Explanation of Design - Ethan Brock

Executive Summary:
Our cloud architecture design focuses on securing the AWS environment for our client by implementing best practices and utilizing key AWS services. We prioritize Identity and Access Management (IAM), server hardening, data protection, SIEM/log aggregation, and cloud monitoring to ensure comprehensive security measures.

IAM:
For the root account, we will follow IAM best practices to ensure strong authentication, including the use of multi-factor authentication (MFA) and regularly rotating access keys. For team members, IAM will be implemented following AWS best practices such as, assigning least privilege permissions, regularly reviewing and removing unused users, roles, permissions, policies, and credentials, and use conditions in IAM policies to further restrict access

Server Hardening and Data Protection:
A Linux and Windows Server domain controller (DC) will be within a private subnet of a Virtual Private Cloud (VPC). Access to the DC's will be restricted to VPN tunneling, providing an additional layer of security. Data at rest will be encrypted using AWS Key ManagSement Service (KMS) and in transit using SSL/TLS protocols. To generate security-relevant system logs, Sysmon will be deployed on the servers.

CIS-compliant Data Server:
A Linux and Windows server instance will be provisioned to host PII and PCI data. Similar to the Windows Server DC, data at rest and in transit will be encrypted using AWS KMS and SSL/TLS protocols, respectively. We will apply CIS benchmarks to ensure compliance and mitigate security vulnerabilities.

SIEM/Log Aggregation System:
We will set up CloudWatch as the SIEM/log aggregation system. CloudWatch will be configured to ingest event logs in real-time from key assets, including EC2 instances. To fulfill the requirement of demonstrating an attack, we will incorporate a Python script to attempt a Brute Force attack on the Linux server.. The attack will trigger an event that gets ingested by the SIEM solution.

Cloud Monitoring:
We will enable VPC Flow Logs to capture traffic in the AWS Cloud, facilitating the detection of attack Tactics, Techniques, and Procedures (TTPs). Additionally, we will utilize AWS Lambda functions to trigger relevant responses to detected threats, such as executing a shell script. Our cloud monitoring solution will monitor for threat activity in the AWS environment, including monitoring security logs for failed SSH attempts on instances.

Conclusion:
Our cloud architecture design addresses the client's requirements for securing their AWS infrastructure. By implementing IAM best practices, server hardening, data protection, SIEM/log aggregation, and cloud monitoring, we ensure comprehensive security measures.