Communiqué de Presse

AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 vloquet@alx-communication.com

Rémunération et positionnement des responsables cybersécurité

Résultats de l'enquête exclusive OpinionWay pour le CESIN

Paris, le 2 septembre 2024 – Le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) dévoile les résultats de son enquête sur la rémunération et le positionnement des responsables cybersécurité (RSSI). Réalisée en collaboration avec OpinionWay, cette enquête exclusive a été menée en juin 2024 auprès de 390 membres du CESIN, responsables de la cybersécurité. Elle offre un éclairage sur l'évolution d'une profession clé, dans un contexte de cyber menaces croissantes.

Cette nouvelle étude sur la rémunération s'inscrit dans une démarche de suivi amorcée par le CESIN en 2017, et renouvelée en 2021. Cette année, elle inclut un nouveau volet explorant le positionnement des RSSI au sein des organisations. Les répondants se sont exprimés sur 33 activités, en précisant leur rôle selon un RACI standard[1].

L'association participe aux perspectives d'évolution du métier, en œuvrant pour une reconnaissance du rôle essentiel des responsables de la cybersécurité au sein des organisations. Pour le CESIN ces résultats mettent en lumière les défis et les opportunités des responsables cybersécurité, en termes de positionnement, rôles et responsabilités, conditions de travail et rémunération.

Profils des responsables cybersécurité et leurs activités

La fonction est multidimensionnelle, avec une forte concentration sur l'axe gestion des risques (73%) et sur l'opérationnel (64%), tandis que la conformité et la résilience ont gagné en importance au cours des cinq dernières années.

1 A : Accountable, qui porte la responsabilité sur l'activité, R : Responsible, qui réalise l'activité, C : Contributeur à l'activité, I : Informé sur l'activité, ou « Hors du champ des activités ».

La population des responsables cyber est très majoritairement masculine, avec une légère augmentation de la part des femmes parmi les répondants, passant de 5% en 2021 à 8% en 2024. A noter que les femmes représentent près de 10% des adhérents du CESIN. Les responsables cybersécurité sont principalement des professionnels expérimentés, 52% d'entre eux ont entre 35 et 49 ans et 37% entre 50 et 64 ans. Plus de la moitié (56%) possède plus de 10 ans d'expérience dans le domaine. En termes de qualifications, 75% sont titulaires d'un Bac+5 ou plus. 58% ont suivi un cursus d'ingénieur, avec une prédominance notable des informaticiens (81%) par rapport aux spécialistes de la cybersécurité (30%).

Les responsabilités managériales varient selon les organisations, et s'exercent en hiérarchique et/ou en fonctionnel. 85% des responsables cyber encadrent des équipes, entre 13 et 20 personnes en moyenne. La majorité des responsables cyber (77%) sont rattachés directement au directeur de leur entité, principalement la DSI (54%) ou la Direction Générale (20%), 50% d'entre eux sont au niveau N-2 de la Direction Générale.

Leurs activités principales sont : les analyses de risques (92%), les politiques de sécurité (89%), la sensibilisation (86%) et la sécurité offensive, tels que les audits, pentests, red teams, bug bounties… (80%). Ces quatre pôles sont communs à plus de 80% d'entre eux.

Concernant les activités de pilotage, trois responsables cyber sur quatre sont en charge de la veille, la stratégie, la roadmap, le budget et le reporting stratégique. Deux sur trois décident des solutions cyber, pilotent leur intégration et les opèrent, les autres y contribuent.
Autrefois, le risque IT était géré séparément du risque cyber, dorénavant l'ensemble des responsables cyber participe à la gestion des risques IT, 60% en sont d'ailleurs responsables.

Tous intègrent la sécurité dans les projets et gèrent les risques liés aux tiers, 67% pilotent ces activités**.** 84% contribuent largement à la sécurité des architectures tandis que 31% en sont responsables.

Tous participent à la gestion des crises cyber, 74% en sont responsables. Environ 80% gèrent ou contribuent à la sécurité opérationnelle (SOC, CERT,…), 60% en sont responsables.

Largement impliqués dans la gestion des vulnérabilités (86%) (veille, scans, détections, alertes, priorisation), 2 responsables cyber sur 3 en sont responsables ou en charge de réaliser cette activité. La gestion des correctifs est dévolue aux équipes IT, tout comme la gestion de l'obsolescence.

84% des responsables cyber contribuent aux plans de continuité d'activité, et un responsable cyber sur 3 en est responsable. 80% conduisent ou sont impliqués dans la gestion des identités, et 38% en assument la responsabilité et la mise en œuvre.

Les responsables cyber sont généralement peu en charge de la lutte contre la fraude, ou de la sûreté en général, et seul un responsable cyber sur deux (49%) est leader sur les questions de conformité.

Une hausse des activités opérationnelles est observée ces 5 dernières années, en lien avec la croissance des attaques et celle des vulnérabilités.

Conditions de travail, satisfaction et aspirations professionnelles

Les responsables cyber jouissent d'une grande autonomie, notamment en matière de budget et de choix des solutions de cybersécurité. Ils sont soutenus par le top management, 83% expriment un soutien suffisant, 33% confirment même un soutien très important.

La satisfaction professionnelle des RSSI est élevée, avec 84% d'entre eux se déclarant satisfaits de leur travail. Ils étaient 20% en 2021 à juger leur niveau de satisfaction élevé ils sont 25% en 2024. Les principaux facteurs de motivation sont la transversalité de la fonction (76%) et la diversité des sujets traités (73%).

66% d'entre eux envisagent de changer d'organisation, 24% se déclarent certains de le faire, en visant des postes de Chief Information Security Officer (CISO) ou de Directeur cyber sur des périmètres à plus grandes responsabilités. Ceux qui envisagent une évolution de carrière au sein de leur entreprise actuelle, ciblent des postes de Chief Security Officer (CSO) ou de CIO (Chief Information Officer).

La continuité pour la responsabilité cyber pose tout de même question puisque seulement 11% des organisations disposent ou sont en train d'élaborer un plan de succession.

Rémunération des responsables cybersécurité

Le salaire annuel fixe moyen des RSSI en 2024 est de 96 543 €, en hausse par rapport à 2020 où il était de 88 342 €. Un tiers des RSSI déclare plus de 105 000 € de salaire fixe. La rémunération moyenne des 10% des salaires les plus bas est de 51 534 € et les plus élevés de 171 809 €. A noter que la disparité des salaires entre les grandes et les petites/moyennes entreprise est encore accentuée par des compléments de salaires dont bénéficient les responsables cyber des grands groupes.

Près de 40% estiment que leur rémunération est insuffisante comparée à d'autres fonctions de l'entreprise. Les autres se déclarent satisfaits de leur rémunération globale, avec 71% ayant reçu une part variable en 2023. 66% bénéficient d'avantages supplémentaires comme l'intéressement pour 55% d'entre eux, une voiture de fonction pour 19%, ou encore d'autres bonus (16%).

On peut observer que les salaires élevés des quelques Directeurs cyber de grands groupes sont dilués avec ceux des responsables cyber intermédiaires au sein de leur entreprise ou ceux d'organisations de plus petites tailles.

POUR CONSULTER L'INTÉGRALITE DU SONDAGE REMUNERATION CESIN-OPINIONWAY :
https://cesin.fr/document.php?d=66d58fcab49cd

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la cybersécurité.

Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.

Le CESIN compte plus de 1 000 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120. Pour en savoir plus www.cesin.fr