Exigences NIS2	Comment WithSecure peut vous aider ?		
Politiques d'analyse des risques, Politiques de sécurité	**WithSecure Consulting:** Ces services comprennent l'alignement du cadre de risque, l'analyse de risque, les évaluations de sécurité et les tests de pénétration. Ils s'alignent sur les exigences de la directive NIS2 en matière d'analyse de risque et d'évaluation de la vulnérabilité.		
Gestion des incidents	**WithSecure Elements XDR:** fournit des capacités de détection des anomalies et de réponse aux incidents, permettant une détection précoce des menaces et des réponses automatisées. Les outils alimentés par l'IA permettent une détection, une investigation et une réponse rapides aux menaces sur les endpoints, les identités, les mails et les services cloud de collaboration.	**WithSecure Incident Response Service:** garantit une réponse et une gestion rapides des incidents de cybersécurité, avec une assistance forensique pour une analyse complète.	**WithSecure Managed Detection and Response (MDR):** service managé qui surveille en permanence les incidents et y répond, améliorant ainsi les capacités de détection des menaces et de réponse aux incidents de bout en bout. L'inclusion d'une expertise en matière de traitement des incidents garantit que les organisations se conforment aux exigences de la directive NIS2 en matière de mesures de sécurité opérationnelle et d'atténuation des violations.
Continuité et reprise d'activité	**WithSecure Elements Exposure Management:** traite les menaces de façon continue en utilisant une priorisation basée sur le risque. Offre des recommandations continues en simulant des attaques, en identifiant les vulnérabilités critiques et en proposant des résultats axés sur les risques afin de renforcer vos défenses de manière proactive.	**WithSecure Consulting:** aide à établir et à tester des plans de continuité des activités, afin que les organisations puissent se préparer rapidement à des incidents et à s'en remettre.	
Sécurité de la supply chain, des fournisseurs et des prestataires de services	**WithSecure Elements Collaboration Protection:** assure la protection des plateformes cloud utilisées par les fournisseurs et les partenaires, en garantissant la sécurité de l'accès et de l'échange de données. Ajoute une protection supplémentaire aux capacités de sécurité natives de Microsoft 365, en s'attaquant aux cybermenaces avancées telles que les malwares, les ransomwares, les comptes compromis, le phishing et les attaques ciblées.	**WithSecure Consulting:** analyse l'état de la supply chain pour mesurer, comprendre et communiquer le niveau de risque de votre organisation.	
Sécurité des réseaux et des systèmes d'information	**WithSecure Elements Exposure Management:** identifie et évalue votre surface d'exposition numérique, avec une visibilité continue des vulnérabilités de votre surface d'attaque. Offre des recommandations continues en simulant des chemins d'attaque et en identifiant les vulnérabilités critiques, offrant ainsi des résultats axés sur les risques pour renforcer vos défenses de manière proactive.	**WithSecure Elements Extended Detection and Response (XDR):** protège les assets en détectant les menaces et en y répondant. Les outils alimentés par l'IA permettent une détection, une investigation et une réponse rapides aux menaces sur les endpoints, les identités, les mails et les services cloud de collaboration.	**WithSecure Co-Monitoring Service:** les threat hunters traitent automatiquement les détections présentant des risques graves et vous fournissent des conseils pour y remédier. Le service valide et étudie les détections afin d'établir la criticité et les mesures correctives nécessaires. Il assure également une visibilité et une protection complètes en surveillant constamment votre environnement informatique.
Evaluation de l'efficacité de la cybersécurité et de la gestion des risques	**WithSecure Elements Exposure Management:** permet de vous faire découvrir votre surface d'attaque, de visualiser les chemins d'attaque potentiels et d'évaluer les risques pour votre entreprise. Offre des recommandations continues en simulant des chemins d'attaque et en identifiant les vulnérabilités critiques, offrant ainsi des résultats axés sur les risques pour renforcer vos défenses de manière proactive.	**WithSecure Consulting:** Gestion des risques liés à la cybersécurité et élaboration d'une stratégie de conformité et de résilience opérationnelle.	
Formation et hygiène en matière de cybersécurité	**WithSecure Elements:** Inclut toutes les capacités de sécurité en une seule plateforme, de l'identification et la protection à la détection et la réponse aux menaces. Elements peut fournir une vue d'ensemble des risques pour les systèmes et les assets orientés vers Internet et de la manière de les atténuer, ce qui peut être utilisé à des fins de formation.	**WithSecure Consulting:** permet de tester votre préparation et d'améliorer vos compétences grâce à un exercice de gestion de crise cyber basé sur un scénario personnalisé.	
Cryptage et communications sécurisées	**WithSecure Elements Collaboration Protection:** Surveille les communications chiffrées sur les plateformes de collaboration, en veillant au respect des normes de chiffrement. Ajoute une protection supplémentaire aux capacités de sécurité natives de Microsoft 365, en s'attaquant aux cybermenaces avancées telles que les malwares, les ransomwares, les comptes compromis, le phishing et les attaques ciblées.	**WithSecure Exposure Management:** Évaluation continue des paramètres de cryptage exposés sur Internet pour une meilleure conformité. Détection continue des vulnérabilités critiques, avec des résultats axés sur les risques pour renforcer vos défenses de manière proactive.	**WithSecure Consulting:** Conseils sur la conception et la mise en œuvre, contrôles de conformité et audits des paramètres de cryptage.
Sécurité du personnel, contrôle d'accès et gestion des assets	**WithSecure Elements Identity Security:** Détecte les identités potentiellement compromises qui sont utilisées par les attaquants pour accéder à Microsoft 365 ou à d'autres services cloud. Aide les organisations à surveiller et à gérer les menaces internes potentielles ou les attaquants externes qui compromettent les informations d'identification du personnel, réduisant ainsi le risque de violations basées sur l'identité.	**WithSecure Exposure Management:** Évaluation continue des risques liés à l'identité. Détection continue des contrôles d'accès non conformes comme des assets exposés et cartographie continue des assets connectés à Internet. Offre des recommandations continues en simulant des chemins d'attaque et en identifiant les vulnérabilités critiques, offrant ainsi des résultats axés sur les risques pour renforcer vos défenses de manière proactive.	
L'utilisation de l'authentification multifactorielle ou de l'authentification continue	**WithSecure Consulting:** Conseils sur la conception et la mise en œuvre, contrôles de conformité et audits de la mise en place de MFA.	**WithSecure Elements Exposure Management:** Détection continue de la surface d'attaque non conforme, par exemple détection de l'authentification statique (absence de MFA). En combinaison avec la catégorisation de la criticité des assets et la catégorisation des risques, il peut surveiller vos assets les plus critiques et fournir des recommandations pour ne pas les exposer.	