CyberDefender Security Suite

Eleven-app product and engineering brief for pitch, planning, and technical review

Suite thesis: CyberDefender is a practical desktop security portfolio: detection, credential protection, data sanitization, infrastructure visibility, hardening, threat intelligence, notifications, hidden-data handling, and incident documentation in one operator-focused ecosystem.

Executive Overview

The CyberDefender suite is built around a clear operational idea: security teams and individual operators need tools that are small enough to run locally, specific enough to solve real problems, and connected enough to support a complete defensive workflow. The eleven apps cover prevention, detection, response, documentation, and evidence preservation.

For pitch use, the suite shows product breadth and a visible roadmap for a coherent security platform. For engineering use, each app is represented as a standalone PyQt6 utility with versioned source, local-state handling, operator workflows, documentation/legal screens, and defined integration points.

Latest App Inventory

Pitch lines and deeper engineering notes are expanded in the individual app briefs below. This table is intentionally compact so the suite can be scanned quickly without splitting rows across pages.

App	Latest	Suite role
CyberDefender Anti-Phishing Suite	1.0.45	URL, file, and phishing intelligence
CyberDefender Data Sanitizer	1.0.88	Data cleanup, secure erase, and privacy operations
CyberDefender Password Manager	1.0.88	Credential vault and access control
CyberDefender AntiVirus Pro	V3.0.55	Endpoint scanning, monitoring, and containment
CyberDefender Hidden Image	1.0.36	Steganography, hidden data, and file encryption
CyberDefender Infrastructure Guard	1.0.35	Network asset visibility and response
CyberDefender Notifier	Version 15	Notification scheduling and API result capture
CyberDefender Security News Scraper	1.0.31	Threat intelligence collection and IoC export
CyberDefender Fortify	1.0.21	System hardening and posture audit
CyberDefender Incident Response Tool	1.0.30	Incident tracking, evidence, standards, and reporting
CyberDefender IronWall	1.0.18	Real-time active defense across network, web, password, and AD attack surfaces

How The Apps Work Together

The suite is strongest when presented as a defensive workflow rather than eleven unrelated utilities. News Scraper collects external security signals and exports IoCs. Anti-Phish and AntiVirus Pro use local detection and optional reputation checks. Infrastructure Guard shows what exists on the network. Fortify checks whether the host platform is hardened. Password Manager protects credentials. Data Sanitizer removes sensitive data and produces proof. CyberDefender Hidden Image handles hidden or encrypted data workflows. Notifier captures scheduled or API-driven status output. IronWall adds a real-time active defense layer across network, web, password, and AD attack surfaces. Incident Response turns all of that activity into structured case records.

Lifecycle layer	Apps	Operational value
Intelligence	Security News Scraper	Collects news, CVSS context, IoCs, bookmarks, and exports feeds.
Prevention	Password Manager, Fortify, Data Sanitizer, IronWall	Reduces credential risk, hardens the endpoint, removes sensitive data exposure, and actively defends against live attack behavior.
Detection	Anti-Phish, AntiVirus Pro, Infrastructure Guard	Finds suspicious URLs, malware signals, endpoint changes, and unknown infrastructure.
Response	AntiVirus Pro, Infrastructure Guard, Incident Response	Quarantines, isolates, documents, and tracks response activity.
Evidence	Notifier, Data Sanitizer, Incident Response	Captures output, certificates, reports, timelines, standards, and exportable records.

App Briefs

1. CyberDefender Anti-Phishing Suite (1.0.45)

Latest source: Anti-Phish\CybAntiPhishv45.py

Pitch line: Stops link-based attacks before they become credential theft, malware delivery, or business email compromise.

What it does: A focused phishing-defense application for checking suspicious links and files, reviewing scan logs, using local heuristics, optional VirusTotal enrichment, AI assistance, model training, and threat-feed input from the News Scraper.

Why it exists: Phishing is usually the first step in a compromise. This app gives an operator a fast, repeatable way to inspect risky URLs, capture verdicts, and build evidence without relying on a browser alone.

Expected workflows

- Scan a URL or suspicious input and receive a clear safe, submitted, or phishing-oriented verdict.
- Use optional VirusTotal API settings and controlled file-upload consent for deeper reputation checks.

- Review scan logs, print reports, export PDF evidence, and feed new samples into training and visualization workflows.
- Consume threat-feed data exported by the CyberDefender Security News Scraper.

Engineering notes

- PyQt6 desktop UI with QThread workers for startup, scanning, training, visualization, VirusTotal upload, and AI requests.
- Combines deterministic URL heuristics, model-backed classification assets, optional external reputation lookup, and user-managed logs.
- Includes EULA, privacy, documentation, print/PDF, API settings, and support menu patterns used across the suite.

2. CyberDefender Data Sanitizer (1.0.88)

Latest source: CyberDefender Data Sanitizer\CybdSanitizerV88.py

Pitch line: Turns data cleanup into a defensible workflow with secure erase, certificates, model-card documentation, and operator evidence.

What it does: A multi-tab privacy and secure-deletion tool covering dashboard metrics, data sanitization, secure erase, model-card generation, AI chat, network operations, and common cyber utilities.

Why it exists: Organizations need proof that sensitive material was scrubbed or destroyed. The app gives that process structure: target selection, execution, reporting, and certificate-style documentation.

Expected workflows

- Load raw data, run a scrub protocol, format cleaned output to JSONL, and save or copy sanitized results.
- Select files or folders for secure deletion and issue a certificate after the destruction workflow.
- Run privacy cleanup tasks such as recycle-bin emptying, temp-folder cleanup, shadow-copy deletion, hibernation disablement, and pagefile encryption.
- Use supporting tools for hashing, Base64 conversion, password generation, OTP key generation, network checks, and AI-assisted review.

Engineering notes

- PyQt6 QMainWindow with dedicated tabs: Dashboard, Data Sanitizer, Secure Erase, Model Card, AI Chat, Network Ops, Cyber Tools, and Settings.
- Uses worker tasks for long-running operations so UI actions can show progress and maintain operator control.
- Includes local configuration, documentation, library import/read mode, AI engine settings, print/PDF support, and license/privacy controls.

3. CyberDefender Password Manager (1.0.88)

Latest source: PasswordMgr\CybPasswordMgrv88.py

Pitch line: Protects credentials with a local vault experience that supports strong generation, review, lock controls, MFA, recovery, and secure documents.

What it does: A standalone password vault for storing, generating, searching, backing up, restoring, importing, and reviewing password records, with a secure document import area and user manual support.

Why it exists: Credentials remain one of the highest-value targets. This app concentrates password storage and review into a controlled local utility instead of scattered files, browser exports, and reused weak passwords.

Expected workflows

- Add, edit, delete, search, copy, and reveal credentials through the vault UI.
- Generate strong passwords with policy and entropy guidance, including a minimum entropy target and character-class requirements.
- Use master-password controls, auto-lock settings, 2FA codes, recovery codes, and FIDO2/security-key registration flows.
- Import documents into a secure vault area and use backup, restore, CSV import, and security review actions.

Engineering notes

- PyQt6 QMainWindow with security-oriented dialogs for lock/unlock, master password setup, MFA, recovery codes, security-key registration, and vault actions.
- Uses worker threads for FIDO2 login and registration, plus structured menus for file, edit, security, documentation, AI, and support workflows.
- Built for standalone operation with local configuration, EULA/privacy state, documentation, print/manual workflows, and export/import controls.

4. CyberDefender AntiVirus Pro (V3.0.55)

Latest source: CyberDefender-AntiVirus\CyberDefender-AntiVirusV3.0.55.py

Pitch line: Anchors the suite with endpoint malware scanning, real-time watching, quarantine, firewall controls, ransomware indicators, and tamper protection.

What it does: A full endpoint security application with scan engine, secondary scanner, VirusTotal support, real-time watcher, ransomware indicators, registry persistence monitoring, process baselining, traffic controls, firewall integration, quarantine, exclusions, and scheduled scans.

Why it exists: The suite needs a central protection layer that can detect, isolate, record, and respond to endpoint threats. AntiVirus Pro provides that core security surface for files, processes, network behavior, and ransomware-style activity.

Expected workflows

- Run manual or scheduled scans and route suspicious results into quarantine or reporting.
- Use real-time monitoring, ransomware IoC monitoring, registry persistence monitoring, process baselines, first-seen connection detection, and RDP brute-force monitoring.

- Configure VirusTotal, exclusions, advanced traffic control, Windows firewall bridge, tamper protection, and OTP/MFA settings.
- Review logs, documentation, license state, scan results, and recover or permanently delete quarantined items.

Engineering notes

- Large PyQt6 application with dedicated worker threads for scanning, definition updates, packet interception, network isolation, firewall emergency actions, and monitoring.
- Implements settings integrity concepts including tamper keys, audit events, versioned baselines, and protected configuration flows.
- Combines local detection, reputation services, quarantine state, firewall commands, network snapshots, and user-facing reporting.

5. CyberDefender Hidden Image (1.0.36)

Latest source: Hidden Image application source

Pitch line: Gives the suite a covert-data and privacy tool for hiding, revealing, encrypting, and controlling sensitive information.

What it does: A hidden-data utility for image steganography, text steganography, emoji encoding, hidden folders, honeypot monitoring, RSA-4096 file encryption, OTP provisioning, and master-password protection.

Why it exists: Some security workflows require private transport, controlled disclosure, or investigation of hidden payloads. CyberDefender Hidden Image provides practical tools for concealment, discovery, and encrypted handling of sensitive files.

Expected workflows

- Create or extract hidden image payloads and hidden ZIP content.
- Generate RSA-4096 keys, encrypt files, and decrypt files through the crypto engine.
- Use emoji and zero-width text steganography tools to encode or reveal hidden messages.
- Manage hidden folders, honeypot monitoring, master-password settings, OTP provisioning, documentation, legal status, and Windows integration.

Engineering notes

- PyQt6 app with worker objects for secret-image creation, hidden-ZIP extraction, RSA operations, and honeypot monitoring.
- Includes separate dialogs for crypto, documentation, legal documents, OTP, emoji encoding, text steganography, hidden folder and honeypot management, and about/status views.
- Uses local configuration and layered utility dialogs rather than a cloud service dependency.

6. CyberDefender Infrastructure Guard (1.0.35)

Latest source: CyberDefender Infrastructure Guard\CIGV1.0.35.py

Pitch line: Maps infrastructure, highlights risky devices, and gives operators response actions such as isolation, quarantine, automation, and lockdown.

What it does: A network and infrastructure monitoring tool for scanning devices, visualizing topology, managing asset labels and criticality, exporting reports, and driving response actions.

Why it exists: Teams cannot defend assets they cannot see. Infrastructure Guard creates a desktop view of the environment and turns discoveries into actionable operations for known, unknown, critical, or suspicious devices.

Expected workflows

- Scan the network, review asset results, and export findings.
- Refresh topology views, zoom or pop out the network map, and inspect device relationships.
- Mark devices with nicknames, tags, known status, and critical status.
- Use response controls for isolate, quarantine, auto response, and lockdown.

Engineering notes

- PyQt6 QMainWindow with NetworkScanner QThread, topology graphics items, zoomable topology view, and report/documentation dialogs.
- Uses local state for scan records, app settings, legal acceptance, and visual topology data.
- Designed as an operational dashboard rather than a passive report generator.

7. CyberDefender Notifier (Version 15)

Latest source: Notifier App\CybNotiAppv15.py

Pitch line: Provides a compact operator tool for scheduling notification runs, calling APIs, and preserving returned results as evidence.

What it does: A small desktop notification and results-capture utility for choosing schedule details, saving API keys/base URLs, running notification checks, displaying returned output, and exporting or printing the results.

Why it exists: Simple operational checks often become scattered across browser tabs, notes, and screenshots. Notifier gives those checks a consistent schedule, result log, and export workflow.

Expected workflows

- Select weekday, calendar date, hour, minute, and AM/PM/UTC, then run Schedule Now.
- Save and manage API keys or base URLs in an app-local api_keys.json file.
- Call saved endpoints or a default public API sample and write output or errors into the Results panel.
- Export or print result evidence as PDF, Excel, Word, Markdown, or printer output.

Engineering notes

- Focused PyQt6 QMainWindow with schedule controls, results QTextEdit, API-key management dialogs, and documentation/print support.

- Uses local JSON key storage and explicit endpoint construction rather than a background service architecture.
- Includes SMS action placeholder behavior so the UI can support future provider integration.

8. CyberDefender Security News Scraper (1.0.31)

Latest source: CyberNews\CyberNewsV31.py

Pitch line: Turns cybersecurity news into usable threat intelligence by tracking articles, extracting IoCs, and feeding the rest of the suite.

What it does: A security news collection tool for RSS and web-scraping modes, article database storage, CVSS lookup, bookmarking/read state, notifications, CSV export, and IoC export into threat-feed paths.

Why it exists: Threat intelligence is useful only when it becomes searchable, exportable, and connected to action. This app converts incoming security news into operator-readable articles and IoCs that other CyberDefender apps can consume.

Expected workflows

- Refresh RSS feeds or use web scraping mode for configured sources.
- Open, bookmark, mark read, search, export CSV, and auto-refresh article data.
- Extract indicators of compromise and export them to Anti-Phish and AntiVirus feed paths.
- Manage feeds, refresh intervals, notification settings, article database state, and IoC export logs.

Engineering notes

- PyQt6 QMainWindow backed by an ArticleDB, RSS fetch worker, web scrape worker, CVSS lookup worker, and HTML link extractor.
- Includes settings dialogs for RSS feeds, auto-refresh, CSV folder, IoC export paths, and database clearing.
- Designed as a bridge between news collection and operational detection workflows.

9. CyberDefender Fortify (1.0.21)

Latest source: CybeFortify\CybFortV1.0.21.py

Pitch line: Shows whether the workstation is hardened at boot, firmware, OS, hardware, and supply-chain layers before attackers exploit weak configuration.

What it does: A hardening audit tool that checks Secure Boot, TPM, BIOS/UEFI version, OS integrity, hardware hardening, boot-loader defense, driver signing, firmware integrity, and full audit results.

Why it exists: Malware defense is weaker when the platform itself is misconfigured. Fortify gives operators a quick hardening posture view and makes platform risks visible before they become incident conditions.

Expected workflows

- Run individual checks from hardening cards or run a full audit.
- Review result dialogs for Secure Boot, TPM, BIOS/UEFI, OS integrity, hardware hardening, boot loader, supply chain/driver signing, and firmware integrity.

- Open previous audits, scan logs, documentation, privacy/EULA screens, and settings.
- Use score gauges and audit summaries to communicate posture quickly.

Engineering notes

- PyQt6 application with HardenCard components, result dialogs, ScoreGauge, AuditWorker QThread, previous-audit storage, and documentation/print support.
- Uses Windows system query patterns such as TPM, BIOS, and Device Guard inspection through local commands.
- Complements AntiVirus by focusing on platform posture rather than file-level malware results.

10. CyberDefender Incident Response Tool (1.0.30)

Latest source: Incident Response Tool\CybIRTV1.0.30.py

Pitch line: Turns security events into organized response records with timeline, evidence, status, notes, standards mapping, and exportable reports.

What it does: An incident-management desktop tool for creating incidents, tracking evidence, adding timeline events, updating status, mapping standards, and exporting incident reports.

Why it exists: Detection alone is not enough; teams need a record of what happened, when it happened, what evidence was collected, and which response steps were taken. This app gives that process structure and documentation.

Expected workflows

- Create, open, save, edit, delete, copy, and export incident records.
- Add timeline events, attach evidence, update status, and review selected incident details.
- Use tabs for overview, timeline, evidence, standards, and notes.
- Select standards for incidents, generate standards summary reports, open source guidance, and print compliance guides.

Engineering notes

- PyQt6 QMainWindow with incident, evidence, timeline, standards selection, standards report, source, and manual dialogs.
- Includes local save/open flows, sample data controls, launch/full-screen window modes, documentation, import files, AI, support, legal, and privacy menus.
- Completes the suite's lifecycle by converting detections and intelligence into response documentation.

11. CyberDefender IronWall (1.0.18)

Latest source: IronWall\IronWallV1_0_18.py

Pitch line: An active defense layer that watches network, web, password, and Active Directory attack behavior in real time and responds with alerts, blocks, and recorded evidence.

What it does: A PyQt6 active defense application covering Network Defense, Web App Defense, Password Defense, and Windows/AD Defense, with a Threat Coverage Matrix mapping each defense

family to the offensive tools and behaviors it addresses, plus a live event log, documentation, and an attack simulation test mode.

Why it exists: Most of the suite detects and documents after the fact. IronWall gives the operator a live, behavior-based active defense layer that recognizes the shared signatures of common offensive tooling, such as scanners, password sprayers, relay attacks, and AD recon and exploitation tools, and reacts while the activity is happening.

Expected workflows

- Monitor the Dashboard for overall status, then drill into Network, Web App, Password, or Windows/AD Defense tabs for category-specific detail.
- Review the Threat Coverage Matrix to see which tool families and behaviors map to each defense category, including detection source and block action.
- Use Simulate Attack test mode to verify alerts and detection wiring without running real offensive tools.
- Review the Live Log for real-time events, export or print log evidence, and consult the Documentation and About tabs for guidance and license details.

Engineering notes

- PyQt6 QMainWindow with Dashboard, Coverage Matrix, Network Defense, Web App Defense, Password Defense, Windows/AD, Live Log, Documentation, and About tabs, plus a system tray icon for status alerts.
- Maintains a TOOL_SIGNATURES catalog mapping defense categories to process names, command-line markers, default ports, user agents, URL patterns, and Windows Security event IDs (including 4625, 4740, 4662, 4768, 4769, 4624, 4688, 7045) for tools such as SQLMap, Nuclei, Nmap, Responder, Hydra, BloodHound, Mimikatz, Rubeus, and common C2 frameworks.
- Includes a Microsoft-protected process and address-space allowlist so containment actions do not block legitimate Microsoft 365, Azure, Edge, Teams, and Windows Update traffic, plus PDF documentation export, live log export and print, and license/EULA handling consistent with the rest of the suite.

Engineering Framing

The eleven apps share a common engineering posture: local desktop execution, explicit versioned builds, PyQt6 interfaces, worker-thread patterns for long operations, exportable evidence, documentation/help dialogs, license/privacy handling, and operator-first controls. This is useful for staged productization because each app can remain standalone while sharing support conventions, legal screens, iconography, and integration paths.

Near-Term Productization Priorities

- Normalize shared Help, EULA, Privacy, About, print/PDF, support, and AI menu patterns across all eleven apps.
- Create a common suite launcher that detects the highest-numbered build of each app and displays version, status, and source folder.
- Standardize local storage locations, export naming, audit logs, and report metadata so evidence from every app can be attached to Incident Response records.
- Define integration contracts: News Scraper to Anti-Phish/AntiVirus feed paths, AntiVirus and Infrastructure Guard alerts to Incident Response, Data Sanitizer certificates to Incident Response evidence.
- Keep the apps independent for resilience, but align branding, update flow, licensing state, and documentation so the suite feels like one product.

Pitch Deck Takeaway

Investor-ready message: CyberDefender is not a single feature. It is a portfolio of eleven working security utilities that cover the defensive lifecycle from threat intelligence and phishing review through endpoint protection, infrastructure visibility, hardening, credential protection, data sanitization, hidden-data handling, notification capture, and incident response documentation, with IronWall adding real-time active defense.

Source Boundary Used For This Document

Authorized source directory: C:\Users\tarap\OneDrive\desktop\Stand-Alone CyberiApps

Versioning rule used: the brief uses the highest-numbered/current source version found for each of the eleven apps in the authorized CyberiApps suite tree.