Prohori

This project, the **Digital Resilience Suite for Smart Bangladesh**, is a sophisticated, all-in-one "Security-as-a-Service" (SECaaS) platform. It is designed specifically for small-to-medium enterprises (SMEs) in Bangladesh that lack the budget for a full-time cybersecurity team but must comply with local laws like the **Cyber Security Act (CSA) 2023**.

Core Features

To make this monetizable and effective, the suite must provide both protection and business management tools:

- **Unified Security Dashboard:** A single view showing real-time threats, server health, and employee access logs.
- **AI-Driven Risk Assessment:** Uses Large Language Models (LLMs) to scan a business's infrastructure and explain vulnerabilities in plain Bangla or English.
- **Localized Compliance Engine:** Automatically generates reports required by the Digital Health Strategy 2027 or Bangladesh Bank regulations.
- **Vulnerability Disclosure Program (VDP):** A mini "Bug Bounty" section where companies can safely allow ethical hackers to report bugs in exchange for rewards.
- **Integrated Payment Gateway:** Automated subscription billing using **bKash, Nagad, or Rocket** APIs for the local market.
- **HRM & Access Control:** Manages who (employees) can access which data, merging security with basic human resource management.

How It Works as a Website

The platform functions as a **SaaS (Software as a Service)** web application. Here is the workflow:

1. **Onboarding:** A business owner signs up and connects their website or local server to your suite using an **agent** (a small piece of code or a script).

2. **Monitoring:** Your backend, hosted on **Oracle Cloud Infrastructure (OCI)**, uses **Wazuh** to watch for suspicious activity (like brute-force attacks).
3. **Processing:** If an attack is detected, the **AI layer (Groq/Gemini)** analyzes the log and sends an alert to the owner's WhatsApp or Email with a "How to Fix" guide.
4. **Compliance:** At the end of the month, the owner clicks a button to download a PDF report that proves they are following Bangladesh's cybersecurity laws.

Elaborate Key Terms

1. Azure for Students (The Student Gold Mine)

Microsoft's dedicated student tier offers a strong foundation for your "Zero-Cost Build". It provides immediate credits and a suite of "Always Free" services that never expire as long as you maintain your student status.

- $100 Credit: You receive an initial $100 credit to use on any Azure service within the first 12 months.
- Virtual Machines (Compute):
    - 750 hours per month of B1s (Intel-based) burstable VMs.
    - 750 hours per month of B2pts v2 (ARM-based) burstable VMs.
    - This is sufficient to run your Wazuh manager and central security engine.
- Storage:
    - Includes free amounts of standard managed disks and 5 GB of LRS Block Blob storage.
    - Perfect for storing and rotating your security logs.
- Database:
    - Azure SQL Database: 100,000 vCore seconds and 32 GB of storage per month.
    - Azure Database for MySQL: 750 hours of a burstable B1MS instance.
    - This provides a robust home for your compliance data and VDP marketplace logs.

2. Wazuh / Security Onion

These are open-source **SIEM (Security Information and Event Management)** tools. They act as the "eyes" of your project, collecting logs from the client's system to detect hackers, malware, and file changes.

3. Groq / Gemini (AI Reasoning Layer)

- **Gemini:** Used for complex analysis and generating natural language reports.

- **Groq:** A hardware-accelerated platform that makes LLMs run extremely fast. You use this to provide **instant** answers when a user asks the dashboard, "Why is my site slow today?"

4. CSA 2023 (Cyber Security Act)

The primary law in Bangladesh governing digital safety. Your project wins by automating the paperwork (compliance) that this law demands from businesses.

5. Bug Bounty Marketplace

Instead of a company hiring one expensive consultant, they "crowdsource" their security. You provide the platform where researchers find bugs, and the company pays a small fee to the researcher and a commission to you.

Implementation Path

As a 3rd-year CSE student with experience in **Next.js, Supabase, and Linux**, you are perfectly positioned to build this:

- **Frontend:** Use **Next.js** and **Tailwind CSS** for the dashboard. It needs to be clean and "executive-friendly."
- **Backend/Database: Supabase** (PostgreSQL) to manage users, subscriptions, and alert history.
- **Security Core:** Set up a **Debian** VPS on OCI. Install **Wazuh** to act as your central manager.
- **Automation:** Use **Python** scripts to bridge the gap between Wazuh alerts and the Gemini API to turn technical jargon into easy-to-read business advice.

1. Cloud Infrastructure (The Foundation)

Microsoft Azure — Student Subscription Unlike other providers that require payment info upfront, Azure for Students allows you to deploy enterprise-grade infrastructure using only your .edu email.

- Compute: You can deploy a Linux VM (specifically a B1s or B2pts v2 instance) to serve as your central Prohori server. While it has less RAM than OCI's ARM instances, it is highly reliable for a student MVP.
- Networking: Every Azure account includes a free dynamic virtual IP (VIP), allowing your Wazuh agents on client sites to communicate back to your dashboard.
- AI Integration: Beyond your $100 credit, you have access to always-free tiers for Azure AI Translator (2 million characters) and AI Search. These can supplement your Gemini/Groq "Reasoning Layer" for translating logs into Bangla.

---

2. Security Monitoring (The Core)

Wazuh (Open Source Edition)

Wazuh is the "engine" of your security portal. It is 100% free and has no "community edition" locks.

- **Capabilities:** Log analysis, file integrity monitoring (FIM), malware detection, and vulnerability scanning.
- **Installation:** You can install the **Wazuh Indexer, Server, and Dashboard** all on one of your OCI ARM instances using their single-line "assisted installation" script.
- **Agent:** The Wazuh Agent is lightweight and can be installed on your client's Debian or Windows servers.

---

3. AI & Logic (The Reasoning Layer)

GroqCloud & Gemini API

Use these for the "AI Security Analyst" features that explain threats to non-technical business owners.

- **Groq API (Free Tier):** Best for **speed**. It offers free access to models like Llama 3.3 (70B) with limits around 30 Requests Per Minute (RPM). Use this for real-time chat assistance on your dashboard.
- **Gemini 2.5 Flash (Free Tier):** Best for **large data**. It offers a **1 million token context window**. You can feed an entire security log file into Gemini to generate a summarized "Human-Readable Audit Report" in Bangla.
    - *Limit:* ~10-15 RPM and 1,500 requests per day (plenty for an MVP).

---

4. Web Development & Backend

Next.js + Supabase

Since you are a 3rd-year student building a "SaaS" (Software as a Service), this combo handles your user accounts and dashboard.

- **Supabase (Free Tier):**
    - **Database:** 500MB PostgreSQL (enough for thousands of security alerts).
    - **Auth:** 50,000 Monthly Active Users (more than enough for your initial clients).
    - **Edge Functions:** 500,000 invocations (use these to trigger alerts to WhatsApp/Email).
- **Vercel:** Free hosting for your Next.js frontend with automated SSL.

---

5. Payments & Compliance

Local Integration & Reporting

- **bKash/Nagad Sandbox:** You don't need a trade license to *start* building. You can use the **bKash Tokenized Checkout Sandbox** (v1.2.0-beta) to simulate payments. You'll use "test" wallet numbers to verify that your subscription logic works.
- **LaTeX (For Compliance):** Use your LaTeX skills to create a backend service that takes security data and generates a "Certificate of Compliance" PDF. A well-formatted LaTeX PDF looks much more professional to a business owner than a basic HTML printout.

Summary Table of Resources

Component	**Tool**	**Why it's Free**
Server Host	Oracle Cloud (OCI)	"Always Free" ARM Instances (24GB RAM)
SIEM / XDR	Wazuh	100% Open Source (GPL v2)
AI Insights	Groq / Gemini	Free API Tiers (No credit card for basic use)
Database/Auth	Supabase	Free up to 50k users / 500MB DB
Payment Test	bKash Sandbox	Free developer credentials for testing

Feature 1: The Unified Security Dashboard (SIEM Integration)

This is the "Control Room" where the user (SME owner) sees everything.

- **How to use:** The user logs in and sees a "Health Status" (Green/Yellow/Red). They can see a list of recent blocked attacks (e.g., "5 Brute-force attempts blocked from Russia").
- **Service/Output:** Real-time visibility into server security and automated alerts.
- **Tech Implementation:**
    1. **Wazuh:** Install the Wazuh Manager on an **OCI Debian instance**.
    2. **Dashboard:** Build the UI with **Next.js**. Fetch data from the Wazuh API using a Secure Middleware.
- **Process:**
    1. Install Wazuh on OCI.
    2. Install the "Wazuh Agent" on the client's website server.
    3. Use Next.js to call the Wazuh `GET /alerts` API and display them in a clean **Tailwind CSS** table.

Feature 2: AI Security Analyst (Reasoning Layer)

This turns scary technical logs into simple Bangla/English advice.

- **How to use:** The user clicks a "Ask AI" button next to a security alert. The AI explains: "Someone tried to guess your password. I have blocked them. You should enable 2-Factor Authentication."
- **Service/Output:** Instant, non-technical explanations and "Next Steps" for the business owner.
- **Tech Implementation:**
    1. **Groq API:** Use the **Llama 3** model for high-speed reasoning.
    2. **Prompt Engineering:** Send the raw Wazuh log to Groq with a system prompt: *"You are a helpful security assistant for a Bangladeshi shop owner. Explain this log in simple terms."*
- **Process:**
    1. Set up a **Supabase Edge Function**.
    2. When a user clicks "Ask AI," the function sends the log to Groq.
    3. Display the text response in a chat bubble on your website.

Feature 3: Localized Compliance Engine (CSA 2023)

Automatically generates reports that Bangladeshi law requires.

- **How to use:** The user goes to the "Compliance" tab and clicks "Generate Monthly Audit."
- **Service/Output:** A professional **PDF report** showing that the business is following the Cyber Security Act 2023.
- **Tech Implementation:**
    1. **LaTeX:** Create a standard template for a security audit.
    2. **Node.js / Python:** Use a library (like `node-latex`) to fill the template with data from your database.
- **Process:**
    1. Draft a LaTeX template with placeholders like `{{company_name}}` and `{{threats_blocked}}`.
    2. Run a script that injects the month's data into the LaTeX file.
    3. Generate the PDF and provide a download link in the dashboard.

Feature 4: SME Bug Bounty Marketplace

A safe place for ethical hackers to report bugs to local companies.

- **How to use:** * **Company:** Sets a budget (e.g., 2,000 BDT for a "Critical" bug).
    1. **Hacker:** Submits a report through a form.

- **Service/Output:** Vulnerability discovery before real hackers find them.
- **Tech Implementation:**
    1. **Database:** Use **Supabase** to store submissions, status (Open/Fixed/Paid), and user roles (Company vs. Researcher).
- **Process:**
    1. Create a "Report a Bug" form in Next.js.
    2. Use **Supabase Row Level Security (RLS)** so only the company can see reports meant for them.

Feature 5: Localized Billing (bKash/Nagad Integration)

Automates the "Security-as-a-Subscription" revenue.

- **How to use:** The user chooses a plan (Basic/Pro) and pays via their mobile wallet.
- **Service/Output:** Seamless subscription management without needing a credit card.
- **Tech Implementation:**
    1. **bKash Sandbox:** Use the bKash v1.2.0 API.
- **Process:**
    1. Create a "Checkout" page.
    2. When the user clicks "Pay," call the bKash `createPayment` API.
    3. On success, update the user's `is_pro` status in Supabase.

3. How The Project is Unique

Based on the current 2026 market research, your project **Prohori** stands out because:

Feature	**Competitor Status**	**Your Innovation**
CSA 2023 Reporting	Almost zero automated tools.	**Automated LaTeX generation** for local law.

AI Reasoning	Exists in high-end Enterprise tools.	**Groq/Gemini** making it affordable for local shops.
Payment	Require USD/Credit Cards.	**bKash/Nagad integration** for local SMEs.
Bug Bounty	Only for huge corporations.	**Shared Marketplace** for even the smallest businesses.

Part 1: The User Journey (How an Organization Uses Prohori)

Let's walk through the lifecycle of a typical user, "Mr. Rahim," who owns a small e-commerce store.

Phase 1: Onboarding & Setup

1. Sign-Up: Mr. Rahim visits the Prohori website and signs up using his email. He selects a plan (e.g., "Basic" or "Pro") on the pricing page.
2. Payment: He clicks "Pay with bKash." The system redirects him to a bKash payment page (or generates a payment token). He pays the subscription fee using his bKash app.
3. Agent Installation: Upon successful payment, his Prohori dashboard unlocks. The first thing he sees is a simple, step-by-step wizard:
    - "Step 1: Copy this one-line command."
    - "Step 2: Log in to your company's server (via SSH) and paste the command. Press Enter."
    - "Step 3: Wait 2 minutes and refresh this page."
4. Connection: Mr. Rahim follows the steps. This command installs the Wazuh Agent on his server, which immediately establishes a secure connection back to Prohori's central server. His dashboard status changes from "Agent Not Installed" to "Connected & Monitoring."

Phase 2: Daily/Weekly Monitoring (The Dashboard)

1. Login: Mr. Rahim logs into his Prohori dashboard. He is not a tech expert, so the UI is clean and graphical.
2. Unified View: He sees his Unified Security Dashboard:
    - Health Status: A big green checkmark (or yellow/red if there are issues).
    - Live Threat Feed: A scrolling list showing events like: "Blocked a login attempt from unusual location (Italy)" or "File 'wp-config.php' was verified as safe."
    - Server Health: CPU and RAM usage graphs for his server.

Phase 3: Incident Handling (The AI Interaction)

1. The Alert: One morning, he receives a WhatsApp message: "⚠️ *Security Alert: Unusual activity detected on your server.* "
2. Investigation: He opens the Prohori app on his phone. He sees an alert: "Multiple failed login attempts for 'admin' user."

3. AI Assistance: Confused, he clicks the "Ask AI" button next to the alert.
4. AI Analysis: A chat bubble opens. The AI (powered by Groq) explains: *"Someone tried to guess your admin password 50 times in the last hour. This is a 'Brute Force Attack'. Prohori has temporarily blocked the IP address. To make this stop permanently, I recommend: 1) Disabling the 'admin' username and 2) Enabling Two-Factor Authentication (2FA). Would you like me to generate a step-by-step guide for your server type (Ubuntu)?"*
5. Resolution: Mr. Rahim clicks "Yes, send guide." He follows the simple instructions and resolves the issue.

Phase 4: Compliance & Reporting (The "Worth" of the Product)

1. End of Month: It's the last day of the month. Mr. Rahim needs to submit a cybersecurity compliance report to his bank (as per Bangladesh Bank regulations).
2. One-Click Report: He goes to the "Compliance" tab in his Prohuri dashboard.
3. Report Generation: He selects the month, clicks "Generate CSA 2023 Audit Report."
4. Output: The system processes the last 30 days of security logs. A few seconds later, a beautifully formatted PDF is ready for download. The report includes:
    - Company Name & Date.
    - Summary of security events (e.g., "Total threats blocked: 132").
    - Uptime monitoring statistics.
    - A formal "Certificate of Compliance" stating they have an active monitoring and vulnerability management system in place.
5. Submission: He emails this PDF to his bank, satisfying their compliance requirement.

Phase 5: Bug Bounty (Optional "Pro" Feature)

1. The Program: As a Pro user, Mr. Rahim wants to be extra safe. He goes to the "Bug Bounty" section.
2. Configuration: He creates a new program: "Looking for bugs in our e-commerce site. Will pay 1,500 BDT for critical bugs." He sets the scope to `https://hisstore.com`.
3. Researcher Submission: A security researcher (hacker) finds a minor bug and submits a report through the Prohori form, including steps to reproduce.
4. Review & Reward: Mr. Rahim gets a notification. He views the report in his dashboard, confirms the bug, and clicks "Accept & Pay." Prohori processes the

payment of 1,500 BDT to the researcher's bKash account, and Prohori takes a small commission.

Part 2: The System Architecture (How It Works)

Here is the technical breakdown of how the frontend, backend, and security engine interact.

High-Level Architecture Diagram (Conceptual)

```
text
[User's Browser] <--> [Vercel (Frontend - Next.js)]
                              |
                              | (HTTPS - API Calls)
                              ↓
                      [Supabase (Backend)]
                      - PostgreSQL DB
                      - Auth (User Mgmt)
                      - Edge Functions
                              ↑
                              | (Triggers & Data Fetch)
                              |
[Client's Server] <----> [Oracle Cloud / Azure (Core Engine)]
- Wazuh Agent            - Wazuh Manager (SIEM)
                         - Python Automation Scripts
                         - AI API Integrations (Groq/Gemini)

                         - PDF Generator (LaTeX)
```

Detailed Component Breakdown

Layer	Technology	Role & How it Works

1. Presentation (Frontend)	Next.js (Hosted on Vercel)	Role: The user interface. How it works: 1. A user logs in, and Next.js calls the Supabase Auth API. 2. It fetches security alerts and server status by calling secure API Routes (also in Next.js). 3. These API routes act as a middleman, forwarding requests to the Wazuh API (on the core engine) or the Supabase database. 4. It uses Tailwind CSS to make the dashboard "executive-friendly."

2. Data & Auth (Backend)	Supabase	Role: The brain for business logic and user data. How it works: 1. Auth: Manages user sign-up, login, and session tokens. 2. Database (PostgreSQL): Stores all non-security data: - `users`: profile info, subscription status (`is_pro`). - `companies`: links users to their company. - `alert_history`: summaries of major alerts pulled from Wazuh for quick dashboard viewing. - `bug_bounty_submissions`: stores reports from researchers. 3. Row Level Security (RLS): Ensures Company A can NEVER see Company B's data.

	4. Edge Functions: Serverless TypeScript/Python functions. Used for: - Triggering WhatsApp/Email alerts when a critical Wazuh alert comes in. - Calling the Groq API when a user clicks "Ask AI."

3. Security Core (The Engine)	Oracle Cloud (OCI) / Azure VM	Role: The heavy lifter for security monitoring. How it works: 1. Wazuh Manager: This is the heart. It listens for connections from all the Wazuh Agents installed on client servers. It receives, analyzes, and indexes security logs. 2. Wazuh Indexer: Stores all the raw security logs for later search and analysis. 3. Automation Scripts (Python): Custom scripts that: - Poll the Wazuh API for new "high severity" alerts. - When an alert is found, they send a webhook to a Supabase Edge Function to notify the user. - Periodically feed summary logs to Gemini for generating monthly compliance reports.

4. AI & Logic Layer	GroqCloud & Google Gemini	Role: Making security understandable. How it works: 1. Groq (for real-time): When a user asks "Ask AI" about a specific alert, a Supabase Edge Function sends the raw log to Groq (Llama 3) with a system prompt. Groq returns a simple, human-friendly explanation almost instantly. 2. Gemini (for batch jobs): Once a month, a Python script on the Core Engine gathers all security logs for a company and sends them (in chunks) to Gemini 2.5 Flash. The prompt: *"Summarize these security logs for a business owner. Create a compliance report highlighting the number of attacks blocked, system health, and recommendations."* The

		output is then sent to the PDF generator.
5. Integration Layer	bKash API, WhatsApp/Email	Role: Connecting to the real world. How it works: 1. bKash/Nagad: The Next.js checkout page uses the bKash API to create a payment session. On successful payment, bKash redirects the user back to Prohori, and a Supabase Edge Function updates the user's `subscription_status` in the database. 2. Notifications: Supabase Edge Functions use a service like Twilio (for WhatsApp) or Resend (for Email) to send alerts to users when triggered by a critical security event from the Wazuh system.

Part 3: Detailed Process Flows

Let's visualize two critical processes.

Process Flow 1: User Asks AI About an Alert

1. User Action: Clicks "Ask AI" next to an alert on the Next.js dashboard.
2. Frontend Request: The Next.js frontend sends a `POST` request to its own internal API route, e.g., `/api/explain-alert`, with the `alert_id`.
3. Backend API Route: The Next.js API route receives the request. It first verifies the user's session (using Supabase Auth) to ensure they own this alert.
4. Fetch Log: The API route fetches the full raw log for that `alert_id` from the Wazuh API running on the Core Engine.
5. Call AI: The API route then calls a Supabase Edge Function (to keep the main serverless function light), sending the raw log text.
6. AI Processing: The Supabase Edge Function takes the raw log, constructs a prompt (e.g., `System: You are a friendly assistant... User: Explain this log: [RAW LOG]`), and sends it to the Groq API.
7. Response: Groq returns the plain-language explanation.
8. Return to User: The explanation is sent back down the chain: Edge Function -> Next.js API Route -> Next.js Frontend -> displayed to the user in a chat bubble.

Process Flow 2: Automated Monthly Compliance Report Generation

1. Trigger: A scheduled job (e.g., a cron job on the Core Engine VM or a Supabase DB scheduled function) runs on the 1st of every month.
2. Data Gathering: A Python script on the Core Engine queries the Wazuh Indexer for all security events from the previous month for a specific company.
3. AI Summarization: The script sends this large batch of log data to the Gemini API with a prompt: "Create a concise executive summary of these logs for a compliance report. Include total threats, top 3 types of attacks, and general server health."
4. Data Injection: The script takes the AI summary and combines it with company details (name, subscription ID) from the Supabase database.
5. PDF Generation: It then fills a pre-designed LaTeX template with this data (e.g., `\newcommand{\companyName}{{{company_name}}}`) and runs the `pdflatex` command to generate a polished PDF.
6. Storage & Notification: The PDF is saved to cloud storage (e.g., Azure Blob Storage or Supabase Storage), and a link is saved in the `compliance_reports` table in the Supabase database for that user.

7. User Retrieval: The user logs in and clicks "Download Report." The Next.js dashboard fetches the signed URL from Supabase and serves the PDF to the user.

1. User Experience: How the Organization Uses Prohori

The user (typically an SME business owner with limited technical knowledge) interacts with Prohori as a "Security-as-a-Service" (SECaaS) web platform. The user journey follows this flow:

• **Step 1: Onboarding & Installation** The business owner signs up on the website. To start protection, they install a lightweight **Wazuh Agent** (a small script) on their company's server or computers,.

• **Step 2: Monitoring via Dashboard** Once logged in, the user sees a **Unified Security Dashboard**. This acts as a "Control Room" displaying a simple health status (Green/Yellow/Red) and a list of blocked threats (e.g., "5 Brute-force attempts blocked"),.

• **Step 3: AI Consultation ("Ask AI")** When the user sees a complex technical alert (e.g., "Port 22 unauthorized access"), they click an **"Ask AI"** button. The system instantly translates the technical log into plain Bangla or English, explaining what happened and advising on next steps (e.g., "Enable 2-Factor Authentication").

• **Step 4: Compliance Reporting** At the end of the month, the user navigates to the "Compliance" tab. With one click, they generate and download a **PDF report**. This document is formatted via LaTeX to look professional and proves the business is complying with the **Cyber Security Act (CSA) 2023**,.

• **Step 5: Managing Vulnerabilities** The user can view a "Bug Bounty" section where ethical hackers submit reports about security holes. The user can view these reports and pay a reward to the researcher through the platform.

• **Step 6: Subscription Payment** The user pays for the service using local mobile wallets like **bKash or Nagad**, making the transaction seamless without needing a credit card.

---

2. System Architecture: How the System Works

The system operates on a hybrid cloud model, leveraging "Zero-Cost" resources to remain sustainable.

• **The "Eyes" (Security Core):** The system uses **Wazuh**, an open-source SIEM tool hosted on **Oracle Cloud Infrastructure (OCI)**. It collects logs from the user's devices to detect malware, file changes, and attacks,.

• **The "Brain" (AI Layer):** When threats are detected, the system uses **Groq** (for speed) and **Gemini** (for deep analysis) to process the data. This "Reasoning Layer" converts raw data into human-readable advice,.

• **The "Face" (Web App):** The user interacts with a modern web interface that hides the complexity of the backend security tools.

---

3. Technical Implementation: Frontend & Backend

The project is split into two distinct backend environments (Security vs. Application) and one frontend.

A. The Frontend (Client-Side)

• **Technology:** Built with **Next.js** and **Tailwind CSS**.

• **Function:** It provides a clean, "executive-friendly" interface. It does not process security logs directly but fetches "summarized" data to display in tables and charts,.

• **Hosting:** Hosted on **Vercel** (Free tier) with automated SSL.

B. The Backend (Application Logic)

• **Technology: Supabase** (PostgreSQL).

• **Function:**

  ◦ **Auth:** Manages user logins and roles (Company vs. Researcher),.

  ◦ **Database:** Stores user profiles, subscription status, and alert history.

  ◦ **Edge Functions:** Triggers alerts to WhatsApp/Email and handles the API calls between the frontend and the AI models,.

C. The Security Backend (Infrastructure)

• **Technology: Oracle Cloud (OCI)** ARM Instances running **Debian Linux**,.

• **Function:** This is where the heavy lifting happens. The **Wazuh Manager** runs here, receiving encrypted logs from client agents, analyzing them against a threat database, and indexing the results,.

---

4. Key Processes & Workflows

Process 1: Real-Time Threat Monitoring

1. **Collection:** The **Wazuh Agent** on the client's server detects an anomaly (e.g., a file change) and sends the log to your OCI server.

2. **Analysis:** The Wazuh Manager analyzes the log.

3. **Display:** The Next.js frontend calls the Wazuh API via a secure middleware to fetch the latest alerts and displays them on the user's dashboard.

Process 2: AI-Powered Analysis

1. **Trigger:** The user clicks "Ask AI" on a specific alert log.

2. **Routing:** A Supabase Edge Function sends the raw log to the **Groq API** with a prompt: *"You are a helpful security assistant... Explain this log in simple terms"*.

3. **Response:** Groq returns a text explanation, which is displayed in a chat bubble on the dashboard.

Process 3: Automated Compliance Generation

1. **Drafting:** A **LaTeX** template is created with placeholders like `{{company_name}}` and `{{threats_blocked}}`.

2. **Injection:** A Node.js or Python script fetches the month's security data from the database and injects it into the template.

3. **Generation:** The system compiles the LaTeX into a PDF and provides a download link for the user to present to regulators.

Process 4: Localized Payments

1. **Initiation:** The user selects a plan and clicks "Pay."

2. **Processing:** The system calls the **bKash Tokenized Checkout API** (currently using the Sandbox for testing).

3. **Completion:** Upon successful payment, the backend updates the user's status to `is_pro` in the Supabase database.

Process 5: Bug Bounty Workflow

1. **Submission:** A researcher submits a vulnerability report via a form on the frontend.

2. **Security: Row Level Security (RLS)** in Supabase ensures only the specific company involved can view that report.

3. **Resolution:** The company marks the bug as "Fixed" and can issue a reward.

Prohori Admin Panel - Complete Design & Functionality Guide

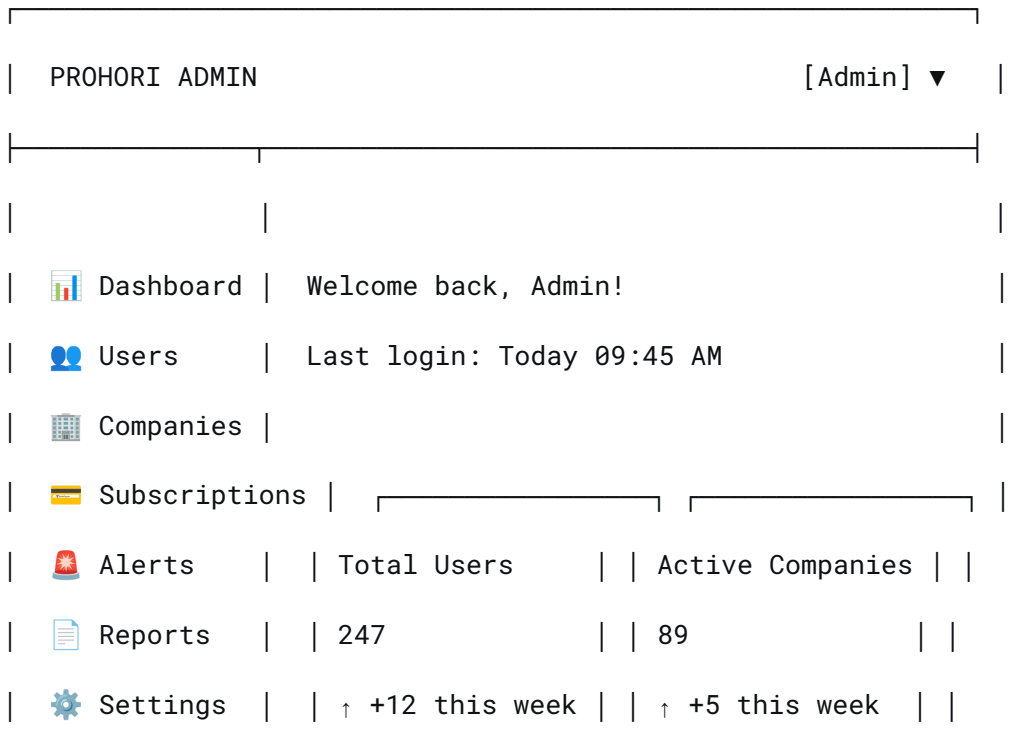
📊 Overview

The Prohori Admin Panel is a comprehensive management interface designed for platform administrators to oversee all organizations, users, subscriptions, security events, and system configurations. It serves as the command center for managing the entire SECaaS platform.

🎨 Admin Panel UI Structure

1. Dashboard Layout

```
text
```



```
| 🔐 Security  |  └──────────────────┘  └──────────────────┘ |
|              |                                            |
| 📊 Analytics |  ┌──────────────────┐  ┌──────────────────┐ |
| 💰 Revenue   |  | Monthly Revenue |  | Active Subs      | |
| 📨 Notifications|  | ৳ 124,500      |  | 156              | |
| 📁 Logs      |  | ↑ 23% vs last   |  | 78% Basic, 22% Pro |
|              |  └──────────────────┘  └──────────────────┘ |
|              |                                            |
|              |  Recent Activities                         |
|              |  ┌──────────────────────────────────────┐   |
|              |  | • New company: Rahim Store joined   |   |
|              |  | • Payment received: ৳2,499 from XYZ |   |
|              |  | • Critical alert: 5 new threats     |   |
|              |  | • Subscription expired: 3 companies |   |
|              |  └──────────────────────────────────────┘   |
|              |                                            |
└──────────────┴────────────────────────────────────────────┘
```

🔧 Core Modules & Features

2. User Management Module

Users List View

```
text
```

```
┌──────────────────────────────────────────────────────────────┐
| 👥 User Management                                  + Add |
├──────────────────────────────────────────────────────────────┤
| Search: [.....................] Filter: All ▼ Export ▼       |
├──────────────────────────────────────────────────────────────┤
| ☐ Name          Email           Role      Company     Status |
├──────────────────────────────────────────────────────────────┤
| ☐ Rahim Khan    rahim@abc.com   Owner     ABC Store   ● Active|
| ☐ Salma Begum   salma@xyz.com   Admin     XYZ Ltd     ● Active|
| ☐ Karim Hossain karim@def.com   User      DEF Shop    ○ Inactive|
| ☐ Nasrin Akter  nasrin@ghi.com  Owner     GHI Mart    ● Active|
| ☐ Jahir Islam   jahir@jkl.com   Viewer    JKL Corp    ○ Suspended|
├──────────────────────────────────────────────────────────────┤
|                                          < 1 2 3 4 >   |
└──────────────────────────────────────────────────────────────┘
```

Quick Actions:

- Click user row → Opens User Detail Panel
- Bulk actions: Suspend, Activate, Delete, Email
- Export to CSV/PDF

User Detail Panel (Slide-out)

```
text
```

```
┌──────────────────────────────────┐
|  ✖ Back                          |
```

👤 User Profile
Name: Rahim Khan
Email: rahim@abc.com
Phone: +8801712345678
Role: Owner
Status: ● Active
Joined: Jan 15, 2026
Company Information
• Company: ABC Store
• Employees: 12
• Agents Installed: 3
• First Seen: Jan 15, 2026
Subscription
• Plan: Pro
• Started: Feb 01, 2026
• Next Billing: Mar 01, 2026
• Amount: ৳2,499/month
• Payment Method: bKash
Activity Log
• Today: Logged in (2 times)
• Yesterday: Updated profile

```
| • Feb 20: Changed password           |
├──────────────────────────────────────┤
| Actions              [Suspend] [Reset]|
|                      [Delete] [Email] |
└──────────────────────────────────────┘
```

---

3. Company/Organization Management

Companies Directory

```
text
```

```
┌──────────────────────────────────────────────────────────────┐
| 🏢 Companies                                        + Add    |
├──────────────────────────────────────────────────────────────┤
| Filter by: All Industries ▼  Status: All ▼  Plan: All ▼      |
├──────────────────────────────────────────────────────────────┤
| Company       Industry   Users   Agents   Plan     Status    |
├──────────────────────────────────────────────────────────────┤
| ABC Store     E-com      3       2        Pro      • Active  |
| XYZ Ltd       Fintech    8       5        Enterp   • Active  |
| DEF Shop      Retail     2       1        Basic    ○ Inactive|
| GHI Mart      Grocery    4       2        Pro      • Active  |
| JKL Corp      Manufac    12      8        Enterp   ⚠ Overdue |
├──────────────────────────────────────────────────────────────┤
| Quick Stats: 89 Total | 72 Active | 12 Overdue | 5 Trial     |
```

```
└──────────────────────────────────────────────────────────┘
```

Company Detail View

```
text
```

```
┌──────────────────────────────────────────────────────────┐
│ 🏢 ABC Store                                  [Edit]     │
├──────────────────────────────────────────────────────────┤
│ 📋 Basic Information                                     │
│   • Business ID: BIN-1234567890                          │
│   • Address: 12/A, Motijheel, Dhaka                      │
│   • Website: https://abcstore.com                        │
│   • Primary Contact: Rahim Khan (Owner)                  │
│   • Phone: +8801712345678                                │
│   • Email: info@abcstore.com                             │
├──────────────────────────────────────────────────────────┤
│ 💳 Subscription Details                                  │
│   ┌──────────────────────────────────────────────┐       │
│   │ Current Plan: Pro (৳2,499/month)             │       │
│   │ Billing Cycle: Monthly                       │       │
│   │ Started: Feb 01, 2026                        │       │
│   │ Next Payment: Mar 01, 2026                   │       │
│   │ Payment Method: bKash (+8801712345678)       │       │
│   │ Invoice History: [View All]                  │       │
│   └──────────────────────────────────────────────┘       │
├──────────────────────────────────────────────────────────┤
```

---

4. Subscription Management Module

Subscriptions Overview

```
text
```

```
┌──────────────────────────────────────────────────────────┐
│ 💳 Subscription Management                               │
├──────────────────────────────────────────────────────────┤
│ Summary Cards                                            │
│ ┌──────────────┐ ┌──────────────┐ ┌──────────────┐ ┌──────────┐│
│ │ Total MRR    │ │ Active Subs  │ │ Churn Rate   │ │ ARPU     ││
│ │ ৳124,500     │ │ 156          │ │ 3.2%         │ │ ৳798     ││
│ └──────────────┘ └──────────────┘ └──────────────┘ └──────────┘│
├──────────────────────────────────────────────────────────┤
│ Plans Breakdown                                          │
│ ┌──────────────────────────────────────────────────┐     │
│ │ Basic (78)    ████████████████████████ 50%       │     │
│ │ Pro (56)      ██████████████████ 36%             │     │
│ │ Enterprise (22) ████████ 14%                     │     │
│ └──────────────────────────────────────────────────┘     │
├──────────────────────────────────────────────────────────┤
│ Active Subscriptions                                     │
├──────────────────────────────────────────────────────────┤
│ Company      Plan      Amount   Status     Next Billing  │
├──────────────────────────────────────────────────────────┤
│ ABC Store    Pro       ৳2,499   ✅ Paid    Mar 01, 2026  │
│ XYZ Ltd      Enterp    ৳9,999   ✅ Paid    Mar 05, 2026  │
```

```
| DEF Shop     Basic     ৳999    ⚠ Pending  Today           |
| GHI Mart     Pro       ৳2,499  ❌ Failed  Feb 25, 2026    |
| JKL Corp     Enterp    ৳9,999  ✅ Paid    Mar 10, 2026    |
├──────────────────────────────────────────────────────────┤
| Payment Issues (12)                                      |
| • 5 Failed payments - Needs attention                    |
| • 3 Expired cards/methods                                |
| • 4 Overdue >30 days                                     |
└──────────────────────────────────────────────────────────┘
```

Subscription Detail Modal

```
text
```

```
┌──────────────────────────────────────┐
| 💳 Subscription Details     [Edit]    |
├──────────────────────────────────────┤
| Company: ABC Store                   |
├──────────────────────────────────────┤
| Plan Information                     |
| • Plan Type: Pro                     |
| • Price: ৳2,499/month                |
| • Billing Cycle: Monthly             |
| • Started: Feb 01, 2026              |
| • Trial Period: No                   |
| • Auto-renew: Yes                    |
├──────────────────────────────────────┤
```

```
| Payment History                          |
| ┌──────────────────────────────────────┐ |
| | Feb 01, 2026 - ৳2,499 - Paid       | |
| | Jan 01, 2026 - ৳2,499 - Paid       | |
| | Dec 01, 2025 - ৳2,499 - Paid       | |
| └──────────────────────────────────────┘ |
|                                    [View All]|
├──────────────────────────────────────────┤
| Invoice Management                       |
| • Last Invoice: INV-2026-02-001          |
| • PDF Available: [Download]              |
| • Send reminder: [Send]                  |
├──────────────────────────────────────────┤
| Actions                                  |
| [Change Plan] [Cancel Subscription]      |
| [Refund Payment] [Pause Subscription]|
└──────────────────────────────────────────┘
```

---

5. Security & Alert Management

Global Alerts Dashboard

```
text
┌──────────────────────────────────────────────────────────────────┐
| 🚨 Security Alerts (System-wide)                                 |
```

```
├──────────────────────────────────────────────────────────┤
| Filter: Severity ▼  Time: Last 24h ▼  Company: All ▼      |
├──────────────────────────────────────────────────────────┤
| Severity  Alert                    Company     Time   Status|
├──────────────────────────────────────────────────────────┤
| 🔴 CRITICAL Ransomware detected    XYZ Ltd    2m ago  Investigating|
| 🟠 HIGH    Brute force attack      ABC Store  15m ago Blocked|
| 🟡 MEDIUM  Suspicious file change  DEF Shop   1h ago  Reviewed|
| 🔴 CRITICAL Data exfiltration      GHI Mart   3h ago  Mitigated|
| 🟢 LOW     New device login        JKL Corp   5h ago  Verified|
├──────────────────────────────────────────────────────────┤
| Statistics                                               |
| • Critical: 2 | High: 7 | Medium: 15 | Low: 32            |
| • Top attack types: Brute force (34%), Malware (23%)     |
| • Most targeted: E-commerce (45%), Fintech (30%)         |
└──────────────────────────────────────────────────────────┘
```

Alert Investigation Panel

```
text
```

```
┌──────────────────────────────────────────────────────────┐
| 🔍 Alert Investigation - Critical Ransomware Detection   |
├──────────────────────────────────────────────────────────┤
| Alert Details                                            |
| • ID: ALERT-2026-02-26-001                               |
| • Company: XYZ Ltd                                       |
```

| • Severity: 🔴 CRITICAL |

| • Detected: 10:23 AM, Feb 26, 2026 |

| • Status: Under Investigation |

├──┤

| Raw Log Data |

| ┌──┐ |

| | [Wazuh] Rule: 12345 (Ransomware Detection) | |

| | File: /data/encrypted_files.lock | |

| | Process: suspicious.exe | |

| | User: unknown | |

| └──┘ |

├──┤

| Affected Systems |

| • Server: web-01 (192.168.1.10) |

| • Agent ID: agent-xyz-001 |

| • Files affected: 23 |

| • Users impacted: 5 |

├──┤

| AI Analysis (Groq/Gemini) |

| ┌──┐ |

| | "Ransomware detected attempting to encrypt files. | |

| | System isolated immediately. Recommend restoring from | |

| | backup and scanning all connected systems." | |

| └──┘ |

├──┤

```
| Actions                                                          |
| [Isolate Server] [Notify Company] [Escalate]                     |
| [Mark as Resolved] [Generate Incident Report]                    |
└──────────────────────────────────────────────────────────────────┘
```

---

6. Revenue & Analytics Module

Financial Dashboard

```
text
```

```
┌──────────────────────────────────────────────────────────────────┐
| 💰 Revenue Analytics                                  Period▼|
├──────────────────────────────────────────────────────────────────┤
| Revenue Metrics                                                  |
| ┌──────────────┐ ┌──────────────┐ ┌──────────────┐ ┌──────────┐|
| | Revenue MTD | | Revenue YTD | | Avg. Deal   | | Pipeline||
| | ৳124,500    | | ৳856,000    | | ৳2,847      | | ৳45,000 ||
| └──────────────┘ └──────────────┘ └──────────────┘ └──────────┘|
├──────────────────────────────────────────────────────────────────┤
| Revenue Chart (Last 6 Months)                                    |
|   150k ┤                                              ╭─╮   |
|   120k ┤                                         ╭    | |   |
|   90k  ┤                                    ╭    ||   | |   |
|   60k  ┤                               ╭    ||   ||   | |   |
|   30k  ┤                          ╭    ||   ||   ||   | |   |
```

```
|     0  ┼──────────────────────┘└──────┘└──────┘└──────┘└──────┘└──────┘   |
|         Sep   Oct   Nov   Dec   Jan   Feb                                |
├──────────────────────────────────────────────────────────────────────────┤
| Revenue by Plan                                                          |
| • Basic: ৳77,922 (32 companies × ৳999)                                   |
| • Pro: ৳139,944 (56 companies × ৳2,499)                                  |
| • Enterprise: ৳219,978 (22 companies × ৳9,999)                           |
├──────────────────────────────────────────────────────────────────────────┤
| Payment Methods                                                          |
| • bKash: 68% (৳297,000)                                                  |
| • Nagad: 22% (৳96,000)                                                   |
| • Rocket: 10% (৳44,000)                                                  |
├──────────────────────────────────────────────────────────────────────────┤
| Outstanding Payments                                                     |
| • Total overdue: ৳32,000 (12 companies)                                  |
| • >30 days: 4 companies (৳12,000)                                        |
| • >60 days: 2 companies (৳8,000) [Send reminders]                        |
└──────────────────────────────────────────────────────────────────────────┘
```

---

7. System Settings & Configuration

Settings Panel

```
text
```

```
┌──────────────────────────────────────────────────────────────────────────┐
```


⚙️ System Settings
Tabs: General | Billing | Security | Notifications | API
[General Settings]
Platform Name: Prohori Security Suite
Support Email: support@prohori.com
Support Phone: +8809612345678
Company Address: Dhaka, Bangladesh
Timezone: Asia/Dhaka (+06:00)
[Billing Configuration]
Currency: BDT (৳)
Tax Rate: 15% VAT
Payment Gateways:
☑ bKash (Live) - Connected
☑ Nagad (Live) - Connected
☐ Rocket - Not Connected
Pricing Plans:
• Basic: ৳999/month - [Edit] [Disable]
• Pro: ৳2,499/month - [Edit] [Disable]

```
| | • Enterprise: ৳9,999/month - [Edit] [Disable]          |  |
| | • Custom plans available                                |  |
| └──────────────────────────────────────────────────────┘  |
|                                                           |
| [Security Configuration]                                  |
| ┌──────────────────────────────────────────────────────┐  |
| | MFA Required for Admins: ☑ Enabled                     |  |
| | Session Timeout: 30 minutes                            |  |
| | Password Policy: Strong (min 12 chars, special)        |  |
| | IP Whitelist: 192.168.1.0/24, 10.0.0.0/8               |  |
| | Audit Log Retention: 90 days                           |  |
| └──────────────────────────────────────────────────────┘  |
|                                                           |
| [Notification Settings]                                   |
| ┌──────────────────────────────────────────────────────┐  |
| | Admin Alerts:                                          |  |
| |   ☑ New user registration                              |  |
| |   ☑ Payment failures                                   |  |
| |   ☑ Critical security alerts                           |  |
| |   ☑ System errors                                      |  |
| |                                                        |  |
| | Channels:                                              |  |
| |   ☑ Email: admin@prohori.com                           |  |
| |   ☑ SMS: +8801712345678                                |  |
| |   ☑ Slack: #prohori-alerts (Connected)                 |  |
```

```
| |   ☑ Telegram: @prohori_bot (Connected)                |  |
| └──────────────────────────────────────────────────────┘  |
└──────────────────────────────────────────────────────────┘
```

🔄 Admin Workflows

8. Key Administrative Processes

A. New Company Onboarding Review

```
text
```

```
Step 1: Registration Alert

┌──────────────────────────────────────────────────┐
| 🔔 New Registration Pending Approval             |
| Company: ABC Store                               |
| Owner: Rahim Khan (rahim@abc.com)                |
| Plan Selected: Pro (৳2,499/month)                |
| Payment: bKash - ৳2,499 (Completed)              |
├──────────────────────────────────────────────────┤
| [Approve] [Reject] [Contact Owner] [Review]      |
└──────────────────────────────────────────────────┘


Step 2: Verification Screen

┌──────────────────────────────────────────────────┐
| Verify Company Details                           |
```

```
├──────────────────────────────────────────────┤
| ✅ Business documents uploaded               |
| ✅ Payment verified                          |
| ✅ Contact info valid                        |
| ⚠️ Website not responding                    |
├──────────────────────────────────────────────┤
| Actions:                                     |
| • Contact owner for website issue            |
| • Manually verify domain                     |
| • Approve with warnings                      |
└──────────────────────────────────────────────┘


Step 3: Agent Deployment Tracking

┌──────────────────────────────────────────────┐
| Agent Installation Status                    |
├──────────────────────────────────────────────┤
| • Server 1: Connected - Active               |
| • Server 2: Pending - Not installed          |
| • Server 3: Disconnected - Last seen 2h ago  |
├──────────────────────────────────────────────┤
| [Send Installation Reminder] [Troubleshoot]  |
└──────────────────────────────────────────────┘
```

B. Payment Issue Resolution

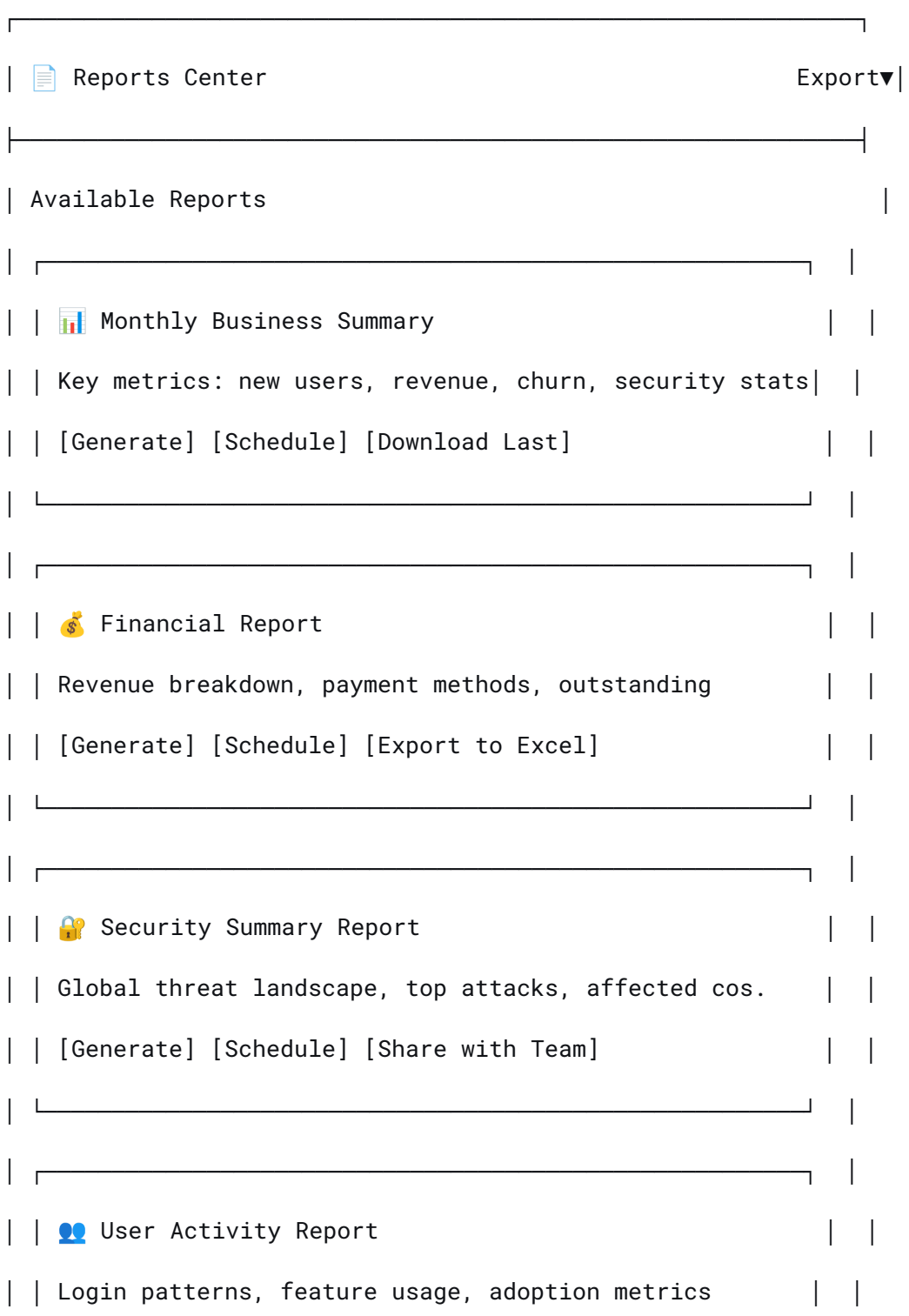
```
text
```

```
┌──────────────────────────────────────────────────┐
│ 💳 Failed Payment - Action Required              │
├──────────────────────────────────────────────────┤
│ Company: DEF Shop                                │
│ Amount: ৳999 (Basic Plan)                        │
│ Date: Feb 26, 2026                               │
│ Error: Insufficient balance (bKash)              │
├──────────────────────────────────────────────────┤
│ Payment History:                                 │
│ • Feb 01 - Success                               │
│ • Jan 01 - Success                               │
│ • Dec 01 - Success                               │
├──────────────────────────────────────────────────┤
│ Customer Contact:                                │
│ • Email: owner@defshop.com                       │
│ • Phone: +8801812345678                          │
├──────────────────────────────────────────────────┤
│ Resolution Options:                              │
│ [Retry Payment] [Send Reminder] [Downgrade]      │
│ [Extend Grace Period] [Suspend Service]          │
└──────────────────────────────────────────────────┘
```

📈 Reports & Analytics

9. Admin Reports Section

```
text
```



```
| | [Generate] [Schedule] [Export]                          |  |
| └──────────────────────────────────────────────────────┘  |
| ┌──────────────────────────────────────────────────────┐  |
| | 📋 Compliance Report (CSA 2023)                       |  |
| | Platform-wide compliance status for regulations       |  |
| | [Generate] [Schedule] [Download PDF]                  |  |
| └──────────────────────────────────────────────────────┘  |
```

🎯 Admin Panel Feature Summary

Core Capabilities

Category	Features
User Management	View all users, filter by role/status, bulk actions, user profiles, activity logs, password reset, suspend/activate
Company Management	Company directory, detailed profiles, team members, security status, agent management, data export

Subscription Control	Plan management, billing overview, payment retry, plan changes, cancellations, refunds, invoice management
Security Oversight	Global alert dashboard, incident investigation, AI analysis view, threat statistics, company isolation
Revenue Analytics	MRR tracking, payment method breakdown, outstanding payments, forecast charts, export financials
System Configuration	Platform settings, payment gateway config, pricing plans, notification rules, API keys, audit logs
Report Generation	Custom reports, scheduled exports, compliance documentation, data visualization
Notification Center	System alerts, admin notifications, broadcast to companies, template management

Administrative Actions

- User Actions: Create, edit, suspend, delete, reset password, send email
- Company Actions: Approve, reject, suspend, contact, export data, delete
- Subscription Actions: Change plan, cancel, refund, pause, retry payment

- Security Actions: Isolate company, investigate alert, notify, escalate, resolve
- System Actions: Configure settings, manage API keys, view logs, backup data

---

🚀 Admin Dashboard KPIs

Metric	Description	Target
Active Companies	Organizations with active subscription	>100
MRR (Monthly Recurring Revenue)	Total monthly subscription revenue	>৳150,000
Churn Rate	% of customers canceling	<5%
Critical Alerts	High-severity incidents requiring attention	<10/day
Avg Response Time	Time to respond to critical alerts	<15 min
Payment Success Rate	% of successful transactions	>95%
Agent Health	% of connected agents	>98%

CSAT Score	Customer satisfaction rating	>4.5/5

📱 Responsive Design Considerations

The admin panel should be fully responsive with:

- Desktop: Full layout with sidebar and detailed tables
- Tablet: Collapsible sidebar, simplified cards view
- Mobile: Bottom navigation, stacked cards, essential actions only