Infosecotb.com with vMeNext Threat Model

Owner: InfoSecOTB
Reviewer: Piotr Kowalczyk
Contributors:
Date Generated: Mon Oct 06 2025

Executive Summary

High level system description

Infosecotb.com is a professional cybersecurity blog hosted on WordPress through BlueHost. The blog serves as a platform for sharing insights, articles, and resources related to information security, targeting cybersecurity professionals and enthusiasts.

Website Structure:
- Content Management System (CMS): Built on WordPress, allowing for easy content creation, management, and publishing.
- User Interaction: Features such as chatbot, comments, contact forms, and newsletter subscriptions that facilitate user engagement.
- Categorized Content: Articles are organized into categories based on topics

Functionality:
- Article Publishing: Regularly updated with new blog posts that include technical guides, best practices, and industry insights.
- Search Functionality: Allows users to search for specific topics or articles.
- Social Media Integration: Links to social media platforms for sharing and promoting content.
- vMeNext AI powered chatbot

User Types:
- Visitors: General users seeking information on cybersecurity topics.
- Administrators: Individuals with backend access for managing content, settings, and website security.

Technical Environment:
- Hosting: Utilizes BlueHost for hosting, which provides shared or dedicated server resources.
- Plugins and Themes: Employs various WordPress plugins for enhanced functionality (e.g., SEO, analytics, security).
- Database: Relies on a MySQL database for storing content, user information, and site settings.
- vMeNext chatbot published using iFrames

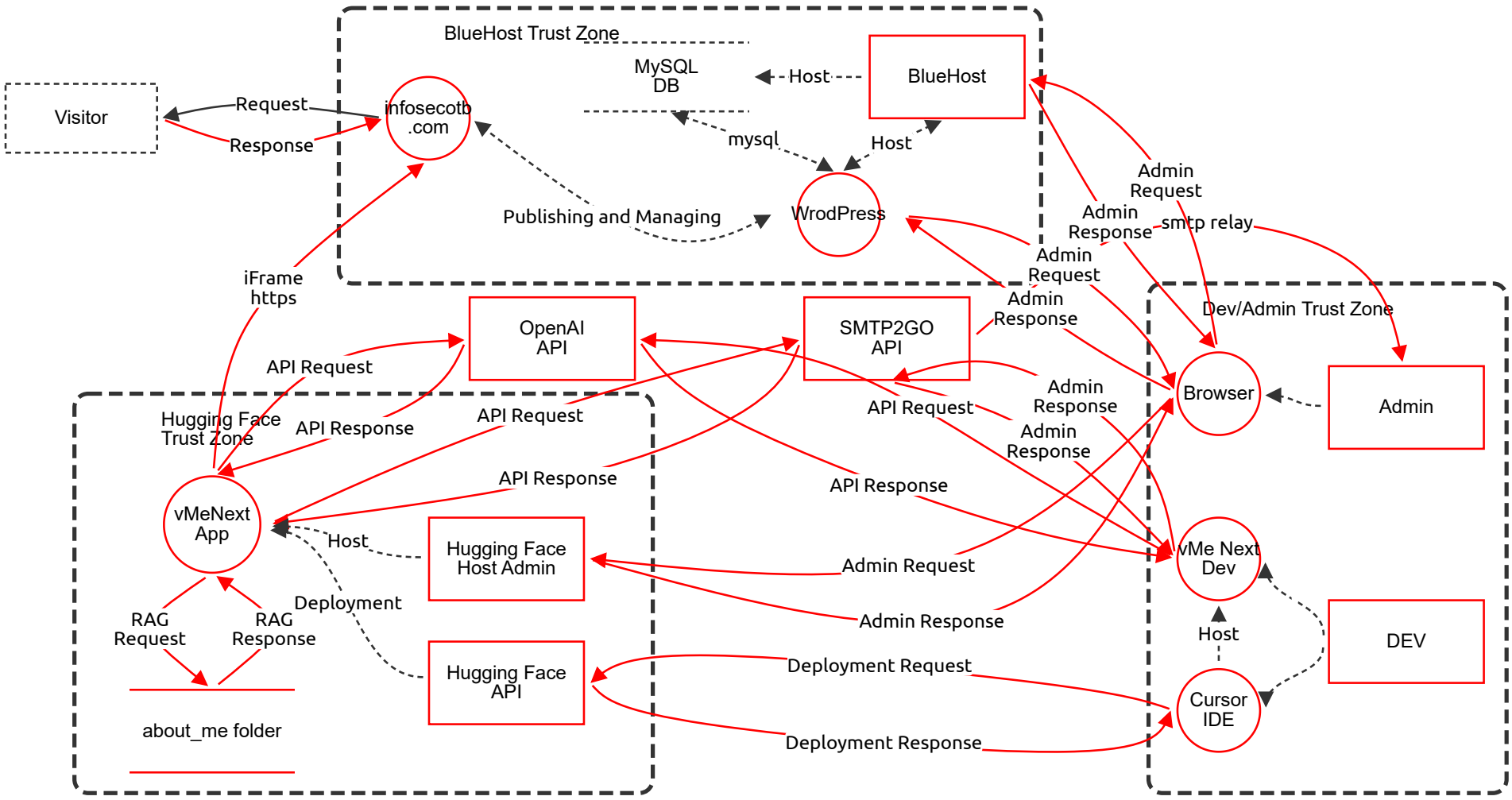
vMeNext is a comprehensive AI-powered chatbot system designed to serve as an intelligent interface for blog content and website management. Built with modern Python technologies, it combines the power of OpenAI's GPT models with automated web scraping, monitoring, and user engagement features.

Key Capabilities:
- Intelligent Conversations: Powered by OpenAI's latest GPT models for natural, context-aware responses
- Blog Content Integration: Automatic scraping, processing, and summarization of blog posts
- Website Monitoring: Continuous availability checking with real-time alerts
- Document Processing: Support for multiple file formats (PDF, DOCX, TXT, MD)
- User Engagement: Automated email notifications and contact management
- Analytics Dashboard: Website uptime statistics with visualizations

Summary

Total Threats	42
Total Mitigated	0
Total Open	42
Open / Critical Severity	0
Open / High Severity	19
Open / Medium Severity	21
Open / Low Severity	2

Infosecotb.com with vMeNext Diagram



Infosecotb.com with vMeNext Diagram

Visitor (Actor) - *Out of Scope*

Reason for out of scope:

Description: Visitor connecting to infosecotb.com using a browser

Number	Title	Type	Severity	Status	Score	Description	Mitigations

vMeNext App (Process)

Description: Gradio ChatBot Python Application with RAG Running on Hugging Face Space

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of iFrame Source	Spoofing	High	Open		The vMeNext App receives an iFrame connection from the infosecotb.com process in the BlueHost Trust Zone, crossing from a different trust boundary. An attacker could spoof the iFrame source to inject malicious content into the chatbot interface.	Implement strict Content Security Policy (CSP) in the iFrame embedding and validate the origin of incoming iFrame requests using certificate pinning and origin checks.
	Information Disclosure via API Responses	Information Disclosure	Medium	Open		The vMeNext App processes and responds to API responses from external actors like OpenAI API and SMTP2GO API over public networks with HTTPS encryption. However, if session data or user inputs are inadvertently included in responses, sensitive information could be disclosed due to adjacency to public flows.	Sanitize all API responses to remove any user-specific or sensitive data, and implement data masking for logs and outputs. Enforce least privilege in API integrations.
	Denial of Service from RAG Requests	Denial of Service	Medium	Open		The vMeNext App handles RAG requests to and from the about_me folder store within the Hugging Face Trust Zone. High-volume or malformed requests could overwhelm the local processing, especially since it's a web application adjacent to external API calls.	Implement rate limiting on RAG endpoints and resource quotas in the Hugging Face Space to prevent abuse. Use asynchronous processing for file reads.

about_me folder (Store)

Description: Folder with documents read by Python application and provided to AI ChatBot as a prompt context.

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Stored Documents	Tampering	High	Open		The about_me folder store holds documents used as prompt context for the vMeNext App within the Hugging Face Trust Zone. As a local store accessible via RAG flows, an attacker with access to the Hugging Face environment could tamper with files, leading to poisoned AI responses.	Apply file integrity checks (e.g., hashes) on documents before use in RAG, restrict write access to the folder using Hugging Face permissions, and regularly audit file contents.
	Information Disclosure of Document Contents	Information Disclosure	Medium	Open		The about_me folder store is read by the vMeNext App for RAG processing. If the store is not properly isolated within the trust boundary, contents could be exposed through misconfigured access or adjacency to deployment flows.	Encrypt documents at rest and enforce read-only access for the application process. Use Hugging Face's secret management for any sensitive file handling.

DEV (Actor)

Description: vMeNext Application Developer

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege via Dev Access	Elevation of Privilege	High	Open		The DEV actor interacts with the Cursor IDE and vMe Next Dev processes in the Dev/Admin Trust Zone. As a human actor with development privileges, weak access controls could allow elevation to affect production deployments crossing to Hugging Face zone.	Enforce role-based access control (RBAC) with multi-factor authentication (MFA) for dev tools, and use separate environments for development and production to prevent privilege escalation.

Cursor IDE (Process)

Description: Cursor IDE used for developing and running vMe Next Dev application and deploying on Hugging Face Space

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Repudiation in Development Flows	Repudiation	Medium	Open		The Cursor IDE process handles hosting and deployment flows to Hugging Face API, within the Dev/Admin Trust Zone. Actions like code changes could be repudiated without proper logging, especially with flows to external APIs.	Implement comprehensive audit logging for all IDE actions and deployments, including timestamps and user attribution, integrated with a central logging service.
	Tampering with IDE Code	Tampering	High	Open		The Cursor IDE process is used for developing the vMeNext application and is adjacent to DEV actor inputs. Malicious code injection or tampering during development could propagate to deployed versions via deployment flows crossing trust boundaries.	Use version control with signed commits (e.g., Git with GPG) and automated code scanning in CI/CD pipelines to detect tampering before deployment.

infosecotb .com (Process)

Description: InfoSec Outside The Box Cybersecurity Blog created and managed with WordPress CMS with vMeNext AI powered chatbot added using iFrame

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of Website Requests	Spoofing	High	Open		The infosecotb.com process receives requests from the Visitor actor over public HTTPS flows, crossing into the BlueHost Trust Zone. Attackers could spoof visitor identities to bypass any content restrictions or inject fake requests via the iFrame to vMeNext.	Implement client-side certificate authentication or robust session management with CSRF tokens for all user interactions, and validate iFrame sources strictly.
	Denial of Service on Website	Denial of Service	Medium	Open		The infosecotb.com process, a WordPress web application in the BlueHost Trust Zone, handles public requests and iFrame embeddings. DDoS attacks on ingress flows could overwhelm the shared hosting resources.	Deploy a Web Application Firewall (WAF) and DDoS protection services from BlueHost, with rate limiting on all endpoints including the chatbot iFrame.
	Information Disclosure through WordPress	Information Disclosure	High	Open		The infosecotb.com process uses WordPress CMS connected to MySQL DB (out-of-scope but adjacent), with public flows. Vulnerable plugins or misconfigurations could disclose admin credentials or user data across the trust boundary.	Keep WordPress core, themes, and plugins updated; conduct regular security scans; and use security plugins like Wordfence for intrusion detection and hardening.

iFrame https (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with iFrame Flow	Tampering	Medium	Open		The iFrame https flow connects the vMeNext App in Hugging Face Trust Zone to infosecotb.com in BlueHost Trust Zone, crossing trust boundaries over a public network with encryption. An attacker could tamper with the embedded content if TLS is not properly validated.	Enforce mutual TLS (mTLS) for the iFrame communication and use HTTP Strict Transport Security (HSTS) to prevent downgrade attacks.

(Data Flow) *- Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

(Data Flow) - *Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

(Data Flow) - *Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Host (Data Flow) - *Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

RAG Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in RAG Request	Information Disclosure	Low	Open		The RAG Request flow from vMeNext App to about_me folder store is internal to Hugging Face Trust Zone but involves sensitive document queries. Misconfigured logging could disclose query contents.	Disable or anonymize logging for RAG requests and ensure no sensitive data is written to accessible logs.

RAG Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with RAG Response	Tampering	Medium	Open		The RAG Response flow returns document contexts to vMeNext App within the trust zone. If the store is compromised, tampered data could alter AI outputs, affecting user interactions.	Validate response integrity with checksums and implement input validation in the app to detect anomalous RAG data.

mysql (Data Flow) - *Out of Scope*

Reason for out of scope: Managed by BlueHost

Description: Managed and secured by BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations

smtp relay (Data Flow)

Description: E-mail sent to administrator

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in SMTP Relay	Information Disclosure	High	Open		The smtp relay flow from SMTP2GO API to Admin actor crosses public networks with encryption but handles email notifications that may contain user data from vMeNext interactions, risking exposure if intercepted.	Encrypt email contents end-to-end and avoid including sensitive user data in notifications; use secure email protocols like SMTPS.
	Spoofing of Email Sender	Spoofing	Medium	Open		The smtp relay flow could be spoofed if API keys are compromised, allowing attackers to send fake admin alerts from the SMTP2GO actor.	Use DKIM/SPF/DMARC for email authentication and rotate API keys regularly with monitoring for unusual activity.

API Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege via API Response	Elevation of Privilege	Medium	Open		The API Response flow to vMeNext App from SMTP2GO API crosses public networks. If responses include privilege tokens or escalate based on external data, it could lead to unauthorized access within the app.	Strictly validate and sanitize all incoming API responses, implementing least-privilege API scopes and no direct privilege grants from external responses.

API Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with API Request to SMTP2GO	Tampering	High	Open		The API Request flow from vMeNext App to SMTP2GO API traverses public networks with HTTPS. Without integrity checks, requests could be tampered with to alter email content or recipients.	Use message signing for API requests and implement request validation at the API endpoint to ensure integrity.

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Denial of Service in Admin Response	Denial of Service	Low	Open		The Admin Response flow from SMTP2GO API to vMe Next Dev process in Dev/Admin zone over public network could be flooded, disrupting admin monitoring.	Apply rate limiting and circuit breakers in the admin integration to handle potential DoS from API responses.

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Repudiation of Admin Interactions	Repudiation	Medium	Open		The Admin Response flow between SMTP2GO API and vMe Next Dev lacks non-repudiation, allowing denial of admin actions like email sends.	Incorporate digital signatures in admin API flows and log all interactions with timestamps for auditability.

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in OpenAI API Request	Information Disclosure	High	Open		The API Request flow from vMe Next Dev to OpenAI API crosses public networks with encryption, but API keys or prompt data could be disclosed if not secured properly.	Use API key rotation, environment variables for secrets, and avoid logging sensitive request payloads.

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of OpenAI API Calls	Spoofing	High	Open		The API Request flow from vMeNext App to OpenAI API over public HTTPS could be spoofed if the endpoint is mimicked, leading to data exfiltration via fake API.	Implement certificate pinning for OpenAI endpoints and validate API responses against expected schemas.

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with OpenAI API Response	Tampering	Medium	Open		The API Response flow from OpenAI API to vMeNext App traverses public networks. Tampering could inject malicious AI-generated content into the chatbot.	Verify response integrity using HMAC signatures from OpenAI and sanitize outputs before rendering in the app.

Deployment (Data Flow) - *Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Host (Data Flow) - *Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Response (Data Flow)

Description: Response from infosecotb.com website including vMeNext chatbot

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in Website Response	Information Disclosure	High	Open		The Response flow from infosecotb.com to Visitor actor over public HTTPS includes chatbot content from vMeNext iFrame, potentially disclosing sensitive blog or user data if not filtered.	Apply data minimization in responses and use secure headers to prevent caching of sensitive content.

Publishing and Managing (Data Flow) - *Out of Scope*

Reason for out of scope: Managed and secured by BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Request (Data Flow)

Description: Request to infosecotb.com website including vMeNext chatbot

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Host (Data Flow) *- Out of Scope*

Reason for out of scope:

Description: Managed by BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Host (Data Flow) *- Out of Scope*

Reason for out of scope: Managed and secured by BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Admin Response (Data Flow)

Description: WordPress Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege in WordPress Admin	Elevation of Privilege	High	Open		The Admin Response flow from WordPress process to Browser in Dev/Admin zone could allow privilege escalation if weak session management permits unauthorized admin access.	Enforce strong password policies, MFA for admin logins, and session timeouts in WordPress.

Admin Request (Data Flow)

Description: WordPress Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Admin Request to WordPress	Tampering	Medium	Open		The Admin Request flow from WordPress to Browser crosses into Dev/Admin zone over HTTPS, but could be tampered with to alter content management actions.	Use CSRF protection and signed requests for all admin operations in WordPress.

Admin Request (Data Flow)

Description: BlueHost Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of BlueHost Admin Requests	Spoofing	High	Open		The Admin Request flow from Browser to BlueHost actor over public networks could be spoofed to gain unauthorized hosting control, affecting the entire BlueHost Trust Zone.	Require MFA and IP whitelisting for BlueHost admin access, with anomaly detection on login attempts.

Admin Response (Data Flow)

Description: BlueHost Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Denial of Service from BlueHost Responses	Denial of Service	Medium	Open		The Admin Response flow from BlueHost to Browser could be delayed or flooded, impacting site management in the trust zone.	Implement resilient admin interfaces with offline capabilities and monitor for response anomalies.

Admin Response (Data Flow)

Description: Hugging Face Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in Hugging Face Response	Information Disclosure	Medium	Open		The Admin Response flow from Hugging Face Host Admin to Browser crosses public networks, potentially exposing deployment secrets or space configurations.	Encrypt all admin responses and use short-lived tokens for session management in Hugging Face admin.

Admin Request (Data Flow)

Description: Hugging Face Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Hugging Face Admin Request	Tampering	High	Open		The Admin Request flow from Browser to Hugging Face Host Admin over HTTPS could be tampered with to deploy malicious updates to vMeNext App.	Sign all deployment requests and use webhooks for verification in Hugging Face integrations.

Deployment Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege in Deployment Request	Elevation of Privilege	High	Open		The Deployment Request flow from Cursor IDE to Hugging Face API crosses from Dev/Admin to Hugging Face zone over public networks, allowing potential privilege escalation if auth is weak.	Use scoped API tokens with minimal permissions for deployments and audit all deployment logs.

Deployment Response (Data Flow)

Description: Hugging Face Space Application Deployment

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Repudiation of Deployment Actions	Repudiation	Medium	Open		The Deployment Response flow from Hugging Face API to Cursor IDE lacks strong non-repudiation, enabling denial of deployment changes.	Require signed acknowledgments for deployments and integrate with a SIEM for immutable logging.

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing in OpenAI Response to Dev	Spoofing	Medium	Open		The API Response flow from OpenAI API to vMe Next Dev process over public networks could be spoofed, misleading development testing.	Validate OpenAI responses with API-specific signatures and use test environments isolated from production.

MySQL DB (Store) *- Out of Scope*

Reason for out of scope: Managed by BlueHost

Description: MySQL Database used for WordPress website

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Admin (Actor)

Description: System Administrator

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Denial of Service Targeting Admin	Denial of Service	Medium	Open		The Admin actor receives SMTP relay flows and manages multiple zones (BlueHost, Dev/Admin). Coordinated DoS could prevent oversight of the system.	Provide redundant admin access paths and train on incident response for DoS scenarios.

vMe Next Dev (Process)

Description: Gradio ChatBot Python Application Development

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in Dev Process	Information Disclosure	Medium	Open		The vMe Next Dev process handles API requests to OpenAI and SMTP2GO within Dev/Admin Trust Zone, adjacent to admin flows. Leaked dev artifacts could expose API keys.	Use secret scanning tools in the dev environment and encrypt all local storage.

Browser (Process)

Description: Browser used by System Administrator

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege via Browser	Elevation of Privilege	High	Open		The Browser process used by Admin actor accesses multiple admin panels (WordPress, BlueHost, Hugging Face) over public flows, risking cross-site scripting (XSS) leading to privilege escalation.	Use browser isolation or sandboxing for admin sessions, and enable site isolation features like Chrome's.

OpenAI API (Actor)

Description: Artificial Intelligence API secured with a key

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Denial of Service on OpenAI API	Denial of Service	High	Open		The OpenAI API actor receives multiple ingress flows from vMeNext App and vMe Next Dev over public networks, vulnerable to API abuse flooding the service.	Configure API rate limits and usage quotas in OpenAI dashboard, monitor for anomalous patterns.

SMTP2GO API (Actor)

Description: E-mail relay hosted system API secured with key

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with SMTP2GO API	Tampering	Medium	Open		The SMTP2GO API actor processes requests from vMeNext App, with flows crossing public networks. Tampering could alter email campaigns or notifications.	Enable API request signing and validate all payloads against schemas at the API level.

Hugging Face Host Admin (Actor)

Description: Hugging Face Hosting Administrator Control Panel

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of Hugging Face Admin	Spoofing	High	Open		The Hugging Face Host Admin actor handles admin requests from Browser over public HTTPS, susceptible to phishing or spoofed logins affecting space deployments.	Enforce MFA and use hardware keys for Hugging Face admin authentication.

Hugging Face API (Actor)

Description: Hugging Face Deployment API

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege in Hugging Face API	Elevation of Privilege	High	Open		The Hugging Face API actor receives deployment requests from Cursor IDE, crossing zones. Weak token scopes could allow over-privileged deployments.	Use fine-grained API permissions and review token scopes regularly for the Spaces API.

BlueHost (Actor)

Description: Administrator access to BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure from BlueHost	Information Disclosure	Medium	Open		The BlueHost actor provides admin responses over public networks, potentially exposing hosting configurations or credentials if logs are queried insecurely.	Limit admin query scopes and use encrypted channels for all BlueHost interactions.

WrodPress (Process)

Description: WordPress Content Management System

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Repudiation in WordPress Operations	Repudiation	Medium	Open		The WordPress process manages content and connects to MySQL DB with bidirectional flows in BlueHost zone. Actions like post edits could be repudiated without audit trails.	Enable WordPress activity logging plugins and integrate with external audit systems for non-repudiable records.