# 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

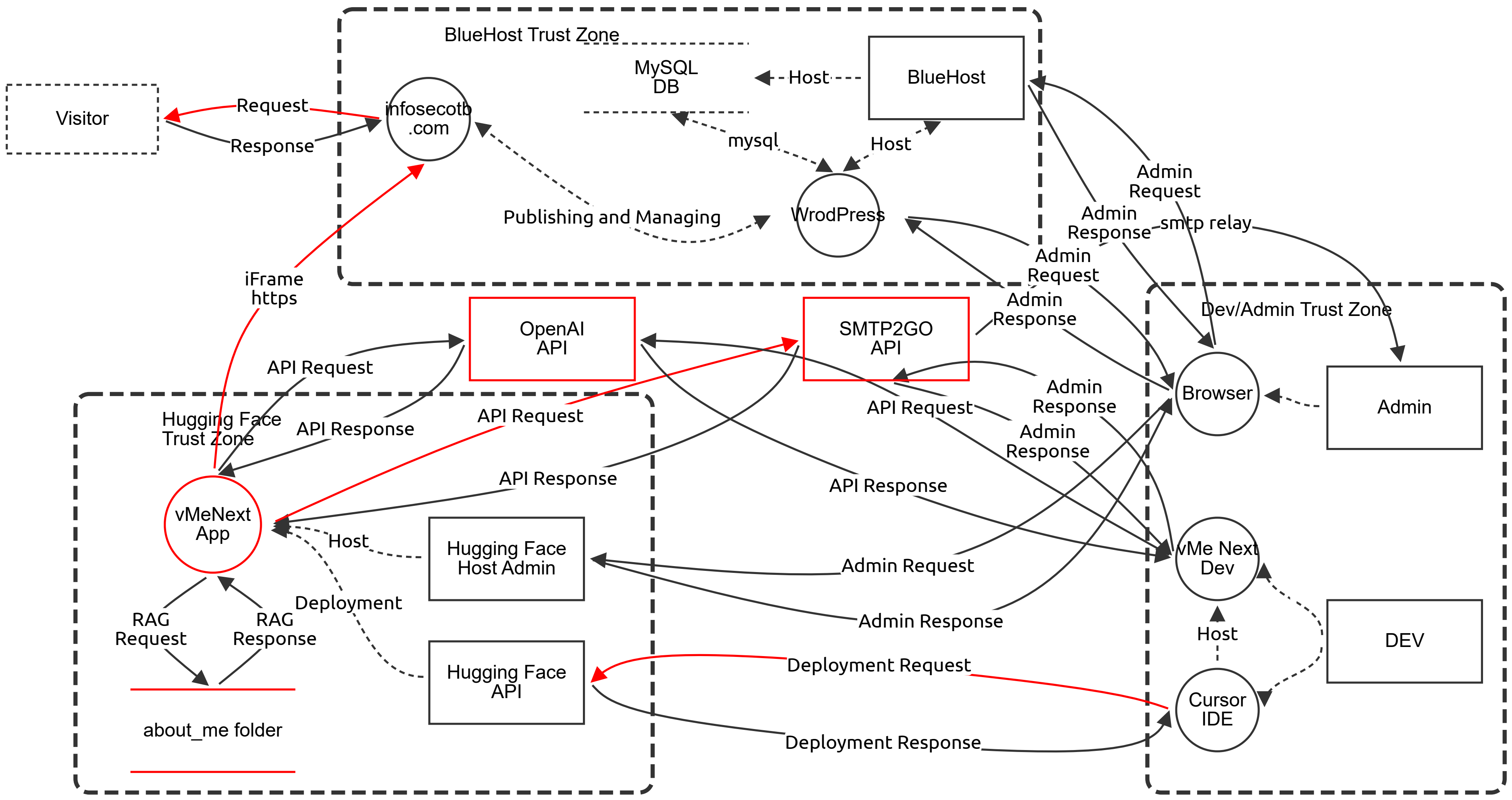
vMeNext is a comprehensive AI-powered chatbot system designed to serve as an intelligent interface for blog content and website management. Built with modern Python technologies, it combines the power of OpenAI's GPT models with automated web scraping, monitoring, and user engagement features.

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** | 9 |
| **Total Mitigated** | 0 |
| **Total Open** | 9 |
| **Open / Critical Severity** | 0 |
| **Open / High Severity** | 5 |
| **Open / Medium Severity** | 4 |
| **Open / Low Severity** | 0 |

# 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 |
|---|---|---|---|---|---|---|---|
| | Chatbot Service Exhaustion | Denial of Service | Medium | Open | | Publicly accessible Gradio app on Hugging Face could be overwhelmed by automated requests due to lack of rate limiting. | Implement request throttling and cloudflare WAF protections |
| | Unauthorized Function Access | Elevation of Privilege | High | Open | | Web application in Hugging Face zone interfaces with multiple APIs without apparent authentication between components. | Implement service-to-service authentication using JWT or mutual TLS |

## 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 |
|---|---|---|---|---|---|---|---|
| | Sensitive Document Exposure | Information Disclosure | High | Open | | about_me folder used for RAG context lacks encryption at rest and shows no access controls in trust boundary diagram. | Encrypt documents with AEAD encryption and implement file integrity monitoring |

## DEV (Actor)

Description: vMeNext Application Developer

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## 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 |
|---|---|---|---|---|---|---|---|

## 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 |
|---|---|---|---|---|---|---|---|

## iFrame https (Data Flow)

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| | Potential iFrame Clickjacking | Spoofing | Medium | Open | | iFrame embedding vMeNext chatbot crosses trust boundaries from Hugging Face zone to BlueHost zone. While HTTPS encrypted, lack of X-Frame-Options header could enable UI redress attacks. | Implement Content Security Policy frame-ancestors directive and X-Frame-Options header |

## (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 |
|---|---|---|---|---|---|---|---|

## RAG Response (Data Flow)

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## 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 |
|---|---|---|---|---|---|---|---|

## API Response (Data Flow)

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## API Request (Data Flow)

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
|  | Unvalidated AI API Inputs | Tampering | High | Open |  | API requests to OpenAI from vMeNext App traverse public network. Missing input validation could allow prompt injection attacks altering chatbot behavior. | Implement strict input validation and output encoding for AI API interactions |

## Admin Response (Data Flow)

Description: SMTP2GO Administration

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## Admin Response (Data Flow)

Description: SMTP2GO Administration

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## API Request (Data Flow)

Description: OpenAI API Request

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## API Request (Data Flow)

Description: OpenAI API Request

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## API Response (Data Flow)

Description: OpenAI API Response

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## 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 |
|---|---|---|---|---|---|---|---|

## 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 |
|---|---|---|---|---|---|---|---|
| | TLS Version Vulnerabilities | Information Disclosure | Medium | Open | | HTTPS flow between infosecotb.com and visitors crosses public network. Outdated TLS versions could expose traffic to decryption. | Enforce TLS 1.3 with modern cipher suites and HSTS headers |

## 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 |
|---|---|---|---|---|---|---|---|

## Admin Request (Data Flow)

Description: WordPress Administration

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## Admin Request (Data Flow)

Description: BlueHost Administration

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## Admin Response (Data Flow)

Description: BlueHost Administration

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# Admin Response (Data Flow)

Description: Hugging Face Administration

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# Admin Request (Data Flow)

Description: Hugging Face Administration

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# Deployment Request (Data Flow)

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| | Insecure Deployment Credentials | Elevation of Privilege | High | Open | | Deployment flow to Hugging Face uses HTTPS but lacks MFA for deployment operations, risking account takeover. | Require short-lived deployment tokens with OAuth2 client credentials flow |

# Deployment Response (Data Flow)

Description: Hugging Face Space Application Deployment

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# API Response (Data Flow)

Description: OpenAI API Response

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# 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 |
|---|---|---|---|---|---|---|---|

# vMe Next Dev (Process)

Description: Gradio ChatBot Python Application Development

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# Browser (Process)

Description: Browser used by System Administrator

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# OpenAI API (Actor)

Description: Artificial Intelligence API secured with a key

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
|  | API Key Compromise | Spoofing | High | Open |  | OpenAI API actor uses static keys stored in Hugging Face environment. Exposed keys could allow impersonation of authorized services. | Rotate keys regularly and use secret management system with RBAC |

# SMTP2GO API (Actor)

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

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
|  | Email Fraud Potential | Repudiation | Medium | Open |  | SMTP2GO API integration lacks audit trails for email sending actions, enabling plausible deniability of transactions. | Implement detailed logging with digital signatures for all email operations |

# Hugging Face Host Admin (Actor)

Description: Hugging Face Hosting Administrator Control Panel

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# Hugging Face API (Actor)

Description: Hugging Face Deployment API

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# BlueHost (Actor)

Description: Administrator access to BlueHost

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## WrodPress (Process)

Description: WordPress Content Management System

| Number | Title | Type | Severity | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|