Consultante en Cybersécurité

COMPETENCES

Programmation	Python, Scapy, Script Shell, C/C++, Kusto, Splunk
Web	HTML/CSS, XML, JavaScript, PHP
Cloud	Azure (Azure Security Engineer Associate AZ500), Azure Sentinel, AWS, Knowbe4
Sécurité	Kali Linux, Nmap, Metasploit, Maltego, Wireshark, BurpSuite, Nexpose, Nessus, CIS, Analyse de Risk, SIEM, SOAR, RGPD, Threat Intelligence, OWASP, EBIOS, CVSS, ISO27001, ISO27005
Base de données	SQL: Oracle, Mysql, PostgreSQL NoSQL: MongoDB
Devops/Containerisation	Ansible, Docker, LXC, Kubernetes
IDE	Visual Studio, VBA
Versionning	SVN/Git
OS	Linux (Redhat, Ubuntu, Debian, Fedora, CentOS), OS X, Windows, Windows server
Méthodologie projet	Agile/Scrum
Langues	Anglais: Niveau intermédiaire
Autres outils	Kaspersky Security Center, IBM QRadar, MS Active Directory, Fortinet, CISCO ASA/IOS, CISCOWorks LMS, Packet Tracer, GNS3, Latex, challenges Root-me

meguenni.yasmina@gmail.com / +33 7 58 00 19 19

EXPERIENCE PROFESSIONNELLE

Depuis Jan 2022

GreenSI

Consultant en Cybersécurité

Analyste SOC chez Bouygues Immobilier :
Au sein de l'équipe CSIRT, en charge d'analyse et remédiation des incidents de sécurité remontés par le SOC :

- Gestion des incidents SOC (qualification, triage, troubleshooting & résolution)
- Réalisation des actions de remédiations et proposition des recommandations sécurité
- Rédaction de fiche réflexe des incidents de sécurité
- Tuning des règles de détection et gestion de Whitelist
- Réalisation des stimulés des usecase
- Analyse et triage des alertes EDR Crowdstrike
- Mise en place des exclusions ML et IOA sur Crowdstrike
- Traitement des alertes Microsoft ATA
- Traitement des alertes de phishing Proofpoint

Environnement technique : Linux, Windows, Azure Sentinel, LogAnalytics, Kusto, Splunk, Syslog, Qradar, CVSS, CVE, Crowdstrike, ATA, Nxlog, Proofpoint

Fév 2020 à Déc 2021

Dataxium

Consultant en Cybersécurité

Assistance technique en sécurité chez SCOR :
Au sein de l'équipe sécurité, en charge de l'analyse des emails frauduleux et demandes liées à la sécurité :

- Analyse technique des emails Abuse
- Simulation des campagnes de phishing
- Sensibilisation des utilisateurs à l'égard des attaques de phishing/scam
- Analyse et filtrage des demandes liées au DLP
- Réponse aux incidents de sécurité : analyse des logs, donner des recommandations aux équipes techniques

Analyste SOC :
Au sein de l'équipe interne de Dataxium, en charge de la construction des produits cybersécurité :

- Mise ne place de l'offre SIEM basée sur Azure Sentinel
- Intégration Datasource et flux de données
- Exploitation du service de Threat Detection and Investigation
- Threat Hunting
- Création des alertes de monitoring en s'appuyant sur le framework MITRE Attack (détection de brut force, connexion anonyme via TOR ou VPN)
- Exploitation et gestion des incidents sécurité (qualification, troubleshooting, résolution & recommandation)

Audit & Pentest:

- Mise en place d'une méthodologie d'évaluation automatique prenant en compte le assessment risk, le vulnerability assessment et le hardening.
- Evaluation automatique des vulnérabilités d'une plateforme Big Data (CDH/HDP).
- Création des dashboard de Key Performance Indicator (KPI) en matière de sécurité.
- Réalisation de pentests applicatifs (conduite du pentest et rédaction des rapports)

Environnement technique : Linux, Windows, Azure Sentinel, LogAnalytics, Kusto, Syslog, Python, CVSS, CVE, EBIOS, CIS, VBA, BurpSuite, Maltego, Nmap, DNS

Mars à Aout 2019

Proxiad Paris

Auditrice Sécurité :

Au sein de l'équipe Sécurité Proxiad responsable de la partie MOE « la maîtrise d'ouvrage » :

- Evaluation des sous-traitants, en termes de conformité aux normes (ISO 27001 et 9001) et/ou aux référentiels (OWASP, RGPD).
- Mise en conformité par rapport aux exigences de sécurité des clients.
- Préparation de l'audit à blanc.

- Audit des salles informatiques.

Environnement technique : ISO27001, ISO9001, ISO27005, OWASP, RGPD.

Mai 2012 à Sep 2017

Ministère du Commerce

Ingénieur de production informatique

Gestion des incidents :

- Exploitation / Run : état de protection des end point (postes client et serveurs en temps réel via le Kaspersky Security Center (KSC)), et du trafic des flux entrant/sortant des firewalls (Fortinet).
- Analyse, classification et gestion des incidents : nombre de malware par poste, nouveaux virus
- Gestion des vulnérabilités et déploiement des mises à jour et correctifs liées à Windows et les applications inconnues via le Kaspersky Security Center.
- Mise en place des stratégies de Kaspersky Security Center (postes de travail et serveurs), modification des règles du pare-feu.
- Sensibilisation des utilisateurs.

Administration du réseau

- Vérification et dépannage des réseaux : LAN, VPN, liaisons internet.
- Configuration et gestion du Wifi (DLink, Aruba, Ruckus, TPLink).
- Administration de la solution Kaspersky Security Center (mise à jour, analyse, installation d'agents).
- Gestion et administration des firewalls (ASA pour les réseaux VPN, Fortinet pour les connexions internet).

Environnement technique: Windows, Linux, ASA, FORTINET, SCCM, SCOM, Kaspersky Security Center, DLINK, TPLink, Ruckus, Aruba, MS-AD, CISCO

CERTIFICATIONS & FORMATIONS

2020	Certificat : Azure Security Engineer Associate (AZ 500)
2020	Master 2 en Sécurité des Systèmes Informatiques *Université Rouen Normandie*
2011	Master 2 Réseaux et Systèmes Distribuées *Université des sciences et de la Technologie Houari Boumediene – Alger*
2009	Licence en Informatique Général *Université des sciences et de la Technologie Houari Boumediene – Alger*
2006	Baccalauréat Sciences Exactes *Alger*