cloud titans

Discovery → Security → SOC for the Microsoft-centric Enterprise

4–6 weeks
Discovery sprint

MSS / 24×7 SOC
Microsoft-first

DORA / NIS2-aligned
EU & Middle East

IHR Insights: Cloud Titans – Challenger Vendor Profile

Discovery → Security → SOC: ROI-led Microsoft defense for EU/UK & Middle East mid-market

About this report

This report distils the Cloud Titans proposition into a clear, decision-ready view for executives and investors. It combines a SCOT analysis (strengths, challenges, opportunities, threats) with an evidence-based Product–Market Fit read, a UK/EU (DACH/Poland) and Middle East market outlook, and a head-to-head competitive heat map across cloud advisory, app-usage discovery, Microsoft security managed services, 24×7 SOC, governance/compliance, and analytics.

We also include an investor take on the revenue model and unit economics (discovery sprints → managed security MRR → SOC expansion), an adoption verdict on what it will take to "cross the chasm" (references, credentials, repeatable runbooks), and a pragmatic buyer-side caution checklist mapped to Cloud Titans' license prerequisites, data handling C sovereignty, SLAs/MTTA-MTTR targets, and partner delivery assurances.

The aim: help you validate scope vs. timeline, quantify value creation (license rationalization → savings C reinvestment; E5 security activation → policy coverage C MTTR gains), and de-risk compliance and operations (DORA/NIS2 alignment, data ownership, incident workflows)—so you can make a confident go/no-go and negotiate the right acceptance criteria, pricing exhibits, and support terms.

Introduction Market Context

Cloud Titans enters a crowded but opportunity-rich arena with a pragmatic "discover → secure → operate" storyline: short, outcomes-driven discovery sprints (AppNavi) to expose shadow IT and shelfware, then tiered Microsoft-first managed security and a 24×7 SOC (Hunters) to harden the estate and sustain value.

The timing is favourable. Across the UK/EU mid-market and lower enterprise, CIO/CISOs are reallocating budgets from one-off projects to recurring assurance as regulatory pressure (DORA/NIS2), rising SaaS sprawl, and board-level demands for measurable risk reduction converge. Buyers with under-utilized E3/E5 licenses want proof that spend converts into policy baselines, faster MTTA/MTTR, and fewer incidents—not more tooling.

At the same time, digital-adoption programs are shifting from pilots to platform plays, making telemetry-led rationalization an easy on-ramp for security and cost outcomes. Incumbent GSIs still win on brand and audit depth, while local boutiques hold relationships; the open space sits with challengers who can mobilize quickly, publish clear runbooks and SLAs, and package advisory with managed services.

Executive Snapshot - Cloud Titans

Cloud Titans is a newly formed, Microsoft-first challenger that packages Advisory → Discovery → Managed Security/SOC into a fast-mobilizing, partner-enabled service stack. The snapshot below distils what matters at a glance: the three-pillar proposition and delivery model, the founders' execution pedigree, a clearly tiered security catalogue mapped to Microsoft license prerequisites and SLAs, the telemetry-led discovery motion that funds itself via rationalization in 4–6 weeks, and current geographic coverage.

Read this as a quick credibility and fit check before diving into PMF, references, and the operating playbook.

© 2025 IHR Insights

COMPANY AT A GLANCE

- **Founded:** 2024 (UK); Poland entity planned. Status: early stage; no bookings declared at time of writing.
- **Offers:**
    - What they do: 3 pillars — Advisory, Discovery (AppNavi-powered), and Managed Security / 24×7 SOC (Hunters-powered). They claim a +1,600-consultant partner network, with mobilization in 3–5 days for internal/external talent pools.
    - Leadership narrative: Founder experience spans Airtel's SharePoint modernization, Di Pocket's PCI→DORA/NIS2 uplift, and SoftwareOne's post-merger GTM (G18 hunting). Company itself is new (UK April 2024; Poland entity planned) and reports no bookings yet.
    - Security catalogue: Tiered M365 Defender services, SOC with Hunters SIEM, clear license prerequisites (E3/E5 add-ons, Entra ID P1/P2) and defined incident/SLA rhythms.
    - Discovery value prop: AppNavi telemetry to expose shadow IT, low usage and rationalization candidates; 4–6-week outcomes driving cost take-out / re-investment.
- **Coverage:** DACH/UK/Nordics/Middle East via named ambassadors; +1,600 consultant partner access.

Why this matters now: EU DORA C NIS2 raise the bar for operational resilience and monitoring. Buyers with E3/E5 estates want measurable value from Microsoft security and rapid ROI from software rationalization. Cloud Titans packages both into a land-and-expand motion.

SCOT ANALYSIS

Strengths

- **Senior operator DNA** with credible programs executed by founders (Airtel; SoftwareOne integration; financial-sector controls at DiPocket).
- **Fast mobilization** and **broad tech bench** (internal C external matrices; multi-stack: Azure/AWS/GCP, SAP, Dynamics, AI/ML).
- **Tightly packaged offers**: Discovery (AppNavi) and Microsoft-first Managed Security (Entra/Defender) with a clear tiering C license map; attachable 24×7 SOC (Hunters).
- **Regional coverage** with named ambassadors in key buyer markets (DACH/UK/Nordics/ME).

Challenges

- **No bookings / new brand** → reference ability C risk checks will be buyer objections #1.
- **High partner reliance** (AppNavi, Hunters, Clouds On Mars, LithyTree, etc.) → margin control C delivery assurance must be proven.
- **Crowded categories** (MSS/MDR, SIEM/SOC, cloud advisory, DAP) with incumbent trust and certifications.

Opportunities

- **Regulatory catalysts**: DORA applies from 17 Jan 2025 to EU financials; NIS2 transposed from 17 Oct 2024—both force uplift in governance, monitoring, and incident readiness.
- **Market tailwinds**:
    - Managed Security Services 2025 est. $39–40B; projected low-double-digit CAGR to 2030.
    - SIEM ≈ $10.8B in 2025, ~12% CAGR to 2030.
    - Digital Adoption Platforms ~$1.9B in 2025, fast growth into the 2030s.
    - Microsoft-centric buyers with E3/E5 estates seeking rationalized security and measurable ROI from licenses (Defender/E5 Security).

Threats

- Global GSIs/Big 4 expanding MSS C cloud security; hyperscaler PS; local boutiques with entrenched logos in DACH/PL; and pure-play MSSPs (SOC-led). The Cloud Titans pack itself lists several regional competitors.

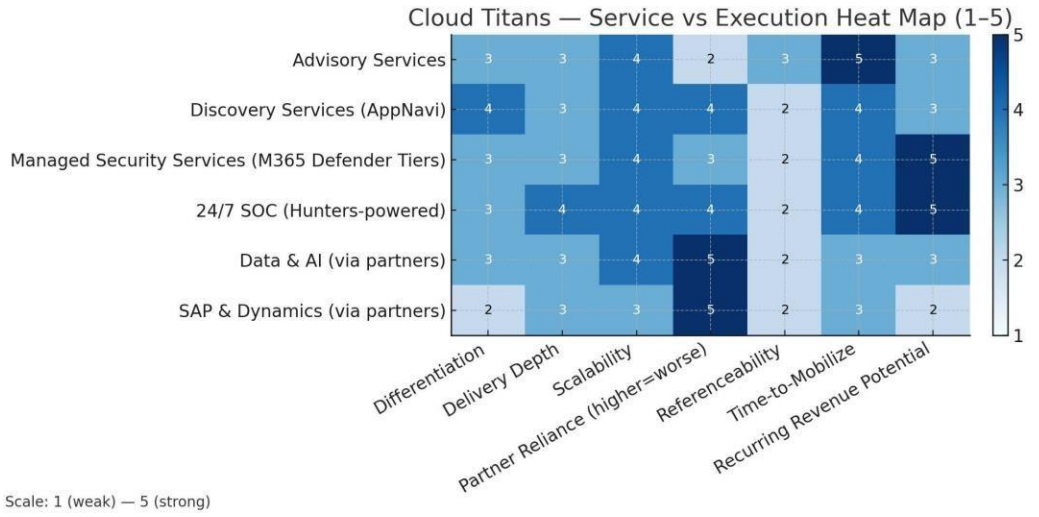
Product–Market Fit (by offer)

Offer	Pain it solves	Fit today	Critical proof needed
Discovery (AppNavi)	Shadow IT, shelfware, low adoption; need quantified rationalization in 4–6 weeks	Strong for cost-pressured CIO/CFO teams; aligns to DAP growth	2–3 anonymized quick-wins showing %license reduction, re-investment funnel, and compliance uplift.
M365 Managed Security (Tiered)	Under-used E3/E5 security; inconsistent policies; rising phishing/endpoint risk	High in 500–5,000 seat enterprises on Microsoft	SOC runbooks, MTTA/MTTR, before/after risk metrics, incident case studies.
24×7 SOC (Hunters)	Signal overload; alert fatigue; lack of correlation/content	Good for orgs wanting SIEM value fast with modern analytics	Prove time-to-detect, false-positive reduction, and integration breadth; 90-day outcomes.
Senior Advisory	Strategy/controls gaps; regulatory uplift	Good wedge into DORA/NIS2 programs	Publish a controls framework C audit-ready artifact (policy sets, playbooks).

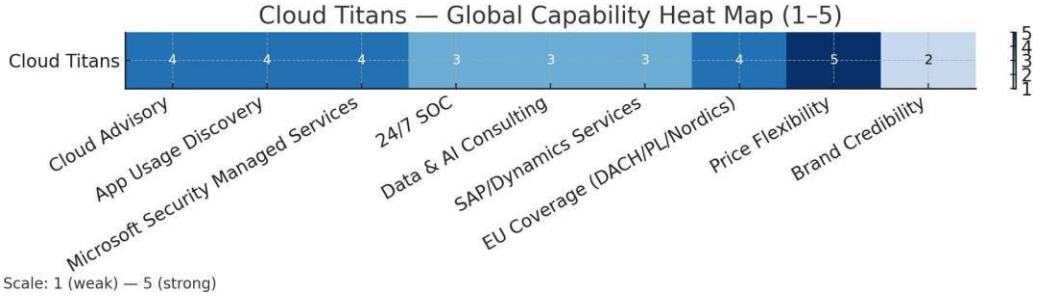
COMPETITORS HOW CLOUD TITANS STACKS UP

The competitive field spans four archetypes: **local boutiques** with entrenched relationships in Poland/DACH, **Big 4/GSIs** with audit-grade assurance and vast benches, **MSSP pure-plays** optimized for SOC execution and certifications, and **DAP vendors** whose platforms drive telemetry and adoption. Against this backdrop, Cloud Titans' edge is a packaged **Discovery → MSS → 24×7 SOC** motion that lands with measurable value and expands into recurring security outcomes. It should out-agile GSIs on price/speed, out-package boutiques with managed services, and out-scope DAPs by pairing telemetry with advisory and run. The trade-offs: Titans must close gaps in **brand/assurance** versus GSIs and **SOC maturity** versus pure-play MSSPs—making references, credentials, and documented runbooks the critical equalizers.

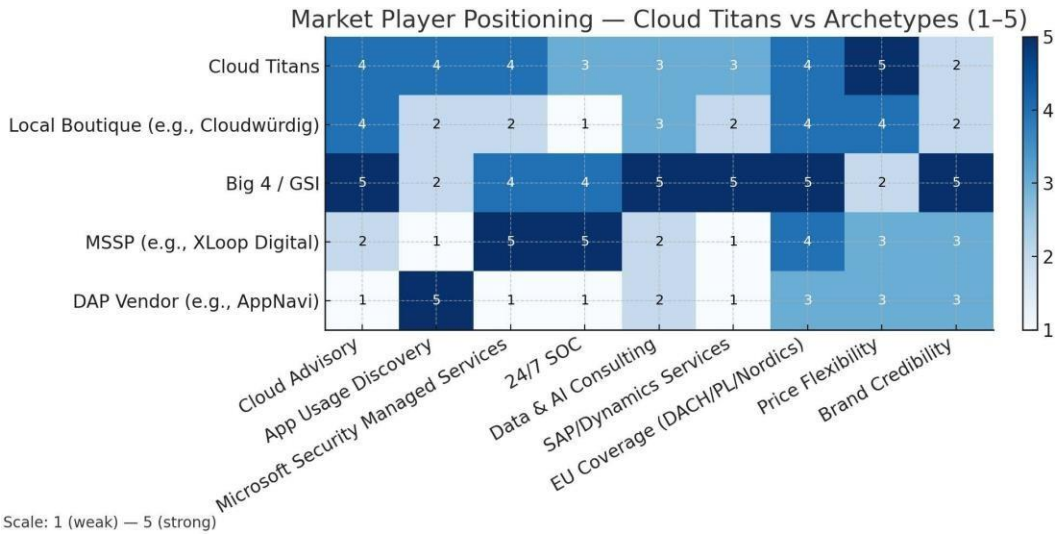
Regional boutiques (Poland C DACH) listed in the pack — e.g., Cloudity, IT-Dev, Cloud Partners, SecuRing, AI Busters, Cloudwürdig, Cloudwerkstatt, Codecentric (small-projects), CloudMounter, AI4BD. These players anchor cloud advisory, security audits, and data/AI for SMEs.



Opinions & Methodology. Capability scores, heat maps, and competitive characterizations are opinions based on our methodology, assumptions, and vendor/public materials as of September 2025; they are directional, not statements of fact, and not a substitute for buyer testing or RFPs. Vendors may submit factual corrections with evidence at the contact listed herein.



Opinions & Methodology. Capability scores, heat maps, and competitive characterizations are opinions based on our methodology, assumptions, and vendor/public materials as of September 2025; they are directional, not statements of fact, and not a substitute for buyer testing or RFPs. Vendors may submit factual corrections with evidence at the contact listed herein.



Opinions & Methodology. Capability scores, heat maps, and competitive characterizations are opinions based on our methodology, assumptions, and vendor/public materials as of September 2025; they are directional, not statements of fact, and not a substitute for buyer testing or RFPs. Vendors may submit factual corrections with evidence at the contact listed herein.

Archetype comparison (summary)

- **Versus Local Boutiques:** Cloud Titans brings packaged MSS/SOC and a broad partner bench; boutiques often win on incumbency and narrow expertise.
- **Versus Big 4/GSIs:** Cloud Titans can beat on price/agility and E5-centric packaging, but will trail in assurance, brand, and bench depth.
- **Versus MSSP pure plays:** Cloud Titans' edge is advisory + discovery landing motion; MSSPs outgun on SOC maturity C certifications.
- **Versus DAP vendors:** Cloud Titans' advisory + DAP-driven rationalization story is broader; DAPs win on platform depth.

WHAT'S DIFFERENT

- **Discovery → Security flywheel:** 4–6-week discovery establishes ROI C compliance angles; security tiering and SOC attach produce recurring value.
- **Microsoft-first packaging:** Clear Entra/Defender license maps and SOC handoffs, easier stakeholder buy-in.

BUYER BENEFITS

- **Fast time-to-value**: quantified license optimization and security baselines within a quarter.
- **Single throat to choke** across advisory, discovery, and run services.

CAUTIONS

1) New-vendor maturity references

Cloud Titans is a new entity (UK Apr-2024; Poland planned) and reports no bookings yet. Require 2–3 like-for-like references (Discovery, MSS, SOC), sample artifacts (runbooks, reports), and named delivery leads before award.

Ask for: client references, anonymized deliverables (policy baselines, detection packs), CVs of named leads, and a 90-day success plan.

2) Partner-reliant delivery (subcontractors, flow-downs)

The model leans on a partner network (+1,600 consultants) and named technology/services partners (e.g., AppNavi for discovery; Hunters for SIEM/SOC; Clouds On Mars for data/AI; LithyTree for SAP/Dynamics; XLoop Digital for 24/7 SOC). Ensure prime-contractor accountability, subcontractor approval rights, and flow-down of SLAs, security, and DPAs.

Ask for: list of named subs, their roles, certifications, data-processing agreements, right to replace/approve subs, and continuity plans if a partner exits.

3) Microsoft licensing prerequisites scope clarity

Security tiers and SOC services have explicit license requirements (e.g., Entra ID P1/P2, M365 E3/E5 and E5 Security add-on). Validate you already own (or budget for) the prerequisites, and ensure the SoW maps which features are included per tier to avoid scope gaps.

Ask for: a license matrix tied to your tenant; confirmation of no upsell dependency mid-term; change-management path if your license posture changes.

4) SOC architecture, data handling SIEM costs

SOC is Hunters SIEM–powered with 24/7 monitoring and monthly status reports. Clarify data residency, log sources, ingestion/retention costs, content ownership (detections, playbooks), and onboarding timeline. Ensure incident handoffs and MTTA/MTTR targets are explicit.

Ask for: architecture diagram (data flows), retention policy, content IP terms, onboarding plan (days), and reporting pack samples.

5) SLAs, KPIs service credits

Documents reference incident rhythms and monthly reporting; lock down numerical SLAs (e.g., MTTA/MTTR by severity), measurement method, and service credits for misses. Include an exit-for-cause clause tied to sustained under-performance.

Ask for: SLA schedule, measurement tooling, governance calendar (QBRs), and remediation plan template.

6) Discovery data privacy (GDPR, DPIA, consent)

Discovery is AppNavi-powered and positioned as GDPR-compliant, collecting browser/app usage to identify shadow IT, low usage, and rationalization targets in 4–6 weeks. Confirm DPIA outcomes, lawful basis, data minimization, pseudonymization/anonymization, and consent flows for end-users.

Ask for: DPIA, data schema, retention C access controls, and the exact fields captured (incl. any PII).

© 2025 IHR Insights

7) Geography, staffing mobilization reality

They cite ambassadors across DACH/UK/Nordics/Middle East and show a mobilization flow with 14-day "mobility period". Validate actual delivery team locations, language coverage, and on-call rotation. Require right-to-review named CVs before mobilization.

Ask for: staffing plan by workstream, language/country coverage, background checks, and substitution policy.

8) Runbooks, content acceptance criteria

Packaged services reference policy baselines, Intune/Defender configurations, and SOC operations. Insist on documented runbooks, versioning, and acceptance tests per deliverable (e.g., policy coverage %, high-severity detection test pass).

Ask for: deliverable checklist, test cases, and sign-off criteria tied to invoice milestones.

G) Commercial terms (TsM vs Managed Service; renewals)

Security tiers denote MS (Managed Service) vs TCM. Protect renewals (price-cap, CPI linkage), onboarding fee vs monthly split, and pro-rata ramp-down. Add co-termination and a fair termination-for-convenience window.

Ask for: rate card by role/tier, indexation rules, discount guardrails, and transition-out assistance priced up front.

10) Regulatory alignment (DORA/NIS2)

If you're EU-regulated, require mapping of services to operational-resilience controls and incident reporting duties. Ensure tabletop exercises and evidence packs meet auditor/regulator expectations (policy, logs, trails).

Ask for: control-to-regulation matrix, evidence templates, and regulator-grade reporting examples.

11) Tooling lock-in reversibility

Define data export for AppNavi telemetry and Hunters content (detections, dashboards), IP ownership of bespoke content, and transition-out SLAs at contract end.

Ask for: export formats, fee caps for transition, and license to use detection content post-contract.

12) Insurance, liability breach handling

Set minimum insurance levels (PII/cyber), define liability caps with carve-outs (e.g., data protection breaches), and require breach notification timelines and regulator support. *(General buyer safeguard—tie to your internal standards.)*

Ask for: insurance certificates, breach playbook, and named contacts for regulator interactions.

13) Performance reporting cadence

They promise monthly status and a metrics/KPI framework. Lock in QBRs, ad-hoc escalation paths, and board-ready reporting packs (trendlines, risk register).

Ask for: sample reports, KPI definitions, and how MTTA/MTTR are calculated (clock start/stop).

© 2025 IHR Insights

14) Change control scope drift

SOCs expand over time (new log sources, use cases). Mandate a change-control board, pre-priced unit costs for additional sources/use-cases, and hard out-of-scope definitions.

Ask for: rate card for new integrations/use cases, lead times, and acceptance tests for added scope.

PRICING PACKAGING (INDICATIVE)

- **Discovery Sprint:** fixed fee (4–6 weeks) + rationalization roadmap.
- **MSS:** tiered MS with license prerequisites; per-user or per-tenant.
- **SOC:** monthly + onboarding, outcome KPIs (MTTA/MTTR).

IDEAL BUYERS

- **FSI / manufacturing** orgs with E3/E5, <5k seats, DORA/NIS2 timelines.

ANALYST POV (IHR INSIGHTS)

Cloud Titans is an execution-focused challenger packaging well-chosen partners (AppNavi, Hunters) into a pragmatic cost-reduction + risk-reduction story. The firm must rapidly accumulate references, lock in Microsoft credentials, and publish SOC outcomes to scale. If they do, we expect competitive win-rates in mid-market EU accounts where GSIs feel "too big" and boutiques lack 24×7 security depth.

IHR Verdict: *Promising early mover for Microsoft-centric DORA/NIS2 programs; shortlist for 500–5,000-seat EU enterprises seeking quick ROI and a unified Discovery → Security motion.*

CONFIDENCE TRIGGERS (UP / DOWN)

Confidence ↑ (bullish if observed in next 90–120 days)

- References: 3–5 live customer references split across Discovery, MSS, and 24×7 SOC, each with quantified outcomes (e.g., ≥15% license rationalization, MTTA ≤15 min / MTTR ≤4 hrs by severity).
- Credentials C assurance: Microsoft Solution Partner for Security (or equivalent badges), ISO 27001 plan in motion, SOC 2 Type I underway; published runbooks C acceptance tests.
- Conversion funnel health: ≥40–50% Discovery → MSS conversion and ≥30% MSS→SOC attach in target ICPs; 3× forward pipeline coverage against next-two-quarter bookings.
- Delivery reliability: On-time onboarding (≤30 days), QBR cadence met, service credits near zero; false-positive rate trending down month over month.
- Regulatory wins: 1–2 DORA/NIS2 programs signed with auditor-grade evidence packs delivered.
- Unit economics: Gross margin on MSS/SOC ≥45–55% with subcontractor mix ≤30% of delivery hours; DSO ≤45 days.
- Team scale C stability: Named leads backed by a bench; voluntary attrition in delivery <12% annualized.

© 2025 IHR Insights

Confidence ↓ (bearish if observed)

- Reference gaps / slips: Still 0–1 verifiable reference after two quarters; missed go-lives or scope rework on first logos.
- Partner fragility: Loss of a key partner (e.g., SIEM/DAP) or SLA/SLO breaches not flowed down to subs; unclear IP/exit terms for content and data.
- License mismatch: Repeated delays due to E3/E5/Entra prerequisite gaps; upsell surprises mid-contract.
- SOC maturity signals: MTTA/MTTR not published or worsening, onboarding >45 days, limited detection content beyond vendor defaults.
- Commercial stress: Margin <35% on managed services, heavy TCM dependence, renewals pushed or discounted >20% to retain accounts.
- Governance misses: Skipped QBRs, weak monthly reporting, or gaps in DPIA/data-sovereignty documentation for Discovery workloads.
- Talent risk: Over-reliance on a few contractors; inability to staff multilingual DACH/PL workstreams inside SLA.

Baseline view: Constructive/Watch — tilt up with proofs on references, credentials, and funnel conversion; tilt down if partner reliance isn't governed by hard SLAs/DPAs or if SOC metrics stagnate.

ABOUT IHR INSIGHTS

IHR Insights is an independent research and advisory firm delivering market intelligence, custom research, and go-to-market consulting across ICT/Cloud, Data & AI, Security/Telecom, GCC and Healthcare. Beyond vendor/product evaluations, we run primary & secondary research, competitive/benchmark studies, opportunity assessment & market entry, and executive content development (CXO reports, buyer guides). Our publications stay vendor-neutral and evidence-based—grounded in live product walk-throughs, reference checks, and scenario testing—so leaders can move from slideware to measurable outcomes with clear fit, value, and risk signals. www.ihrinsights.com

Independent research provided "as is"; no warranties or liability. No endorsement or professional advice. Findings may change without notice.

Disclaimer & Limitation of Liability. This report is independent, vendor-neutral research and is provided "as is," for informational purposes only. IHR Insights makes no warranties (including accuracy, completeness, timeliness, merchantability, fitness, or non-infringement) and disclaims liability, to the maximum extent permitted by law, for any loss or damages arising from use of or reliance on this report. No endorsement or professional advice is implied. Findings reflect IHR Insight's opinions as of the publication date and may change without notice; no duty to update is assumed.

***Corrections.** If you believe this report contains a factual error or uses your IP beyond fair use, email sreeni@ihrinsights.com with supporting evidence; we will review and, if substantiated, issue a correction or takedown within 10 business days.*