CV Stella Stoyanova – Analyste SOC | Cybersécurité | Réponse aux Incidents

@✉

GitHub:

LinkedIn:

06.60.70.81.86.

Expérience Professionnelle

DataScientTest – Analyste SOC
Avril 2024 – Janvier 2025 | Paris, France

Analyse des incidents de sécurité à l'aide de Splunk et de la stack ELK

Threat hunting avec des outils EDR/XDR (Cortex XDR, Cybereason, Tehtris)

Enquêtes forensiques sur des postes Windows, rapports techniques détaillés

Application du cadre MITRE ATT&CK dans la détection et la remédiation

Surveillance de la compromission des comptes Active Directory

Hogan Lovells – Analyste Support Informatique N2/N3
Février 2023 – Février 2024 | Paris, France

Support bureautique personnalisé pour les outils du CIO

Gestion des accès, création/suppression de comptes via Active Directory

Déploiement de postes, configuration de smartphones, M365, VPN

Sécurisation des salles de réunion, traitement des incidents critiques

Louis Vuitton – Analyste Informatique
Juin 2022 – Décembre 2022 | Paris, France

Assistance utilisateurs, déploiement de postes et périphériques

Monitoring de l'environnement IT et application des politiques de sécurité

Support à distance (outil Lync/Teams), formation à l'utilisation des outils

Johnson & Johnson – Spécialiste Systèmes d'Information
Septembre 2018 – 2022 | Issy-les-Moulineaux, France

Gestion des backups cloud (AWS, SaaS, Veeam, NetBackup, Azure)

Suivi des KPIs, rapports Nexthink, coordination des incidents selon SLA

Collaboration avec les équipes américaines sur les projets de cybersécurité

Eversheds Sutherland – Analyste Support
Mars 2018 – Août 2018 | Paris, France

Support technique N2 pour les applications métier, téléphonie, mobile

Dépannage Windows 7/10, gestion des accès et équipements

Préparation des comptes pour onboarding, intervention VIP

ENGIE – Technicien Support Informatique
Janvier 2018 – Mars 2018 | Paris, France

Support N1 multicanal pour les nouveaux arrivants

Réinitialisation de mots de passe, gestion des droits, configuration VPN

Support mobile et tokens RSA, rédaction de procédures FR/EN

LCH Clearnet – Technicien Support N2
Février 2017 – Décembre 2017 | Paris, France

Gestion des accès, maintenance des postes, support Microsoft O365

Suivi des incidents via Remedy, configuration d'imprimantes/Visioconf

Hermès / Givenchy – Support Événementiel (Fashion Week)
Février 2017 | Paris, France

Support VIP multilingue (français, anglais, russe)

Déploiement de smartphones, configuration Wi-Fi et messagerie

Formation utilisateurs pour Outlook, VPN, et authentification mobile

ESCP Europe – Technicien Informatique
Janvier 2015 – Décembre 2016 | Paris, France

Support des postes Windows, installation d'imprimantes, pack Office

Gestion des stocks IT, préparation de matériels pédagogiques

Déploiement logiciels, création d'identifiants, suivi technique

École Alsacienne – Stage Technicien Support
Avril – Mai 2014 & Août – Septembre 2014 | Paris, France

Remplacement de postes, installation de logiciels, configuration GPO

Gestion des salles informatiques, câblage réseau et bornes Wi-Fi

AURA – Technicien Informatique
Août 2011 – Décembre 2013 | Paris, France

Mises à jour, migrations vers Windows 7, support poste de travail

Déploiement de logiciels de gestion (planning, facturation, caisse)

Assistance technique aux utilisateurs et gestion du parc IT

Info-Save (Bulgarie) – Administrateur Réseau / Support
Août 2007 – Mai 2011 | Sofia, Bulgarie

Installation de réseaux TCP/IP, configuration routeurs/switches

Gestion des serveurs (Windows Server), comptes utilisateurs, sécurité

Support technique sur Windows XP/7, maintenance sur site et à distance

Compétences Techniques

SIEM & EDR/XDR

Splunk, Sentinel, QRadar, ELK

Cortex XDR, Cisco Secure Endpoint, Cybereason, Tehtris

Infrastructure et Réseaux

Active Directory, Exchange, Windows Server, Office 365

TCP/IP, DNS, DHCP, VPN (Citrix, OpenVPN), pare-feux, Wireshark

Virtualisation : VMware, Hyper-V

Cloud & Sauvegarde

AWS, Azure, NetBackup, Veeam, SaaS/IaaS

Gestion des KPIs, tableaux de bord Nexthink

Scripts & Langages

Python, PowerShell, Bash, SQL

Intégration d'IOCs, enrichissement automatique des journaux

Cadres & Conformité

MITRE ATT&CK, ISO 27001, NIST, RGPD

ITIL, SLA, gestion du cycle de vie des actifs

Formations & Certifications

Certificat de Cybersécurité – Sorbonne Université (Avril 2024 – Février 2025)

Formation diplômante axée sur les SOC, la réponse aux incidents, le threat hunting, la forensique et les normes ISO/NIST.

Analyste SOC – Cyber Université (2024 – 2025)

Technicien Supérieur Réseaux & Systèmes – GRETA Paris Centre (2014)

Diplôme BAC+4 en Informatique – Université Technique de Sofia, Bulgarie (2007)

Formation continue – Cybersécurité, forensique, intelligence des menaces

Projets en Cybersécurité

Cyber Threat Map

Développement d'une carte interactive en temps réel des attaques cyber à l'échelle mondiale

Technologies : JavaScript, Leaflet.js, Flask, REST API, GeoJSON

Intégration de données provenant d'AbuseIPDB, VirusTotal, etc.

Phishing Detector

Outil web d'analyse automatisée des e-mails suspects (.eml)

Moteur de scoring basé sur le machine learning (scikit-learn)

Analyse des en-têtes, liens, et contenu HTML

Playbook de Threat Hunting

Détection mappée au cadre MITRE ATT&CK

Scripts Python pour enrichissement IOC, corrélation dans Splunk

Création de dashboards et automatisation des procédures SOC

Langues

Français – courant

Anglais – courant

Russe – intermédiaire

Bulgare – langue maternelle

Centres d'Intérêt

OSINT, veille cyber

Analyse forensique

Lecture de cartes, musique, cinéma

Portfolio – Projets de Cybersécurité

 Cybersecurity Portfolio – https://www.stellabarbarella.comhttps://www.stellabarbarella.com

 Interactive Threat Map – https://www.stellabarbarella.com/cyber-threat-map.htmlhttps://www.stellabarbarella.com/cyber-threat-map.html

 Threat Hunting Dashboard – https://www.stellabarbarella.com/threat-hunting.htmlhttps://www.stellabarbarella.com/threat-hunting.html

 Phishing Analysis Platform – https://www.stellabarbarella.com/phishing-detector.htmlhttps://www.stellabarbarella.com/phishing-detector.html

 SIEM Analytics Center – https://github.com/stellababy2004https://github.com/stellababy2004

⚡ **Live Threats Monitor –** https://www.stellabarbarella.com/live-threats.htmlhttps://www.stellabarbarella.com/live-threats.html