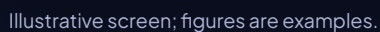




S.A.L.T CI PERISAI

Air-gapped by default





01 · WHY PERISAI

Serious security tools, **without the expertise barrier**

The best security tools are open source and powerful, but each demands deep expertise just to operate. Most organisations cannot staff that expertise, so the tools sit unused while attacks arrive every hour.



Tools need specialists

Scanners, frameworks and forensic suites each have their own commands, outputs and pitfalls.



Findings in silos

Reconnaissance, defence, forensics and compliance live in separate products that do not share evidence.



Compliance by hand

Auditors ask for proof that controls work. Teams assemble screenshots and spreadsheets every year.

ONE SUITE FOR EVERY LEVEL OF USER

PERSON	WHAT PERISAI GIVES THEM
New analyst	Describe the goal in plain language; PERISAI plans the steps, runs them and explains every output
Security professional	Full tool access with AI acceleration: chained scans, MITRE ATT&CK mapping and written reports
IT and system administrator	Scans, hardening checks and compliance gaps on their own infrastructure, without being a specialist
CISO and management	Risk posture, compliance status and board-ready reports generated from live data

PERISAI in one line

A full-spectrum security intelligence suite on top of the industry's most capable open-source tools, run by AI on the organisation's own servers, and built for air-gapped, classified and sovereign networks.

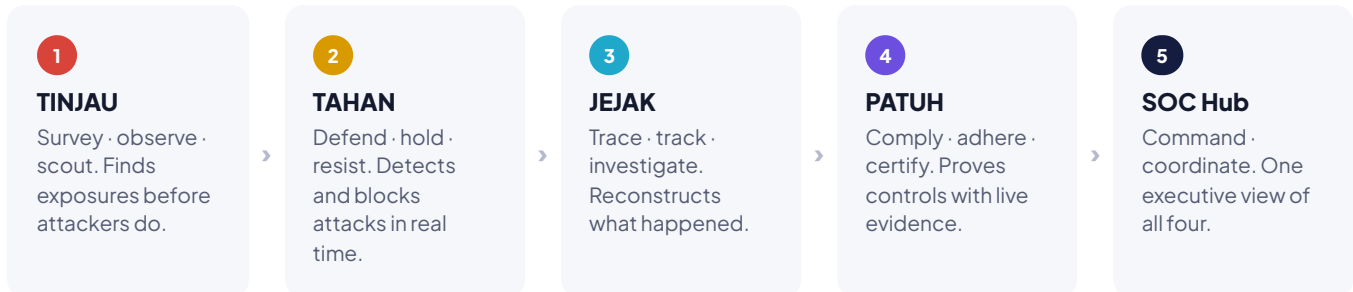




02 · FIVE SEGMENTS

Find, defend, investigate, prove, **command**

PERISAI is five connected segments. Each works on its own, and together they pass evidence along the whole security lifecycle.



SEGMENT 1 · RECONNAISSANCE & INTELLIGENCE
PERISAI TINJAU
State an objective in plain language; PERISAI builds the attack chain, runs it and delivers the intelligence.

SEGMENT 2 · DEFENCE & REAL-TIME SOC
PERISAI TAHAN
Monitor any number of hosts, detect attack patterns and block sources automatically.

SEGMENT 3 · FORENSICS & INCIDENT RESPONSE
PERISAI JEJAK
From alert to evidence package: timeline, artefacts, attack chain and a written forensic report.

SEGMENT 4 · COMPLIANCE & GOVERNANCE
PERISAI PATUH
Map controls to PDPA, ISO 27001, NIST CSF, CIS and ISMS-P, with evidence linked from TAHAN and JEJAK.

Evidence flows forward

A TINJAU finding becomes a TAHAN watch rule; a TAHAN alert escalates into a JEJAK case with full context; JEJAK artefacts and TAHAN blocks become PATUH compliance evidence; the SOC Hub reads all four.



03 · INTELLIGENCE LAYER

The tools are open source. The intelligence is S.A.L.T CI.

PERISAI places an AI intelligence layer over a curated arsenal of established security tools, so people state intent and PERISAI handles tool choice, sequencing, interpretation and reporting.

**Plain language to attack chain**

An objective in English or Malay becomes a planned, sequenced chain of tools.

**Multi-tool orchestration**

Outputs of one stage feed the next automatically.

**MITRE ATT&CK mapping**

Findings and attacks tagged with tactics and techniques.

**Risk scoring**

Severity, exposure and context combined into a priority.

**Written reports**

Assessment, forensic and compliance reports drafted with remediation.

**Threat intelligence**

Attacker IPs enriched with reputation, origin and history.

INTEGRATED TOOL ARSENAL

DOMAIN	TOOLS
Recon and OSINT	Nmap, Masscan, Amass, Subfinder, theHarvester, DNSrecon, Whois, Shodan
Web and vulnerability	Nuclei, Nikto, OWASP ZAP, Burp Suite, Gobuster
Exploitation testing	Metasploit, CrackMapExec, Responder, Evil-WinRM, PowerSploit
Network defence	Suricata, Zeek, Wireshark, fail2ban, iptables
Forensics	Volatility, Autopsy, YARA, Timesketch, strings
Threat intel and malware	MITRE ATT&CK, OpenCTI, MISP, Cuckoo Sandbox, VirusTotal

Tools run in an isolated Kali Linux worker with no public port. Online intelligence services are used only where the organisation allows them.

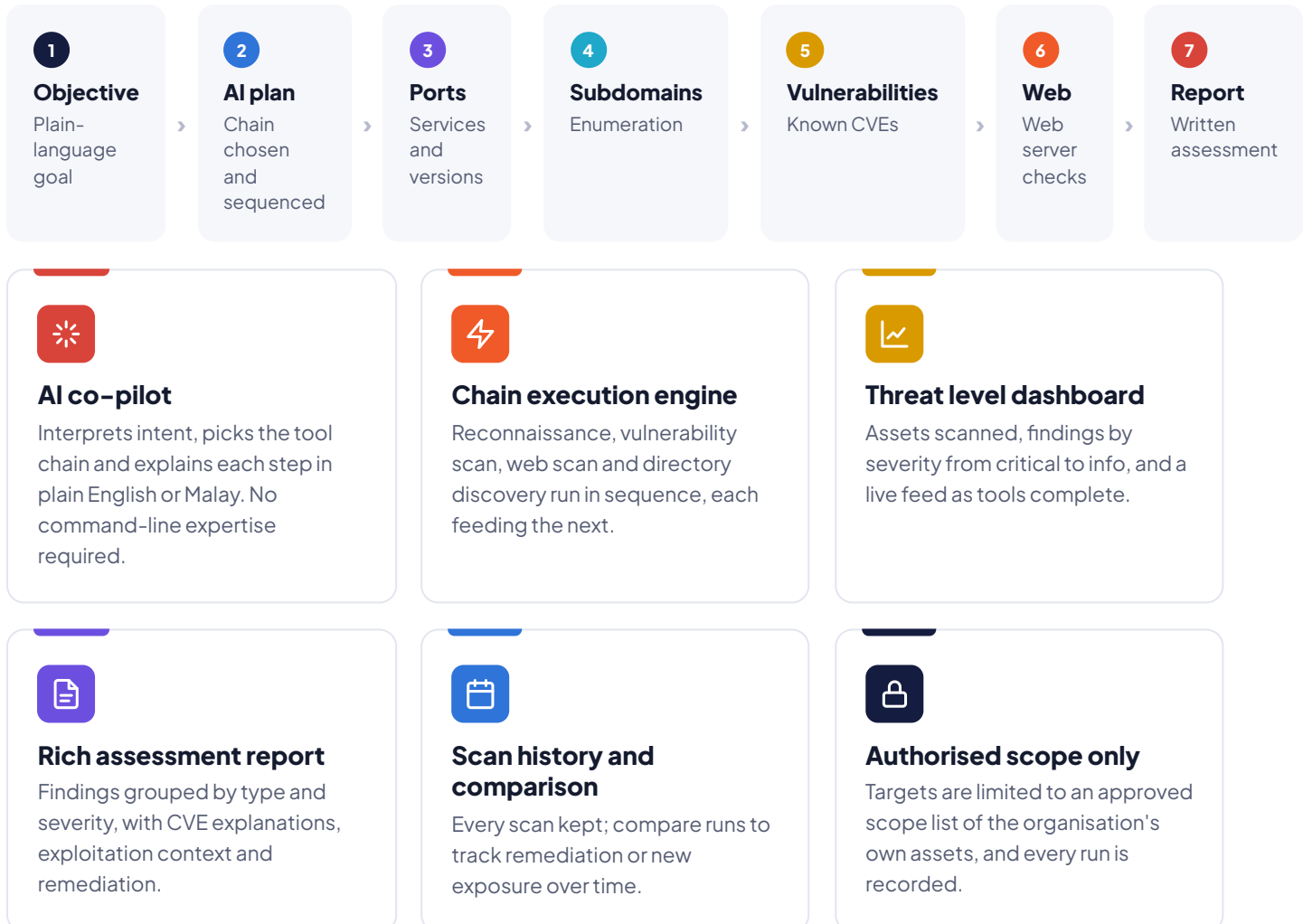




04 · TINJAU · RECONNAISSANCE

Find the exposure **before an attacker does**

TINJAU is an AI-powered reconnaissance console. State the objective in plain language, and it selects the tools, explains each step, runs them and narrates the findings.



```
PERISAI TINJAU · AI co-pilot

you > semak keselamatan portal awam kami, portal.contoh.gov.my
tinjau > Plan: ports → subdomains → known CVEs → web checks. Target is on the approved scope list.
tinjau > nmap · 6 open services · nginx 1.18 on 443
tinjau > subfinder · 11 subdomains · 2 not in the asset register
tinjau > nuclei · 1 high outdated TLS configuration · 3 medium
tinjau > Report ready: 2 forgotten subdomains and one high finding, with fixes in priority order.
```

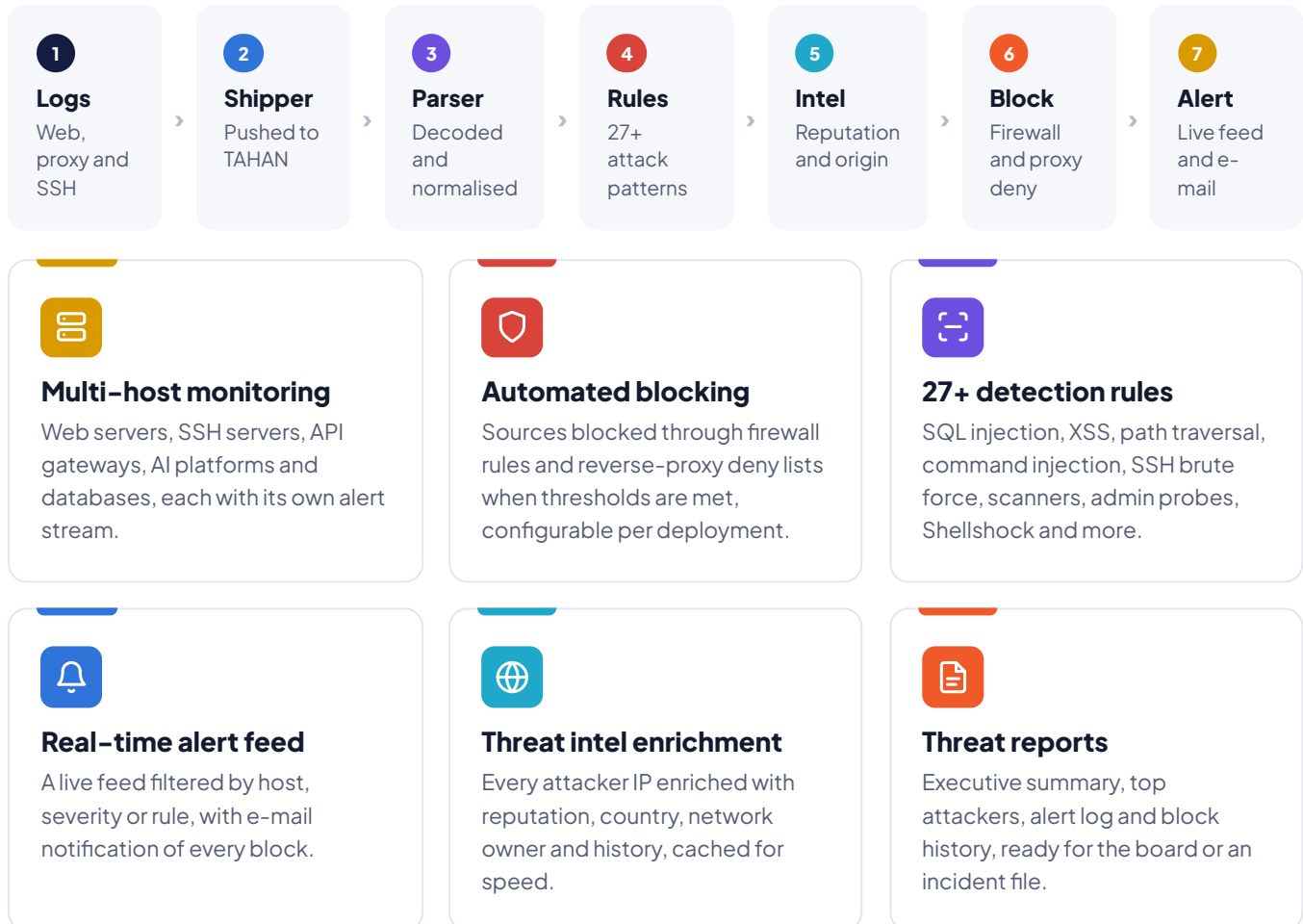
Illustrative session; host names are examples.



05 · TAHAN · ACTIVE DEFENCE

An always-on shield that **blocks by itself**

TAHAN is a real-time security operations centre. It watches any number of hosts, recognises attack patterns in their logs and blocks the source automatically.



Proven on S.A.L.T CI's own servers

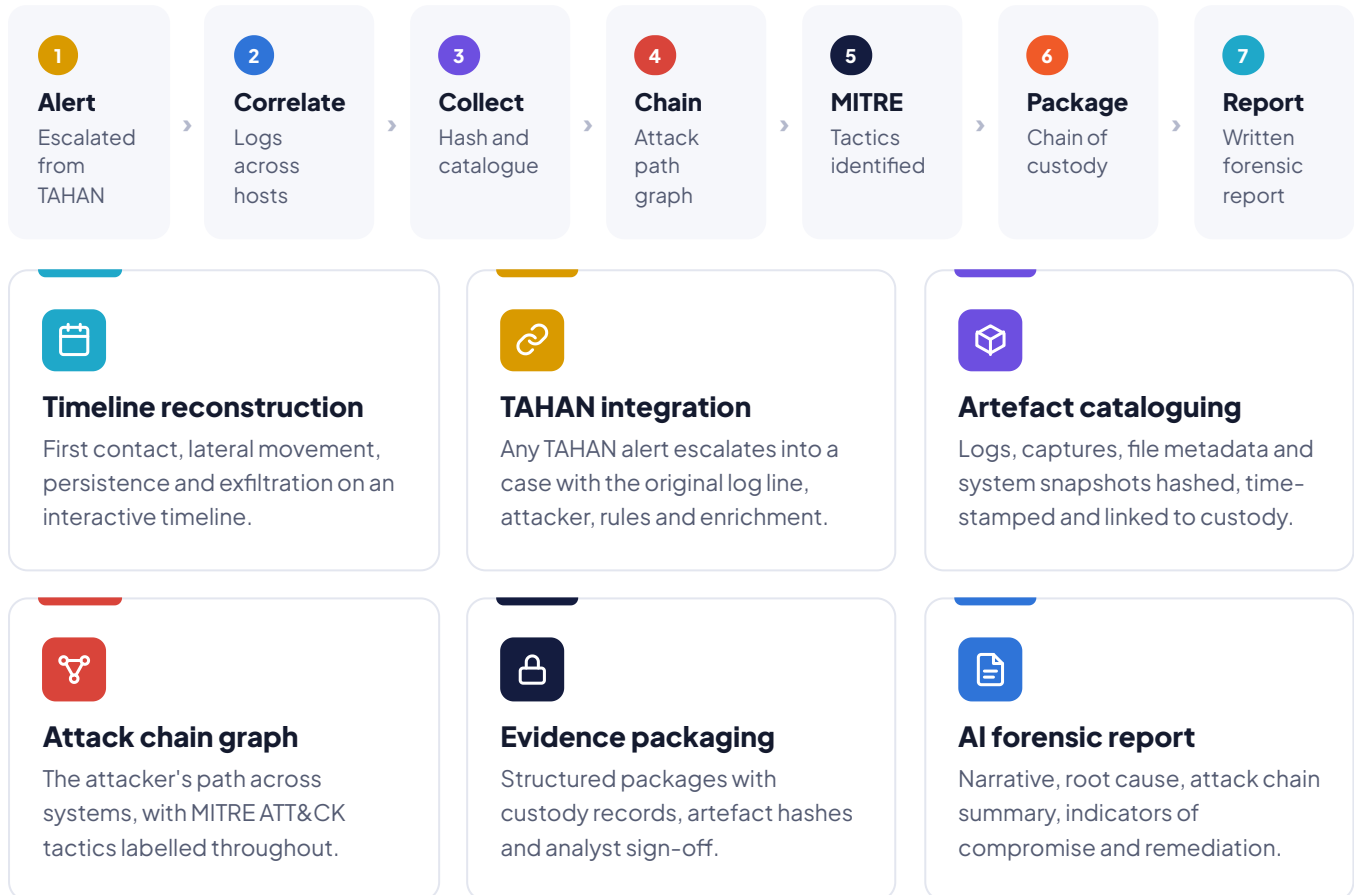
TAHAN defends S.A.L.T CI's own public services. By May 2026 it had handled more than 250,000 live alerts, with over 900,000 more in its archive, and permanently blocked more than 150 attacking sources.



06 · JEJAK · FORENSICS

From alert to evidence package

JEJAK is a digital forensics workspace that reconstructs what happened, when and by whom, and produces evidence fit for management, regulators or law enforcement.



Evidence that stays on site

Artefacts are kept in an encrypted evidence vault on the organisation's own servers. Nothing is uploaded to an outside sandbox unless the organisation chooses to.



07 · PATUH · COMPLIANCE

Compliance proven with **live evidence**

PATUH maps the organisation's controls to the frameworks it must meet and links real evidence from TAHAN and JEJAK, so compliance is shown, not asserted.

MALAYSIA

PDPA

Personal Data
Protection Act
2010

ENTERPRISE

ISO 27001

ISO/IEC
27001:2022

GLOBAL

NIST CSF

CSF 2.0: identify
to recover

TECHNICAL

CIS v8

18 critical security
controls

GOVERNMENT

ISMS-P

Public-sector
information
security

Further frameworks, such as RMIT for financial institutions, are added as control libraries.

**Framework mapping**

Controls mapped across
frameworks, with pass or fail per
control and AI remediation
guidance.

**Compliance score**

An organisation-wide score by
domain, framework and risk tier,
updated as controls are met.

**Live evidence linking**

TAHAN alerts, JEJAK artefacts,
policies and configurations
attached to controls with
timestamps.

**Control checklist**

Status, notes, owners and
evidence for every control, with
full history.

**AI gap analysis**

Missing controls and evidence
found, with a prioritised roadmap
by effort and risk.

**Audit export**

Board-ready reports and auditor
packages: scorecard, evidence
index, gaps and trends.



08 · SOC HUB · COMMAND

The whole security picture, **on one screen**

The SOC Hub unifies live intelligence from all four segments into one executive view, built for CISOs, SOC managers and command-level personnel.



AI executive assessment

One click analyses all four segments at once: security posture, active threats and compliance status, with recommendations.



Four command panels

Live figures from TINJAU, TAHAN, JEJAK and PATUH, each linking to its own dashboard.



Offline threat map

Attacker origins geolocated on a self-contained world map. No external map service needed.



Top attackers

A live leaderboard of the most active sources, with country attribution and intensity.



Severity breakdown

Critical, high and medium alerts at a glance, without opening TAHAN.



Ecosystem health

Live health and latency of every segment, refreshed automatically.

HOW THE HUB ASSEMBLES THE PICTURE

1

TINJAU

Scans,
findings,
assets



2

TAHAN

Alerts,
severity,
attackers



3

JEJAK

Cases,
artefacts



4

PATUH

Scores, gaps



5

Locate

Sources to
countries



6

Brief

AI command
assessment



09 · ARCHITECTURE & DEPLOYMENT

Security software that is secure itself

PERISAI runs entirely on the organisation's infrastructure, inside the S.A.L.T CI platform, with its tools isolated from the network and its evidence encrypted.

SEGMENTS

what people use

TINJAU

TAHAN

JEJAK

PATUH

SOC Hub

INTELLIGENCE AGENTS

through the S.A.L.T CI gateway

Attack chain parser

MITRE ATT&CK engine

Risk scoring

Threat intel enrichment

Forensic analysis

Compliance checker

TOOLS AND STORAGE

inside the organisation

Isolated Kali Linux worker

Detection engine

Scan and finding history

Encrypted evidence vault

Local CVE mirror

IOC feed store

**Air-gapped capable**

Local models and a local CVE mirror; online intelligence only where allowed.

**Isolated tooling**

Security tools run in a worker with no public port.

**Platform identity**

Sign-in, roles and audit through the S.A.L.T CI core.

**Any hardware**

Containers on the organisation's servers, VMs or private cloud.

**Many analysts**

Concurrent sessions, and project isolation for multiple clients.

**White-label reports**

Reports in the organisation's or partner's own brand.

**Part of S.A.L.T CI**

PERISAI uses the TERAS core for models, identity and audit, and its modules can watch and report on the S.A.L.T CI platform itself.

**Works with the platform**

TERAS agents can query PERISAI as a tool; S.A.L.T NEXUS operators can act on its findings on the affected servers.

**Self-run software**

PERISAI is software the organisation's own team runs. Partners can add training, setup and managed support.



10 · WHY PERISAI

One sovereign suite instead of a shelf of tools

PERISAI compared with the usual ways organisations assemble security capability.

CAPABILITY	PERISAI	SEPARATE OPEN-SOURCE TOOLS	CLOUD SECURITY SERVICES
Runs on your own servers, air-gapped	Yes	Yes	No
Usable without specialist training	Yes, plain-language AI	No	Partly
Recon, defence, forensics and compliance together	Yes, five segments	Separate tools	Partly
Evidence shared across the lifecycle	Yes	By hand	Partly
Malaysian frameworks (PDPA, ISMS-P)	Built in	No	Varies
Written reports in English or Malay	Yes	No	Partly
Data stays in the country	Yes	Yes	Varies

Categories describe typical offerings; individual products differ.

WHO PERISAI IS FOR

MARKET	TYPICAL NEEDS
Enterprise security teams	Banks, telcos, utilities, energy, healthcare and manufacturing: cover more ground with fewer people; integrate with an existing SIEM
Government and defence	Full air-gap, classified networks, Malay responses, offline CVE data and government frameworks
Universities and agencies	Self-run security for the organisation's own team, plus a guided mode for training and CTF exercises
Security consultancies	Faster engagements, client project isolation and white-label deliverables



Prepared by **CAPTZEDs**, Founder and Creator of S.A.L.T CI

www.salt.ci · info@salt.ci · perisai.salt.ci

S.A.L.T CI · Managed by Pemangkin Teknologi



PEMANGKIN TEKNOLOGI REKA PLT · 202604002776
(LLP0048022-LGN)

Catalysing Sovereign Intelligence

www.pemangkin.tech · info@pemangkin.tech

S.A.L.T CI and its components are proprietary technology, managed and commercialised by Pemangkin Teknologi. Screens and names in this document are illustrative.