Feuilles de calcul vs EGERIE Platforme

Dans le paysage actuel de la cybersécurité, complexe et en constante évolution, s'appuyer uniquement sur des feuilles de calcul peut laisser les organisations exposées et mal préparées. Voici un comparatif des fonctionnalités qui ont conduit nos clients à choisir EGERIE comme alternative privilégiée pour la gestion de leurs risques cyber:

	Feuilles de calcul	EGERIE platforme
Discovery	Cette phase est cruciale pour l'identification et la compréhension de l'environnement de sécurité de l'organisation. Cette phase comprend plusieurs activités et composants clés afin de garantir une compréhension complète des actifs, des menaces et des risques.	
	Offre une plateforme de base pour consolider et structurer les données de cybersécurité par une saisie manuelle, mais ses capacités sont limitées aux connaissances et aux efforts de l'utilisateur. Chaque feuille de calcul est une ardoise vierge dont la conception et l'alimentation nécessitent un travail manuel important. Les utilisateurs doivent créer leurs propres structures de données, formules et flux de travail, ce qui peut entraîner des incohérences et des erreurs, en particulier lorsque la complexité augmente.	Il offre **une approche complète et proactive** pour identifier et combler les lacunes en matière de sécurité en intégrant des données provenant de sources multiples. Il s'appuie sur des méthodologies **prêtes à l'emploi** basées sur les meilleures pratiques, adaptées à l'environnement spécifique de l'organisation, et favorise l'amélioration continue grâce à des mises à jour dynamiques et à l'intégration du retour d'information.
Evaluation des risques	Un processus critique et systématique utilisé pour identifier, évaluer et surveiller les risques afin de maintenir une posture de sécurité solide.	
	Les utilisateurs sont confrontés à des difficultés importantes en raison de la nature manuelle du processus. Ils doivent appliquer manuellement des formules personnalisées pour calculer les paramètres de risque tels que les scores de risque, l'impact et la vraisemblance. Cela nécessite une compréhension approfondie des méthodologies d'évaluation des risques et peut être sujet à des erreurs et à la subjectivité, en plus d'être une tâche qui prend beaucoup de temps.	Améliore l'évaluation des risques grâce à la mise à **jour automatique des indicateurs clés de risque et des plans de traitement**. Cela permet d'assurer un suivi efficace et précis des risques et des actions à mener. Le système fournit **une évaluation guidée des risques**, aidant les utilisateurs à interpréter les données et à évaluer efficacement la vraisemblance et l'impact des risques. Il permet d'ajuster en temps utile les stratégies de sécurité et de **renforcer la posture globale de l'organisation en matière de sécurité.**
Contextualisation	Une étape critique au cours de laquelle les risques sont placés dans le contexte spécifique d'une organisation afin de garantir que les évaluations des risques et les stratégies pour les réduire sont pertinentes et efficaces. Il s'agit de comprendre et d'évaluer les risques par rapport à l'environnement, aux objectifs et aux opérations de l'organisation.	
	Offre une certaine souplesse dans la contextualisation des risques, en permettant aux utilisateurs de créer manuellement des cadres et des méthodologies adaptés à leurs besoins spécifiques. Toutefois, cette flexibilité s'accompagne de défis importants car elle nécessite une structuration méticuleuse des données, des mises à jour manuelles fréquentes et une analyse détaillée, ce qui peut prendre beaucoup de temps. La nature manuelle de ces tâches augmente la probabilité d'erreurs, ce qui peut compromettre l'exactitude des évaluations des risques.	**Analyse les menaces dans leur contexte stratégique**, ce qui implique d'évaluer leur nature et leur gravité afin de fournir des informations cruciales pour une prise de décision éclairée. Elle garantit que les menaces sont évaluées non seulement de manière isolée, mais aussi **en relation avec les objectifs stratégiques et l'environnement opérationnel plus larges de l'organisation**. En comprenant l'impact et les implications des menaces dans ce contexte, les décideurs peuvent faire des choix **plus éclairés et plus efficaces** pour traiter les risques potentiels de manière proactive et plus stratégique.

Feuilles de calcul vs EGERIE Platforme

	Feuilles de calcul	EGERIE platforme
Prioritisation	Il s'agit de classer les risques identifiés en fonction de leur importance pour l'organisation. Permet de déterminer les risques qui requièrent une attention immédiate et ceux qui peuvent être traités ultérieurement. L'objectif est d'allouer les ressources de manière efficace et de s'assurer que les risques les plus critiques sont gérés en premier.	
	S'il permet de tagguer et de suivre efficacement les menaces, le système ne parvient pas à utiliser des algorithmes avancés pour évaluer avec précision les risques et les classer par ordre de priorité. Cela signifie que même si les menaces peuvent être identifiées et surveillées efficacement, le processus d'évaluation de leur importance et de détermination des menaces à traiter en priorité est moins précis et peut ne pas refléter pleinement leur véritable impact ou vraisemblance.	**Évaluer et hiérarchiser les risques** en examinant les risques, la vraisemblance et l'impact potentiel de chaque menace. Ce processus permet de s'assurer que l'attention et les ressources sont dirigées vers les problèmes les plus critiques, ce qui contribue à **traiter en premier lieu les risques les plus importants.**
Accélération de la remédiation	Il s'agit d'accélérer le processus de traitement et de résolution des problèmes de sécurité identifiés. Il est essentiel de veiller à ce que les risques et les menaces soient atténués aussi rapidement et efficacement que possible afin de minimiser les dommages potentiels.	
	Il offre la possibilité de créer des modèles structurés pour faciliter l'élaboration de stratégies de traitement, offrant ainsi une approche systématique pour traiter les problèmes de sécurité. Cependant, il manque de capacités d'analyse automatisée, ce qui signifie que bien qu'il soutienne la création de stratégies, il ne fournit pas d'informations avancées pour l'analyse des données ou l'orientation de la prise de décision.	Offre une méthodologie structurée pour l'identification et l'atténuation des menaces, l'évaluation des niveaux de risque et **une vue d'ensemble du paysage des risques**. Cela permet d'optimiser les efforts de traitement des risques et d'allocation efficace des ressources, en veillant à ce que tous les aspects de la gestion des risques soient pris en **compte et traités de manière efficace.**
Suivi et révision	Il s'agit de superviser et d'évaluer en permanence l'efficacité des stratégies de gestion des risques et des mesures de sécurité. Cela permet de s'assurer que les mesures mises en œuvre fonctionnent comme prévu et d'identifier de nouveaux risques émergents.	
	Il fournit une vision claire du paysage des risques cyber grâce à des registres structurés et des outils de visualisation simplistes, mais nécessite des vérifications régulières et un travail manuel. Il permet aux petites organisations de gérer et de comprendre plus facilement leurs risques en matière de cybersécurité, en leur garantissant une vision claire et organisée de leur profil de risque. Pour les grandes organisations, cela devient moins efficace et prend beaucoup de temps.	La plateforme EGERIE offre des **tableaux de bord, des rapports et des analyses détaillés** qui permettent de mieux comprendre les niveaux de risque, les impacts et les plans d'action. Il améliore votre capacité à gérer et à atténuer les risques en offrant une compréhension claire des conditions de risque actuelles et en soutenant une prise de **décision éclairée et des stratégies de gestion des risques efficaces.**