Brad Baack
Ethan Pham
Gilbert Collado

System Selection Document

Members:
Brad Baack
Ethan Phan
Gilbert Collado

Our Company:
ShieldWall IT

Hiring company:
Valhalla Solutions

Scenario & 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.

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 Implementation

Tools:

- **AWS IAM**: Manages user access and permissions for AWS resources.
- **AWS IAM Policy Simulator**: Tests and troubleshoots IAM policies to ensure they work as intended.

How does it fit into your scenario's requirements?

We'll use AWS IAM to implement best practices for securing user access to AWS resources, which is crucial for protecting Valhalla Systems' cloud infrastructure. This ensures that only authorized personnel can access critical systems.

Brad Baack
Ethan Pham
Gilbert Collado

What problem or pain point does it solve?

This setup prevents unauthorized access by securing the root account, creating specific roles and policies, and implementing MFA. It minimizes the risk of breaches and unauthorized access.

Server Hardening and Data Protection

Tools:

- **AWS EBS and AWS ACM**: Tools for data encryption..
- **CIS-CAT Lite**: Configuration assessment tool to check for CIS compliance.
- **AWS site-to-site VPN**: Tool for creating secure VPN tunnels.

How does it fit into your scenario's requirements?

These tools help harden servers and protect data, ensuring secure configuration and compliance with security standards. This significantly reduces the risk of data breaches and enhances overall security.

What problem or pain point does it solve?

This ensures servers are securely configured, with data encryption both at rest and in transit, protecting sensitive data from breaches and unauthorized access. It ensures Valhalla Systems' sensitive information is secure and complies with industry standards.

SIEM / Log Aggregation System

Tools:

- **AWS CloudWatch**: Monitors and logs AWS resource activity.

How does it fit into your scenario's requirements?

These SIEM tools aggregate and analyze logs from various sources to detect security incidents in real time. Implementing a SIEM solution enhances Valhalla Systems' ability to detect and respond to security incidents.

Brad Baack
Ethan Pham
Gilbert Collado

What problem or pain point does it solve?

They provide real-time log ingestion and monitoring, allowing for quick identification and response to security threats, ensuring comprehensive security monitoring. This real-time monitoring and analysis provide a robust defense mechanism against potential cyber threats.

Cloud Monitoring

Tools:

- **AWS CloudWatch**: Monitors network traffic and logs.
- **AWS Lambda**: Automates responses to detected threats.

How does it fit into your scenario's requirements?

These tools capture network traffic and automate responses to detected threats, ensuring continuous security oversight. Setting up cloud monitoring allows Valhalla Systems to continuously monitor their network for suspicious activities and respond quickly to threats.

What problem or pain point does it solve?

They enable the detection of suspicious activities and trigger automated responses to mitigate threats, enhancing the overall security of the cloud environment. This proactive approach helps prevent potential breaches and maintains a secure cloud infrastructure.

Novelty

Tools:

- **Amazon Macie:** A fully managed data security and privacy service that uses machine learning to find and protect sensitive data in AWS.

How does it fit into your scenario's requirements?

Introducing Amazon Macie shows we're on top of new security challenges and ready to innovate. Macie's ability to discover and protect sensitive data aligns perfectly with our need for advanced security and compliance solutions. It's a smart way to enhance our security measures and stay ahead of threats.

Brad Baack
Ethan Pham
Gilbert Collado

What problem or pain point does it solve?

Amazon Macie tackles the problem of protecting sensitive data by automating data discovery, classification, and monitoring. It helps us identify and manage critical information like PII in our AWS environment. By adding Macie, we're boosting our data privacy and compliance efforts, showing a proactive stance on data security and advanced threat protection.

Minimum Viable Product (MVP) Definition

MVP Requirements:

- Secure root account and IAM roles/policies with MFA.
- Bastion Host in a public subnet with VPN access
- CIS-compliant Windows Server DC in a private subnet with Sysmon deployed for logging.
- CIS-compliant Linux Data Server
- Data encryption at rest (AWS EBS) and in transit (AWS ACM).
- SIEM solution configured for real-time log ingestion and event triggering.
- Cloud monitoring setup with VPC Flow Logs and AWS Lambda for automated responses.

Stretch Goals:

- Deploy and configure a Linux Data Server with equivalent security measures.
- Implement additional security measures or novel tools not covered in prior labs.