Final Project Response Form

Evaluate and Design Hybrid Security, IAM, and Compliance Architecture

Instructions

Use this document to record your responses for the Final Project.

- There are 6 questions in this form.
- Type your answers directly under each question.
- Base your responses on the scenario and architecture reference provided in the Final Project Overview.
- Follow the **expected number of items** indicated for each question.
- Focus on clarity, logical reasoning, and professional judgement.
- Your responses should reflect how a security or cloud architect would analyse the environment, propose improvements, and justify design decisions.

When complete, upload this document to **the AI-graded tool** as your final submission.

Question 1: Identify key issues in security operations and Identity and Access Management (IAM) in the HealthSync Global architecture

Hint: *Identify key issues in the current security operations and Identity and Access Management (IAM) approach based on the scenario and current-state architecture. Focus on gaps or weaknesses in the approach rather than listing individual tools or features.* ***The response must consist of five sentences.***

Your response:

1. The primary security operations issue is **limited security visibility**, stemming from monitoring events in isolation across separate environments and lacking a centralized view of critical security activities like authentication and authorization, hindering effective threat detection and incident correlation.

2. In the IAM domain, a major weakness is **identity fragmentation**, caused by separate identity systems for on-premises and cloud platforms, which prevents centralized governance and makes enforcing least-privilege access controls challenging.

3. Another critical IAM issue is the reliance on **long-lived credentials and standing privileges**, specifically using static API keys and service accounts stored insecurely, significantly increasing the blast radius and risk of compromise if credentials are breached.

4. Furthermore, the security operations are hampered by **manual compliance and audit processes**, lacking automation and continuous monitoring, which creates inefficiencies, potential errors, and hinders the ability to demonstrate ongoing compliance effectively.

5. Lastly, the overall approach suffers from **inconsistent security controls**, particularly in encryption and key management practices across environments, leading to operational complexity and security gaps that violate the principle of a unified security posture.

Question 2: Propose architecture-level improvements for IAM and security controls for HealthSync Global

Hint: *Propose architecture-level improvements that address the security and IAM issues identified in the scenario. Focus on high-level design changes rather than detailed implementation steps.* ***The response must consist of five sentences.***

Your response:

1. Implement a **unified Identity and Access Management (IAM) platform** that serves as a single source of truth for identities, enabling centralized governance, consistent access policies, and potentially single sign-on (SSO) across both on-premises and cloud environments to address identity fragmentation.

2. Integrate **Just-In-Time (JIT) access provisioning and privileged access management (PAM)** capabilities into the architecture to replace long-lived credentials and standing privileges, thereby reducing the blast radius and enhancing security posture by limiting access duration and scope.

3. Adopt a **consistent approach to encryption standards and key management** across all environments, potentially leveraging a centralized cloud Key Management Service (KMS) or a hybrid model with clear orchestration, to ensure end-to-end data protection and simplify key lifecycle management.

4. Establish a **centralized Security Operations Center (SOC) and orchestrate security tools** (like SIEM and SOAR) to provide unified visibility, correlation, and automated response across the entire hybrid architecture, improving overall security operations and threat detection capabilities.

5. Embed **automated compliance monitoring and evidence collection** directly into the architecture, utilizing cloud-native compliance frameworks and SIEM integrations to support continuous compliance auditing and reduce reliance on manual, periodic checks.

Question 3: Justify expected outcomes for security posture and operations for HealthSync Global

Hint: *Justify how the proposed improvements strengthen security posture and improve operational effectiveness across the hybrid environment.* ***The response must consist of five sentences.***

Your response:

1. Implementing a unified IAM platform will **strengthen the security posture** by eliminating identity fragmentation, ensuring consistent enforcement of least-privilege access controls, and reducing the risk of privilege creep or unauthorized access across the hybrid environment.

2. The introduction of JIT access and PAM capabilities will **significantly improve operational security** by minimizing the exposure window for compromised credentials and reducing the overall risk and blast radius associated with security incidents, leading to a more resilient system.

3. Adopting consistent encryption and key management practices will **enhance the overall security posture** by ensuring data protection standards are uniformly applied and managed end-to-end, mitigating risks related to inconsistent or poorly managed encryption across on-premises and cloud resources.

4. Establishing a centralized SOC with orchestrated security tools will **improve operational effectiveness** by providing unified visibility, faster threat detection through event correlation, and streamlined incident response across the entire hybrid architecture, leading to quicker remediation times.

5. Embedding automated compliance monitoring will **strengthen the security posture** and **improve operational effectiveness** by ensuring continuous adherence to regulatory requirements, reducing manual effort and potential errors, and providing readily available, accurate compliance evidence, thus lowering audit exposure and risk.

Question 4: Identify key issues in monitoring and compliance in the HealthSync Global architecture

Hint: *Propose architecture-level improvements that enhance monitoring coverage, logging practices, and automated policy enforcement across the hybrid environment.* ***The response must consist of five sentences.***

Your response:

1. A primary issue is **limited security visibility** due to monitoring security events in isolation within each platform, creating blind spots and preventing a comprehensive, unified view of threats and activities across the entire hybrid environment.

2. The architecture suffers from **inadequate logging practices**, characterized by inconsistent log retention policies across different environments, which hinders comprehensive forensic analysis, incident reconstruction, and the ability to meet regulatory requirements for data persistence.

3. There is a significant reliance on **manual compliance and audit processes**, lacking automation and continuous monitoring, which makes it difficult to demonstrate ongoing compliance consistently and efficiently between periodic audits, increasing exposure to non-compliance risks.

4. The current setup lacks effective **centralized correlation and analysis** of security events, meaning threats might be detected slower or missed entirely due to the inability to connect disparate events across on-premises and cloud systems into a meaningful threat picture.

5. Crucially, there is an absence of **automated policy enforcement** mechanisms across the hybrid environment, relying instead on disparate tools and manual reviews, which leads to potential inconsistencies, operational inefficiency, and slower response times when configurations deviate from security baselines.

Question 5: Propose improvements for monitoring, logging, and policy-as-code for the HealthSync Global architecture

Hint: *Propose architecture-level improvements that enhance monitoring coverage, logging practices, and automated policy enforcement across the hybrid environment.* ***The response must consist of five sentences.***

Your response:

1. Implement a **centralized Security Information and Event Management (SIEM) system** integrated across both on-premises and cloud environments to unify monitoring coverage, providing a single pane of glass for security event collection, correlation, and analysis, thereby enhancing visibility and threat detection capabilities.

2. Establish a **standardized, automated logging framework** enforced across all components within the hybrid environment, ensuring consistent log formats, collection, and retention policies that meet regulatory requirements and enable comprehensive forensic analysis and compliance reporting.

3. Adopt **policy-as-code methodologies** using Infrastructure as Code (IaC) tools and configuration management systems, allowing security policies and compliance rules to be defined, versioned, and automatically enforced across the entire hybrid infrastructure during deployment and runtime.

4. Integrate **automated alerting and incident response workflows** linked to the SIEM and policy enforcement mechanisms, enabling faster detection of anomalies and security events and facilitating quicker, more consistent responses across the hybrid environment.

5. Leverage **Cloud-native monitoring services and automated compliance tools** (where applicable) within both on-premises and cloud platforms, integrating them into the centralized framework, to enhance monitoring granularity, simplify log management, and strengthen automated policy enforcement and compliance monitoring.

Question 6: Justify expected outcomes for visibility and compliance readiness

Hint: *Justify how the proposed improvements enhance operational visibility and support compliance and audit readiness.* ***The response must consist of five sentences.***

Your response:

1. Implementing a centralized SIEM and unified logging framework will **significantly enhance operational visibility** by providing a comprehensive, real-time view of security events, authentication attempts, and configuration changes across the entire hybrid environment, eliminating previous blind spots.

2. The adoption of standardized logging practices and automated collection ensures that **compliance readiness is improved** through consistent, readily available, and persistent log data that meets regulatory requirements, making audit evidence gathering more efficient and reliable.

3. Policy-as-code and automated enforcement mechanisms will **strengthen operational visibility** by providing immediate feedback on policy compliance status and configuration drift across the hybrid infrastructure, allowing for proactive identification and remediation of potential issues.

4. Automated alerting and response workflows linked to monitoring and policy enforcement will **improve visibility into security incidents** by providing faster detection and clearer context, enabling quicker investigation and response, which in turn supports audit readiness by demonstrating effective security monitoring and operational control.

5. Integrating cloud-native monitoring and compliance tools, along with leveraging SIEM for correlation, **enhances overall visibility** and **strengthens compliance readiness** by providing granular insights, standardized reporting, and automated checks that support continuous compliance monitoring and evidence generation, reducing the burden of manual audits and improving security posture.