ÉVALUATION DE MATURITÉ DEVSECOPS

INSTAURER LA CONFIANCE DANS LA LIVRAISON SÉCURISÉE

Améliorations axées sur les personnes et guidées par les données, avec tableaux de bord, analyses d'écarts et preuves auditables.

POURQUOI UNE ÉVALUATION DE MATURITÉ ?

- Posture de sécurité mesurable pour la direction
- Accompagnement pratique pour les équipes
- Preuves démontrables pour les audits
- Focalisée sur personnes + processus + outils

CE QUE NOUS ÉVALUONS

- **Personnes** : rôles, compétences, collaboration
- **Processus** : CI/CD, gouvernance, gestion des incidents
- **Technologie** : pipelines, IaC, outils de sécurité, observabilité
- **Auditabilité** : traçabilité des changements et facilité de preuve

PORTÉE ET APPROCHE DE L’ÉVALUATION

- **Démarrage & cadrage :** préciser objectifs, services inclus, contraintes.
- **Découverte :** collecter les artefacts (pipelines, IaC, politiques, rapports d’incident).
- **Connecteurs de données :** brancher CI/CD, dépôts, analyseurs et systèmes d’incident pour recueillir des preuves.
- **Tableaux de bord de référence :** premier jet des DORA, âge des vulnérabilités, métriques d’auditabilité.
- **Entrevues & ateliers :** rituels d’équipe, façons de travailler, irritants.
- **Synthèse & feuille de route :** écarts, gains rapides, plan 90 jours, KPIs cibles.

PERSONNES : CE QUE NOUS ÉVALUONS

- **Rôles & responsabilités :** propriété claire de la sécurité dans la livraison.
- **Compétences & habilitation :** codage sécurisé, modélisation des menaces, littératie pipeline.
- **Rituels :** mêlées, post-mortems, heures de bureau sécurité, guildes/chapitres.
- **Collaboration :** passages dev-sec-ops, revues de PR, pair/mob sur zones à risque.
- **Culture d’apprentissage :** post-mortems sans blâme, formations internes, guides et playbooks.

PROCESSUS : CE QUE NOUS ÉVALUONS

- **Stratégie de branches & release :** trunk vs gitflow, feature flags, promotion vers la prod.
- **Gestion du changement :** preuves automatisées plutôt que CAB manuel.
- **Réponse aux incidents :** astreinte, MTTR, qualité des post-mortems et suivi.
- **Modélisation des menaces :** cadence, gabarits, lien avec le backlog et les tests.
- **Hygiène du backlog :** priorisation du risque, limites WIP, maîtrise des délais.

TECHNOLOGIE : CE QUE NOUS ÉVALUONS

- **Capacités CI/CD :** étapes de build/test/déploiement ; vérifications et garde-fous requis.
- **IaC & règles « policy-as-code » :** détection de dérive, garde-fous, parité des environnements.
- **Outils de sécurité :** SAST/SCA/DAST, secrets, analyse conteneurs/IaC.
- **Chaîne d'approvisionnement :** SBOM, signature des artefacts, provenance (SLSA) et attestations.
- **Observabilité :** journaux/métriques/traces, budgets d'erreurs, SLO pour services critiques.

AUDITABILITÉ : COMMENT NOUS LA NOTONS

- **Disponibilité des preuves :** manuel → semi-automatisé → collectées via API.
- **Intégrité des preuves :** modifiables (docs/captures) → immuables (journal append-only, signées).
- **Observabilité des changements :** clics console → PR/IaC traçables avec propriétaire.
- **Facilité d'audit :** jours → heures → minutes pour assembler un dossier de contrôle.

Métriques : - % de contrôles avec preuve automatisée
- délai de production d'un dossier d'audit
- ratio de ressources gérées par IaC
- MTTD de dérive / % d'auto-remédiation
- % ratio IaC vs EaC

COMMENT NOUS MESURONS

- Référentiels : SAMM, BSIMM, SSDF, SLSA
- Données réelles : DORA, délais de remédiation des vulnérabilités
- Attestations & détection de dérive pour la preuve
- Tableaux de bord : tendances, écarts, trajectoire de progression

INDICATEURS & CIBLES

- **DORA :** fréquence de déploiement, délai de changement, taux d’échec, MTTR.
- **Flux sécurité :** P95 temps de correction des critiques, vieillissement des vulnérabilités, critiques ouvertes.
- **Chaîne d’approvisionnement :** niveau SLSA par service, % de builds avec attestations signées.
- **Cibles :** seuils Bronze/Argent/Or selon le risque et la préparation à l’audit.

Métriques d'équipe

Score des dernières métriques

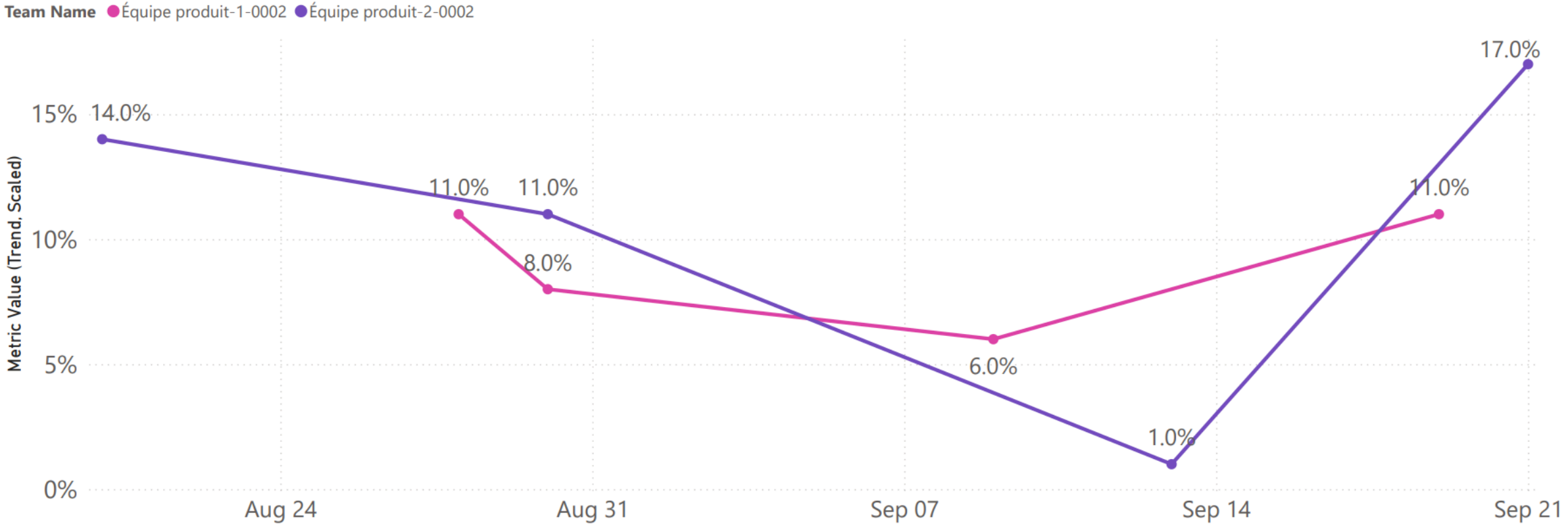
Organisation	Délai pour les changements	Fréquence de déploiement par semaine	Taux d'échec de changement	Taux Eac par lac	Temps moyen de récupération
Organisation-0002					
Équipe produit-1-0002	26.00	47.00	0.11	0.40	4.00
Équipe produit-2-0002	104.00	9.00	0.17	0.22	16.00

Moyenne générale du score des métriques

Organisation	Délai pour les changements	Fréquence de déploiement par semaine	Taux d'échec de changement	Taux Eac par lac	Temps moyen de récupération
Organisation-0002					
Équipe produit-2-0002	54.25	15.00	0.11	0.13	13.50
Équipe produit-1-0002	39.75	23.00	0.09	0.29	9.00

Tendances des Équipes

Valeur métrique (Tendance, Échelle) par Année, Mois, Jour et Nom de l'équipe

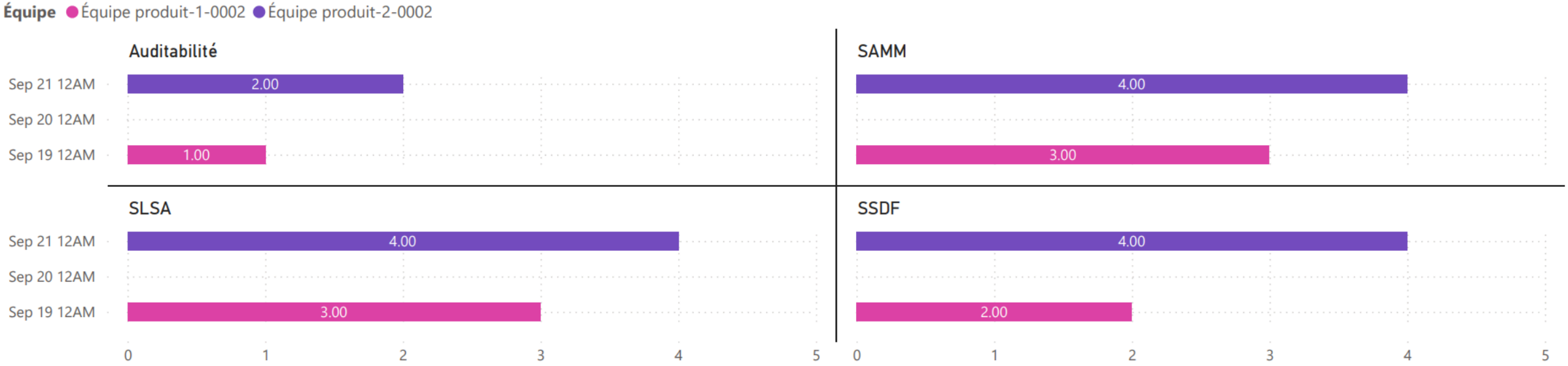


Nom de Métrique

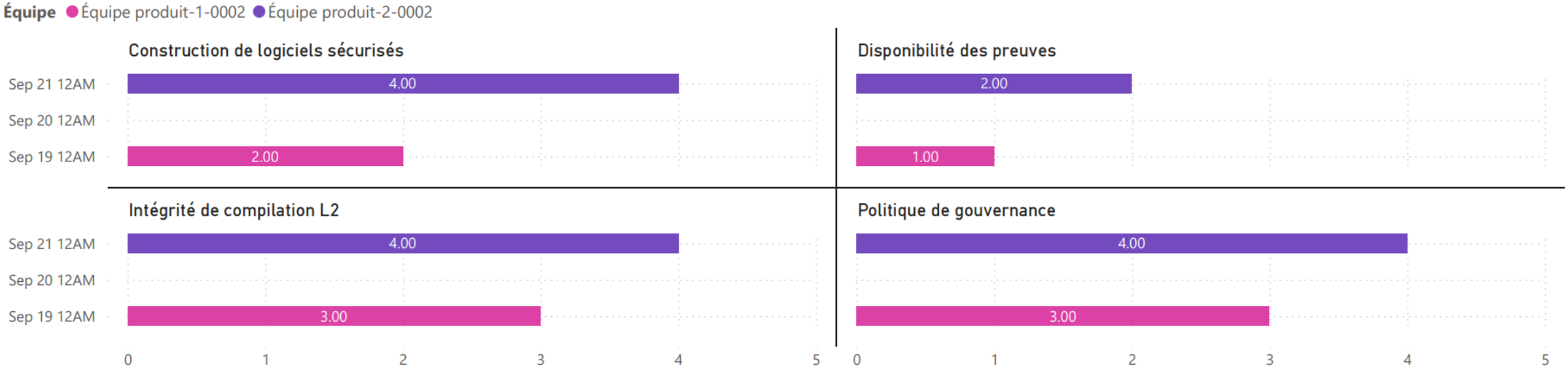
- ○ Délai pour les changements
- ○ Fréquence de déploiement par se...
- ◉ Taux d'échec de changement
- ○ Taux Eac par Iac
- ○ Temps moyen de récupération

Scores de maturité les plus récents

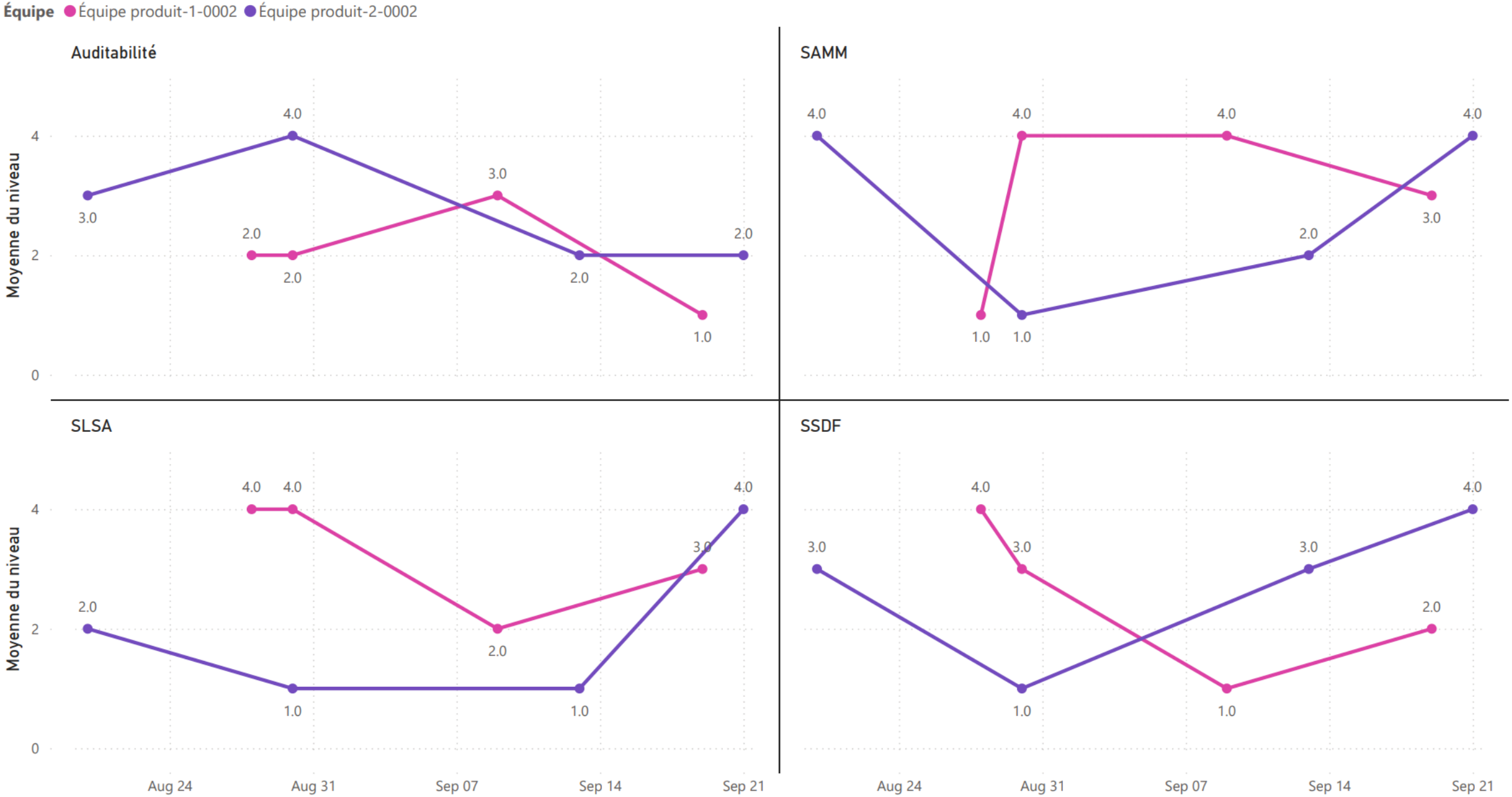
Maturité des modèles par équipes



Niveau de maturité par équipe et par pratique (le plus récent)



Tendance de maturité par modèle et par équipe



CONNECTEURS DE DONNÉES & PREUVES

- **CI/CD :** déploiements, résultats de build, approbations (Azure DevOps / GitHub).
- **Code & qualité :** métadonnées de PR, revues, métriques Sonar, couverture.
- **Constats sécurité :** SAST/SCA/DAST consolidés en un tableau unique.
- **Incidents :** billets, alertes, temps de détection/atténuation ; suivi post-mortem.
- **Contrôles :** règles, déclenchements de garde-fous, dérive IaC, attestations signées.

LIVRABLES

- **Sommaire exécutif :** posture actuelle, risques, impacts d’affaires.
- **Fiches d’équipe :** cartes de maturité et améliorations priorisées.
- **Tableaux de bord :** tendances DORA & sécurité ; score d’auditabilité & liens de preuve.
- **Feuille de route 90 jours :** gains rapides, responsable, effet KPI, plan de vérification.
- **Inventaire des preuves :** preuves récoltables par machine pour chaque contrôle.

ÉCHÉANCIER TYPE (4 À 6 SEMAINES)

- **Semaine 1 :** démarrage, cadrage, accès, connecteurs, premiers tableaux de bord.
- **Semaines 2–3 :** entrevues/ateliers, échantillonnage des menaces, analyse approfondie.
- **Semaine 4 :** écarts & options, OKR/KPI, ébauche de feuille de route.
- **Semaines 5–6 (optionnel) :** pilotes d’amélioration, re-mesure du baseline.

ANALYSE DES ÉCARTS

- Référentiel 0–3 par pratique
- **Forces vs faiblesses**
- **Gains rapides** et **objectifs stratégiques**
- Feuille de route vivante

RÉSULTATS OBTENUS

- **Clarté** sur votre position
- **Confiance** pour les audits et les menaces
- **Feuille de route** liée à la valeur d’affaires
- **Culture** de livraison sécurisée et durable

AVERTISSEMENT SUR LA PORTÉE & LA CAPACITÉ

- **Engagement « solo » :** pour respecter 4–6 semaines, la base couvre jusqu'à **3 services critiques**, **2 dépôts** et **2 systèmes CI/CD** (p. ex. Azure DevOps + GitHub).
- **Outils sécurité inclus :** jusqu'à **2 analyseurs** (p. ex. SAST + SCA) consolidés ; des outils additionnels peuvent allonger l'effort.
- **Fenêtre incidents :** derniers **90 jours** pour MTTR/changements ; plus ancien facultatif.
- **Entrevues :** jusqu'à **8 parties prenantes** (~60 min chacune) en Développement, Sécurité et Opérations.
- **Accès lecture seule :** aucune ingestion de PII/PHI ; secrets masqués ou exclus.

Note : dépasser ces seuils peut exiger des ajustements d'échéancier et de budget.

HYPOTHÈSES & DÉCLENCHEURS DE CHANGEMENT DE PORTÉE

- **Prérequis d'ici J+5 :** accès lecture seule aux dépôts, CI/CD, outils qualité/sécurité et système d'incident ; inventaire des services avec propriétaires.
- **Disponibilité du client :** planifier le démarrage et les entrevues dans les **10 jours ouvrables** initiaux.
- **Déclencheurs de changement :** plus de 3 services ou 2 dépôts ; ajout de cadres (p. ex. ISO 27001, PCI) ; nouveaux outils ; périmètre multi-BU ; travaux de remédiation/implémentation requis.
- **Dates de livraison :** l'échéancier démarre après obtention des accès ; les retards d'accès décalent le calendrier.

PROCHAINES ÉTAPES

- **Prérequis :** accès lecture seule à CI/CD, dépôts, analyseurs et système d’incident.
- **Périmètre initial :** 3–5 services critiques pour un premier référentiel.
- **Planification :** 60–90 minutes pour le démarrage et la mise en place des accès.
- **Résultat :** premiers tableaux de bord et ébauche de plan d’amélioration en 2 semaines.

À PROPOS DE JPSOFTWORKS

- **Fondateur :** Jean-Paul Lizotte: leader des transformations SecDevOps, 30+ ans en ingénierie et opérations.
- **Focus :** automatisation centrée sur l'humain, Everything-as-Code, Azure DevSecOps, IaC (Bicep), préparation SOC 2 Type II.
- **Nos services :** évaluations de maturité, exécution de feuilles de route, coaching, durcissement de pipelines, sécurité de la chaîne d'approvisionnement.
- **Secteurs :** public et privé ; environnements infonuagiques et hybrides.
- **Langues & présence :** prestation bilingue français & anglais.

En savoir plus : www.jpsoftworks.com · blogfr.jpsoftworks.com

POURQUOI NOUS CHOISIR?

- **Humain d’abord :** des processus et outils au service des équipes.
- **Basé sur la preuve :** tableaux de bord, DORA + flux de sécurité, contrôles auditables.
- **Everything-as-Code :** IaC + policy-as-code + attestations → assurance répétable.
- **Feuilles de route pragmatiques :** gains en semaines, capacités durables en trimestres.
- **Neutre vis-à-vis des éditeurs :** s’intègre à votre pile (Azure DevOps/GitHub, Sonar, Snyk, etc.).

ON COMMENCE ?

Faisons de la maturité sécurité un levier mesurable, auditable et centré sur l’humain.