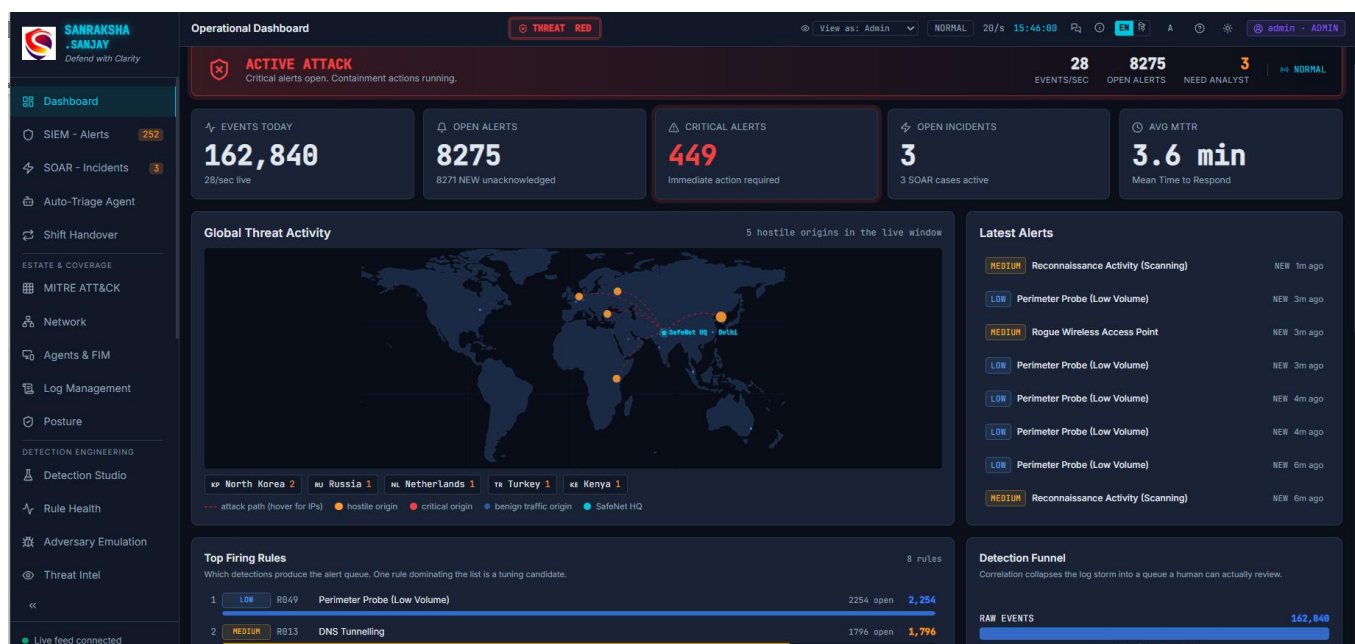




Graduate SOC analysts, not just cybersecurity graduates.

Sanraksha.SANJAY is a complete Security Operations Centre in a box, built for the classroom. Students work a live SIEM alert queue, write correlation rules, run SOAR playbooks and defend an attackable enterprise estate, on synthetic data, with no internet, no cloud accounts and no per-seat tool licences. Faculty run whole cohorts through timed attack drills and grade from what students actually did.

60+	25+	750+	20+	10+	0
correlation rules	attack scenarios	auto-graded Range questions	guided labs	certification tracks	internet required



WHY INSTITUTIONS CHOOSE SANJAY

Zero infrastructure burden

One lab PC or one department server. Runs fully offline, so it works in air-gapped labs, during exams and in campuses with restricted internet. No cloud subscriptions, no vendor SIEM licences to renew every semester.

Industry-real workflow

The alert queue, MITRE ATT&CK mapping, Sigma rule import, playbook runner and threat-intel competencies follow the same workflow as in the industry. Students will meet in their first job, transfer, not just concepts.

Assessment built in

Range questions grade automatically. A 13-area competency matrix fills in from real actions, not self-reporting. Ten certification tracks map to Security+, CySA+, BTL1/2 and GCIH objectives, with timed exams and printable certificates.



Drops into the syllabus you already teach.

Each SANJAY module maps to a unit that already exists in B.Tech, M.Tech, BCA/MCA and diploma cybersecurity programmes. Theory hours stay yours. SANJAY supplies the practical component, with evidence of completion for every student.

COURSE UNIT	HANDS-ON ACTIVITY IN SANJAY	EVIDENCE FOR GRADING
Network security & log analysis	Log Management pipeline view; Event Search with a KQL-style query language across firewall, DNS, proxy, EDR, identity and OT sources	Range questions (auto-graded)
Intrusion detection & SIEM	Work the Alert Queue: acknowledge, triage, escalate. Tune thresholds and windows on multiple correlation rules in Detection Studio; import Sigma rules	Rule Health report; lab completion
Incident response	Open SOAR incidents, run response playbooks, walk the per-attack kill chain, isolate hosts and block IOCs	Playbook steps completed; MTTR
Threat intelligence & hunting	Pivot 88 curated IOCs on the world attack map; complete 9 structured threat hunts	Hunt findings; Range questions
Adversary tactics (MITRE ATT&CK)	Coverage matrix across tactics and techniques, updated live from the alerts students generate	Coverage snapshot per cohort
Capstone / team project	Instructor-run live exercise: cohorts as SOC teams in private tenants, timed attack timeline, real-time scoreboard	Printable after-action report

The screenshot displays the SIEM - Alert Queue interface. The top navigation bar includes a search bar, filters for severity (CRITICAL, HIGH, MEDIUM, LOW, INFO), and a status filter (NEW, ACKNOWLEDGED, IN_PROGRESS, ESCALATED, CLOSED, FALSE_POSITIVE). The main table lists alerts with columns for Severity, Rule, MITRE Tactic, Assets, Time, SLA, Status, and Assign. The selected alert is a 'Perimeter Probe (Low Volume)' event, categorized as 'Reconnaissance' under the MITRE ATT&CK framework. The detailed view on the right shows the alert's response SLA, acknowledgment status, and a timeline of events. It also includes a 'KILL CHAIN - THIS ATTACK' section, which provides a visual representation of the attack stages and the corresponding alerts generated.



Run a class of sixty like a SOC shift.

A faculty controller builds a live exercise: teams, an isolated estate per exercise and a timed attack timeline. Each team defends inside its own tenant on the same server while the instructor drives the drill, pauses for discussion, and watches the scoreboard update in real time.

The screenshot displays the 'Adversary Emulation' interface. At the top, there's a status bar with 'THREAT RED', 'View as: Admin', 'NORMAL', '20/s', '15:42:48', and user 'admin ADMIN'. Below this, a section titled 'Adversary Emulation' shows 'validated: 11/11' and a 'Run all' button. The main area contains a grid of attack scenarios, each with a title, a brief description, a 'Run test' button, and a 'last run: detected - 3d ago' status. The scenarios include: Brute force (Credential Access, T1118), Kerberoasting (Credential Access, T1558.003), DCSync (Credential Access, T1083.006), Golden Ticket (Defense Evasion, T1558.001), MFA fatigue (Credential Access, T1621), LOLBin abuse (Defense Evasion, T1218), Shadow-copy deletion (Impact, T1498), SQL injection (Initial Access, T1190), Container crypto-mining (Impact, T1496), Perimeter probing (Reconnaissance, T1595), and Removable media (Collection, T1091).

INSTRUCTOR CONTROL

- **Lifecycle** with autosave and restore: pause, resume, restart, archive. Stop mid-drill to teach, then continue.
- **Attacks** timed on a schedule or triggered by hand. 21 scenarios from phishing and DDoS to APT, insider threat and OT/ICS.
- **Roles** students sign in as L1, L2, L3, CISO or Board; faculty as Controller; department admin manages accounts and the estate.
- **Reporting** printable after-action report: standings, timeline, per-team detection and response metrics.
- **Collaboration** team war-room chat and shared investigation notes inside each tenant.
- **Bilingual UI** English and Hindi, switchable per user.

ASSESSMENT & PROGRESS

- **750+ Range questions** auto-graded across investigation, ATT&CK, cloud and AI security. New sets unlock weekly so question banks do not go stale between batches.
- **20+ guided labs** from Beginner to Expert, each completing from real console actions rather than a quiz.
- **25+ challenges** grouped by scenario, ready for hackathons, CTF days and inter-college competitions.
- **5 learning paths** sequenced tracks for a semester, an elective, or a short certificate course.
- **Competency matrix** 13 skill areas scored Novice to Expert from each student's own work.
- **Certificates** Ten tracks aligned to Security+, CySA+, BTL1, BTL2, GCIH and SIEM Analyst objectives. Timed exams, score report, printable certificate.

Detection Studio

THREAT RED

View as: Admin

NORMAL

20/s

15:42:23

EN

A

admin · ADMIN

Detection Studio

Write a correlation rule

templates...

Sigma

Import Sigma

How do I build a good rule? (5-step guide)

RULE NAME

Port scan (firewall denies)

DESCRIPTION

e.g. Catches slow RDP sweeps the perimeter rule misses; expect FPs from the vuln scanner

what it detects & why - carried into every alert it raises

ALERT SEVERITY

MEDIUM

THRESHOLD

15

WINDOW (SEC)

30

matching events

GROUP BY

src_ip

RESPONSE PLAYBOOK

default

threshold counts per group

runs when the rule fires

MITRE TACTIC

unmapped

MITRE TECHNIQUE

e.g. T1110 - Brute Force

COOLDOWN (SEC)

0

optional - joins the ATTACK matrix

format: "T1110 - Brute Force"

per-group alert suppression; 0 = auto (2x window, min 120s)

EVENT FILTERS (AND)

SOURCE TYPE

FIREWALL

EVENT SEVERITY

any

EVENT TYPE CONTAINS

CONN_DENY

SOURCE IP EQUALS

e.g. 203.0.113.45

Backtest results

671 of 50,000 events matched - 0 groups would fire

src_ip	matches	peak/window	verdict	last seen
198.51.100.120	44	5	below threshold	30m ago
198.51.100.33	37	4	below threshold	30m ago
198.51.100.77	36	4	below threshold	31m ago
203.0.113.21	48	4	below threshold	29m ago
198.51.100.44	41	4	below threshold	30m ago
192.0.2.210	43	4	below threshold	30m ago
192.0.2.100	43	4	below threshold	30m ago
203.0.113.130	37	4	below threshold	30m ago
198.51.100.100	43	4	below threshold	29m ago
203.0.113.45	39	4	below threshold	29m ago
203.0.113.7	29	4	below threshold	30m ago
203.0.113.170	34	4	below threshold	31m ago
192.0.2.66	31	3	below threshold	31m ago
192.0.2.140	37	3	below threshold	30m ago
198.51.100.10	37	3	below threshold	31m ago
203.0.113.80	36	3	below threshold	30m ago
203.0.113.199	35	3	below threshold	30m ago
203.0.113.110	29	3	below threshold	30m ago

SAMPLE MATCHES - PIVOT ON ANY ENTITY

15:12:18	MEDIUM	FIREWALL	203.0.113.21	CONN_DENY
15:12:17	MEDIUM	FIREWALL	203.0.113.45	CONN_DENY
15:12:16	HIGH	FIREWALL	198.51.100.100	CONN_DENY

SOAR - Incident Management

THREAT RED

View as: Admin

NORMAL

20/s

15:59:21

EN

A

admin · ADMIN

Sanraksha Playbook Engine | 19 playbooks loaded

Search incidents...

need action

OPEN

INVESTIGATING

CONTAINED

ERADICATED

RECOVERED

CLOSED (1)

3 shown - open

MEDIUM

Wi-Fi Authentication Failure Burst - MEDIUM

ACTION REQUIRED

Sanraksha Wireless Threat Response Playbook

AWAITING_ANALYST

INVESTIGATING

Unassigned

overdue 8153m

View --

MEDIUM

Rogue Wireless Access Point - MEDIUM

ACTION REQUIRED

Sanraksha Wireless Threat Response Playbook

AWAITING_ANALYST

INVESTIGATING

Unassigned

overdue 8131m

View --

MEDIUM

Service Account Interactive Login - MEDIUM

ACTION REQUIRED

Sanraksha Insider Threat & Account Compromise Playbook

AWAITING_ANALYST

INVESTIGATING

Unassigned

overdue 8152m

View --

MEDIUM

Wi-Fi Authentication Failure Burst - MEDIUM

Report

INVESTIGATING

Playbook: Sanraksha Wireless Threat Response Playbook

Assigned: Unassigned

Open 3d ago

1 Detect

2 Investigate

3 Contain

4 Eradicate

5 Recover

6 Close

Playbook Runner

Kill Chain

Timeline

Linked Alerts

Evidence

IOCs

Locate the rogue device / attack source

AUTO

Triangulate the rogue BSSID or 802.1X failure source using WLAN-controller RSSI data from nearby managed APs

hide result

WLAN triangulation complete: offending BSSID located to within ~8m - ap-dept-01.dept.safenet.in area, floor 2 east wing - using RSSI from 4 managed APs. Broadcasting SSID mimics the corporate network. First seen 16:16:11 UTC, strongest signal -245 dBm at sensor ap-2e-04.

Contain the rogue SSID over the air

ANALYST

Enable WLAN-controller rogue containment (targeted deauth of the rogue BSSID) and blacklist it on all managed APs

hide result

Analyst decision: Execute containment. Notes: (none)

Identify exposed clients and accounts

AUTO

List corporate clients that associated with the rogue AP or accounts with 802.1X failure bursts

ANALYST: Physical sweep decision

ANALYST

Dispatch facilities/security to physically locate and remove the device, or stand down if it is a neighbouring network

show result

Rotate credentials for exposed clients

ANALYST

Force credential rotation / certificate re-issue for accounts and devices that touched the rogue AP

show result

Simulator Controls

THREAT RED

View as: Admin

NORMAL

20/s

15:45:03

EN

A

admin · ADMIN

PROXY 7.62/s

DNS 5.88/s

AUTH 5.2/s

FIREWALL 4.9/s

ENDPOINT 3.62/s

NETWORK 2.98/s

EOR 1.57/s

EMAIL 1.42/s

IDS 0.5/s

CLOUD 0.33/s

FIN 0.32/s

Scenario

NORMAL

Beginner

+ LIVE

Routine operations - baseline monitoring.

ATTACK_IN_PROGRESS

Intermediate

Active credential attack - brute force to lateral movement.

fires: R001 R002 R004 R016 R033

RANSOMWARE

Advanced

Ransomware outbreak with active C2 communications.

fires: R005 R006 R008 R015 R030 R031

INSIDER_THREAT

Advanced

Malicious insider - data theft and exfiltration.

fires: R007 R011 R012 R021 R035 R037 ~4

APT

Expert

Low-and-slow advanced persistent threat - 3-day campaign.

fires: R005 R006 R015 R044

DDOS

Intermediate

Volumetric denial of service - network-level attack.

fires: R014 R045

WEB_ATTACK

Intermediate

SQL injection against the public web server (R017).

fires: R017

PHISHING

Beginner

Phishing campaign with click-through to a credential-harvest domain (R010).

fires: R010 R032

SUPPLY_CHAIN

Expert

Trojanised software update beaconing to C2 across endpoints (R018).

fires: R018

CREDENTIAL_STUFFING

Intermediate

Reused-credential spray across many accounts from one source (R003).

fires: R003

LATERAL_MOVEMENT

Advanced

Remote-admin tooling (PsExec/WMI) hopping host to host (R005).

fires: R005

DATA_EXFILTRATION

Advanced

Large outbound transfers to a known-malicious destination (R007).

fires: R007 R035 R039

DNS_TUNNELING

Advanced

Covert channel via long-label / rotating-subdomain DNS queries (R013).

fires: R013

PRIVILEGE_ESCALATION

Advanced

Registry Run-key persistence and SYSTEM-level escalation (R009).

fires: R009

OT_ATTACK

Expert

Unauthorized Modbus commands to ICS/SCADA control devices (R019).

fires: R019 R042

LOTL

Advanced

Living-off-the-land: abuse of signed system tools (PowerShell, certutil, mshta...) to evade defences (R022).

fires: R022 R054

CLOUD_IDENTITY

Advanced

Cloud/identity attack: MFA fatigue/push-bombing, illicit OAuth consent, impossible-travel sign-in, BEC inbox rule (R023-R026).

fires: R023 R024 R025 R026 R046

CICD_COMPROMISE

Expert

Supply-chain / CI-CD compromise: pipeline secret exfil and malicious dependency (SolarWinds/kx-style) (R027).

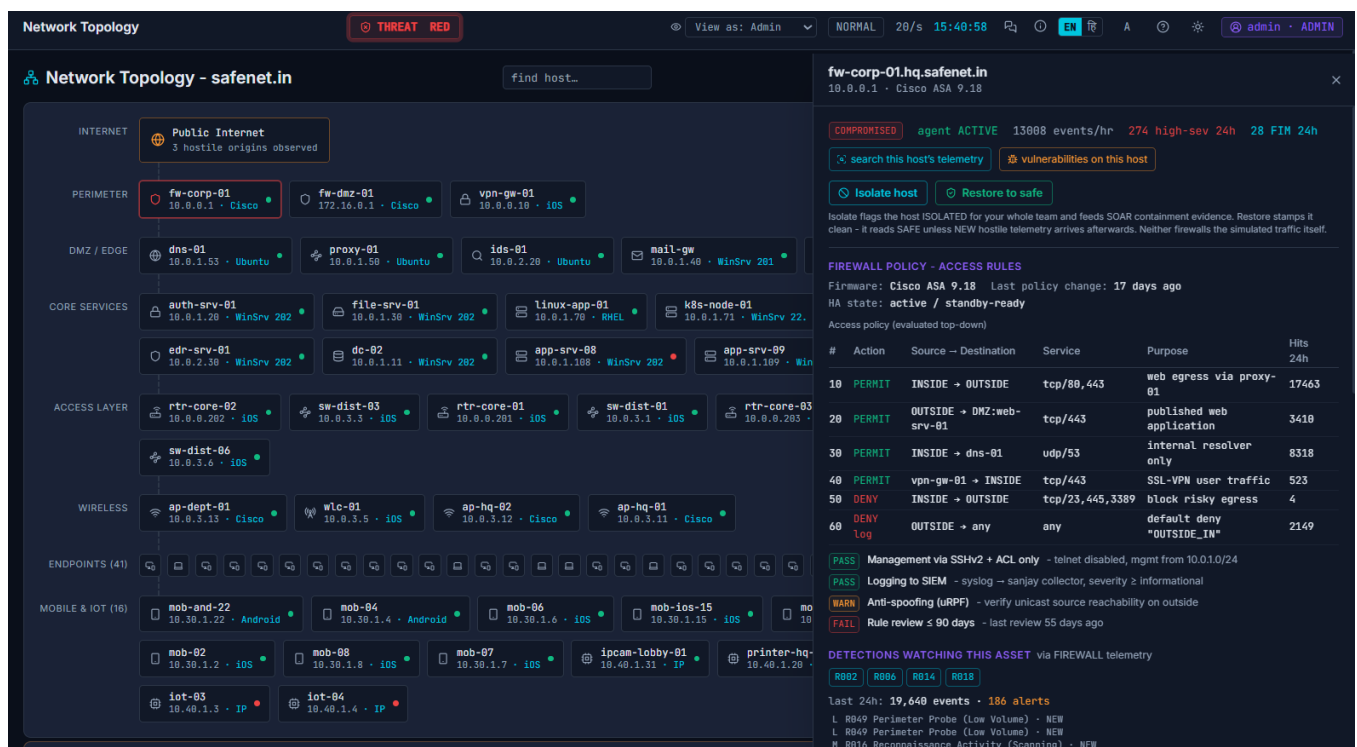
fires: R027



One server. One afternoon. The whole department.

SANJAY ships as a single application with an optional Docker package. It has run for 50-user, 5-team cohorts on one cloud instance and for individual students on a laptop. Install once, then create as many students, teams and exercises as the course needs.

DEPLOYMENT OPTION	SUITED TO	WHAT YOU NEED
Single lab PC or laptop	Self-paced study, faculty evaluation, small electives	Python 3.11+ and Node 18+, or Docker. No internet after install.
Department server (on campus)	Full cohorts, multiple sections, live exercises, exams	One mid-range server or VM running Docker. Optional TLS via the bundled reverse proxy.
Hosted by Sanraksha	Institutions that prefer not to operate infrastructure	A browser. We host a private instance for your institution and manage updates.



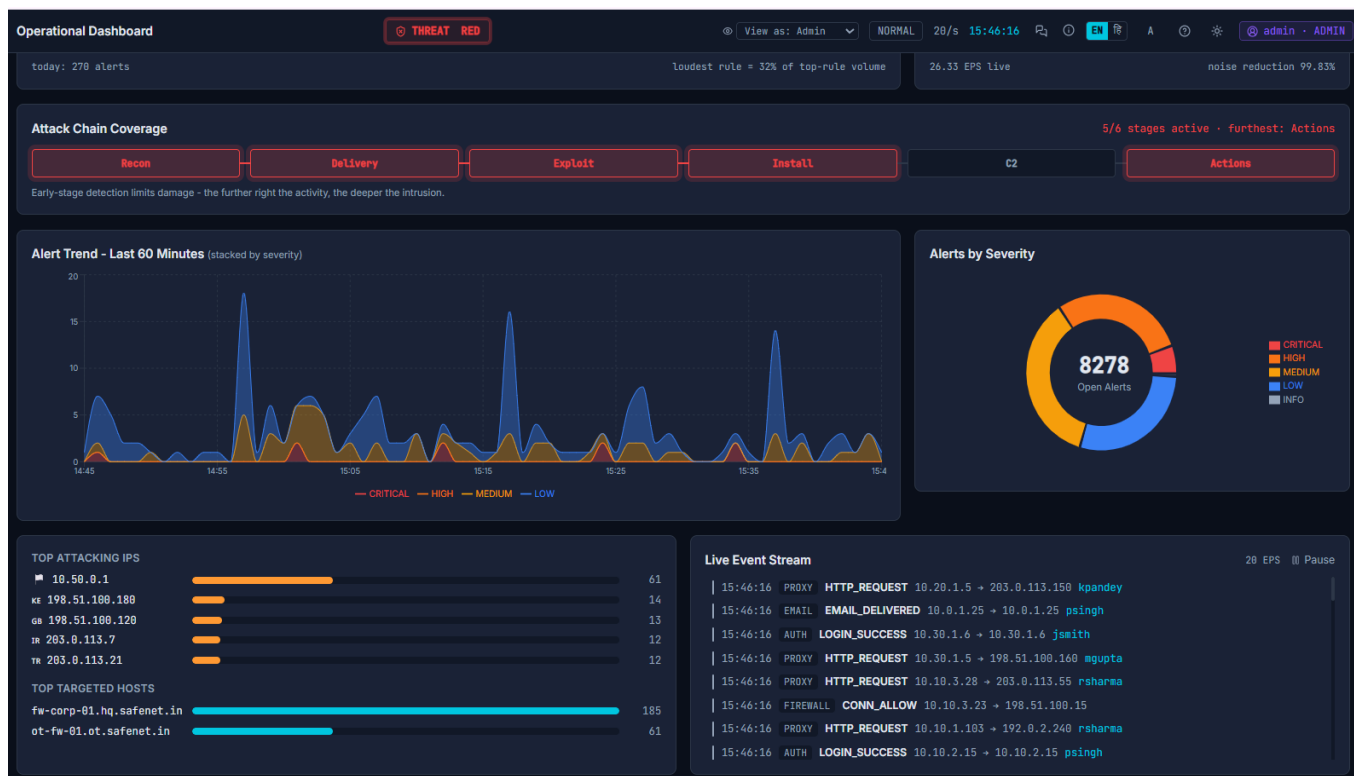
The attackable estate: enterprise tiers plus an OT/ICS network on the Purdue model. It can be re-drawn to mirror your own campus.

DATA, PRIVACY & COMPLIANCE

- **All telemetry is synthetic.** No real logs, no real personal data ever enters the platform.
- **Student data stays on campus** when self-hosted. Nothing is sent to external AI or analytics services.
- **Offline by design.** Works in air-gapped labs and during proctored exams.
- **Role-based access** with audit logging of logins and administrative actions.

ACADEMIC ENGAGEMENT MODEL

- **Institutional licence** covering unlimited students and faculty on your instance.
- **Faculty onboarding workshop** so instructors can run their first live exercise with confidence.
- **Curriculum pack** with lab manual, grading rubrics and the suggested 16-week plan.
- **Custom estate and scenarios** modelled on your network, your sector, or a partner industry's.
- **Competition support** for hackathons, CTF events and inter-college SOC challenges.



BOOK A CAMPUS DEMO

See SANJAY run a live drill with your own faculty.

We set up a trial instance, walk your department through one scenario end to end, and map the platform to your syllabus. Universities, engineering colleges, polytechnics and training academies welcome.

<https://sanraksha.ai>

contact@sanraksha.ai