X'EYE

AI-POWERED CYBER SECURITY & SURVEILLANCE SYSTEM

System Documentation & Commercial Brief

Facial Recognition · Weapon & Threat Detection · Multi-Site Surveillance · Emergency Response

PROTECT • DETECT • MONITOR • ALERT

Developed by **ANABA** • stelnex.com • +233 55 563 3900

Version 1.0 | 2026 | Confidential — for evaluation & procurement

1 Executive Summary

X'EYE is an end-to-end, AI-powered surveillance and emergency-response platform built for law-enforcement and high-security environments. It turns ordinary IP and USB cameras into an intelligent watch network that recognises persons of interest, detects weapons and violent incidents, and routes every event to a central command console in real time — securely, and even across many separate sites.

What it does

Continuously analyses camera feeds for watchlisted faces, weapons (guns/knives), fights, loitering and crowding — and raises a typed, reviewable alert with evidence the moment something happens.

Who it is for

Police & national security, airports & ports, banks, campuses, malls, casinos, critical infrastructure, government buildings, gated estates and event venues.

How it is deployed

A lightweight agent runs at each facility; a hardened API server (Windows, Linux, Docker or cloud) is the hub; commanders use a desktop console at HQ. Sites stay protected even if the network or HQ goes down.

Why it is different

Multi-tenant by design, fully encrypted, tamper-resistant, works offline-first, and ships an on-device AI assistant (STELLA) — with no per-frame cloud costs and no exposure of camera credentials.

Headline capabilities

Watchlist face recognition · Weapon detection (YOLO) · Fight / altercation detection · Loitering & crowd analytics · Silent panic button · Unified typed alert feed · Secure live feed relay · STELLA AI coworker · SMS notifications · Facility maps · Evidence packaging · Continuous recording · PTZ control · Multi-company tenancy · Tamper resistance · Hash-chained audit log

2 System Overview

Traditional CCTV records everything and helps after the fact. X'EYE is **proactive**: it watches every frame with AI and acts in seconds — sounding alarms, texting responders, capturing court-ready evidence, and showing commanders exactly what is happening and where.

Three cooperating tiers

Facility Client
Runs at each site. Owns the cameras, runs AI locally, queues when offline, presses panic.

→

X'EYE Server
Hardened API hub. Verifies, stores alerts & evidence, enforces tenancy & policy.

→

HQ Console
Command center. Review alerts, watch live feeds, manage watchlists, dispatch.

Tier	Role	Runs on
Facility Client (agent)	Discovers & runs the site's cameras; performs face, weapon and fight detection; uploads signed detections & snapshots; offline queue; floating panic button; tamper-resistant.	Windows PC at each site (background / system tray)
X'EYE Server API	Authenticates every request, stores alerts/evidence, manages companies & licenses, relays permissioned live feeds, serves the HQ console.	Windows, Linux, Docker, or cloud (VPS / Railway / Hostinger)
HQ Command Console	Operator desktop: dashboard, alert review, live monitoring wall, maps, panic board, STELLA assistant, settings.	Windows desktop at the operations center

Technology stack

AI / VISION
SCRFD + ArcFace face recognition, YOLOv8 weapon detection, motion-energy fight detection, anti-spoof liveness — all via ONNX Runtime, on-device.

PLATFORM
.NET 10, C#, WPF desktop, ASP.NET Core minimal API, OpenCV, SQLite + Dapper.

ASSISTANT
STELLA — an operations coworker that answers from live data, with a secure on-device mode (no cloud credits needed).

3 Core Features in Depth

3.1 Watchlist facial recognition

Operators enroll persons of interest (wanted, missing, banned) with reference photos and case details. Every camera frame is scanned; matches are scored 0–100 (a *trust score*) and banded **Medium / High / Critical**. A confirmed face raises an alert with the snapshot, camera, time and a side-by-side comparison. An optional AI second opinion can confirm a match.

3.2 Weapon detection

A YOLO object-detection engine flags firearms and knives in real time. Detections must clear a high confidence bar and persist across several frames before they escalate — eliminating single-frame false alarms. No model loaded means the feature stays dormant; it never invents a detection.

3.3 Fight / altercation detection

Because a fight is an *action over time*, X'EYE measures violent motion energy across frames and flags a **possible altercation** when intense movement is sustained — with tunable sensitivity. Needs no special model.

3.4 Behavioural analytics

Loitering (a subject lingering too long) and crowd density (too many people, too fast) are detected and surfaced as their own alert types for early situational awareness.

3.5 Unified, typed alert feed

All threats land in one reviewable feed, each tagged by **type** with a colour-coded chip so an operator knows instantly what tripped it:

WEAPON FIGHT WANTED / MISSING (watchlist) LOITERING CROWD

Filter by type or status, search, review (confirm / dismiss / escalate / false-positive), and export a court-ready evidence package — every action written to a tamper-evident audit log.

3.6 Silent panic button & emergency response

A floating, always-on-top panic button lets on-site staff raise a silent duress alert with one click; enabled cameras snapshot automatically and the alert reaches HQ even across the internet. A short, silent cancel window guards against false presses.

3.7 Secure live feed relay

When a commander needs eyes on a remote camera — and the site permits it — the client streams JPEG frames up the encrypted channel and HQ views them live. **The camera's address and credentials never leave the site**, every frame is individually signed, and the session is time-limited and token-gated.

STELLA AI coworker

Ask plain-English questions about alerts, panics, cameras and companies; STELLA answers from

SMS notifications

Critical matches, weapons, fights and panics text the response team instantly (Arkesel gateway), rate-limited and audited.

Facility maps

Upload floor plans per company and place cameras with labels; zoom, pan and scale to hundreds of cameras.

live data, with a secure offline mode.

Evidence management

One-click export of snapshot + metadata + SHA-256 hash for chain-of-custody integrity.

Continuous recording

Optional watermarked recording with rotation and storage caps (oldest evicted first).

PTZ control

Pan/tilt/zoom ONVIF cameras directly from the live tile.

4 How It Operates

The detection pipeline is the same whether a camera is at HQ or at a remote facility:

1. Capture
Camera frame grabbed locally (USB or ONVIF/RTSP).

→

2. Analyse
Face, weapon & motion AI run on-device.

→

3. Sign
Hit + snapshot HMAC-signed with the site license.

→

4. Server
Verifies & stores as a typed Alert.

→

5. Review
HQ sees it, acts, exports evidence.

If the network drops, the client **queues detections encrypted on disk** and uploads them when the link returns — nothing is lost. The site keeps monitoring even when HQ or the server is offline.

Live-feed flow (permissioned)

HQ requests
Commander asks for camera X (Supervisor+).

→

Server authorises
Checks the company's "allow live feed" switch; issues a one-time session token + nonce.

→

Client pushes
Streams signed JPEG frames — no URL/creds leave site.

→

HQ watches
Pulls frames with its viewer token; session auto-expires.

5 Security & Privacy

Encryption everywhere

Face embeddings, camera credentials and evidence are AES-256-GCM encrypted at rest; keys are wrapped with Windows DPAPI (or a protected key file on Linux).

Signed, tenant-scoped sync

Every client–server message carries an HMAC signature, timestamp and replay-nonce, scoped to the site's license key. Tampered or replayed requests are rejected.

No credentials exposed

Camera RTSP URLs and passwords never leave the facility — not in detections, not in live feed. Only JPEG pixels are transmitted.

Tamper-evident audit log

Every review, export and configuration change is recorded in a hash-chained audit trail that detects alteration.

Access & tamper control

Role-based access (Viewer→Administrator); password-gated exit and camera management; an optional watchdog relaunches the facility agent if it is killed.

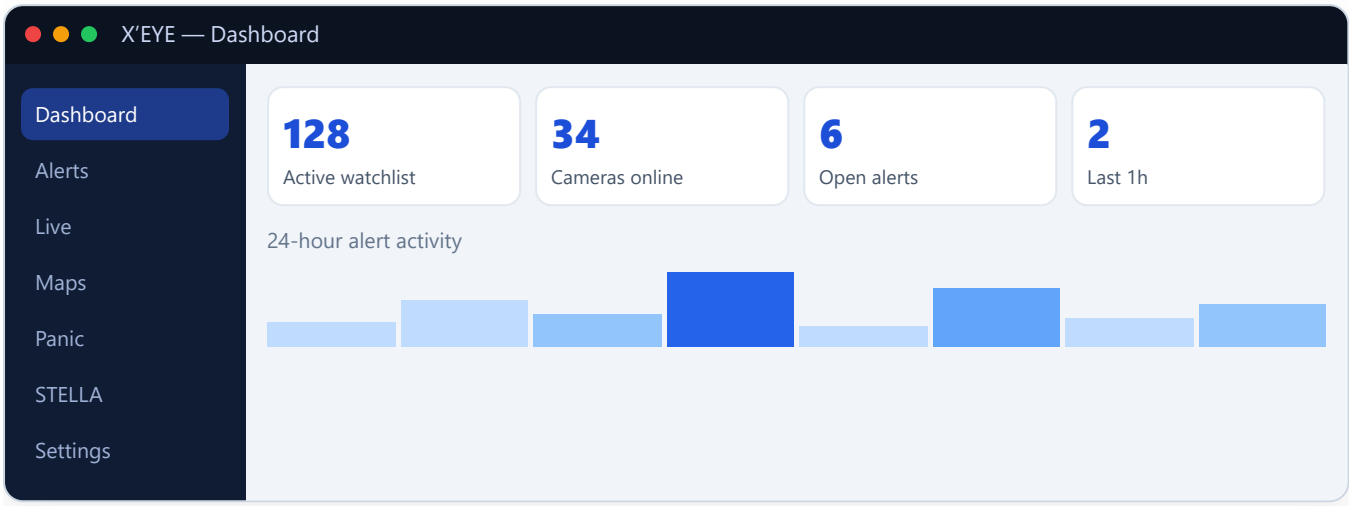
Privacy by design

Biometric data is encrypted and never shared with third parties for matching. Retention limits purge old data automatically.

Privacy note for this document: any real captured face snapshots shown in screenshots should be **blurred** before sharing externally. The interface previews on the next page use blurred / synthetic placeholders for exactly this reason.

6 Interface Overview

Representative previews of the HQ console (layouts reflect the shipping application; captured face images are blurred for privacy).

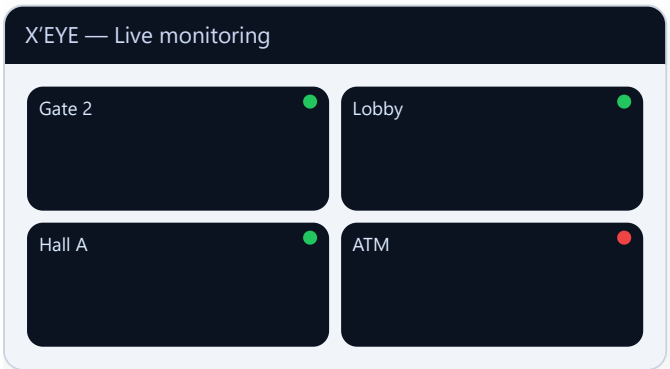


Dashboard — live KPIs, a clickable 24-hour alert histogram, camera health and recent activity.

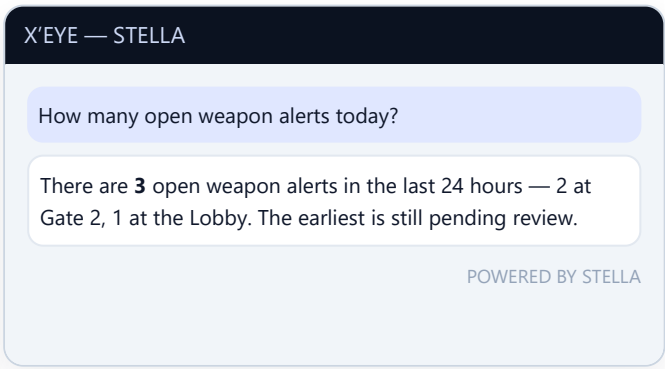
X'EYE — Alerts

Snapshot	Type	Subject	Camera	Severity	Status
	Weapon	pistol	Gate 2	91/100	Pending
	Fight	Possible altercation	Lobby	78/100	Pending
	Wanted	J. Mensah	Hall A	88/100	Under review
	Loitering	Loitering 42s	ATM	50/100	Pending

Unified Alerts feed — every threat type in one place, colour-coded, searchable and filterable. Face snapshots blurred for privacy.



Responsive camera wall with search, online/offline status & fullscreen.



STELLA answers from live console data — on-device, no cloud credits.

7 Where X'EYE Is Useful

Law enforcement & national security
City-wide watchlist hits, wanted/missing persons, multi-station command, court-ready evidence.

Airports, ports & borders
Person-of-interest screening, weapon detection at checkpoints, crowd management.

Banks & financial
ATM & branch monitoring, silent duress panic, robbery weapon alerts, after-hours loitering.

Campuses & schools
Weapon & fight detection, banned-person alerts, rapid lockdown signalling.

Malls & retail
Known-shoplifter watchlists, fight detection, crowd density, multi-store tenancy.

Critical infrastructure
Power, water, telecom & data centers — perimeter intrusion, loitering, intruder alerts.

Government buildings
Access screening, VIP protection, panic response, full audit trail.

Casinos & hospitality
Banned-patron recognition, altercation detection, incident evidence.

Estates, events & mines
Gated communities, stadiums, concerts and remote mine sites with offline-tolerant agents.

8 Setup & Deployment Configuration

8.1 Requirements

Component	Minimum	Recommended
Facility Client PC	Windows 10/11, 4-core CPU, 8 GB RAM, .NET 10 runtime	6-core CPU, 16 GB RAM, SSD; a GPU helps with many cameras
Server	2 vCPU, 4 GB RAM, Windows/Linux or Docker	4 vCPU, 8–16 GB RAM, HTTPS certificate, daily backups
HQ Console PC	Windows 10/11, 8 GB RAM	16 GB RAM, dual monitors for the video wall
Cameras	USB webcams or ONVIF/RTSP IP cameras	IP cameras (PoE), 1080p, on a dedicated VLAN

8.2 Server deployment options

- **Cloud VPS** (Hostinger / DigitalOcean / AWS) — the recommended production path with a real HTTPS domain (e.g. *anaba.com*).
- **Docker / Railway** — a container image is provided; binds to `$PORT`, honours forwarded headers behind a TLS proxy.
- **On-premise** — Windows Service or Linux host inside the customer's network for fully air-gapped operation.

> **Security toggles:** HTTPS is required in production (`Fras:RequireHttps=true`); the HQ console authenticates with a 32+ character API key (`Fras:HqApiKey`); the master key path and database path are configurable for hardened or clustered installs.

8.3 First-run configuration checklist

1. Stand up the server (HTTPS domain or proxy) and set the HQ API key.
2. Register each company/site and issue its license key.
3. Install the Facility Client on each site PC; on first run enter the **license**, the **server URL** and an **admin password**.
4. In the Client's (password-gated) Camera Manager, scan the network (ONVIF) or add USB cameras — they sync to the server automatically.
5. On the HQ console, configure the API base URL + key (Settings → Integrations), enroll the watchlist, and optionally add SMS (Arkesel) and the AI assistant key.
6. Enable per-company options as needed: live feed, continuous recording, threat-detection models.

The Facility Client runs continuously in the system tray, survives reboots, and can only be closed with the admin password.

9 Indicative Pricing

X'EYE is licensed per deployment tier, with optional per-camera capacity, annual support & updates, and managed hosting. Figures below are **indicative starting estimates** to frame a quotation; final pricing depends on camera count, number of sites, support level, customisation and procurement model.

9.1 Ghana — local market (GH¢ / Cedis)

Edition	Scope	License (one-time)	Annual support	Or SaaS / month
Starter	1 site, up to 8 cameras, core recognition + alerts + panic	GH¢ 45,000	GH¢ 9,000	GH¢ 2,200
Professional	Up to 5 sites, 40 cameras, + weapon/fight, live feed, maps, STELLA	GH¢ 180,000	GH¢ 36,000	GH¢ 7,500
Enterprise / Gov	Unlimited sites & cameras, full suite, on-prem/private cloud, SLA, training	from GH¢ 650,000	GH¢ 130,000	by tender

Add-ons: extra camera capacity ~GH¢ 1,800/camera (one-time) · managed cloud hosting ~GH¢ 1,500/month · on-site installation & training quoted separately.

9.2 United States (USD)

Edition	License (one-time)	Annual support	Or SaaS / month	Per camera
Starter	$6,500	$1,300	$300	$250
Professional	$24,000	$4,800	$1,200	$220
Enterprise / Gov	from $85,000	$17,000	custom	$180

U.S. pricing reflects higher support expectations, compliance and integration services. Government/large enterprise typically procured as a multi-year contract.

9.3 International market (USD)

Edition	License (one-time)	Annual support	Or SaaS / month	Per camera
Starter	$5,000	$1,000	$220	$180
Professional	$18,000	$3,600	$850	$160
Enterprise / Gov	from $65,000	$13,000	custom	$140

What drives the price: number of cameras and sites; live-feed & recording usage; on-prem vs managed hosting; SLA & 24/7 support; integrations (access control, body-cams, national databases); training and on-site commissioning.
Context: comparable commercial face-recognition VMS platforms commonly run US $200–$1,000 per camera plus annual licensing — X'EYE is positioned competitively while bundling weapon/fight detection, panic and an AI assistant that are usually paid add-ons.

Note: currency conversions assume roughly US$1 ≈ GH¢15 (2026, approximate). All amounts are pre-tax estimates for proposal-building, not a binding quotation.

10 Summary

X’EYE delivers a complete, secure, multi-site intelligent surveillance and emergency-response platform: it sees threats other systems miss, acts in seconds, protects privacy and credentials by design, and scales from a single shop to a national deployment — all from one command console with an AI coworker at the operator’s side.

Proactive, not just recorded
AI on every frame: faces, weapons, fights, behaviour.

Resilient & secure
Offline-first, encrypted, signed, tamper-resistant, fully audited.

Multi-site by design
One server, many facilities, strict tenant isolation.

Lower cost of ownership
On-device AI, no per-frame cloud fees, bundled capabilities.

DEVELOPER & CONTACT

ANABA

Website **stelnex.com** · Tel **+233 55 563 3900**

X’EYE — AI-POWERED CYBER SECURITY & SURVEILLANCE SYSTEM