DEVSECOPS MATURITY ASSESSMENT

BUILDING TRUST IN SECURE DELIVERY

People-first, data-driven improvements with dashboards, gap analysis, and auditable evidence.

WHY A MATURITY ASSESSMENT?

- Measurable security posture for leadership
- Practical guidance for teams
- Provable evidence for audits
- Focus on people + process + tooling

WHAT WE ASSESS

- **People**: roles, skills, collaboration
- **Processes**: CI/CD, governance, incident handling
- **Technology**: pipelines, IaC, security tools, observability
- **Auditability**: change traceability & proof ease

ASSESSMENT SCOPE & APPROACH

- **Kickoff & Scoping:** clarify goals, services in scope, constraints.
- **Discovery:** collect artifacts (pipelines, IaC, policies, incident reports).
- **Data Connectors:** wire CI/CD, repos, scanners, incident systems for evidence.
- **Baseline Dashboards:** first cut of DORA, vuln age, auditability metrics.
- **Interviews & Workshops:** people/rituals, ways of working, pain points.
- **Synthesis & Roadmap:** gaps, quick wins, 90-day plan, target KPIs.

PEOPLE: WHAT WE EVALUATE

- **Roles & Responsibilities:** clear ownership for security in delivery.
- **Skills & Enablement:** secure coding, threat modeling, pipeline literacy.
- **Rituals:** standups, postmortems, security office hours, guilds/chapters.
- **Collaboration:** dev-sec-ops handoffs, PR reviews, pair/mob for risky areas.
- **Learning Culture:** blameless postmortems, internal training, playbooks.

PROCESSES: WHAT WE EVALUATE

- **Branching & Release:** trunk vs gitflow, feature flags, promo to prod.
- **Change Management:** automated evidence over manual CAB queues.
- **Incident Response:** on-call, MTTR, postmortem quality & follow-through.
- **Threat Modeling:** cadence, templates, linkage to backlog and tests.
- **Backlog Hygiene:** prioritization of risk work, WIP limits, lead time control.

TECHNOLOGY: WHAT WE EVALUATE

- **CI/CD Capabilities:** build, test, deploy stages; required checks & gates.
- **IaC & Policy-as-Code:** drift detection, guardrails, environment parity.
- **Security Tooling:** SAST/SCA/DAST, secrets, container/IaC scanners.
- **Supply Chain:** SBOMs, artifact signing, provenance (SLSA) & attestations.
- **Observability:** logs/metrics/traces, error budgets, SLOs for critical services.

AUDITABILITY: HOW WE SCORE IT

- **Evidence Availability:** manual → semi-automated → API-harvested.
- **Evidence Integrity:** mutable (docs/screenshots) → immutable (append-only, signed).
- **Change Observability:** console clicks → PR/IaC with traceable ownership.
- **Ease of Audit:** days → hours → minutes to assemble a control pack.

Metrics: - % controls with automated evidence
- time to produce audit pack
- IaC-managed ratio
- drift MTTD/% auto-remediated.
-% Ratio of IaC .vs EaC

HOW WE MEASURE

- Benchmarks: SAMM, BSIMM, SSDF, SLSA
- Real data: DORA, vuln remediation times
- Attestations & drift detection for proof
- Dashboards: trends, gaps, progress path

METRICS & TARGETS

- **DORA:** Deployment Frequency, Lead Time, Change Failure Rate, MTTR.
- **Security Flow:** P95 time-to-patch criticals, vuln age buckets, open criticals.
- **Supply Chain:** SLSA level by service, % builds with signed attestations.
- **Targets:** Bronze/Silver/Gold thresholds tied to risk tier and audit readiness.

Team Metrics

Latest Metrics Score

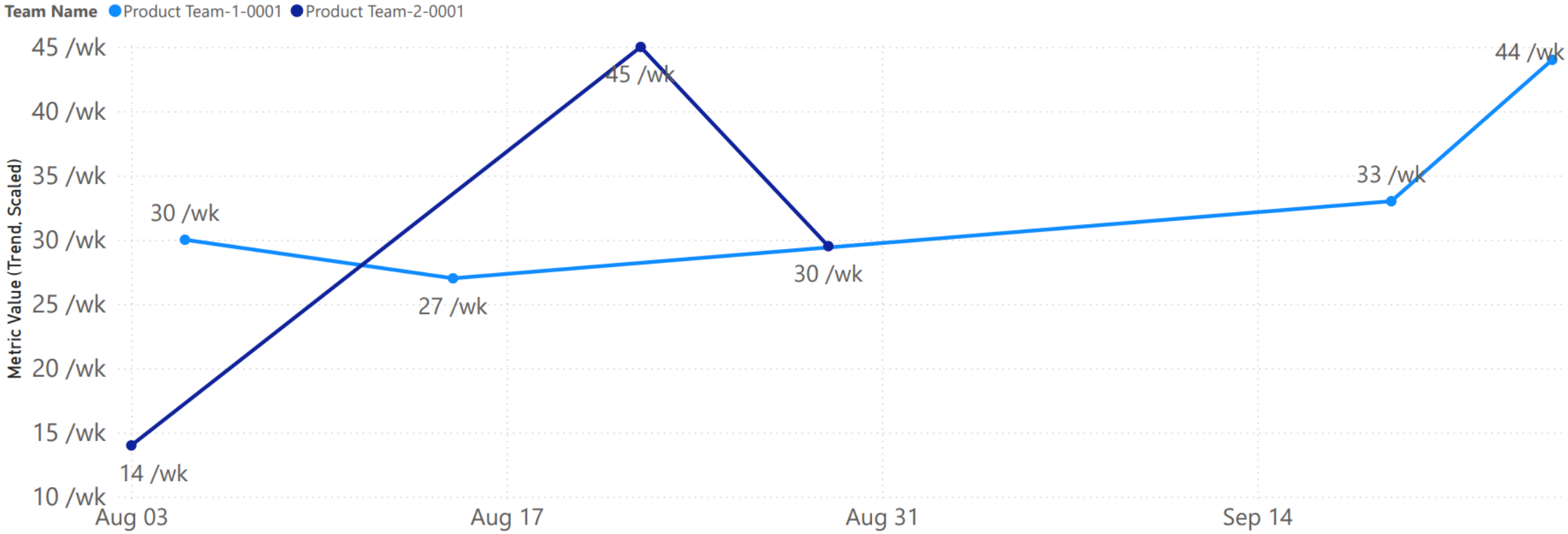
Company Name	Change Failure Rate	Deployment Frequency per Week	Eac per Iac Rate	Lead Time for Changes	Mean Time to Recovery
Organisation-0001					
Product Team-1-0001	0.14	44.00	0.18	60.00	9.00
Product Team-2-0001	0.03	49.00	0.39	80.00	1.00

General Average of Metrics Score

Company Name	Change Failure Rate	Deployment Frequency per Week	Eac per Iac Rate	Lead Time for Changes	Mean Time to Recovery
Organisation-0001					
Product Team-1-0001	0.11	33.50	0.16	75.50	14.75
Product Team-2-0001	0.10	29.50	0.35	68.75	5.00

Team Trends

Metric Value (Trend, Scaled) by Year, Month, Day and Team Name

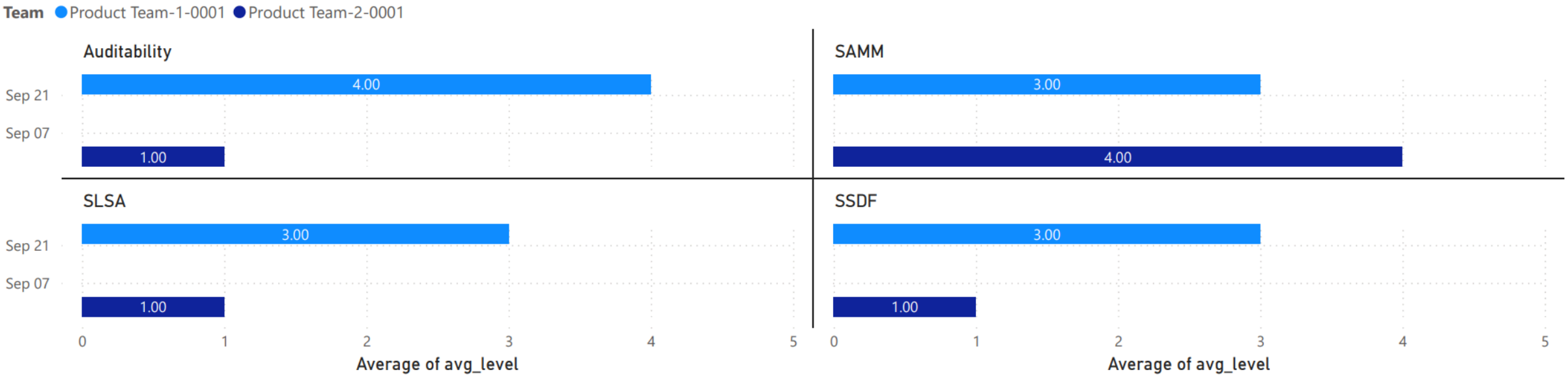


Metric Name

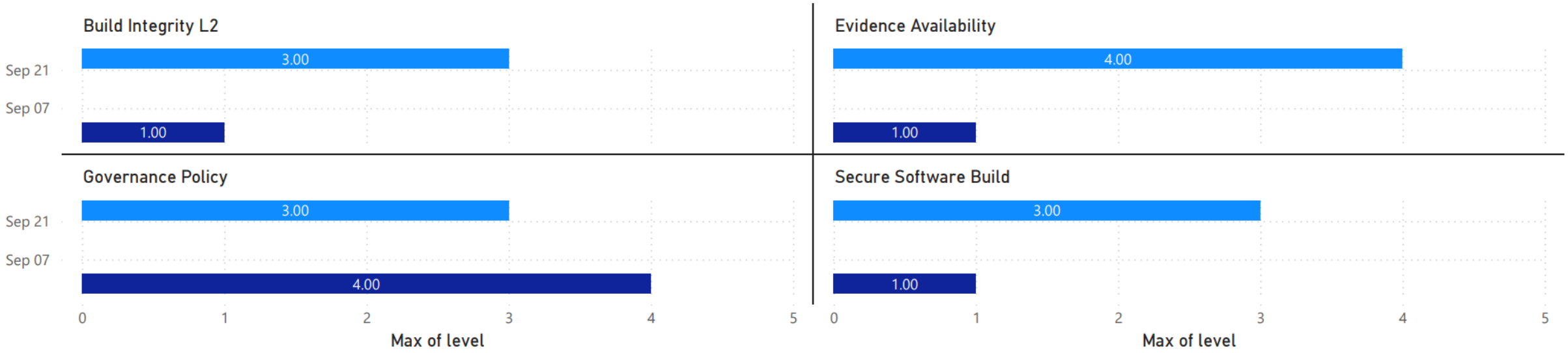
- ○ Change Failure Rate
- ◉ Deployment Frequency per Week
- ○ Eac per lac Rate
- ○ Lead Time for Changes
- ○ Mean Time to Recovery

Latest Maturity Scores

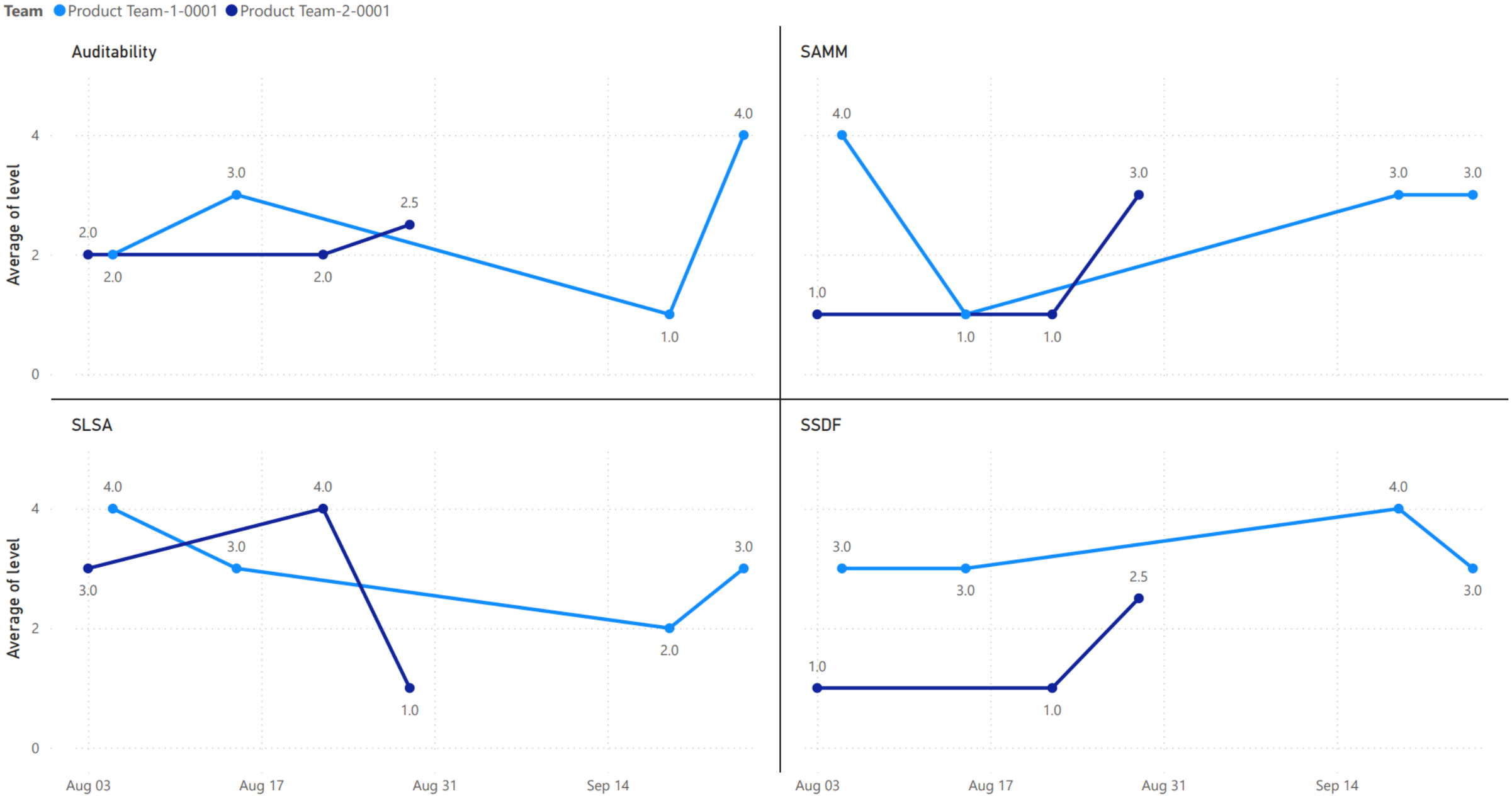
Model Maturity by Teams



Level of Maturity by Team and Practice (latest)



Maturity trend by model and by team



DATA CONNECTORS & EVIDENCE

- **CI/CD:** deployments, build results, approvals (Azure DevOps / GitHub).
- **Code & Quality:** PR metadata, reviews, Sonar metrics, coverage.
- **Security Findings:** SAST/SCA/DAST tools consolidated into a single pane.
- **Incidents:** tickets, alerts, time-to-detect/mitigate; postmortem follow-ups.
- **Controls:** policies, guardrail hits, IaC drift events, signed attestations.

DELIVERABLES

- **Executive Summary:** current posture, risks, and business impacts.
- **Team Scorecards:** maturity heatmaps and prioritized improvements.
- **Dashboards:** DORA & security trends; auditability score & evidence links.
- **90-Day Roadmap:** quick wins, owner, KPI movement, verification plan.
- **Evidence Inventory:** machine-harvestable proof per control.

SAMPLE TIMELINE (4–6 WEEKS)

- **Week 1:** kickoff, scoping, access, connector setup, first dashboards.
- **Weeks 2–3:** interviews/workshops, threat-model sampling, posture deep-dive.
- **Week 4:** gaps & options, OKRs/KPIs, draft roadmap.
- **Optional Weeks 5–6:** pilot improvements, baseline → re-measure.

GAP ANALYSIS

- Baseline 0–3 per practice
- **Strengths vs weaknesses**
- **Quick wins** and **strategic goals**
- Living improvement roadmap

OUTCOMES YOU GAIN

- **Clarity** on where you stand
- **Confidence** for audits & threats
- **Roadmap** tied to business value
- **Culture** of sustainable secure delivery

SCOPE & CAPACITY DISCLAIMER

- **Single-consultant engagement:** to meet the 4–6 week timeline, the baseline covers up to **3 critical services**, **2 repositories**, and **2 CI/CD systems** (e.g., Azure DevOps + GitHub).
- **Security tooling in scope:** up to **2 scanners** (e.g., SAST + SCA) consolidated; additional tools may extend effort.
- **Incident data window:** last **90 days** for MTTR/changes; older data optional.
- **Interviews:** up to **8 stakeholders** (~60 minutes each) across Engineering, Security, and Operations.
- **Read-only access:** no PII/PHI ingestion; secrets must be masked or excluded.

Note: Exceeding the above thresholds may require schedule and budgeting adjustments.

ASSUMPTIONS & CHANGE-ORDER TRIGGERS

- **Prereqs by Day 5:** read-only access to repos, CI/CD, quality/security tools, and incident system; service inventory with owners.
- **Client availability:** scheduling a kickoff and interviews within the first **10 business days**.
- **Change-order triggers:** more than 3 services or 2 repos; adding compliance frameworks (e.g., ISO 27001, PCI); onboarding new tools; cross-BU scope; required remediation/implementation work.
- **Deliverable dates:** timeline starts after prerequisites are met; delays in access shift the delivery calendar correspondingly.

NEXT STEPS

- **Prereqs:** read-only access to CI/CD, repos, scanners, and incident system.
- **Seed Scope:** 3–5 critical services for an initial baseline.
- **Scheduling:** 60–90 minutes for kickoff and access setup.
- **Outcome:** first dashboards and a draft improvement plan in 2 weeks.

ABOUT JPSOFTWORKS

- **Founder:** Jean-Paul Lizotte: SecDevOps transformation leader with 30+ years in engineering and operations.
- **Focus:** people-first automation, Everything-as-Code, Azure DevSecOps, IaC (Bicep), SOC 2 Type II readiness.
- **What We Do:** maturity assessments, roadmap execution, coaching, pipeline hardening, supply-chain security.
- **Industries:** public & private sector; cloud and hybrid environments.
- **Languages & Location:** bilingual French & English delivery.

More: www.jpsoftworks.com · blog.jpsoftworks.com

WHY CLIENTS CHOOSE US

- **People-first:** processes & tools in service of teams.
- **Evidence-based:** dashboards, DORA + security flow metrics, auditable controls.
- **Everything-as-Code:** IaC + policy-as-code + attestations → repeatable assurance.
- **Pragmatic roadmaps:** quick wins in weeks, sustainable capability in quarters.
- **Vendor-neutral:** integrates with your stack (Azure DevOps/GitHub, Sonar, Snyk, etc.).

READY TO BEGIN?

Let’s make security maturity measurable, auditable, and people-first.