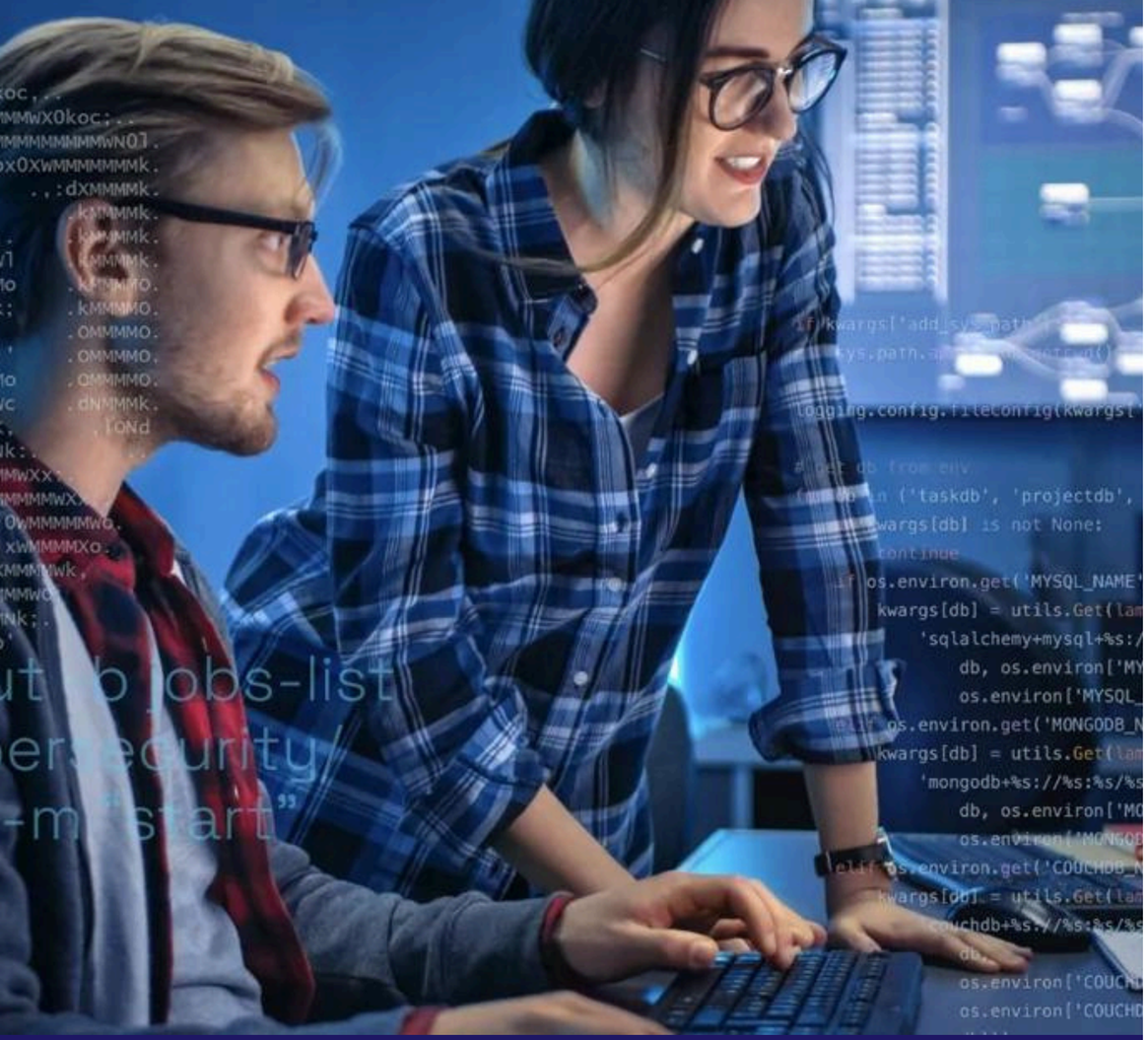
CYBERNETIC-SECURITY

SALON DE

CYBERSECURITÉ



SALON DE CYBERSECURITY

Thème

EXPLORER LES DOMAINES DE LA SECURITE INFORMATIQUE

(Cybersécurité)

L'Équipe

DR PAPA MORY GYEUE
Expert en Cybersécurité
Spécialiste des Méthodes et Systèmes de Protection de l'Information
Enseignant chercheur

M. ERHAD FALEU
Ingénieur en Cybersécurité
Risk Manager

M. ISSIAGA KALTAMBA
Responsable SOC 1 et 2
ASTO (Analyste SI)
Consultant en Cybersécurité

Sommaire

OBJECTIF DU SALON

- DÉFINITION DE LA CYBERSÉCURITÉ - SÉCURITÉ INFORMATIQUE
  - HACKING ET PIRATAGE INFORMATIQUE
- MÉTIERS ET ROLE DE LA CYBERSÉCURITÉ
  - MISSIONS
  - COMPÉTENCES
  - FORMATIONS
- GUIDE COMPLET

DÉFINITIONS

Cybersécurité désigne l'ensemble des pratiques, technologies et processus conçus pour protéger les systèmes informatiques, les réseaux, les programmes et les données contre les attaques, les dommages ou les accès non autorisés.

Hacking est le processus d'exploration et de manipulation des systèmes informatiques pour comprendre leur fonctionnement, améliorer leurs performances ou exploiter des vulnérabilités.

Piratage informatique (ou cyberpiratage) *est l'acte d'accès illégal ou non autorisé à des systèmes informatiques, des réseaux ou des données.*

GESTION ET PILOTAGE DE PROJET DE SECURITE

CONCEPTION ET MAINTIEN D'UN SI DE SECURITE

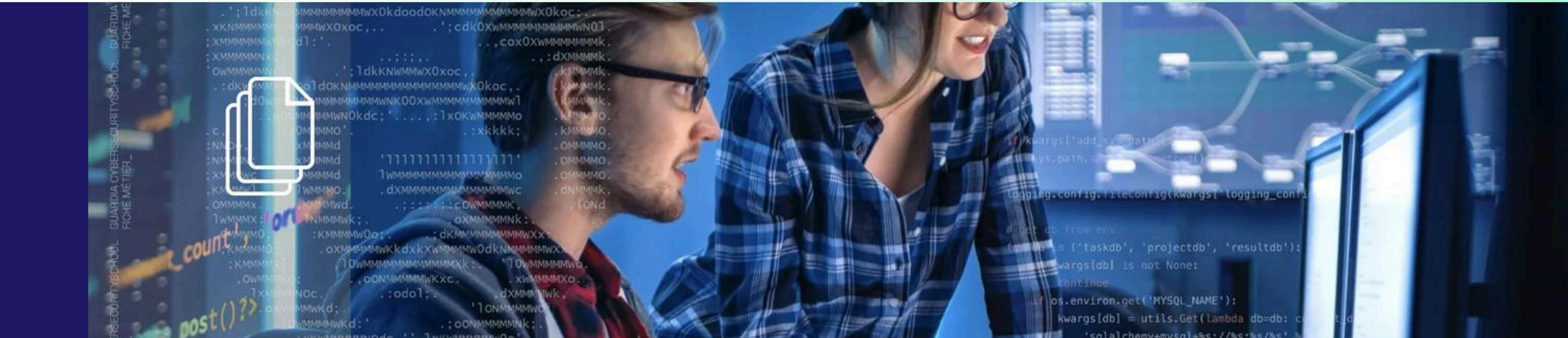
GESTION ET DES INCIDENTS DES CRISES

CONSEILS, SERVICE ET RECHERCHES

ANALYSTE DE LA MENACE CYBERSÉCURITÉ

Missions Ses missions sont d'une part, de détecter toutes les menaces et activités suspectes ou malveillantes sur les différents systèmes d'information, d'autre part, de faire de la prévention au sujet des cyberattaques et autres menaces potentielles sur le système d'information d'une entreprise

Compétences Travailler en tant qu'analyste demande de mettre en pratique une série de compétences acquises en formation puis au fil des expériences. Elles sont donc fondamentales.



ANALYSTE DU SECURITY OPERATION CENTER

Missions Les SOC sont composés d'analystes, d'ingénieurs en sécurité, ainsi que de managers supervisant les opérations de sécurité. Les équipes SOC travaillent étroitement avec les équipes d'intervention afin de s'assurer que le problème de sécurité soit bien réglé une fois qu'il a été découvert.

Compétences Compétences Pour exercer en qualité d'opérateur analyste SOC, il est indispensable de posséder un socle de compétences informatiques solides orientées cybersécurité. Il est également nécessaire de connaître le cadre réglementaire relatif à la sécurité informatique : Sécurité des systèmes d'exploitation · Sécurité des réseaux et protocoles · Et en matière de cyberdéfense

ANALYSTE DU CSIRT OU CERT

CERT (COMPUTER EMERGENCY RESPONSE TEAM) OU CSIRT (COMPUTER SECURITY INCIDENTRESPONSE TEAM).

Missions

Dans un monde où les réseaux globaux prennent toujours plus d'expansion et une importance stratégique qui ne se dément pas, les systèmes d'information d'une organisation doivent pouvoir résister aux différentes menaces qui pèsent sur eux.

Compétences

Devenir expert des réponses aux incidents de sécurité nécessite de posséder de solides compétences informatiques et des connaissances pointues en cybersécurité

ARCHITECTE CYBERSÉCURITÉ

Missions

L'architecte cybersécurité définit et structure les choix techniques en matière de sécurité des systèmes d'information en réponse aux besoins du client et veille à leurs applications.

Compétences

Exercer à ce poste demande un niveau d'exigence certain ainsi que la maîtrise de compétences indéniables. A savoir : · Le système d'information, de l'urbanisation et de l'architecture du SI · La sécurité des systèmes d'exploitation · La sécurité des réseaux et protocoles · La contribution des architectures à la sécurité : conception et modèles · La contribution des architectures à la sécurité : intégration des systèmes · Les connaissances des solutions de sécurité du marché · La veille technologique cybersécurité et étude des tendances · L'innovation cybersécurité · La capacité de compréhension des menaces en matière de cybersécurité

CHEF·FE DE PROJET CYBERSÉCURITÉ

CONSULTANT·E EN CYBERSÉCURITÉ

CRYPTOLOGUE

DIRECTEUR·RICE CYBERSÉCURITÉ

GESTIONNAIRE CRISE CYBERSÉCURITÉ

HACKER·EUSE ÉTHIQUE

PENTESTER

Missions

Les entreprises de plus en plus sujettes aux cybermenaces doivent se doter d'experts en cybersécurité capables de raisonner de la même manière que leurs potentiels attaquants, ceci afin de limiter et anticiper au maximum les failles et intrusions malveillantes dans leur système informatique.

Compétences

Exercer comme pentester demande des compétences nombreuses et étendues : · Capacité de compréhension des menaces cybersécurité · Capacité à exploiter des sources ouvertes de manière sécurisée · Mise en place de plans de veille sur un ou plusieurs secteurs déterminés · Détection, qualification et analyse d'informations pertinentes · Connaître le droit et les réglementations en vigueur en matière de cybersécurité

RESPONSABLE DU SOC

Missions

Missions Le responsable du SOC assure la planification, la gestion et le suivi quotidiens des opérations.

Compétences

Pour devenir responsable du SOC, il est indispensable de posséder un socle de compétences informatiques solides orientées cybersécurité. Il est également nécessaire de connaître le cadre réglementaire relatif à la sécurité informatique. Cela se traduit par : · La sécurité des systèmes d'exploitation · La sécurité des réseaux et protocoles · La gestion de crise · L'analyse de journaux (systèmes ou applicatifs) · L'analyse de flux réseaux · Les outils et de méthodes de corrélation de journaux d'événements (SIEM) · Les solutions de supervision sécurité · Les techniques d'attaques et d'intrusions · Les vulnérabilités des environnements · Le scripting

RESPONSABLE DE LA SÉCURITÉ DES S.I. (RSSI)

ÉVALUATEUR·RICE DE LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

COORDINATEUR·RICE CYBERSÉCURITÉ

SPÉCIALISTE EN DÉVELOPPEMENT SÉCURISÉ

AUDITEUR·RICE DE SÉCURITÉ ORGANISATIONNELLE

ANALYSTE EN RÉPONSE À INCIDENTS

HACKER·EUSE ÉTHIQUE

AUDITEUR·RICE DE SÉCURITÉ TECHNIQUE

Missions

Missions L'auditeur de sécurité technique conduit des évaluations techniques de la sécurité d'environnements informatiques. Son rôle est d'identifier les vulnérabilités et de proposer des actions de remédiation. Il peut réaliser différents types d'audits en fonction de son périmètre d'activité (tests d'intrusion, audit de code, revue de configuration, etc.).

Compétences

Exercer en qualité d'auditeur de sécurité technique suppose de disposer de solides compétences en sécurité des systèmes d'information, en cyberdéfense ainsi qu'en droit informatique .

ANALYSTE CYBERSÉCURITÉ

Missions

L'analyste cybersécurité assume un double rôle : il doit être force de proposition pour prévenir les risques cyber et le moteur de la réaction lorsqu'une faille de sécurité a été exploitée par un attaquant.

Compétences

Le métier d'analyste en menace de cybersécurité se nourrit de compétences techniques très solides. Il requiert également une aptitude à cerner les enjeux globaux : ceux de la cyberdéfense en général, ainsi que les enjeux propres à la structure défendue. À ce titre, il sera essentiel de bien connaître les métiers existants au sein de la structure et leur lien avec les problématiques de sécurité informatique.

MANAGER DE RISQUES

Missions

Le manager de risques en cybersécurité est l'un des premiers remparts de la protection et l'un des premiers maillons de la réaction en cas d'attaque avérée contre les systèmes informatiques.

Compétences

Le manager de risques cyber assume un double rôle : il doit être force de proposition pour prévenir les risques cyber et le moteur de la réaction lorsqu'une faille de sécurité a été exploitée par un attaquant.

ANALYSTE FORENSIC

Missions

L'analyste forensic prend une part active à toutes les missions d'investigation et de réponse à incidents, généralement gérés par un CERT (Computer Emergency Response Team) ou un CSIRT (Computer Security Incident Response Team).

Sur le plan des compétences purement techniques, plus le nombre d'environnements informatiques qu'il maîtrise est important, plus un analyste forensic prend de la valeur aux yeux des entreprises et des employeurs potentiels. Son aisance au sein de différents systèmes cryptés est un atout de taille pour assurer une réactivité complète, face à tous les dangers cyber.

MALWARE ANALYST

Missions

Bien qu'ils ne soient généralement pas considérés comme faisant partie de l'équipe de réponse aux incidents à proprement parler, et bien qu'ils ne soient pas tout à fait en première ligne de défense, les malware analysts sont souvent appelés à la rescousse pour les premières étapes de réaction à une attaque.

Compétences

Il est important de préciser, d'entrée de jeu, que chaque structure est susceptible de rechercher un ensemble de compétences uniques, correspondant à ses besoins propres

OSINT ANALYST

Missions

Les missions d'un OSINT Analyst sont intimement liées aux enjeux de threat intelligence. Ce professionnel est chargé de centraliser et d'analyser un maximum de données en accès public, dans le but de rassembler de nouvelles connaissances sur des attaquants potentiels, leurs motivations, leurs méthodes et leurs outils.

Compétences

L'OSINT analyst est amené à mobiliser des compétences en lien avec l'investigation et l'analyse, mais aussi la gestion de projet et l'approche technique des données.

BUG BOUNTY HUNTER

Missions

Il a deux tâches principales : · Trouver des bogues et des failles de sécurité · Signaler ces bogues et ces failles de sécurité de manière responsable. Lorsqu'un pirate découvre une faille dans un système, il signale sa découverte par courrier électronique. Un responsable du programme de bug bounty examine toutes les découvertes signalées et décide de récompenser ou non la personne responsable

Compétences

Les bugs bounty hunter connaissent les principes fondamentaux de la cybersécurité, mais ils doivent surtout acquérir des connaissances approfondies et se perfectionner dans de nombreux domaines tels que le réseau, le codage, la sécurité, le cloud et la façon dont tout fonctionne ensemble.

EXPERT·E EN CYBERSÉCURITÉ

Missions

Avec l'avancée de la technologie, de nouvelles menaces de sécurité peuvent apparaître à tout moment. L'expert en cybersécurité doit donc rester vigilant et se tenir au courant des dernières tactiques des pirates informatiques.

Compétences

Outre les compétences générales de base comme la communication, le leadership, le travail d'équipe et la résolution de problèmes,

MERCI

POUR VOTRE ATTENTION

WWW.REALLYGREATSITE.COM

PHASE DES QUESTIONNAIRES

Plus d'information

SITE WEB: CYBERNETIC-SECURITY.COM

EMAIL: INFO@CYBERNETIC-SECURITY.COM

TÉLÉPHONE:

+221 78 833 88 47

+221 78 896 49 96

+221 76 355 19 09

@CYBERNETIC-SECURITY

@CYBERNETIC-SECURITY

@CYBERNETIC-SECURITY