DOMINIQUE ASMAR

INFORMATICIEN SENIOR

0660653535 | asmar.dom@laposte.net | Paris
Français | permis A + B

PROFIL

Analyste SOC en cybersécurité avec une expertise dans la surveillance des incidents, l'analyse des menaces et la gestion des réponses aux incidents de sécurité. Capable de détecter et de résoudre les vulnérabilités de sécurité à l'aide de technologies de pointe telles que SIEM, EDR et IDS/IPS.

Maîtrise des techniques d'EthicalHacking, de Cyber Threat Intelligence, des études d'attaque APT & MITRE ATT&CK, et des tests Atomic Red Team pour une meilleure protection des données sensibles et pour la prévention des cyberattaques. Doté d'un fort esprit d'analyse et d'une capacité à réagir rapidement dans des environnements à haute pression, tout en travaillant en collaboration avec des équipes pluridisciplinaires pour garantir la sécurité globale de l'infrastructure IT.

FORMATIONS

Analyste Cybersécurité

CyberUniversity - 10.2023 / 07.2024

Protection des réseaux et systèmes
Détection et analyse des attaques

Master Gestion des entreprises

Paris-Dauphine - 1984

Gestion financière des PME
Informatique de Gestion

Analyste Programmeur

SII Sagesse, Versailles - 1986

Méthodes Meryse, Grantt
Fortran Cobol Basic IBM400

COMPETENCES TECHNIQUES

SIEM (Security Information and Event Management) : Gestion et optimisation des plateformes SIEM via Splunk pour la détection et l'analyse des menaces.
Détection et réponse aux incidents : analyse et remédiation des incidents de sécurité à l'aide d'outils EDR (Endpoint Detection and Response).
Gestion des vulnérabilités : Utilisation d'outils de scanning pour identifier et corriger les vulnérabilités du système.
Surveillance des réseaux et des systèmes : Surveillance des infrastructures réseau (IDS/IPS, pare-feux, proxy, sondes snort) et analyse des logs pour identifier les activités suspectes.
Threat Intelligence : Utilisation de sources de renseignements sur les menaces pour identifier les tendances d'attaques et proposer des actions proactives.
Réponse aux incidents : Développement et mise en œuvre de processus de réponse aux incidents de sécurité (IRP), en coordination avec les équipes concernées.
Forensic : analyses approfondies sur les malwares et à comprendre leur fonctionnement pour proposer des mesures correctives.

LANGUES

Français

Très bonne maitrise de l'écrit et l'oral

Anglais

Anglais technique

EXPÉRIENCES PROFESSIONNELLES

Directeur de l'informatique

AirOzone technologie bio, Paris - 2019 / 2023

Réalisation de l'ERP et du SIC, incluant les modules de prise de RDV onLine (type RDV doctolib), intervention techniciens, devis-factures, E-marketing...

Développement informatique

diverses entreprises, France et étranger - 2000 / 2019

Supervision de projets informatiques articulés autours de Bases de données SQL, au moyen de langages dynamiques (PHP, XML,ActionScript), et web (HTML, CSS, Bootstrap, Javascript)

PROJET PROFESSIONNEL

Architecture et paramétrage du réseau d'entreprise sur hyperviseur : Windows / Linux - firewall Pfsense.
KaliLinux pour cyberattaques (mail de phishing, récupération des ID, altération VPN, modification règles pare-feux, faux serveur HTTP...).
Détection des attaques sur SIEM Splunk par Universal Forwarder, IPS Snort .

INTÉRÊTS

QUALITES

Responsable
Facultés de compréhension
Humain
Commercial
Motivant
Esprit de synthèse, méthode
Creatif
Capacite d'adaptation
Recrutement
Honnêteté

CENTRES d'INTERETS

Histoire des civilisations
Géopolitique
Montage photo et video
Technologies
Architecture urbaine
Soutien à l'Open Source

RÉSEAUX SOCIAUX

@dominique-asmar-5b923b240