IDYSSEUS

Identity Visibility Accelerator

Engagement Framework

Tier Classification → Visibility Assessment → Onboarding & Enablement → Measured Visibility

Read-only identity visibility platform

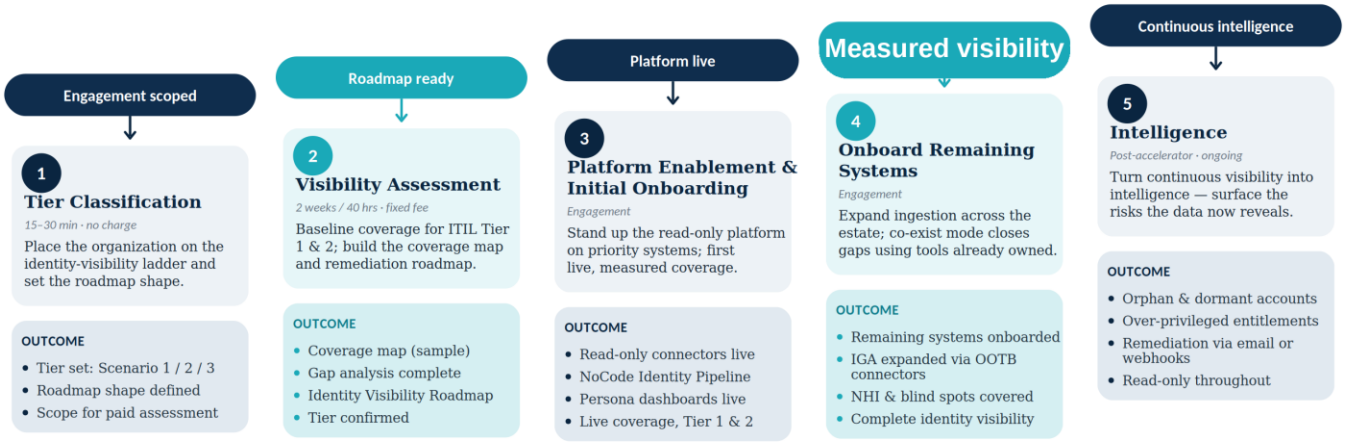
Purpose

Most medium-to-large organizations are assessment-weary. What they want is remediation. This workflow is built for that. It keeps assessment to a tight, fixed gate and moves quickly to the part that delivers value — onboarding systems until identity visibility is measured across the onboarded estate.

The gap it closes is the visibility gap. Most organizations already run IGA and PAM; each governs a slice of the estate, and none can report the complete identity ecosystem or how much of it is actually covered. The Accelerator establishes that coverage and then closes the visibility gap, system by system, to measured coverage — reusing what the customer already owns and pointing new effort only where a genuine blind spot exists.

The Engagement Pipeline

Four stages, in order. The first two are deliberately small gates; the engagement's substance — and the customer's value — is in Stages 3 and 4, where the visibility gap is actually closed to measured coverage.



1. Engagement Scenarios

Tier classification (Stage 1) places the organization on an identity-visibility ladder. Idysseus's role is constant across all three tiers — the same read-only centralized visibility-intelligence and access-certification framework sitting on top of whatever exists underneath. Only the size of the blind spot changes: largest in the fully manual shop, smallest in the mature IGA shop. None of these organizations can measure their coverage today, which makes the platform relevant across the entire spectrum rather than one segment.

Scenario	What they have today	Governance	Biggest blind spot	Idysseus's role
1 — Fully manual	No ILM / IGA automation; JML by ticket, spreadsheet, manual account creation	Manual	Everything — no tool gives even a partial inventory; NHI entirely dark	First unified identity ecosystem and the centralized framework to certify and oversee access from
2 — ILM, manual governance	ILM tool automates human joiner / mover / leaver	Manual	Whether the resulting access is appropriate; NHI sits outside the ILM	Visibility-intelligence and certification layer on the ILM; adds the NHI the ILM never sees
3 — IGA, mixed governance	IGA governs some systems and identities	Mixed	Ungoverned humans and NHI in the gaps (the Salesforce / OAuth case)	Co-exist mode: expand the existing IGA with low-cost OOTB connectors; Idysseus fills the rest of the blind spots and covers the certification gap

Scenario 1 — Fully manual (manual ILM, manual governance)

The largest gap on the ladder. With no IGA or PAM, nobody can produce even a partial identity inventory, so orphaned accounts, leaver access, entitlement creep, and every non-human identity sit completely dark. Idysseus delivers the first unified identity ecosystem and a centralized framework to certify and oversee access from — one view of who-has-what across the estate, blind-spot and excessive-entitlement surfacing, audit completeness, and structured access certification. It makes the manual process measurable and shows exactly where lifecycle automation is worth buying later. It does not automate JML and does not write back to or revoke in source systems.

Scenario 2 — ILM tool (human), manual governance

Lifecycle mechanics are handled for humans, but no one can see whether the access those identities accumulate is appropriate, and NHI lives entirely outside the ILM. Idysseus is the centralized visibility-intelligence and access-certification framework layered on the ILM: the ILM moves identities through their lifecycle, Idysseus measures the result, structures certification, and surfaces the NHI the ILM never touches. Manual governance goes from blind to measured and certifiable, without replacing the ILM.

Scenario 3 — IGA, mixed governance (most common)

IGA governs part of the estate, but blind spots remain — ungoverned Salesforce humans, ungoverned OAuth tokens. Idysseus runs in co-exist mode: it works with the client to expand the existing IGA using low-cost, out-of-the-box connectors, then fills the rest of the blind-spot gaps itself, and its certification covers the gap where the IGA does not.

2. Stage 1 — Tier Classification

A 30-minute intake conversation that places the organization on the identity-visibility ladder. It runs before any statement of work and carries no charge. It is a sales and scoping step — not the paid assessment — and it collects no coverage data.

Element	Definition
Objective	Place the organization on the identity-visibility ladder (Scenario 1, 2, or 3) and set the shape of the remediation roadmap.
When	Pre-engagement, before the SOW. Does not consume assessment hours.
Effort	30 minutes · no charge.
What we ask	Do you run manual / ILM / IGA today? What is governed vs. ungoverned? How many systems are ITIL Tier 1 & 2?
Output	Tier classification and roadmap shape, used to scope the paid assessment.
Not in this stage	No inventory collection, no coverage measurement. That begins — and ends — in Stage 2.

3. Stage 2 — Visibility Assessment (Paid)

A fixed **2-week / 40-hour** engagement, pivoted strictly on identity-visibility coverage. It baselines current coverage and produces a sequenced remediation roadmap, anchored in the customer's **ITSM** (ServiceNow et al.) as the authoritative system inventory and output from key stakeholders— so the assessment measures the real estate rather than a guess.

Element	Definition
Objective	Baseline current-state visibility coverage and produce the Enterprise Identity Visibility Roadmap.
Effort	2 weeks / 40 hours · fixed fee. ITIL Tier 1 & 2 first; lower tiers sequenced into Stage 4.
Participants	System owners, security / IAM stakeholders, GRC, and the Idysseus engagement team.
Input	ITSM system inventory; existing IGA / PAM / ILM configuration; HR source of truth (e.g., ADP).
Deliverable	Enterprise Identity Visibility Roadmap: current-state coverage map plus prioritized remediation roadmap.
Exit criteria	Coverage map signed off; remediation roadmap sequenced and costed; tier confirmed.

3.1 Assessment activities

1. **Reconcile inventory.** Pull in-scope systems from ITSM / CMDB; confirm ownership and ITIL criticality.
2. **Map identities.** Human (FTE, contractor, vendor) and non-human (service accounts, OAuth tokens, SPNs) per system — and what governs each.
3. **Analyze the gap.** Record the action per system: confirm where coverage is complete, existing IGA / PAM where a tool fits, Idysseus where nothing else sees the identities.

4. **Sequence the roadmap.** Order by ITIL criticality so new spend lands only on genuine blind spots.

3.2 Deliverable — the "sample" coverage map

A sample across three representative systems: one fully covered, one partial, one blind spot.

ITIL	Category	System	Human identities	Human mgmt	NHI	NHI mgmt	Coverage action
Tier 1 & 2	HRIS / HRMS	ADP	HR employees	None	n/a	—	Idysseus Platform
Tier 1	IDP	Active Directory	FTE, contractor, 3rd-party vendor	IGA (Saviynt)	Service accounts	PAM (Delinea)	Complete coverage
Tier 1 & 2	CRM	Salesforce	Sales, customer service	None	4 OAuth tokens (integration)	None	Saviynt (human) + Idysseus (NHI)

Reading the map

Active Directory is the model. Humans governed by Saviynt, service accounts vaulted in Delinea — coverage is already complete. Idysseus confirms and measures it; it replaces nothing.

ADP is the authoritative HR source but isn't "managed" by IGA / PAM in a coverage sense. Idysseus provides the visibility that ties ADP HR users to the rest of the estate.

Salesforce is the classic blind spot. Human access isn't governed (onboard into the existing Saviynt instance); the four OAuth integration tokens are governed by nothing — Idysseus provides that NHI visibility. Right tool for each gap, not rip-and-replace.

4. Stage 3 — Platform Enablement & Initial Onboarding

Idysseus deploys as the continuous, read-only visibility and access-certification layer on the priority (Tier 1 & 2) systems mapped in the assessment. The platform ingests identity data uni-directionally and never writes to, provisions in, or revokes from source systems.

This is typically performed by Idysseus's Service team.

Element	Definition
Objective	Stand up continuous coverage measurement and access certification on the priority systems, without disrupting or replacing the existing IGA / PAM / ILM stack.
Architecture	Data plane (connector and agent-based ingestion, no-code pipeline, privacy gateway, drift detection) and control plane (persona views for CISO, Zero-Trust / identity teams, SOC / IR, GRC).

4.1 Initial Onboarding steps

1. **Environment provisioning.** Stand up the customer tenant.
2. **Configure Two Read-only connectors.** Configure least-privilege, read-only credentials and scopes to each priority source (AD, Entra, Salesforce, ADP).
3. **Deploy Two No-code pipeline (Agent-based).**
   - Map legacy and non-standard systems through the no-code pipeline so onboarding does not require custom development.
   - Privacy gateway to detect and mask or hash sensitive data from source system.
   - Detect source system's scheme drift and provides alerts.
   - Deploy ingestion agents and establish uni-directional data flow from source systems into the platform.
4. **Coverage views & dashboards.** Activate control-plane views — board-grade coverage KPI for the CISO, operational detail for identity, SOC / IR, and GRC teams.
5. **Access-certification framework.** Configure certification: present access to reviewers and capture attest decisions in-platform.

5. Stage 4 — Onboard Remaining Systems → Measured Visibility

Expand ingestion identified in assessment report.

Element	Definition
Objective	Extend coverage from the Tier 1 & 2 baseline to the full estate, achieving continuously measured identity visibility across the estate.
Co-exist mode	Where IGA governs part of the estate, help expand it with low-cost out-of-the-box connectors; Idysseus fills the remaining blind spots and covers the certification gap.
Exit criteria	Measured coverage across the estate; drift detection live; operational handoff complete.

5.1 Remaining-systems steps

1. **Prioritize remaining systems.** Sequence the rest of the estate by ITIL criticality and effort, following the Stage 2 roadmap.
2. **Expand IGA via OOTB connectors (co-exist).** Where the customer's IGA already governs, identify low-cost out-of-the-box connectors to extend its coverage.
3. **Onboard remaining systems to Idysseus.** Ingest the identities no out-of-the-box IGA's connector reaches, including NHI and blind-spot accounts and entitlements.
4. **Close the certification gap.** Where the IGA does not certify, Idysseus's certification covers it.
5. **Confirm measured coverage & hand off.** Verify the coverage view shows measured coverage across the estate; deliver the runbook and transition to steady state.

6. Stage 5 — Intelligence (Post-Accelerator)

Once coverage is measured, the platform turns continuous visibility into intelligence — surfacing the risks the data now makes visible. This runs after the Accelerator, as an ongoing program.

- **Orphan and dormant accounts.** Flag accounts with no owner or no recent activity.
- **Over-privileged entitlements.** Surface excessive access and entitlement outliers.
- **Remediation action.** Deliver the fix via email or webhooks for the customer's XSOAR/Ticket systems to execute — Idysseus stays read-only.