Bloc	Formation qualifiante à l'ENSIAS
Header  	**Formation : Cybersécurité & Cloud Computing** Sous-titre : Deviens **Administrateur de la cybersécurité et du cloud**, en 03 mois avec une formation intensive adoptant l'approche « Learning by doing » et un accompagnement à l'insertion professionnelle. **Infos clés** • Durée : 03 mois • Lieux de formation : ENSIAS • Prochaine session : Avril 2024 • Pré-requis : Bases de l'informatique (Notions de systèmes d'exploitation, Eléments de Programmation).
Débouchés : les postes que vous pourrez occuper après cette formation	• Analyste de la cybersécurité • Administrateur de la sécurité du cloud • Consultant en sécurité informatique • Architecte cloud
Pourquoi devenir administrateur de bases de données en 2024 ?	**Perspectives de carrière** Le domaine de la cybersécurité et du cloud computing étant en constante évolution, les professionnels bien formés et continuellement mis à jour ont de nombreuses opportunités pour progresser dans leur carrière et contribuer à la protection des systèmes d'information. Un Administrateur de la sécurité du cloud peut se spécialiser dans la sécurisation des infrastructures cloud, assurer la protection des données et des applications dans des environnements tels que AWS, Azure ou Google Cloud. Il peut également Superviser la politique de sécurité globale d'une organisation, élaborer des plans de gestion des incidents et assurer la conformité aux normes de sécurité.
Compétences : ce que vous allez apprendre	A l'issue de cette formation, l'apprenant sera en mesure de : • Reconnaître les différents types de virtualisation et de service de cloud • Maîtriser les bases des réseaux informatiques (équipements, architectures, protocoles, …) • Comprendre les principaux concepts liés à la sécurité des SI et les exigences des politiques de sécurité qui préservent un équilibre entre les besoins métiers et ceux relatifs à la confidentialité, l'intégrité et la disponibilité. • Effectuer des évaluations des menaces (y compris les scénarios d'attaque) et des vulnérabilités afin d'évaluer les risques de sécurité au niveau des réseaux ou des services Cloud et recommander des mesures de protection appropriées ; • Choisir les mesures défensives appropriées aux systèmes d'exploitation, aux réseaux et aux services Cloud afin de les protéger contre les menaces. • Administrer et configurer convenablement un système d'exploitation (en particulier Linux) ou un réseau y compris les commutateurs, les multiplexeurs, les routeurs, les firewalls de telle façon de réduire les risques d'exposition. • Assurer les configurations de la sécurité dans un environnent cloud (en particulier AWS).

Programme de la formation	Modules complémentaires • Initiation à l'Entreprenariat • Projet Entrepreneurial • Préparation à l'insertion professionnelle : Correction de CV, Simulation d'entretiens… • Organisation des jobs dating (ateliers de demi-journées) • Communication professionnelle et Anglais des affaires Modules techniques • Renforcement de prérequis en Informatique • Fondamentaux des Systèmes & Réseaux • Fondements de la Cybersécurité • Réseaux : Interconnexion & Sécurité • Virtualisation & Bases du Cloud Computing • Fondements de la sécurité du Cloud • Projet Cloud & Sécurité
Notre méthode	La formation adoptera la méthode « Learning By Doing » qui est plus basée sur la pratique, l'apprentissage groupé, avec une approche d'apprentissage par projet.
A quoi s'attendre pendant le bootcamp ?	Une formation complète permettant aux apprenants un(e) : - Montée rapide en compétences techniques opérationnelles ; - Renforcement des compétences transversales indispensables à une insertion réussie dans le monde professionnel du secteur du digital ; - Aptitude à élaborer un projet professionnel aligné à la formation et répondant aux besoins du marché de travail ; - Meilleure opportunité d'insertion professionnelle via un stage encadré. Les apprenants bénéficieront de l'accompagnement et du suivi dans l'instauration des méthodologies de travail, du sens critique et d'un ensemble d'aptitudes nécessaires au monde du travail à l'ère du digital, comme **l'autonomie, l'auto-apprentissage, l'adaptabilité, le travail de groupe, l'esprit d'entreprenariat** et l'aptitude à appréhender un problème dans le cadre d'un projet à gérer et réaliser de manière agile et efficace. En plus des séances en présentiel dédiées au profil visé, il y aura : - Renforcement des prérequis suite à un test de positionnement - Encadrement de Projet - Tutorat - Accompagnement professionnel par les coachs professionnels lors des ateliers correction - Mentorat - Encadrement de stage - Aide à la préparation des certifications
Présentation de l'opérateur	Fleuron de l'Université Mohammed V de Rabat, l'Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS) est la plus grande école d'ingénieur spécialisée dans les Technologies d'Information et de la Communication depuis 1992 qui prône les valeurs d'équité, d'égalité des chances et d'inclusion sociale. Durant 31 années, l'ENSIAS a su anticiper l'évolution de l'informatique vers la digitalisation, puis vers la transformation et

	la réinvention digitale. C'est l'école génératrice de connaissances et de richesses à grande valeur ajoutée pour accompagner la croissance économique du Pays. Aujourd'hui l'ENSIAS, a atteint une maturité académique, pédagogique et scientifique qui l'érige aux premiers rangs des grandes écoles d'ingénieur spécialisées dans les Technologies d'Information et de la Communication. Depuis sa création en 1992, l'ENSIAS compte plus de 5300 lauréats ingénieur(e)s, du cycle Master et celui du doctorat occupant divers métiers du numérique et du digital aussi bien à l'échelle national qu'à l'international. Des lauréats très prisés qui occupent des postes stratégiques dans les administrations, dans le secteur privé et plusieurs ont créé leurs propres entreprises dont certaines sont cotées en bourse. L'ENSIAS a la chance de se situer dans une région très dynamique avec de nombreux projets de grande envergure. Il s'agit d'une réelle opportunité pour la multiplication des contrats-projets de recherche, et des programmes de formation avec les opérateurs socioéconomiques. Grâce à son expertise, l'école est à même d'offrir des services de formation continue, de formation tout au Long de la vie, du consulting et des études. Elle compte à son actif plusieurs conventions de partenariats nationaux et internationaux en formation, recherche, innovation et production industrielle pour le montage de formations, le sponsoring de conférences, l'incubation d'entreprises, le recrutement des lauréats, ainsi que pour les certifications professionnelles. Sa réputation et sa place privilégiée en tant qu'acteur et partenaire incontournable pour les opérateurs socio-économiques publics et privés à l'échelle nationale et internationale sont le fruit de la conjugaison de tous les efforts louables de la famille ENSIAS : enseignants-chercheurs, personnel administratif et technique, agents et étudiants. L'ENSIAS s'est orientée depuis 2020 vers un nouveau modèle de développement et parie, avec l'ensemble de ses acteurs, sur la transformation digitale intelligente afin de poursuivre sa contribution active dans le développement économique et social et de réaliser dans ce domaine un saut significatif au niveau pédagogique, recherche et innovation et au niveau de sa gouvernance et de son partenariat national et international. Son offre de formation, son ingénierie de formation, ses modes pédagogiques et ses dispositifs d'accompagnement sont en constante évolution et s'orientent vers le développement de l'innovation et de l'entrepreneuriat et le développement de compétences répondant aux nouveaux métiers du Digital et des technologies émergentes.
Candidature	- **Pré-requis** : BAC+3 ou BAC+5 scientifique ou informatique. - **Critères de sélection** : Etude de dossier et Entretien oral. Une lettre de motivation justifiant les compétences techniques et les expériences professionnelles éventuelles est souhaitable. - **Modalités, étapes de candidature** : Présélection via le portail deJobInTech, étude de dossier, convocations des candidats présélectionnés pour un test technique et un entretien oral.
FAQ	**Quel est le rôle d'un Administrateur de la Sécurité et du Cloud ?** Un administrateur de la sécurité et du cloud est chargé de gérer la sécurité des infrastructures informatiques basées sur le cloud d'une organisation. Cela comprend la configuration, la surveillance et la gestion des outils de sécurité cloud, ainsi que la mise en œuvre de politiques de sécurité pour

	protéger les données et les systèmes. **Quels sont les principaux défis auxquels les Administrateurs de la Sécurité et du Cloud sont confrontés ?** Les défis comprennent la gestion des configurations de sécurité dans des environnements cloud dynamiques, la protection des données sensibles contre les menaces internes et externes, la conformité réglementaire, la résolution des problèmes de performance et de disponibilité, ainsi que la gestion des incidents de sécurité **Quelles sont les meilleures pratiques en matière de sécurité cloud ?** Les meilleures pratiques comprennent la mise en œuvre d'une gestion des identités et des accès solides, le chiffrement des données sensibles en transit et au repos, la surveillance continue de l'environnement cloud pour détecter les activités suspectes, la mise en place de politiques de conformité et de gouvernance, ainsi que la formation des employés sur les bonnes pratiques de sécurité. **Quelles sont les conséquences d'une mauvaise gestion de la sécurité cloud ?** Les conséquences peuvent inclure des violations de données, des temps d'arrêt coûteux, des amendes réglementaires, des dommages à la réputation de l'entreprise, la perte de confiance des clients, ainsi que des pertes financières et des litiges. **Quels outils sont généralement utilisés par les Administrateurs de la Sécurité et du Cloud ?** Les outils couramment utilisés comprennent les plates-formes de gestion des identités et des accès (IAM), les outils de surveillance des journaux et des activités, les pare-feu cloud, les outils de gestion des vulnérabilités, les solutions de détection et de réponse aux incidents (EDR), ainsi que les outils de gestion de la conformité. **Comment les Administrateurs de la Sécurité et du Cloud peuvent-ils prévenir les fuites de données ?** Les précautions incluent la mise en œuvre de politiques strictes de contrôle d'accès, le chiffrement des données sensibles, la surveillance des activités des utilisateurs et des systèmes, la gestion des vulnérabilités, la sensibilisation des employés sur les risques de sécurité, ainsi que la mise en place de mécanismes de détection des menaces avancées. **Quelles sont les tendances émergentes dans le domaine de la sécurité cloud ?** Les tendances incluent l'adoption croissante de l'automatisation et de l'intelligence artificielle pour renforcer la sécurité, le développement de solutions de sécurité cloud natives, l'intégration de la sécurité dans le cycle de vie du développement logiciel (DevSecOps), ainsi que l'évolution des réglementations et des normes de conformité liées à la protection des données dans le cloud.