KGMM

PRACTICE BRIEF

STRATEGIC ADVISORY & EXECUTION

Threat Defense & Ops

Threat visibility, identity protection, and operational resilience that support day-to-day decisions.

THE BUSINESS CHALLENGE

Disconnected intelligence, access controls, and recovery arrangements can slow decisions during disruption. Operational teams need relevant signals, clear responsibilities, and tested response paths.

OUR APPROACH

Start with critical operations and dependencies. Review detection, access, and continuity needs; agree coverage and escalation responsibilities; and exercise the procedures that matter.

SERVICES IN THIS PRACTICE

Actionable Threat Intelligence

Translate relevant threat information into specific defensive and business actions.

ICS & OT Industrial Security

Assess industrial environments with safety, availability, and operating constraints in view.

Identity-First Security & PAM

Connect access, privilege, lifecycle changes, and accountable business ownership.

Managed Detection & Response

Structure coverage, escalation, and response responsibilities around your environment.

Cyber Resiliency & Continuity

Link recovery priorities, dependencies, and tested continuity procedures.

TYPICAL ENGAGEMENT OUTPUTS

- Threat priorities and action plans
- Detection coverage and escalation model
- Access and privilege improvement roadmap
- Recovery dependencies and exercise findings

Request a consultation

Explore this practice online

Monitoring coverage, response availability, and service levels are confirmed within the agreed engagement.