Cover Page

- **Team Name:** Cyber Shawties (SIEM-KMS-1)
- **Project Title:** Aegis Health Security: A Cloud-Native SIEM-as-a-Service for Specialized Healthcare Data Protection
- **Team Members:**
  - Timorra Rogo: Technical Lead, UI/UX Developer
  - Tanvin Farjana: Technical Lead
  - Kayla Hewlett: Project Manager, KMS Team Lead, AI Developer
  - Marshae Bryant: Project Manager, KMS Team
  - Nadia Haji Abukar: Documentation Lead, KMS Team
  - Edona Mema: Documentation Lead, SIEM Team
- **Course:** Phase 3 Capstone Project
- **Date:** September 29, 2025

1. Project Charter & MVP Scope

This project establishes the vision, scope, and direction for a new Managed Security Service Provider (MSSP) specializing in healthcare data protection.

- **Problem Statement**: The SIEM market is dominated by high-cost commercial vendors like Splunk, whose pricing models create unpredictable costs for customers. Furthermore, existing healthcare-focused MSSPs offer generic security solutions that fail to address the unique privacy requirements, political sensitivities, and legal risks associated with women's reproductive health and mental health data. This leaves a critical market gap for specialized, high-assurance, and cost-effective security services.
- **Purpose & Goals**: Our purpose is to build and commercialize a cloud-native SIEM-as-a-Service on a license-free, open-source technology stack (Wazuh and Amazon OpenSearch). This strategic decision shifts the business model from reselling expensive software to monetizing in-house operational expertise. The primary goal is to provide enterprise-grade, affordable security services tailored to the specific needs of reproductive and mental health providers, leveraging the cryptographic superiority of AWS KMS with FIPS 140-3 validated HSMs.
- **Desired Outcomes & Success Metrics**:
  - **Security Metrics**: Achieve a Mean Time to Detect (MTTD) of minutes for critical alerts, a Mean Time to Respond (MTTR) of hour for P1 incidents, 100% encryption coverage for sensitive data, and a 100% compliance audit success rate.
  - **Business Metrics**: Target a Customer Acquisition Cost (CAC) under $7,200 for the Advanced tier, achieve 20% quarterly MRR growth, maintain a monthly churn rate under 2%, and realize 120%+ net revenue retention.
  - **Service Levels**: Maintain 99.9% monthly platform uptime and achieve a Customer Satisfaction (NPS) score above 70.
- **MVP Scope (Sprint 6 Demo)**: The Minimum Viable Product will be a demonstration of our **"Advanced Tier - Comprehensive Care Protection"** service.

    - **Features**: We will demonstrate end-to-end monitoring of a simulated mid-size telehealth platform, including log ingestion, threat detection with Wazuh, data analysis in OpenSearch Dashboards, and dual-domain data encryption using AWS KMS.
    - **Acceptance Criteria**: The demo must successfully:
        1. Ingest and normalize logs from simulated endpoints and cloud services.
        2. Trigger a P1 alert based on a simulated threat (e.g., unauthorized data access).
        3. Show the encrypted patient data at rest, protected by KMS.
        4. Display relevant security events on a role-specific dashboard.
- **Out-of-Scope (For Now)**: Features from the **"Sovereign Tier"** are intentionally deferred. This includes the patient-facing transparency portal, geo-fenced encryption capabilities, and custom AI-driven risk modeling.

2. Research & Market Analysis

- **Landscape**: The modern Security Information and Event Management (SIEM) paradigm has evolved from simple log aggregation into a sophisticated, intelligence-driven pipeline. This pipeline is defined by seven pillars: Data Aggregation, Normalization & Enrichment, Storage, Correlation & Analysis, Threat Detection, Alerting, and Incident Response. The industry has also shifted decisively toward cloud-native solutions. Legacy, on-premises SIEMs are architecturally unsuited for the cloud, as they are difficult to scale, follow an inefficient CapEx cost model, and struggle to integrate with modern, API-driven data sources. This makes cloud-native architecture a foundational requirement for any modern MSSP.
- **Comparators (2-3)**:
    1. **Commercial SIEM Vendors (e.g., Splunk, Exabeam)**: These platforms offer polished user experiences and extensive support but come with high recurring licensing fees based on data volume, which is a primary concern for customers. Our open-source model eliminates these fees entirely.
    2. **Fortified Health Security**: A leading healthcare MSSP recognized as "Best in KLAS". While strong in general healthcare security, they lack a specialized focus on the nuanced privacy risks of reproductive or mental health data and do not offer patient-facing transparency features.
    3. **IBM Managed Security Services**: A global leader with powerful AI capabilities. However, their high cost and generic enterprise approach are not tailored to the specific compliance or political risk challenges faced by our target market.
- **Differentiation**: Our service stands out through a unique combination of technology, market focus, and business strategy.
    - **Business Model Innovation**: By building on the license-free Wazuh and OpenSearch stack, we reframe the value proposition: clients pay for our operational expertise in managing a complex, powerful security platform, not for expensive software licenses. This allows for highly competitive pricing.
    - **Domain-Specific Specialization**: Unlike competitors offering a generic "healthcare"

solution, we are laser-focused on the unmet needs of the women's reproductive health and mental health sectors. This includes managing the complex political and state-level legal risks that other providers ignore.
    - **Superior Security Foundation**: We utilize AWS KMS, which is built on FIPS 140-3 Level 3 validated Hardware Security Modules (HSMs). This provides a hardware-enforced root of trust, ensuring master keys never leave the secure HSM boundary—a level of cryptographic assurance that exceeds standard compliance requirements and differentiates our technical architecture.
- **Citations**:
    1. Blueprint for a Cloud-Native MSSP. (2025). Course Capstone Document.
    2. Exabeam. (2023). Legacy vs. cloud-native SIEM: Weighing the pros and cons.
    3. TechTarget. (2024). Splunk pricing concerns grow as customers face cost increases.

3. Team Roles & Responsibilities (+ RACI)

Clear roles and responsibilities are assigned to ensure accountability and effective project execution.

- **Technical Leads**: Tanvin Farjana, Timorra Rogo
- **Project Managers**: Kayla Hewlett, Marshae Bryant
- **KMS Team**: Kayla Hewlett, Marshae Bryant, Nadia Haji Abukar
- **SIEM Team**: Timorra Rogo, Edona Mema, Tanvin Farjana
- **Developers**: Kayla Hewlett (AI), Timorra Rogo (UI/UX)
- **Documentation Team**: Nadia Haji Abukar, Edona Mema

RACI Chart

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

Task / Deliverable	Project Manager	Technical Lead	KMS Team	SIEM Team	Documentation Team
Project Charter & MVP	A	C	C	C	R
Market Research	R	C	R	R	C
Sprint Plan & Board Setup	A	R	I	I	I

Initial Topology Diagram	C	A	R	R	I
KMS Architecture	C	R	A	C	R
SIEM Configuration	C	R	C	A	R
MVP Demo	A	R	R	R	C

4. Workflow & Sprint Schedule (Sprints 1-6)

This plan outlines the deliverables, milestones, and owners for each sprint, culminating in the MVP demo in Sprint 6.

Sprint	**Dates (MM/DD)**	**Goals / Deliverables**	**Key Milestones**	**Owner(s)**	**Definition of Done**
1	09/15-09/29	Charter, Research, Roles/RACI, Plan, Tools, Initial Topology	Sprint 1 Assignment Submitted	All	All sections of this document are complete & consistent.
2	10/01-10/14	Core Platform Engineering & Data Pipeline	AWS environment built (IaC), Wazuh/OpenSearch deployed.	Tech Lead, SIEM Team	Basic log ingestion from a test EC2 instance is functional.
3	10/15-10/28	Multi-Tenant Architecture & KMS	KMS key hierarchy implemented; tenant	KMS Team, Tech Lead	Data keys can be generated and used

		Integration	data segregation tested.		for encryption via API.
4	10/29-11/11	Intelligence-Driven Detection	Custom detection rules written; MITRE ATT&CK mapping complete.	SIEM Team	Alerts are successfully generated for simulated attacks.
5	11/12-11/25	Automated Response & Service Definition	Lambda functions for automated containment created; Dashboards built.	Devs, SIEM Team	A P1 alert automatically isolates the source EC2 instance.
6	11/26-12/09	Commercialization & MVP Demo	Final presentation polished; MVP demo script finalized.	Demo Ready	Project Managers

5. Tools & Services List

The following AWS services and external tools have been chosen to support the MVP.

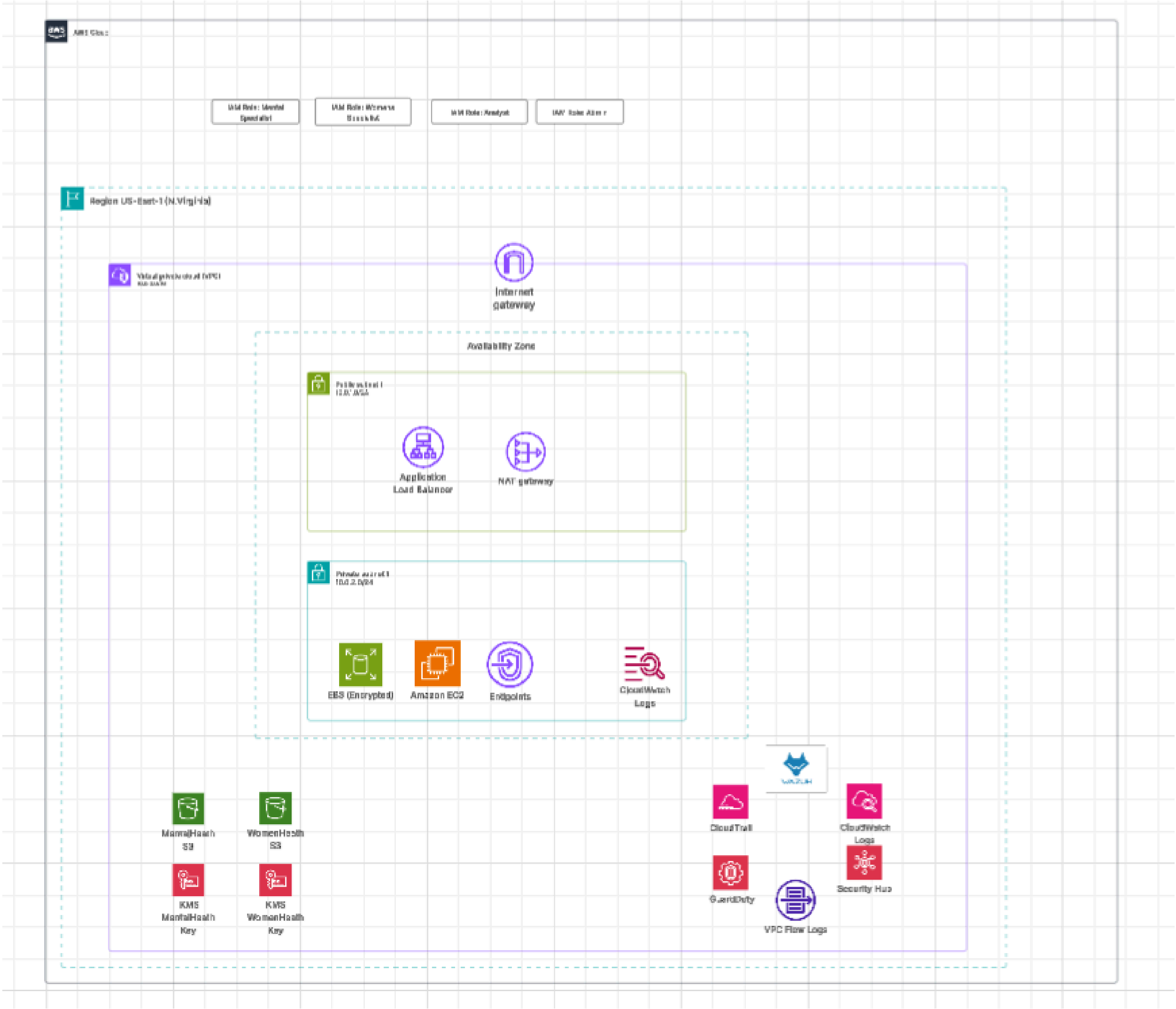
Category	**Service / Tool**	**Why Chosen**	**How We Will Use It**	**Owner**
AWS	**VPC, IAM, EC2**	Core infrastructure for networking, identity, and compute.	To create a secure, isolated network for the SIEM	Technical Lead

			platform and manage all permissions.	
	Amazon OpenSearch	A scalable, open-source analytics and search engine.	The core data store and analytics engine for SIEM logs, providing visualization via Dashboards.	SIEM Team
	AWS KMS	FIPS 140-3 validated HSMs provide a high-assurance root of trust.	To manage the entire lifecycle of cryptographic keys and perform envelope encryption on sensitive patient data.	KMS Team
	S3, CloudTrail, GuardDuty	Foundational services for storage, audit logging, and threat detection.	S3 for immutable log storage; CloudTrail and GuardDuty logs will be primary data sources for the SIEM.	SIEM Team
External	**Wazuh**	A license-free, unified SIEM and XDR platform.	To collect, analyze, and correlate log data, perform vulnerability detection, and enable active	SIEM Team

			response.	
	GitHub	Industry standard for version control and collaborative development.	To host all Infrastructure as Code (IaC) scripts, application code, and documentation.	Technical Lead
	Jira / Trello	Project management tools for agile workflows.	To manage the sprint backlog, track tasks, and monitor project progress.	Project Manager

6. Initial Topology Diagram (High-Level)

The conceptual architecture below illustrates the major services and data flows for the platform within the AWS us-east-1 region.



Architectural Overview

The architecture is designed within a single VPC. External traffic enters through an **Internet Gateway** and is routed to an **Application Load Balancer (ALB)** in a public subnet. The ALB distributes requests to the core application fleet (e.g., Wazuh Manager) running on **EC2 instances** within a private subnet to protect them from direct internet exposure.

A **NAT Gateway** allows outbound internet access for services in the private subnet for tasks like software updates. The architecture leverages **VPC Endpoints** for secure, private communication with other AWS services like S3 and KMS, ensuring traffic does not traverse the public internet.

Data protection is enforced using **AWS KMS**, with separate keys defined for different sensitive data categories like "MentalHealth" and "WomensHealth" to ensure cryptographic separation.

Logging and monitoring are comprehensive: **CloudTrail** (API calls), **VPC Flow Logs** (network traffic), and **GuardDuty** (threat detection) feed into **CloudWatch Logs** and **AWS Security Hub**, providing centralized data sources for the SIEM to analyze.