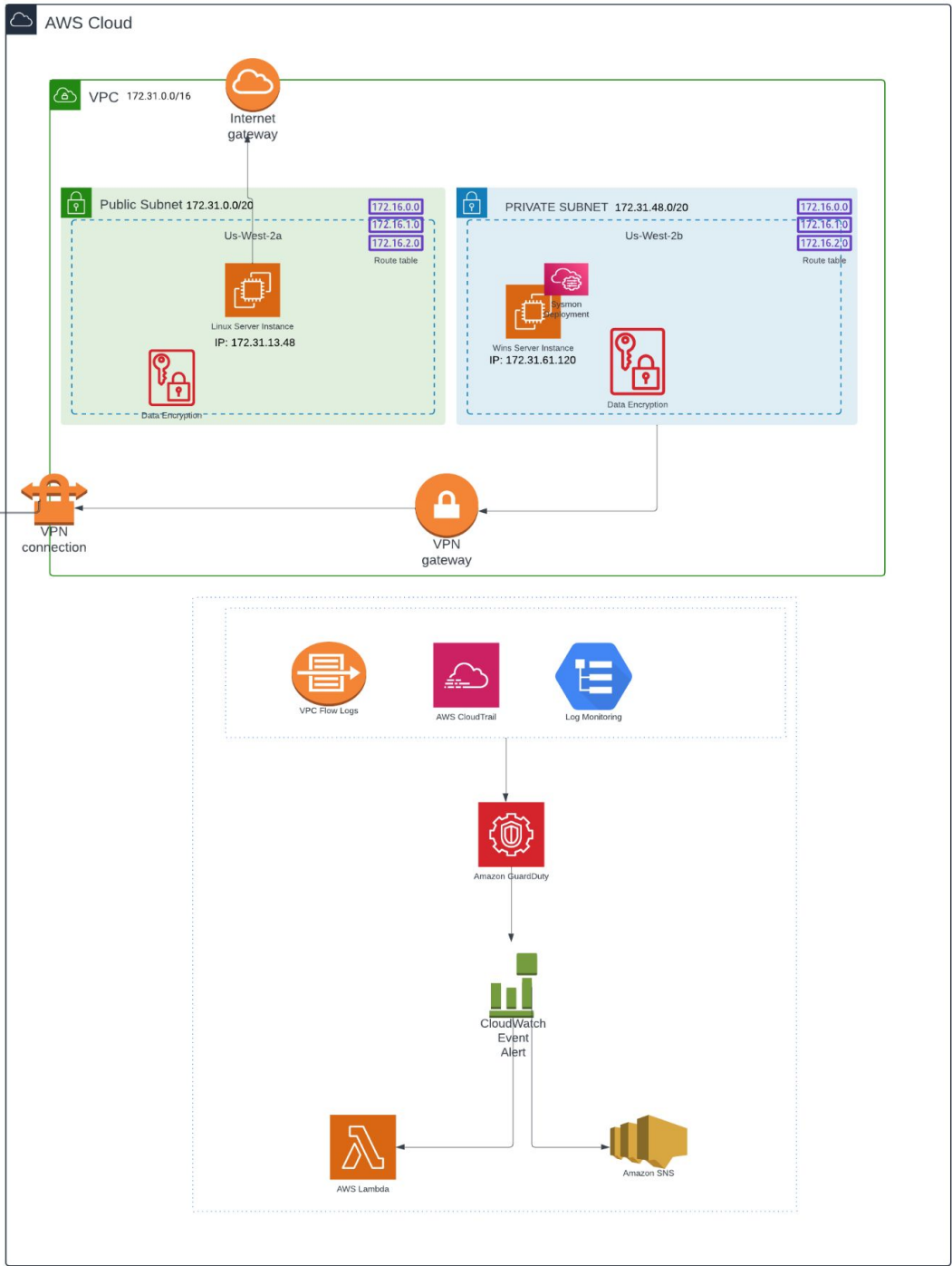Establish Secure IAM Configurations: Ensure proper management of user access and permissions within AWS services.

Server Hardening: Implement measures to strengthen the security of servers within the AWS infrastructure.

Data Protection: Develop and implement strategies for safeguarding sensitive data stored or processed in the cloud.
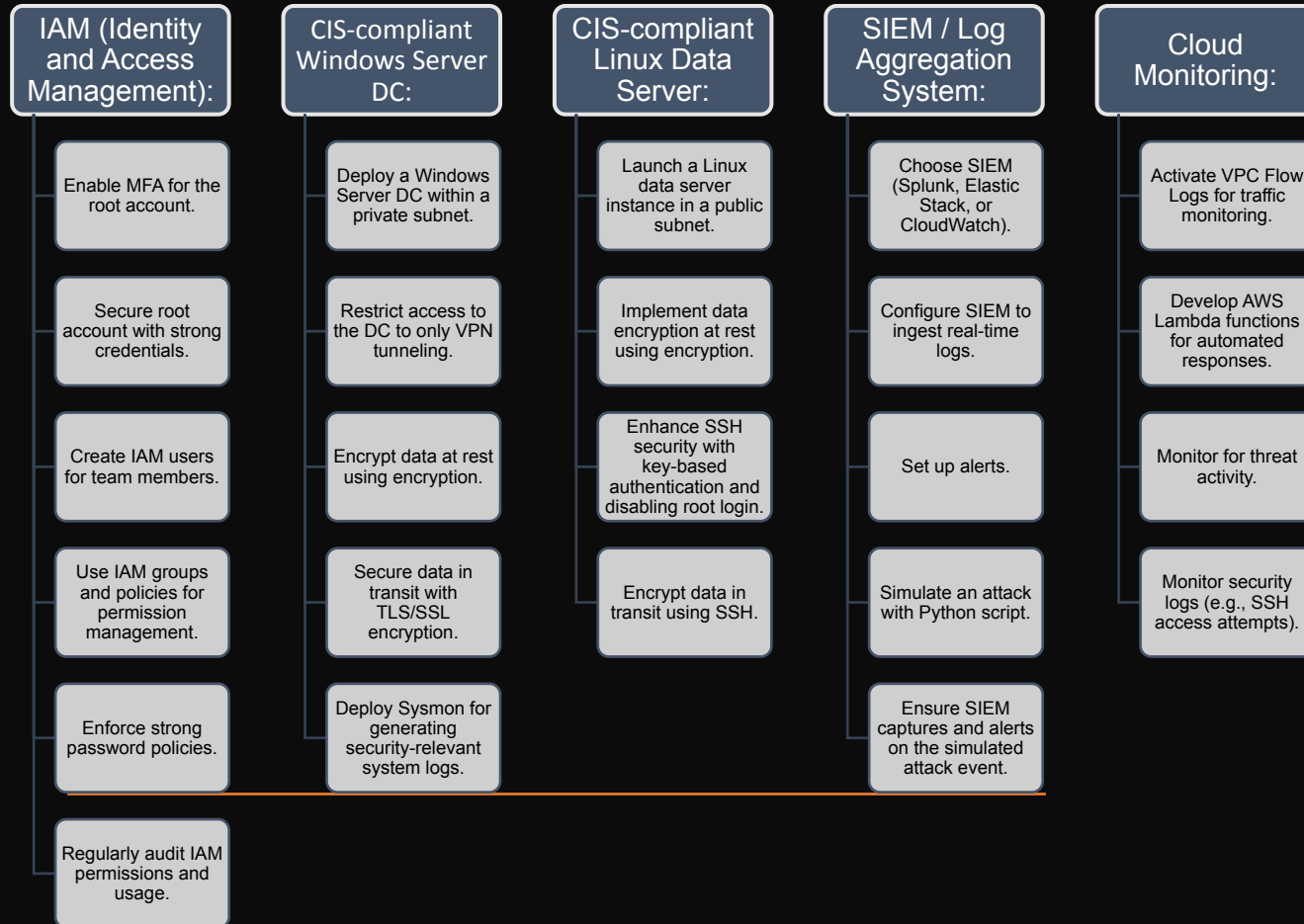
SIEM Implementation: Set up a robust Security Information and Event

NotOurJob Solutions

SOLUTIONS

IAM (Identity and Access Management):

- Enable MFA for the root account.
- Secure root account with strong credentials.
- Create IAM users for team members.
- Use IAM groups and policies for permission management.
- Enforce strong password policies.
- Regularly audit IAM permissions and usage.

CIS-compliant Windows Server DC:

- Deploy a Windows Server DC within a private subnet.
- Restrict access to the DC to only VPN tunneling.
- Encrypt data at rest using encryption.
- Secure data in transit with TLS/SSL encryption.
- Deploy Sysmon for generating security-relevant system logs.

CIS-compliant Linux Data Server:

- Launch a Linux data server instance in a public subnet.
- Implement data encryption at rest using encryption.
- Enhance SSH security with key-based authentication and disabling root login.
- Encrypt data in transit using SSH.

SIEM / Log Aggregation System:

- Choose SIEM (Splunk, Elastic Stack, or CloudWatch).
- Configure SIEM to ingest real-time logs.
- Set up alerts.
- Simulate an attack with Python script.
- Ensure SIEM captures and alerts on the simulated attack event.

Cloud Monitoring:

- Activate VPC Flow Logs for traffic monitoring.
- Develop AWS Lambda functions for automated responses.
- Monitor for threat activity.
- Monitor security logs (e.g., SSH access attempts).

DEMO

Thank You!

CyberShield-Team
Marco Vazquez
Roger Huba
TAs

CyberShield Github

QUESTIONS ?