Pentesting en ethical hacking Pentesting et ethical hacking

I.D.: 90298679

Data publicarii	05.12.23	Coduri CPV	72000000

Pretul estimativ:	600.000,00 EUR 600.000,00 EUR

Descriere: Het doel van deze overeenkomst is NMBS en haar filialen toe te laten de cybersecurity van hun websites, webservices, applicaties, apps, cloud en IOT te beoordelen op basis van onafhankelijke tests door een derde partij.Het resultaat van de tests omvat een rapport dat de gevonden kwetsbaarheden linkt aan potentiële impact en dat concreet en specifiek remediëringsadvies levert op maat de IT-omgeving, -capaciteiten en -veiligheids-doelstellingen van NMBS. Dit rapport dient om NMBS en haar filialen te helpen bij het verbeteren van hun informatie- en cyberveiligheidsbeleid, procedures en infrastructuur. De tests en rapporten dienen tevens om NMBS en haar filialen te helpen aantonen dat ze maatregelen hebben getroffen om de risico's tot een minimum te beperken en onbevoegde toegang zoveel mogelijk te beletten.NMBS of haar filialen onderhouden een heterogene en veranderende omgeving van systemen waarmee de werknemers, klanten en businesspartners van NMBS in interactie kunnen treden. Het managementteam is zich bewust van de risico's waaraan het netwerk en de applicaties van NMBS dagelijks onderhevig zijn en wenst daarom een doorlichting op het vlak van cyberveiligheid van zijn systemen en websites die toegankelijk (of blootgesteld) zijn via het internet, de (bekabelde/draadloze) netwerken, (mobiele) applicaties en hun interfaces.Het veiligheidsbeleid en de bijhorende informatie risicomethodologie die bij NMBS worden gehanteerd zijn gebaseerd op de ISO/IEC 27000-series, ook gekend als de 'ISMS Family of Standards' of 'ISO27K'. Kriticiteit van kwetsbaarheden wordt gemeten aan de hand van CVSS scores.GEBRUIK HET BIJGEVOEGDE ANTWOORDFORMULIER OM UW KANDIDATUUR IN TE DIENEN L'objectif de cet accord est de permettre à la SNCB et à ses filiales d'évaluer la cybersécurité de leurs sites web, services web, applications, apps, cloud et IOT sur la base de tests effectués par des tiers indépendants.Le résultat des tests comprend un rapport qui relie les vulnérabilités trouvées à l'impact potentiel et fournit des conseils de remédiation concrets et spécifiques adaptés à l'environnement informatique, aux capacités et aux objectifs de sécurité de la SNCB. Ce rapport permet à la SNCB et à ses filiales d'améliorer leurs politiques, procédures et infrastructures en matière d'information et de cybersécurité. Les tests et les rapports permettent également à la SNCB et à ses filiales de démontrer qu'elles ont pris des mesures pour minimiser les risques et empêcher autant que possible les accès non autorisésLa SNCB ou ses filiales maintiennent un environnement hétérogène et changeant de systèmes avec lesquels les employés, les clients et les partenaires commerciaux de la SNCB peuvent interagir. Consciente des risques auxquels le réseau et les applications de la SNCB sont quotidiennement soumis, l'équipe de direction souhaite procéder à une revue de la cybersécurité de ses systèmes et sites web accessibles (ou exposés) via l'internet, les réseaux (filaires/sans fil), les applications (mobiles) et leurs interfaces.La politique de sécurité et la méthodologie de gestion des risques liés à l'information utilisées à la SNCB sont basées sur la série ISO/IEC 27000, également connue sous le nom de 'ISMS Family of Standards' ou 'ISO27K'. La criticité des vulnérabilités est mesurée par les scores CVSS.VEUILLEZ UTILISER LE FORMULAIR ATACHÉ POUR SOUMETTRE VOTRE CANDIDATURE