La minute de l'expert

Khadidiatou BA, Solution Engineer

Defender for Cloud : une sécurité unifiée et tournée vers l'avenir

Avec la généralisation du cloud et désormais des agents d'IA, le défi de la cybersécurité évolue au delà de la détection des incidents, vers une réduction proactive et continue de l'exposition aux risques. À l'occasion de Microsoft Ignite 2025, Defender for Cloud franchit une nouvelle étape décisive pour répondre à ces enjeux.

Une expérience unifiée dans le portail Defender (Preview)

Ignite 2025 marque une étape clé pour Defender for Cloud, la solution **CNAPP** de Microsoft désormais étroitement intégré au portail Microsoft Defender. Cette évolution vise à transformer la sécurité fragmentée en une approche centralisée et cohérente. Les équipes de sécurité bénéficient d'une **vue consolidée sur la posture, l'exposition et les menaces**, accessible au même endroit que les outils XDR et SIEM. Cela permet une meilleure **corrélation des signaux**, une **navigation fluide entre posture et détection**, ainsi qu'une **priorisation alignée sur les risques métier**. En particulier l'intégration native avec Microsoft Security Exposure Management **étend l'analyse des chemins d'attaques** en reliant ressources cloud, identités, postes de travail et agents d'IA, pour une vision contextualisée et des remédiations efficaces.

Couverture étendue aux agents avec Defender for AI (Preview)

Face à l'essor des agents IA dans les entreprises, Defender for Cloud adopte une approche innovante : il traite désormais les agents IA comme des actifs à part entière. Il inventorie les agents Microsoft **Foundry** et **Copilot Studio** entre autres, analyse leur posture de sécurité, les accès associés à différentes données, évalue les risques d'exposition et détecte les menaces ciblant les services IA grâce à **Defender for AI**.

Intégration renforcée avec GitHub Advanced Security (Preview)

L'intégration entre Defender for Cloud et GitHub Advanced Security renforce l'approche DevSecOps en offrant aux équipes de développement et de sécurité une **visibilité commune** sur l'usage des artefacts de build et les risques associés après déploiement. Cela combine l'analyse du code source, la détection des secrets et vulnérabilités et le contexte d'exécution (internet, données sensibles) afin de prioriser les remédiations. C'est un enrichissement de l'offre sécurité DevOps déjà disponible dans Defender for Cloud.

Couverture étendue au serverless (Preview)

Defender for Cloud étend désormais sa gestion de la posture aux ressources serverless comme **Azure Functions**, **Azure Web Apps**, **AWS Lambda** permettant d'identifier les mauvaises configurations, d'évaluer leur exposition réelle et de prioriser les recommandations selon les chemins d'attaque identifiés. Cela assure une protection cohérente sur tous les types d'architectures traditionnels, conteneurisés ou serverless.

Conclusion

Avec ces avancées, Defender for Cloud offre une sécurité cloud intelligente, unifiée et adaptée aux usages modernes, du DevSecOps aux agents d'IA. Dans un contexte d'évolution rapide des environnements, cet outil aide les organisations à **maîtriser leur exposition aux risques** et à **sécuriser l'innovation** sans compromis sur l'agilité.

Envie de mieux maîtriser votre exposition au risque cloud ? Démarrez ici et parlez-en avec votre équipe ou partenaire Microsoft.