

Introduction - Welcome to CFM

☐☐ CFM Feature Summary

CFM is a powerful system for managing threat intelligence, spam filtering, phishing protection, and reputation data — backed by automation and agent-based sync.

☐☐ Security & Threat Intelligence

- **Blocklist & Whitelist Management** (IP & domain)
 - **Reverse DNS, ASN, GeoIP, and country resolution**
 - **Keyword-based spam detection**
 - **Phishing URL detection & logging**
-

☐☐ Automation & Scheduling

- Scheduled **feed imports, auto-deletion, and rule generation**
 - Commands for IP list generation, rule updates, config sync
 - Cron-style job scheduling with overlap protection
-

☐☐ Agent Infrastructure (C++-Based)

- Syncs config and rule files
 - Reports **blocks, unblocks, and last seen**
 - Triggers service restarts after updates
 - Integrates with unblock portal for auto-removal
 - Sends **Slack alerts** for offline agents
-

☐☐ Antivirus & RBL Integration

- Generates **ClamAV signatures** from phishing URLs and file hashes (MD5/SHA1/SHA256)
 - Maintains **SpamAssassin-compatible phishing DB**
 - Exports **RBL and URIBL zones** for RBLDNSD
-

☐☐ API & External Access

- Token-authenticated API for:
 - Checking block status
 - Reporting blocks/unblocks
 - Fetching rules/feeds
 - Submitting config/trigger reports
 - Optional **rate limiting** and **IP filtering**
-

☐☐ Admin Panel (Filament)

- Dashboard with real-time widgets and charts
 - Interfaces for:
 - Spam keywords
 - Block/allow lists
 - Feed logs
 - Unblock requests
 - Agent activity
-

☐☐ Web Interface

- Public-facing **Unblock Request Form**
 - Feed endpoints (IP, domain, phishing, etc.)
 - Admin redirect and login flow
-

☐☐ Bonus Features

- File-based config sync with integrity hashing
- Config-targeting for agent groups
- Slack alerts and activity logs

- Multi-source feed support (manual, API, auto)

☐ Key Features

☐ **Blocklist & Whitelist Management**

Manage IPs and domains across multiple lists, including manual entries, feed imports, and API-reported threats.

☐ **Spam & Phishing Protection**

- Keyword-based spam filtering (supports Greek/Greeklish, loose/strict)
- Maintains a live phishing URL database
- Generates **ClamAV-compatible** virus definitions from phishing URLs and file hashes (MD5/SHA1/SHA256)

☐ **RBL & URIBL Generator**

Creates real-time blocklists and URI lists (RBLDNSD format) for DNS-based blacklisting — used by SpamAssassin, Postfix, etc.

☐ **GeoIP Intelligence for Blocklist Entries**

Automatically resolves:

- Reverse DNS (PTR)
- ASN and ISP
- Country and region This enables rich filtering, analytics, and decision-making.

☐ **Automated Feed Processing**

Processes threat feeds on a schedule with logs and rule generation.

☐ **Agent Communication & API**

Lightweight agents (or servers) can:

- Report blocked IPs back to CFM
- Fetch updates and policy
- Submit files, triggers, logs, etc.

☐ **Dashboard with Widgets & Metrics**

Summarized view of:

- Top IPs by country or source
- Phishing trends
- Recent feed activity
- System health and jobs

☐ **Unblock Request Portal**

Public-facing form for users to request delisting — reviewed via admin panel.

☐ **Full Admin UI via Filament**

Modern interface for managing:

- Spam keywords
- Feeds & logs
- Phishing database
- Block/allow lists
- Scheduled jobs
- Settings & tokens

☐ **Scheduled Jobs & Artisan Tools**

- Generate IP and domain blocklists
- Run cleanup jobs
- Sync filesystem configs
- Rebuild ClamAV signatures
- Trigger per-feed processing

☐ **Agent Infrastructure (C++ Powered)**

Includes high-performance **C++ agents** deployed on remote servers that:

- ☐ Sync configuration and rule files from CFM
- ☐ Report blocked and unblocked IPs
- ☐ Remove blocks upon updates or unblocks
- ♻️ Restart services (e.g., mail, firewall) when needed
- ☐ Report "last seen" heartbeat to monitor health
- ☐ Trigger Slack alerts if an agent goes offline
- ☐ Integrate with the public unblock form to re-allow mistakenly blocked users

☐ **Blocklist & Whitelist Management**

Manage IPs and domains across multiple lists (manual, API, or feed-driven), enriched with PTR, ASN, country, and GeolIP.

☐ **Phishing & Spam Defense**

- Greek-aware spam keyword detection (strict/loose)
- Maintains a phishing URL database
- Generates **ClamAV virus signatures** from URLs and hashes (MD5/SHA1/SHA256)
- Exports phishing data for **SpamAssassin compatibility**

☐ **RBL & URIBL Generation**

Creates and serves real-time DNS blacklists (RBLDNSD format) for both IP and domain-based blocklists.

☐ **Scheduled Feed Ingestion & Rule Generation**

Automates external feed syncing and keyword/rule building via Laravel Scheduler and Artisan commands.

☐ **Admin Dashboard**

Modern UI with dashboard widgets, charts, and management panels for:

- Blocked items
- Keyword rules
- Feed logs
- Unblock requests
- Agent status

☐ **Unblock Request Portal**

Frontend form where blocked users can request removal — triggers backend unblock workflows and agent sync.

☐ **API Interface**

Secure, token-authenticated API to:

- Check IP/domain status
- Report blocks/unblocks
- Pull feed or rule updates
- Trigger diagnostics or config checks

☐ **ClamAV + CSF Integration**

Outputs live files for:

- IP blocklists (`csf.deny`)
- ClamAV custom signatures
- RBLDNSD-based DNS lists

☐☐ **Bonus Features**

- Slack integration for agent down alerts
- Per-country analytics of blocked IPs
- Top reporters / sources breakdown
- File-based config sync and hashing
- Agent group targeting for rules

☐☐ **Use Cases**

- Internal **spam firewall**
 - Self-hosted **RBL/URIBL provider**
 - **CSF / UFW / iptables** blocklist hub
 - Aggregator for multiple **threat feeds**
 - **Email security gateway** enhancement
 - Coordinated threat response via **reporting agents**
-

Built With

- Laravel + Filament (UI)
 - MySQL (DB)
 - Tailwind (optional UI)
 - GeoLite2 (GeoIP)
 - Artisan + Laravel Scheduler
 - RBLDNSD & SpamAssassin compatibility
 - API-first design
-

Revision #1

Created 4 April 2025 18:19:22 by Chris

Updated 4 April 2025 18:23:49 by Chris