

AI · GOVERNANCE · SECURITY

Gun Chun Len

Adopt AI with ambition—
and with control

Managing Director & CEO · Tech Titan Group

A balanced approach to AI opportunity, cyber risk,
trusted data and accountable decision-making.



Connect on LinkedIn

THE PERSPECTIVE

Accelerate value.
Govern the risk.

DATA

MODEL

ACCESS

OVERSIGHT

Practical security leadership
connects technology
decisions to business
outcomes.

THE STRATEGIC CONTEXT

AI changes both the opportunity and the attack surface

AI can help teams analyse more information and respond faster, while also giving attackers new ways to scale deception and exploitation.

Secure adoption begins with clear use cases, appropriate data, controlled access and human accountability for consequential decisions.

Gun Chun Len's outlook treats AI as a capability that should strengthen proven security foundations rather than replace them.

01

THE OPERATING AGENDA

Four foundations for trustworthy AI adoption

01

PURPOSE

Define the business use case

Start with a measurable problem and determine whether AI is the appropriate solution.

02

DATA

Protect what powers the model

Control sensitive information, provenance, retention and access throughout the AI workflow.

03

SECURITY

Assess new attack paths

Consider model abuse, exposed interfaces, manipulated inputs and excessive automation privileges.

04

OVERSIGHT

Keep people accountable

Set review points, decision boundaries and escalation routes for AI-supported outcomes.

02

THE LEADERSHIP LENS

Balance innovation and assurance

VALUE

Pilot where impact is visible

Choose focused use cases that can demonstrate improvement without uncontrolled exposure.

GUARDRAILS

Set boundaries before scale

Define approved data, users, integrations and decisions early.

LEARNING

Monitor outcomes continuously

Review accuracy, security signals and unintended effects as use expands.

FROM STRATEGY TO ACTION

Move from AI experiment to trusted capability

Build evidence at every stage so leaders can increase adoption with confidence.

[Read the AI & Cybersecurity Article](#)

01

Classify the proposed use case

Assess its data sensitivity, decision impact and integration requirements.

02

Design access and data controls

Limit who and what can interact with models and connected systems.

03

Test security and output quality

Challenge assumptions, misuse cases and failure modes before wider deployment.

04

Scale with monitoring

Track performance, incidents and human-review outcomes over time.