

PJN
Analyste SOC
6 ans d'expérience

Consultant en cybersécurité et cyberdéfense disposant de 6 ans d'expérience, spécialisé dans la détection, le traitement et l'amélioration des dispositifs SOC/CERT. Son parcours couvre la mise en œuvre de SMSI ISO 27001, la gestion des risques selon ISO 27005 / EBIOS RM, l'intégration de SIEM comme Splunk, ELK et Microsoft Sentinel. Il intervient sur des missions de conception de scénarios de détection, collecte et corrélation de logs, développement de règles avancées SPL/KQL/DSL, traitement d'incidents de sécurité, préparation d'audits ISO 27001, automatisation SOAR et amélioration continue des processus SOC. Ses expériences récentes chez Banque de France et BDO France démontrent une forte orientation opérationnelle autour de Splunk, Sentinel, Microsoft Defender, Tenable Nessus, Active Directory, Entra ID, Intune et TheHive.

FORMATION ET CERTIFICATIONS

2023 - 2024 : Mastère spécialisé [Bac+6] Cybersécurité et Cyberdéfense - Institut Polytechnique de Paris / Télécom Paris - Bien

2020 - 2022 : Master 2 [Bac+5] Sécurité des Systèmes d'Information - ICT University - Très Bien.

2017 - 2020 : Licence [Bac+3] Sécurité Informatique - École Normale Supérieure de Yaoundé - Assez bien.

COMPETENCES TECHNIQUES

Compétences principales

Administration Splunk

Administration et exploitation de plateformes Splunk : Forwarder, Indexer, Search Head, Deployment Server, Cluster Master et Data Input ; intégration des sources de logs, gestion des sourcetypes, développement de règles de corrélation SPL, création de tableaux de bord, supervision des performances, automatisation de la réponse via Splunk Phantom / SOAR et amélioration continue des cas d'usage SOC.

Analyse et détection d'incidents

Analyse des événements de sécurité, la corrélation de logs et la création de règles de détection avancées dans Splunk, Microsoft Sentinel et ELK. Il utilise SPL, KQL et DSL pour analyser les logs en temps réel et identifier les comportements suspects.

Traitement des incidents SOC

Traitement des incidents de sécurité tels que l'impossible travel, les téléchargements massifs, les malwares et le phishing, avec prise en compte des mécanismes DMARC, DKIM et SPF.

Développement de cas d'usage SOC

Il a développé des use cases de détection d'anomalies, notamment avec Splunk, en utilisant des fonctions de recherche avancées comme search, eval, stats, where, top et rare.

SIEM et supervision sécurité

Il dispose d'une expérience sur la mise en place et l'exploitation de SIEM, notamment Splunk, ELK et Microsoft Sentinel, pour la surveillance, la détection et la gestion des incidents de sécurité.

SOC N1/N2/N3 et CERT

Son parcours couvre plusieurs niveaux d'intervention SOC : SOC N1/N2, SOC N3, VOC et SOC/CERT, avec des missions allant de la supervision à l'analyse avancée, la qualification, la réponse et l'amélioration continue des détections.

Investigation et réponse aux alertes

Il a contribué à l'automatisation du traitement des alertes, à la rédaction de procédures de réponse aux incidents et à la capitalisation sur les incidents pour améliorer la maturité SOC.

Vulnérabilités et priorisation du risque

Il maîtrise Tenable Nessus pour la planification de scans de vulnérabilités, la priorisation selon le score CVSS et le suivi des remédiations de type patch, configuration et GPO.

Compétences techniques

Gouvernance & risques : SMSI ISO 27001, ISO 27005, EBIOS RM, PCA/PRA, procédures de réponse aux incidents, préparation d'audit ISO 27001.

Cyberdéfense : SOC N1/N2/N3, CERT, VOC, traitement d'incidents, MITRE ATT&CK, phishing, malware, impossible travel, massive download, DMARC, DKIM, SPF.

IAM & Microsoft : Keycloak, SSO, fédération d'identités, SoD, MFA, Entra ID, Intune, Microsoft 365 Defender, Microsoft Defender for Endpoint, Purview, Active Directory, GPO.

SIEM & détection : Splunk, Microsoft Sentinel, ELK, SPL, KQL, DSL, règles de corrélation, KPI, tableaux de bord, The Hive, Splunk Phantom / SOAR.

Sécurité infrastructure : PKI OpenSSL, cryptographie RSA, ABE, post-quantum, FortiGate, MikroTik, IDS/IPS, VPN, WAF, NAC, TLS/SSL, DNS, DHCP, Kerberos, LDAP, RDP.

Vulnérabilités & audit : Tenable Nessus, PingCastle, planification des scans, priorisation CVSS, traitement des correctifs et configurations.

Langages & scripting : Python, C, Scala, PowerShell, Bash.

Langues : Anglais B2.

EXPERIENCES PROFESSIONNELLES

BANQUE DE FRANCE, 2025 / 2026

Consultant cybersécurité SOC / CERT

Contexte du projet : Intervention au sein d'un environnement SOC/CERT pour renforcer la détection et le traitement des incidents de sécurité sur des environnements Azure et Microsoft 365.

Missions réalisées :

- Conception et mise en œuvre de scénarios d'attaque simulés sur Azure et Microsoft 365 selon MITRE ATT&CK.
- Définition et mise en œuvre d'une politique de collecte des logs Splunk : identification des sources, sourcetypes et tables pertinentes, intégration des flux, corrélation des événements et mise en production de règles de détection avancées en SPL
- Développement de règles de détection avancées dans Splunk, de l'intégration à la mise en production.
- Rédaction et maintien des procédures de traitement des incidents de sécurité en cohérence avec les processus SOC.
- Conception et suivi de KPI et tableaux de bord pour mesurer l'efficacité des règles et optimiser la couverture de détection.
- Contribution à la maturation du SOC par la capitalisation sur les incidents et les cas d'usage.

Impact : renforcement de la couverture de détection, fiabilisation du traitement des alertes et amélioration du pilotage opérationnel SOC.

Environnement technique : Splunk, Microsoft Sentinel, Entra ID, Intune, Purview, Microsoft Defender for Endpoint, Tenable Nessus, The Hive, MITRE ATT&CK, Azure, Microsoft 365.

BDO FRANCE, 2024 / 2025

Consultant cybersécurité SOC N3 / VOC

Contexte du projet : Mission orientée détection, analyse et traitement des incidents au sein d'un dispositif SOC, avec contribution aux activités de vulnérabilité, audit et résilience.

Missions réalisées :

- Exploitation avancée de Splunk pour la détection d'anomalies, la création de use cases SOC, l'utilisation des commandes SPL search, eval, stats, where, top/rare, et l'automatisation de la réponse avec RBA, MLTK et Splunk Phantom / SOAR
- Traitement des incidents signalés par le SOC et l'EDR : impossible travel, massive download, malware et phishing.
- Contribution aux détections RBA et MLTK et à la réduction du temps de réponse via Splunk Phantom / SOAR.
- Planification des scans de vulnérabilités avec Tenable Nessus et priorisation des traitements selon le score CVSS.
- Participation à la préparation de l'audit AFNOR pour la certification ISO 27001.
- Rédaction des procédures de réponse aux incidents et participation aux tests et améliorations du PCA/PRA.

Impact : amélioration de la détection des anomalies, réduction du risque opérationnel et structuration des pratiques de réponse aux incidents.

Environnement technique : Splunk, GLPI, Active Directory, Entra ID, Intune, Microsoft Defender for Endpoint, Tenable Nessus, PingCastle, Splunk Phantom / SOAR, ISO 27001, PCA/PRA.

NEW BASE TECHNOLOGIES, 2020 / 2023

Consultant cybersécurité SOC N1 / N2

Contexte du projet : Mise en place et exploitation de dispositifs de supervision et de sécurité pour le monitoring réseau, la gestion des incidents, l'administration Microsoft et la sécurisation des échanges.

Missions réalisées :

- Supervision de la mise en place de SIEM ELK et Splunk pour le monitoring des ressources réseau.
- Développement de playbooks Splunk Phantom / SOAR afin d'accélérer la réponse aux incidents.
- Création de tableaux de bord Splunk pour l'analyse et la gestion des incidents de sécurité.
- Mise en œuvre d'alertes intelligentes pour limiter les faux positifs et améliorer le traitement des événements.
- Cartographie des risques cyber, identification des actifs critiques, analyse des menaces et définition des mesures de protection.
- Mise en place d'une PKI avec OpenSSL pour sécuriser les échanges e-mail et garantir confidentialité et intégrité.
- Supervision réseau avec FortiGate et MikroTik : règles de sécurité, IDS/IPS, VPN, RADIUS, filtrage web et journaux.
- Administration Active Directory : utilisateurs, groupes, droits d'accès, GPO et scripts PowerShell.

Impact : fiabilisation de la supervision sécurité, amélioration de la réactivité aux incidents et renforcement de la protection des actifs critiques.

Environnement technique : Splunk, palybook Splunk Phantom, ELK, Filebeat, Metricbeat, Winlogbeat, Packetbeat, MikroTik, FortiGate, OpenSSL, Windows, Linux, Active Directory, PowerShell.