Une nouvelle façon de travailler

- DevSecOps = transformation technique et business
- Coopération Dev, Ops, Sec + Business
- Automatisation et “Shift Left”
- Mesure de l’efficacité → adoption facilitée

La règle du IN (Input, Involve, Invest)

- Impliquer les stakeholders dès le début
- Contributions précoces = éviter de partir dans la mauvaise direction
- Anticiper audits et conformité en amont
- Investir temps et ressources (formation, architecture)

Le “Shift Left”

Tests de sécurité le plus en amont possible

S’applique au code, à l’architecture, aux images Docker…

Exemple : images durcies avant d’être mises à dispo des Devs

Moins de pertes de temps, plus de sécurité dès le début

Quelques statistiques clés

93 % des entreprises → stratégie digitale adoptée ou en cours

Objectifs : productivité (51 %), sécurité des données (40 %), meilleure visibilité

Axes : IA, ML, Cloud-Native, cybersécurité, AR/VR

DevSecOps, business et sécurité

Sécurité intégrée au quotidien = “Secure by Design”

Outils : SIEM (Splunk, ELK, Sentinel, GuardDuty)

Mise en conformité (ISO, PCI-DSS, sectoriels)

Mutation business profonde, pas juste du code