Consultant en Cybersécurité

Killian FERRIER

Pierrick CARON

Fichier métier d’un consultant en cybersécurité

Description	
	Le consultant en cybersécurité est un expert qui protège les données confidentielles des entreprises en analysant les risques et en proposant des solutions personnalisées. Il commence par réaliser un diagnostic pour identifier les failles du système et tester la vulnérabilité des installations, puis propose des solutions adéquates en termes de choix techniques, équipes, et procédures de sécurité.
Niveau d’étude	
	Niveau bac + 3:
	- Diplôme d'école spécialisé (type bachelor) en cybersécurité (Epita, Esiea)
	- BUT Réseaux et télécommunications
	Niveau bac + 5:
	- Master en informatique parcours cybersécurité (EIT digital master School)
	- Master ingénierie des systèmes complexes
	Différents parcours :
	- SSI : sécurité des systèmes d'information (université de technologies de Troyes)
	- Diplôme d'ingénieur avec spécialisation en cybersécurité (ISEP, Esme Sudria, Epita, Télécom Sud Paris, Eurecom, Esiea)
	- Diplôme d'école spécialisée (type MBA, Msc, Mastère) en cybersécurité ou sécurité informatique (institut Léonard de Vinci, Epita,

	Em Lyon Business School, - ESGI Paris, EFREI, ESAIP)
	Niveau bac + 6:
	- MS (master spécialisé) sécurité de l'information des systèmes (ESIEA)
	- MS (master spécialisé) cybersécurité et cyberdéfense (Télécom Paris)
	- MS (master spécialisé) architecte réseaux et cybersécurité (Télécom Paris)
	- MS (master spécialisé) conception architecture de réseaux et cybersécurité (Télécom Paris)
	- MS (master spécialisé) cybersécurité : attaque et défense des systèmes d'information (Mines Nancy)
	- MS cybersécurité des opérateurs de services essentiels (Télécom Sud Paris)
Meilleures écoles en France	
	CentraleSupélec / IMT Atlantique ;
	Télécom Paris ;
	INSA Lyon ;
	UTT – Université de Technologie de Troyes ;
	Télécom SudParis.
Compétence requises	
	- Posséder de solides connaissances techniques dans les domaines de la prévention, de la détection, et de la lutte contre la cybercriminalité.
	- Avoir une forte capacité d'analyse et de synthèse pour évaluer les risques encourus par une entreprise et proposer des solutions adaptées.
	- Maîtriser l'anglais à l'écrit comme à l'oral, qui est la langue de référence dans le domaine de la cybersécurité.
	- Être inventif, curieux et ingénieux pour anticiper les nouvelles menaces et proposer

	des solutions innovantes.
	- Assurer une veille constante sur les nouveaux outils et méthodes de hacking en vogue.
	- Pouvoir établir un diagnostic pour repérer les failles d'un système, définir des scénarios d'intrusion et tester la vulnérabilité des installations.
	- Proposer des solutions adéquates en termes de choix techniques, équipes, et procédures de sécurité qui répondent aux besoins du client.
	- Être en mesure d'imaginer, d'anticiper et de savoir s'adapter à de nouvelles menaces pour protéger les données confidentielles des entreprises.
Journée type d’un consultant en cybersécurité	
	La journée type d'un consultant en cybersécurité peut varier en fonction de son lieu de travail (cabinet spécialisé, entreprise cliente, travailleur indépendant...) et de la nature de sa mission. Cependant, voici un aperçu général de ce qu'une journée type peut inclure :
	8h30 - 9h00 : Arrivée au lieu de travail et consultation des e-mails pour repérer les urgences et les tâches prioritaires.
	9h00 - 10h30 : Réunion avec l'équipe projet ou le client pour discuter des objectifs, de l'état d'avancement de la mission, et des solutions à mettre en place.
	10h30 - 12h30 : Analyse de la sécurité du système informatique de l'entreprise cliente pour repérer les vulnérabilités et les failles.
	12h30 - 14h00 : Pause déjeuner.
	14h00 - 16h30 : Proposition de solutions pour améliorer la sécurité du système informatique de l'entreprise cliente. Le consultant peut travailler sur des procédures de sécurité, des

	plans de continuité d'activité, des architectures de sécurité, ou des solutions techniques.
	16h30 - 18h30 : Rédaction de rapports pour le client, synthétisant les actions effectuées, les résultats obtenus, et les solutions proposées.
	18h30 - 19h00 : Échanges avec les membres de l'équipe pour faire le point sur la journée, débriefer les résultats et anticiper les prochaines étapes.
	19h00 - 19h30 : Préparation de la journée du lendemain et sauvegarde des documents importants.
	19h30 - 20h00 : Départ du lieu de travail. Il est important de noter que les journées peuvent être beaucoup plus intenses en cas de crise, par exemple en cas de cyberattaque ou de piratage informatique. Les horaires peuvent donc être variables en fonction des impératifs de la mission.
Salaire	
	entre 3 000 et 3 300 € pour un débutant
	entre 3 750 et 5 800 € pour un profil senior
Avantage	
	- Un travail qui peut être très enrichissant
	- Bénéficier des opportunités d’affaires
	- Flexibilité de travailler a partir de n’importe où
Inconvénient	
	- Peut travailler tard le soir et le weekend
	- Peut être amené a travail sur des projets dont il n’a pas connaissance auparavant
	- Gérer les priorités et gérer les délais
	- Chaque société demande un niveau de compétence en cybersécurité particulier
Évolution de carrière possible	
	- Responsable de sécurité informatique

	- Responsable sécurité des systèmes d’informations
	- Expert en sécurité informatique
	- Expert en cybersécurité

Fiche statistique d’un consultant en cybersécurité

Genre	
Homme	88,1%
Femme	11,1%
Age	
Mois de 30 ans	40%
50 ans et plus	10,5%
Niveau de qualification	
Bac+5 et plus	83,7%
Salarier	
Non-salarier	15,6%
Structure	
Spécialisée en cybersécurité	64,4%
Mois de 10 salarier	15%
1000 salarier et plus	51,3%
Prestation spécialisé	28,8%
Spécialisée en informatique/numérique	24,3%
Service aux entreprises	18,9%