Consultant Cybersécurité

04 années d'expérience

EWANGUE / Eric

COMPETENCES

Fonctionnelle	- Gouvernance de la sécurité du SI : Elaboration de la PSSI, Campagne de sensibilisation (phishing, reflexe cybersécurité…) - Analyse des risques Cyber : identifier et classifier les biens supports et valeurs métiers, définir le socle de sécurité, réaliser des analyses de risques EBIOS RM - Evaluation des besoins sécurité en DICT - Evaluation des écarts de conformité par rapport aux objectifs/politiques cybersécurité existants - Reporting et suivi de la mise en place des mesures de sécurité
Opérationnelle	- SOC/ Gestions des vulnérabilités : • Analyse, qualification, détection, réponses (Qradar, Splunk, Cortex, Proofpoint, ThreatQ, any.run, …) • Analyse Forensique • Reporting et amélioration continue • Mise à jour des règles (SourceFire …) • Scan des ressources du SI via Qualys • Suivi des vulnérabilités et mise en place des patchs de sécurité via CyberWatch • Dump de mémoire ou du traffic (TCPDUMP, memoryze DUMP) - IAM/PAM gestion des privilèges • Création, modification et suppression des coffres (CYBERARK-BASTION) - PKI gestion des certificats internes • Création, renouvellement et révocation des certificats via VENAFI - Gestions de flux • Analyse de la conformité Cyber des flux • Transcriptions des flux • Implémentation des flux sur PaloAlto, Juniper, F5 • Elaboration des dérogations
Outils / Technologies	TENACY, EGERIE, O365, Qradar, SPLUNK, CORTEX, CyberWatch, Proofpoint, CyberArk, VENAFI, ServiceNOW, VirusTotal, PaloAlto, Juniper Junos, F5, TCPDUMP WIRESHARK
Méthodes	EBIOS RM
Normes	ISO27001, ISO27005, DORA, NIS2, RGPD, LPM, HIPAA

FORMATION

2021	*DIGITAL SCHOOL OF PARIS / INSTITUT F2I* *MASTERE SPECIALISE EN CYBERSECURITE*

CERTIFICATIONS

2024	***ISO27001 LEAD IMPLEMENTER***
2024	***ISO27005 RISK MANAGER***
2023	***SPLUNK ADMINITRATION***
2022	***NSE 1 et 2***

LANGUES

FRANÇAIS	COURANT (écrire et parler)
ANGLAIS	TECHNIQUE (écrire et Parler)

EXPERIENCE PROFESSIONNELLE

10/2022 – 09/2024

e.SNCF SOLUTIONS (DIRECTION CYBERSECURITE)
TRANSPORT-FERROVIER
ANALYSTE CYBERSECURITE

SOC/ GESTION DES VULNERABILITES :

- Analyse, qualification, détection, réponses des incidents (Qradar, Splunk, Cortex, Proofpoint, ThreatQ, any.run, …)
- Elaboration des rapports d'incidents
- Analyse Forensique (isolation de la machine, faire de la sauvegarde et un dump, rechercher les traces d'intrusion et/ou compromision, garder les preuves, remasteriser la machine, implémenter les patchs de sécurité, reporting)
- Reporting et amélioration continue
- Mise à jour des règles (SourceFire …)
- Scan des ressources du SI via Qualys
- Suivi des vulnérabilités et mise en place des patchs de sécurité via CyberWatch
- Dump de mémoire ou du traffic (TCPDUMP, memoryze DUMP)
- Veille sur les actualités cybersécurités ANSSI

IAM/PAM gestion des privilèges

- Création, modification et suppression des coffres (CYBERARK-BASTION)

PKI gestion des certificats internes

- Création, renouvellement et révocation des certificats via VENAFI

Gestion des flux

- Analyse de la conformité Cyber des flux
- Transcriptions des flux
- Implémentation des flux sur PaloAlto, Juniper, F5
- Elaboration des dérogations sur MyDerog

GRC/ISP

- Gouvernance
- Élaboration et mise en œuvre de la PSSI
- Conduite de campagnes de sensibilisation à la cyber (phishing, réflexes cyber, bonnes pratiques)
- Collaboration avec les parties prenantes (chefs de projet, métiers, RCS, RSSI, etc.)
- Reporting périodique et synthèses concernant la prise en charge de la sécurité du SI, de leur niveau sécurité et des risques associés
  - Risque
- Identification & cartographie des besoins cyber (besoins DICT)
- Classification des actifs clients et valeurs métiers
- Définition du socle de sécurité
- Élaboration de scénarios stratégiques & opérationnels
- Mise en place et suivi des mesures de réduction des risques
-
  - Conformité
- Identification et correction des non-conformités de sécurité des flux internes

- Evaluation des écarts de conformité des projets SI par rapport aux objectifs/politiques de cybersécurité existant(e)s

04/2019 – 09/2021

SFR
TELECOMMUNICATION
Analyse SOC N1

SOC N1

- Traitement des alertes et des incidents de sécurité
  - ✓ Analyser les logs venant des OS, des agents, des switchs et routeurs
  - ✓ Investiguer sur les alertes
  - ✓ Qualifier le niveau de sévérité des incidents
  - ✓ Rédiger les rapports d'incidents
  - ✓ Escalader vers les analystes SOC N2
  - ✓ Superviser les alertes d'incidents sur Qradar
- Evaluer et corriger les vulnérabilités :
  - ✓ Exposition des portails d'authentification (vérifier la légitimité d'exposition, vérifier les données du certificat, proposer de passer par un bastion ou par un SSO ou une autre méthode d'authentification forte)
  - ✓ Exposition des comptes users et mots de passes (vérifier la légitimité d'exposition, modifier le mot de passe du compte en respectant la PSSI vérifier les impacts, sensibilité sur l'utilisation des adresses emails professionnel suivant la PSSI)
  - ✓ Scan des ports (vérifier la légitimité des scans, bloquer cette action, vérifier les données scannées, demande d'attribution des privilèges nécessaires.)
  - ✓ Assurer le veille technologique et sécuritaire sur les menaces
  - ✓ Sensibilisation des équipes à la Cybersécurité.