Risk Platform

User Manual

Home Network Security Assessment & Risk Management

February 2026

Risk Platform — User Manual

Table of Contents

1. Requirements & Installation

System Requirements

Component	Requirement
OS	Windows 10/11, Linux, or macOS
Python	3.12+
Node.js	20+
Docker	Docker Desktop (for frontend)

Component	Requirement
Nmap	Installed and on PATH
RAM	4 GB minimum
Disk	1 GB free

Optional

Component	Purpose
Ollama	Local AI for Copilot and Threat Intel briefs (recommended: `llama3.2`)
OpenAI-compatible API	Alternative AI provider

Installation

1. Clone the repository:

```
git clone <repo-url> D:\Risk-App3.0
cd D:\Risk-App3.0
```

2. Configure environment:

```
cp .env.example .env
```

Edit `.env` — all variables use the `RISK_` prefix:

```
# Core
RISK_DEBUG=true
RISK_DATABASE_URL=sqlite+aiosqlite:///data/risk_platform.db
RISK_DATA_DIR=data
RISK_CONFIG_DIR=config
RISK_ARTIFACTS_DIR=data/artifacts

# CORS (match your frontend URL)
RISK_CORS_ORIGINS=["http://localhost:3000","http://localhost:5173"]

# AI (optional — leave blank to disable AI features)
RISK_AI_PROVIDER=ollama
RISK_AI_BASE_URL=http://localhost:11434
RISK_AI_MODEL=llama3.2
RISK_AI_API_KEY=

# Scanner
RISK_DEFAULT_SCAN_RATE=100
RISK_SCAN_TIMEOUT=300
```

3. Start the backend:

```
cd backend
pip install -r requirements.txt
uvicorn app.main:app --host 0.0.0.0 --port 8000 --reload
```

The database (`data/risk_platform.db`) is created automatically on first start.

4. Start the frontend (Docker):

```
cd ..
docker-compose up -d --build
```

This builds the React app and serves it via nginx on port 3000.

5. Open the browser:

Navigate to `http://localhost:3000`. You should see the Dashboard.

6. (Optional) Start Ollama for AI features:

```
ollama serve
ollama pull llama3.2
```

Verify AI connectivity in **Settings > AI Configuration > Test Connection**.

2. First Launch

On first launch the database is empty. The recommended first step:

1. Go to **Workflow** (`/workflow`)
2. Enter your home subnet (e.g. `192.168.178.0/24`)
3. Click **Start Pipeline**
4. Wait for all 8 steps to complete

This single action populates the entire platform: assets, findings, threats, risks, MITRE mappings, and a drift baseline.

---

3. Dashboard

Route: `/dashboard`

The dashboard shows your security posture at a glance:

- **4 stat cards:** Total Assets, Findings, Risks, Threats
- **Findings by Severity:** Click any severity badge to see all findings of that level
- **Risk Distribution:** Breakdown by risk level (critical/high/medium/low)
- **Quick Actions:**
- *Start Scan* — jump to the Workflow page
- *AI Triage* — jump to the AI Copilot
- *Generate Report* — jump to Reports
- **Recent Findings:** The 5 latest discoveries

---

4. Workflow — Running a Full Assessment

Route: `/workflow`

The Workflow page runs the complete 8-step security assessment pipeline.

How to use

1. Enter a subnet in CIDR notation (e.g. `192.168.178.0/24`)
2. Click **Start Pipeline**
3. Watch the 8 steps execute in real-time:

Step	What it does
1. Asset Discovery	Enumerates hosts on the network via ARP/nmap
2. Fingerprinting	Identifies services, OS, and versions on each host
3. Threat Modeling	Generates STRIDE threats per zone and trust boundary
4. Vulnerability Scanning	Runs HTTP, TLS, SSH, DNS, credential checks on each asset
5. Exploit Analysis	Assesses which findings are actively exploitable
6. MITRE Mapping	Links findings and threats to ATT&CK techniques
7. Risk Analysis	Calculates risk level using ISO 27005 matrix (likelihood x impact)
8. Baseline Snapshot	Creates a drift detection baseline from the current state

Live Console

A terminal at the bottom displays real-time progress messages via WebSocket. Each step broadcasts status updates as it runs.

Controls

- **Pause** — Suspend the pipeline (can resume later)
- **Resume** — Continue a paused pipeline
- **Cancel** — Abort the pipeline

Results

When complete, a summary card shows: - Hosts discovered - Assets created/updated - Findings created - Threats created - Risks created

The **Recent Runs** sidebar lists the last 5 runs for quick reference.

---

5. Nmap Scanner

Route: `/nmap`

A custom nmap scanner with security guardrails for ad-hoc scans.

How to use

1. Enter a target IP or CIDR range
2. (Optional) Add nmap arguments (e.g. `-sV -sC -p 1-1000`)

3. Set a timeout in seconds
4. Toggle **Auto-Pipeline** to run the full 8-step pipeline after the scan
5. Click **Scan**

Safety Guardrails

The scanner blocks dangerous arguments: - No file output flags (`-oN` , `-oG` , `-oS` , `-oA`) - No input from files (`-iL`) - No shell redirects (`>` , `|`) - No command substitution (backticks, `$()`) - **Scope restricted to RFC 1918 private networks** (192.168.x.x, 10.x.x.x, 172.16-31.x.x)

Live Output

The NmapConsole shows real-time nmap output as it runs. If Auto-Pipeline is enabled, the pipeline steps are displayed after the scan completes.

---

6. Assets

Route: `/assets`

Asset List

A paginated table of all discovered network assets showing: - IP address and hostname - Asset type (workstation, NAS, camera, smart plug, router, etc.) - Zone (LAN, IoT, Guest, DMZ) - Criticality (low, medium, high, critical) - Last scanned timestamp

Asset Detail (`/assets/:id`)

Click any asset to see: - Full network information (IP, MAC, DNS) - Service ports and exposure profile (HTTP, SSH, SMB, RDP, etc.) - Associated findings and their severity - Related risks and threats - OS guess and vendor info

---

7. Findings

Route: `/findings`

Finding List

All vulnerability and misconfiguration findings with filters:

Filters: - Severity: critical, high, medium, low, info - Status: open, in_progress, fixed, accepted - Category: vuln, misconfig, exposure, info

Columns: Severity, Title, Description, Asset, Category, Source Tool, MITRE Techniques, Status, Date Found

Run Vulnerability Scan

Click **Run Vuln Scan** to trigger an on-demand scan: 1. (Optional) Select a specific target asset, or leave blank to scan all 2. Click **Start Scan** 3. Results modal shows: findings created, duplicates skipped, errors

The scan runs these checks per asset: - HTTP security headers (CSP, HSTS, X-Frame-Options, etc.) - TLS/SSL (certificate validity, weak ciphers, protocol versions) - SSH (banner, weak auth methods, outdated versions) - DNS (zone transfer, DNSSEC) - Default credentials (admin/admin, SNMP community strings, etc.)

Finding Detail (`/findings/:id`)

Click any finding to see: - Full description and evidence - Affected asset with context - Remediation guidance - CWE reference - MITRE technique mappings - Related risks

---

8. Vulnerability Management

Route: `/vulnmgmt`

A triage-focused view for managing findings through their lifecycle.

Metrics Section

Top-level cards showing totals by: - Severity (critical, high, medium, low, info) - Status (open, in_progress, fixed, accepted) - Category (vuln, misconfig, exposure, info)

Finding Management

Expandable rows with: - Status dropdown to change status (open > in_progress > fixed/accepted) - Asset context (hostname, IP) - Evidence view - CWE reference - MITRE mappings - Related risks

---

9. Pentest Module

Route: `/pentest`

Guardrailed penetration testing actions with live terminal output.

How to use

1. **Select a target:**
2. Use the dropdown to pick an asset from inventory
3. Or type an IP/hostname manually
4. **Choose an action card** and click **Execute**
5. Watch the **live console** as probes run in real-time
6. Review the **results modal** when complete

Available Actions (10)

Action	Risk	What it does
Port Verification	low	Scan for open ports and verify service availability
HTTP Security Headers	low	Check for HSTS, CSP, X-Frame-Options best practices
TLS Configuration Check	low	Verify certificate, protocol versions, cipher strength
SSH Hardening Check	low	Audit SSH for weak algorithms and auth settings
UPnP Discovery Check	low	Detect UPnP services exposed to the network
Admin Interface Exposure	medium	Probe for web panels and management ports
WAF Detection	low	Detect WAFs using probes, signatures, behavioral analysis
Web Vulnerability Probe	medium	Test CORS, clickjacking, XSS, SQLi, open redirect, debug disclosure
Service Fingerprint	low	Detect CMS, frameworks, web servers, languages
Exploit Chain Analyzer	low	Analyze existing findings for multi-step attack chains

Tabs

- **Actions** — The action grid with execute buttons
- **Results** — Session findings accumulated from all executions
- **History** — Execution log with timestamps and targets

Live Console

The terminal at the bottom shows timestamped progress messages as each action runs — which probes are sent, what's being checked, findings as they're discovered.

10. Threats

Route: `/threats`

STRIDE-based threat modeling for your network.

Tabs

Threats Tab: - List of all identified threats - Each shows: title, STRIDE type, zone, source (rule/manual/ai_suggested) - Color-coded STRIDE badges: S (Spoofing), T (Tampering), R (Repudiation), ID (Info Disclosure), DoS, EoP (Elevation of Privilege) - Add or delete threats manually

Generate Tab: - Click **Generate** to auto-create threats from your discovered assets - The system applies STRIDE rules per zone: - IoT zone: higher tampering/DoS risk - Guest zone: higher spoofing/info disclosure risk - LAN zone: privilege escalation focus - DMZ zone: all threat types

Trust Boundaries Tab: - Visual diagram of zone boundaries - Trust levels per zone (LAN: high, IoT: low, Guest: very low, DMZ: medium) - Boundary controls (firewall, NAT, VLAN isolation, client isolation)

11. Threat Intelligence

Route: `/intel`

Security intelligence dashboard with AI-generated daily briefs.

Period Selector

Toggle between 1 day, 7 days, or 30 days.

Stat Cards

- Total Threats (all-time)
- New Threats (in selected period)
- Open Critical/High findings

- Critical Risks

Daily Threat Brief

An AI-generated analysis (requires Ollama or OpenAI) summarizing: - Current threat landscape for your network - Priority areas of concern - Recommended actions

Click **Refresh** to regenerate.

Analytics

- **Findings by Severity** — horizontal bar chart
- **Threat Categories (STRIDE)** — breakdown by type
- **Top MITRE Techniques** — most frequently mapped techniques
- **Asset Exposure** — table of most-threatened assets
- **Recent Threats** — latest discoveries with confidence scores

---

12. Risks

Route: `/risks`

ISO 27005-compliant risk management.

Risk Register Tab

Complete risk inventory with: - Scenario description - Likelihood and Impact scores - Risk Level (derived from 5x5 matrix) - Linked asset and finding - Status lifecycle: identified > analyzed > evaluated > treated > monitoring - SLA tracking (Critical: 7 days, High: 30 days, Medium: 90 days)

Risk Matrix Tab

Interactive 5x5 matrix visualization:

```
                    Impact
              Negl.  Low   Med   High  Crit
very_high     Med    High  High  Crit  Crit
high          Med    Med   High  High  Crit
Likelihood:
medium        Low    Med   Med   High  High
low           Low    Low   Med   Med   High
very_low      Low    Low   Low   Med   Med
```

Click any cell to see all risks in that category.

Risk Analysis Tab

AI-driven risk analysis showing correlations between threats, findings, and risks.

Treatment Tab

Apply treatment to risks: 1. Select treatment option: **Mitigate**, **Accept**, **Transfer**, or **Avoid** 2. Write a treatment plan narrative 3. Select specific treatment measures (checklist) 4. Assign an owner 5. Set a due date 6. Assess residual risk level

Treatment progress is tracked and audited.

13. MITRE ATT&CK

Route: `/mitre`

Technique Matrix

A 14-column layout matching the official ATT&CK framework. Each column is a tactic:

Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command & Control, Exfiltration, Impact

Technique Cards

Each card shows: - Technique ID (e.g. T1133) - Technique name - Confidence percentage - Finding and asset counts - Red border if actively exploitable

Click a card to see: - Linked findings with severity - Affected assets with IPs - Drill-down navigation to findings and assets

ATT&CK Navigator Export

Click **Export** to download a JSON file compatible with the official MITRE ATT&CK Navigator. Red = exploitable, gray = mapped.

14. Drift Monitor

Route: `/drift`

Detect changes in your network since the last baseline.

Status Indicator

- **STABLE** (green) — No unexpected changes
- **DRIFTED** (yellow) — Changes detected
- **ALERT** (red) — Critical/high severity changes

Summary Cards

- Baselines count
- Changes detected
- Alerts (critical/high)
- Zones monitored

Changes Timeline

Grouped by date, showing: - **New Asset** (green +) — new host discovered - **Removed Asset** (red -) — host disappeared - **New Ports** (orange triangle) — new services detected - **Closed Ports** (blue arrows) — services shut down - **Exposure Change** (red triangle) — security exposure increased/decreased

Expand any change to see raw detail data.

Baseline Management

Create new baselines: 1. Select zone: LAN, IoT, Guest, DMZ 2. Select type: full, ports_only, services_only 3. Click **Create Baseline**

The baseline list shows each snapshot with zone, type, age, and asset count.

Workflow

1. Run a Workflow assessment (creates baseline automatically at step 8)
2. Run another assessment later
3. Visit Drift Monitor to see what changed
4. Investigate alerts and changes
5. If changes are expected, create a new baseline to accept the new state

---

15. AI Copilot

Route: `/copilot`

AI-guided investigation and remediation of findings. Requires an AI provider (Ollama or OpenAI).

6-Step Workflow

Step 1 — INVESTIGATE: - Select a finding from the triage list (sorted by severity) - The copilot gathers context: asset info, MITRE mappings, related risks - Displays analysis: What the finding is, why it matters, business impact

Step 2 — PLAN: - AI generates a step-by-step remediation plan - Shows: actions, effort level, required resources, risk notes

Step 3 — CONFIRM: - Review the plan - Click **Confirm & Execute** or go back to adjust

Step 4 — EXECUTE: - Finding status changes to `in_progress` - Action is logged in the audit trail - Apply the fix manually (or automated if applicable)

Step 5 — VERIFY: - The copilot runs a verification scan against the affected asset - Checks if the finding is still present - Verdict: **LIKELY_FIXED** or **STILL_VULNERABLE**

Step 6 — REPORT: - If fixed: mark finding as `fixed` - If still vulnerable: iterate (go back to planning) or escalate - Complete audit trail preserved

---

16. Reports

Route: `/reports`

Executive Summary

A posture card at the top showing: - Overall posture badge (CRITICAL / HIGH / MEDIUM / LOW / HEALTHY) - Metric cards: Assets, Findings, Risks, Threats - Severity and risk breakdown bar charts

Report Types

Type	Format	Best for
HTML Report	.html	Interactive web report with full evidence
PDF Report	.pdf	Printable document for stakeholders
JSON Export	.json	Machine-readable full data export
CSV Export	.csv	Spreadsheet analysis (findings, risks, assets, MITRE)

How to generate

1. Click **Generate** on the desired report type
2. Wait for generation (spinner)

3. Click **Download** to save the file
4. Click **Preview** (HTML only) to view in browser

Reports include: executive summary, risk matrix, findings by severity, asset inventory, detailed findings with evidence, MITRE heatmap, risk scenarios, and recommendations.

17. Settings

Route: `/settings`

Scan Policy Tab

- **Policy Name** — identifier for this policy
- **Scope Allowlist** — CIDR ranges to include in scans (e.g. `192.168.178.0/24`)
- **Scope Denylist** — CIDR ranges to exclude
- **Action Allowlist** — which scanning actions are permitted
- **Rate Limits:**
- Scan: requests/min (default 100)
- Check: requests/min (default 50)
- Pentest Action: requests/min (default 10)
- **Time Windows:**
- Allowed hours (default: 00:00–23:59)
- Maintenance windows

AI Configuration Tab

- **Provider:** Ollama (local) or OpenAI-compatible
- **Model:** Model name (default: `llama3.2`)
- **Base URL:** API endpoint (default: `http://localhost:11434`)
- **Enable AI:** Toggle on/off
- **Test Connection:** Verify connectivity

Evaluation Thresholds Tab

- **Risk Acceptance:** Max acceptable risk level (Low/Medium/High/Critical)
- **Auto-Triage:** Enable auto-triage on new findings, minimum priority score (0–100)
- **Baseline Auto-Creation:** Auto-create baselines after scans, zone selection

Schedules Tab

Create automated recurring scans:

1. Enter a schedule name
2. Select scan type: Full, Discovery Only, Vulnerability Scan Only, Threat Modeling Only
3. Choose schedule type:
4. **Interval:** every 1h, 2h, 4h, 8h, 12h, 1d, 7d
5. **Cron:** custom cron expression or preset (Daily 2AM, Weekly Sunday 3AM, Monthly 1st 4AM)
6. Set CIDR scope
7. Toggle **Enable Immediately**
8. Click **Create**

Use **Run Now** to trigger any schedule immediately.

18. Recommended Workflow

Initial Setup (Day 1)

1. Install prerequisites (Python, Node, Docker, Nmap, optionally Ollama)
2. Configure `.env` with your network settings
3. Start backend and frontend
4. Go to **Settings** — configure your scan policy scope (your home subnet)
5. Go to **Workflow** — run a full assessment on your subnet
6. Wait for all 8 steps to complete
7. Review **Dashboard** for your security posture

Regular Use

1. **Dashboard** — Check posture, review recent findings
2. **Findings** — Triage new findings, run vulnerability scans as needed
3. **Risks** — Review risk register, apply treatments to high/critical risks
4. **AI Copilot** — Investigate critical findings, follow guided remediation
5. **Drift Monitor** — Check for network changes since last baseline
6. **Pentest** — Run targeted tests against specific assets
7. **Reports** — Generate reports for documentation

Scheduled Automation

Set up recurring scans in **Settings > Schedules**: - **Daily at 2 AM:** Full vulnerability scan - **Weekly Sunday 3 AM:** Full pipeline assessment - **Monthly:** Generate reports for compliance

After Network Changes

When you add new devices or change your network: 1. Run a new **Workflow** assessment 2. Check **Drift Monitor** for detected changes 3. Review new findings and risks 4. Create a new baseline once changes are accepted

Configuration Files Reference

Located in `D:\Risk-App3.0\config\`:

File	Purpose
`default_policy.yaml`	Scan scope, allowed actions, rate limits, time windows
`risk_matrix.yaml`	ISO 27005 5x5 risk matrix, treatment thresholds, SLA timers
`zone_model.yaml`	Network zones (LAN, IoT, Guest, DMZ), trust levels, boundary controls
`baselines.yaml`	Expected ports/services per device type, compliance checks
`mapping_rules.yaml`	MITRE ATT&CK technique mapping rules with confidence scores

API Health Check

Verify the backend is running:

```
GET http://localhost:8000/api/health
```

Response:

```
{"status": "healthy", "version": "1.0.0"}
```

Troubleshooting

Problem	Solution
Frontend shows blank page	Check Docker is running: `docker-compose ps`
Backend won't start	Check Python 3.12+ and all requirements installed
Nmap scan fails	Verify nmap is installed and on PATH
AI features disabled	Install Ollama and pull a model, or configure OpenAI API key
WebSocket not connecting	Check nginx config has WebSocket upgrade headers
Database locked	Restart backend — WAL mode handles most concurrency
Scan scope rejected	Only RFC 1918 private ranges are allowed