PT ALPHA CODE TECHNOLOGIES

Cyber Security Services

Defend. Assess. Educate.

An end-to-end cyber security partner for **Indonesian BFSI and enterprise.**

Founder-led from Jakarta. Built on accepted frameworks. Locally accountable.

Driven by Trust. Designed for Tomorrow.

We help Indonesian banks and enterprises defend, assess and educate across the full cyber security lifecycle, with one local team that owns the outcome.

01 DEFEND

24/7 Managed SOC

Streaming SIEM + MDR run from Jakarta on Coralogix infrastructure. Median 30-second response, 1-hour resolution.

02 ASSESS

Cyber Maturity & IT Audit

Independent maturity assessment cross-walked to NIST, to NIST, ISO 27001 and OJK. Audit-ready evidence by evidence by design.

03 EDUCATE

Human Risk Management

Bahasa-first awareness training and phishing behavior measurement via Claro. Closes the human attack surface.

Indonesia is in the middle of a cyber risk acceleration, and the regulator is moving with it

Public-record data points from BSSN, OJK, IBM and Verizon DBIR · as of March 2026

1.6B+

Cyber attacks on Indonesian targets in 2024

Source: BSSN annual telemetry report · bssn.go.id

USD 4.88M

Average financial-sector breach cost worldwide

IBM Cost of a Data Breach 2024

~25%

Industry baseline phish-prone rate, financial services

Verizon DBIR 2024

USD 1.4B

Indonesia cyber security market size, projected 2026

Statista / Mordor

THE REGULATORY TIMELINE · ALL IN-FORCE TODAY

What an audit sees vs. what an audit misses

The visible failures are well known. The deeper failures are why the visible ones keep recurring.

01

Breach headlines

Public incidents at peer institutions making board pages every quarter

02

Audit findings repeat

Same control gaps cited again year over year. Remediation Remediation plans never close.

03

Vendor sprawl

Five boutiques, five SLAs, no single accountable owner when something fires

WATERLINE

04

No single source of truth

Asset, identity and access inventories live in three different tools. No 24-hour answer to 'what do we have?'

05

Detection gaps in critical systems

Core banking, payments and customer-facing apps have less telemetry coverage than the IT infra around them

06

Human attack surface ignored

Phishing and credential theft are top breach causes, but the awareness program is annual SCORM only

Below the waterline is where Alpha Code starts. Fix the root causes once, and the visible failures stop repeating.

One local team. Three integrated workstreams. Run any of them, or all of them.

Each pillar is a complete service. Together, they form a single managed cyber program.

01 · DEFEND

Managed Detection & Response

24/7 SOC built on Coralogix, run from Jakarta

02 · ASSESS

Cyber Maturity & IT Audit

12-week PACT methodology, board-level roadmap

03 · EDUCATE

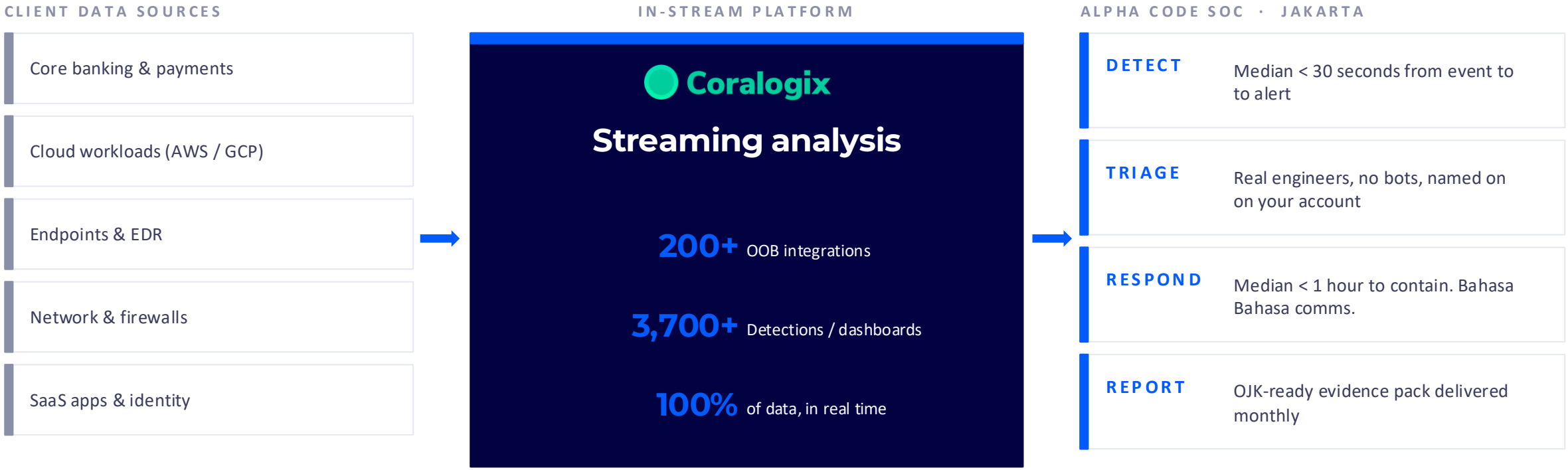
Human Risk Management

Bahasa-first awareness and phishing via Claro

The shared layer beneath all three: one PM, one steering committee, one set of SLAs, one quarterly review.

A streaming SIEM and 24/7 SOC, built on Coralogix and run by engineers in Jakarta

Real-time data flow: from your stack, through in-stream analysis, into a Jakarta-staffed response loop



Alpha Code is the SOC operator and accountable owner. Coralogix is the streaming-observability platform underneath.

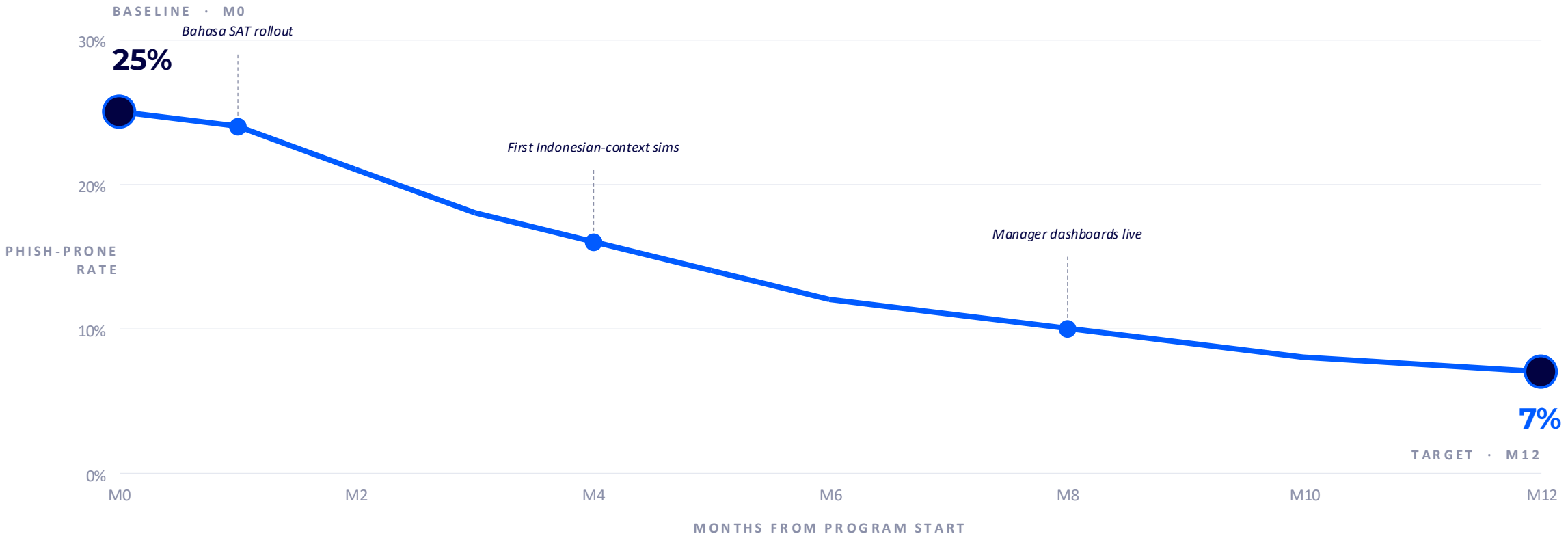
12 weeks. Four phases. One defensible board-level cyber maturity report.

Our PACT methodology — Plan, Assess, Report, Track — anchored to NIST CSF v2.0 and OJK SEOJK 29 Ch. 6

ANCHORED IN NIST CSF v2.0 · ISO/IEC 27001 Annex A · CIS Controls v8 · OJK SEOJK 29/2022 Ch. 6 · BSSN Reg 1 & 2/2024

We turn the human attack surface into a measurable, declining curve

Claro: Bahasa-first awareness training and Indonesian-context phishing, with monthly behavior measurement



*Standard target: **70% reduction** in phish-prone rate over 12 months · **~60% lower TCO** vs KnowBe4 / Proofpoint list pricing*

What you get with us that you don't get with anyone else in the market

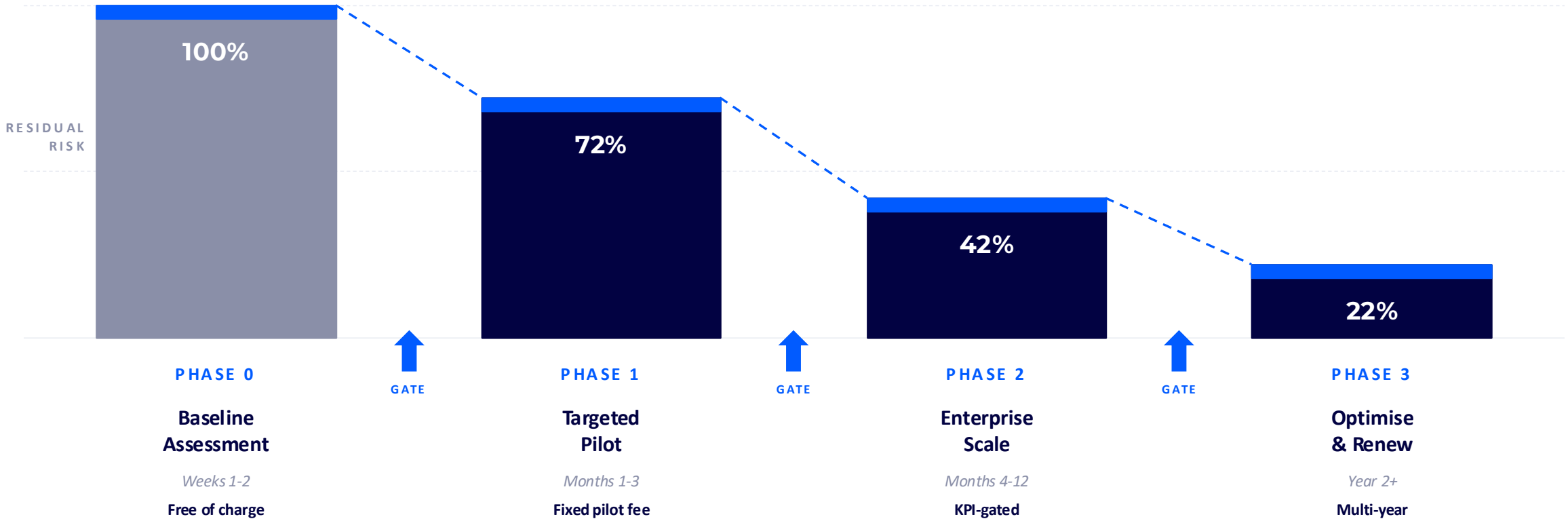
Same questions every CISO asks. Honest scoring against the two alternatives you're already considering.

	LOCAL PRESENCE	FOUNDER ACCESS	FRAMEWORK RIGOR	BAHASA SUPPORT	AGENTIC SOC
Global vendor *Global SOC, EU/US led*	◐	✗	✓	◐	✗
Offshore boutique *Outsourced to India / PH*	✗	◐	✗	✗	◐
Alpha Code *Founder-led from Jakarta*	✓	✓	✓	✓	✓

Three honest checkmarks beat five hopeful ones. We'll talk you through every cell on this slide if you want.

Residual risk drops at every phase gate. You only commit to scale once it works.

Risk-shared structure: walk at any phase boundary if KPIs are not met. No annual lock-in.



Agentic L1 SOC – the optional upgrade tier

AI agents do continuous triage and investigation. Treat alerts as hypotheses. Full audit trail. In pilot today; GA H2 2026.

STANDARD SOC . INCLUDED TODAY

- Human L1 / L2 analysts work the triage queue 24×7.
- Median signal-to-finding ≤ 5 min for critical (per SLA matrix).
- True-positive rate ≥ 80% within 30 days of go-live.
- Best fit: alert volume up to ~5K / day at parity coverage.
- Pricing: tied to log-volume slab — included in base contract.

AGENTIC L1 SOC . PREMIUM TIER

- AI agents continuously detect, investigate, and triage across the stack - 24×7, no - 24×7, no shift handovers.
- Each alert treated as a hypothesis. Agent queries, correlates evidence, produces a root-cause verdict - not a guess.
- Auto-close on confirmed false positives. Only triaged P2+ findings escalate to humans, with full audit trail of what the agent queried and why it concluded.
- Approval gates on every response action. Least-privilege access. Every action signed and logged.
- Best fit: alert volumes > 5K / day, leaner SOC operations, scale beyond standard L1 capacity.
- Pricing: separate uplift on top of base contract. Quoted in scoping.

When to layer it on: *alert volume scales beyond standard L1 capacity, OR you want triaged-only escalations to your team. In pilot today; GA H2 2026 - pre-commit slots available.*

Source: Alpha Code Agentic SOC pilot program, April 2026. Capability tier; not a swap-out for human L2 / response.

Clear ownership at every cadence. Escalation by design, not by accident.

Three lanes, five cadences, one operating rhythm - whether you buy one pillar or all three

	DAILY	WEEKLY	FORTNIGHTLY	MONTHLY	QUARTERLY
CUSTOMER *Security & IT leadership*			●	●	●
JOINT *Both teams in the room*	Operations stand-up Alert triage In-channel updates	● Project SPOC sync Status snapshot Risks & blockers	● Program management Milestone tracking Resource alignment	● KPI review Evidence drop Security readout	● Steering committee OJK evidence pack Board readout
ALPHA CODE *PM, engineers, analysts*	●	●			●

Escalation: unresolved items in weekly sync escalate to fortnightly governance, then to steering committee within one week.

You meet our directors. The same people who scope the work also run it.

> **We're the people you'll actually work with.** Not a sales team, not a CSM-by-ticket, not an offshore handover. The directors who scope it run it.

Bhavna Laroya

Managing Director

25+ years in financial-services leadership across the US, India and SE Asia. Former MD of PT Akraya International. Visiting Faculty at IFC.

Mohit Bhansali

Head of Technology

Technology leader with 15+ years across financial services, blockchain and ecommerce. Former CTO of Star Max. Cybersecurity Cybersecurity and platform delivery.

Naren Krishnan

Cyber Security SME

12+ years in Big-4 cyber consulting. Audits, technical reviews, infosec assessments and BIA. Former Asst. Director, Cyber Risk.

Plus a delivery bench of Jakarta-based security analysts, SOC engineers and content authors. Surge capacity from a regional partner network.

Credentials that match the standard you're held to

Every engagement is led and reviewed by certified practitioners. No silent juniors on critical work.

AUDIT & COMPLIANCE

Lead Auditor

Qualified to conduct certification-grade ISMS audits against ISO/IEC 27001:2023

Lead Implementer

Designs and operationalises information security management systems end to end

Governance, Risk & Compliance

OCEG-certified in governance, risk and compliance program design and design and oversight

SECURITY & RISK

Certified Information Systems Auditor

ISACA's gold standard for IS audit, control and assurance professionals

Certified Ethical Hacker

Offensive security certification covering attacker tools, tactics and techniques

Incident Response

Trained in incident triage, containment, forensics and post-incident review

Held by named individuals on your engagement team - not just by the firm on a website.

A two-week baseline. On us.

Before you commit to anything, see exactly what we would see - and what we would do about it.

COMPLIMENTARY

Cyber Security Baseline Assessment

Two weeks · Zero cost · Zero commitment to proceed

WHAT YOU COMMIT	Two of your security or IT team for ~6 hours, spread across two weeks.
WHAT YOU RECEIVE	Current-state audit, tooling and integration scoping, risk baseline baseline and an OJK gap assessment - delivered as an executive-executive-ready report.
WHAT IT COSTS	Zero. No procurement, no purchase order, no obligation to proceed.

LET'S TALK

Mohit Bhansali

Head of Technology

mohit@alphacode.tech

+62 21 29885600

PT Alpha Code Technologies
DBS Bank Tower 19F
Jl. Prof. Dr. Satrio Kav. 3-5
Jakarta 12940

Driven by Trust. Designed for Tomorrow.