Imad Haijoub

Dossier de compétences

Consultant en Cybersécurité

Technologies de l'information

Synthèse

J'accompagne les entreprises de tous les secteurs à renforcer leur posture de sécurité et à garantir leur conformité réglementaire. Fort de plus de 12 ans d'expérience, j'ai aidé des organisations à maîtriser la cybersécurité ainsi que le support IT pour les outils matériels et logiciels.

Expertises

Analyse et Supervision des Technologies Télécom

- Analyser l'écosystème télécom, incluant **WIFI**, **LTE**, **WAN**, **MPLS, SD-WAN**, **LAN** et **réseau Datacenter**.
- **Surveiller** les performances et les événements à l'aide d'outils de monitoring tels que **Dynatrace**, **Zabbix** et **DinaTrax**.

Intégration des Solutions EDR

- Intégrer les solutions **EDR (Endpoint Detection Response)** dans l'écosystème de supervision pour renforcer la sécurité des terminaux.
- Utiliser des outils comme **Microsoft Defender** et **CrowdStrike** pour surveiller les menaces en temps réel et garantir la sécurité des infrastructures.

Vision d'Observabilité

- Construire une vision d'observabilité en analysant et en agrégeant les données **(logs, métriques, événements)** des différents outils.
- **Intégrer** Dynatrace à la **CMDB ServiceNow** pour centraliser la gestion des ressources.

Analyse des Besoins Utilisateurs

- Recueillir et analyser les besoins des utilisateurs en collaborant avec les équipes de **support et fonctionnelles**.
- Comprendre les attentes pour garantir des solutions de monitoring personnalisées.

Analyse de Sécurité - SOC

- Surveiller en continu les alertes de sécurité et les incidents à l'aide d'outils **SIEM** tels que **Splunk, ELK Stack et Microsoft Sentinel**.
- **Analyser** les menaces potentielles et réagir rapidement pour remédier aux incidents de sécurité.
- Utiliser des outils de détection de menaces comme **Nessus, Snort et Burp Suite** pour identifier et **corriger les vulnérabilités**.

Élaboration de l'Architecture de Supervision

- Concevoir une architecture de supervision robuste en partenariat avec des architectes techniques.
- Participer aux études techniques de **Proof of Concept (PoC)** pour évaluer les solutions de monitoring.

Mise en Œuvre et Suivi des Solutions de Monitoring

- S'impliquer dans **l'implémentation des solutions de monitoring** pour assurer une mise en œuvre efficace.
- Produire des **KPI** pour évaluer la **qualité de service (QoS)**, fournissant des insights stratégiques pour l'optimisation.
- Démontrer une expertise dans l'analyse des performances et l'observabilité sur des infrastructures IT et télécom.

Intégration avec ServiceNow

- Assurer l'intégration des solutions de monitoring avec la **CMDB ServiceNow** pour faciliter la gestion des configurations.

Méthodologies Agiles et Communication

- Travailler dans un environnement agile, idéalement **Scrum**, pour favoriser une collaboration efficace.
- Développer des KPI pertinents pour suivre et améliorer la performance des services.

Outils techniques

Normes et Gouvernances	ISO 27001 EBIOS	RGPD
Forensic	Forensic Toolkit	Encase Forensic
Pentest	Nmap Hydra SQLmap	Metasploit Wireshark Zabbix
Développement sécurisé	OWASP	
SIEM	Splunk Tanium.	Elastic SIEM
Scan De Vulnérabilité	Openvas Qualys	Nessus
Supervision	Zabbix Nagios	DinaTrax Grafana
IDS/IPS/HIDS	Snort	
Linux	Ubuntu CentOS Redhat	Debian KaliLinux ArchLinux
Windows	Windows Server	
Development languages	Python, Bash, PowerShell C/C++, Java, Go Wordpress, Shopify, PHP, SQL	
Développement Web	HTML/CSS	JavaScript

PARCOURS PROFESSIONNEL

De Février 2024 à ce jour Consulting Management World

Projet : Sécurisation SIEM et IAM

Assurer la sécurité continue des systèmes d'information et des accès par le biais d'une maintenance proactive, d'une veille technologique et d'analyses régulières des vulnérabilités pour Univers AP et BeSoft.

Fonction : Responsable de la Gouvernance des Identités et des Accès (IAM) & CTO

- Appréhension de l'Écosystème Télécom
  - Comprendre les technologies **WIFI, LTE, Radio, WAN, LAN et réseau Datacenter**.
- Surveillance et Monitoring
  - Surveiller les performances et événements à l'aide d'outils comme **Dynatrace, Zabbix et DinaTrax**.
  - Construire une vision d'observabilité en analysant et en agrégeant les données (**logs, métriques, événements**).
- Intégration avec la CMDB
  - Intégrer **Dynatrace** à la **CMDB ServiceNow** pour centraliser la gestion des ressources.
- Analyse des Besoins Utilisateurs
  - Recueillir et analyser les besoins en collaborant avec les équipes de **support de niveau 1 et fonctionnelles**.
- Élaboration de l'Architecture de Supervision
  - Concevoir une architecture de supervision robuste en partenariat avec des architectes techniques.
  - Participer aux études techniques de **Proof of Concept (PoC)** pour évaluer les solutions.
- Implémentation des Solutions
  - Garantir une mise en œuvre efficace des **solutions de monitoring**.
- Production et Suivi des KPI
  - Produire des **KPI** pour évaluer la qualité de service, fournissant des insights stratégiques pour l'optimisation.
- Expertise en Analyse et Observabilité
  - Démontrer une expertise en analyse des performances sur **des infrastructures IT et télécom**.
- Gestion des Configurations
  - Assurer l'intégration des solutions de monitoring avec la **CMDB ServiceNow**.
- Collaboration Agile
  - Travailler dans un environnement agile (**Scrum**) pour favoriser la collaboration.
  - Développer des indicateurs de performance pour améliorer l'efficacité des services.

- Gouvernance des Identités et des Accès (IAM)
    - Contribuer aux audits internes, identifier les non-conformités et proposer des actions correctives.
    - Élaborer des documents conformes aux normes **ISO 27001**.
    - Mettre en place un système de traçabilité des habilitations, réduisant le temps de recherche d'informations de **30 %**.
    - Animer des réunions inter-équipes pour clarifier les rôles et améliorer la collaboration.
    - Actualiser régulièrement les documents en lien avec les **résultats des audits**.

- Gestion des Informations et des Événements de Sécurité (SIEM)
    - Utiliser des outils **SIEM** comme **Splunk et Microsoft Sentinel** pour analyser les alertes en temps réel.
    - Créer et tester des plans de réponse aux incidents pour assurer une réactivité optimale.
    - Réaliser des scans avec **Microsoft Defender** et produire des rapports sur l'état de sécurité.
    - **Documenter les incidents** de sécurité et l'efficacité des mesures de protection.

- Responsabilités Techniques
    - Configurer la solution d'Asset et **Vulnerability Management « Tanium »** dans l'environnement IT.
    - Spécifier et intégrer les **Use Cases IT** et Métiers dans **Tanium**.
    - Participer aux **recettes techniques des Use Cases** pour garantir leur efficacité.
    - Renforcer la gestion des postes de travail et des vulnérabilités dans une infrastructure dynamique.
    - Collaborer avec les équipes techniques pour assurer une **intégration fluide**.
    - Former les utilisateurs finaux sur l'utilisation de **Tanium** pour maximiser son adoption.
    - Évaluer les performances de **Tanium** et proposer des améliorations basées sur les retours utilisateurs.
    - **Documenter les processus et configurations** pour assurer la traçabilité et conformité.

- **Environnement Technique :**

IAM (Identity and Access Management), Okta, Microsoft Azure AD, **ISO 27001** (Normes de sécurité), **AWS** (Amazon Web Services), Gestion des Informations et des Événements de Sécurité (SIEM), Microsoft Sentinel, **Splunk**, Elastic Stack (**ELK** (Elasticsearch, Logstash, Kibana), **Nessus**, OpenVAS, **WAF** (Web Application Firewall), IVVQ (Inspection et Validation Visuelle de la Qualité), EBS RM (Expression des Besoins et Identification des Objectifs de Sécurité), OSINT (Open Source Intelligence), DevSecOps, Infrastructure as Code (Ansible, Docker, Kubernetes)

De Mai 2022 à Janvier 2024 Collège supérieur de Montréal

Projet : projet infrastructure et sécurité réseaux collège

Développer une architecture réseau sécurisée et automatiser les processus de sécurité pour protéger les données sensibles du Collège tout en facilitant l'accès aux ressources éducatives.

Fonction : Consultant en cybersécurité et support informatique

- **Gestion et Amélioration des Solutions EDR**
  - **Chef de produit EDR** : Agir en tant qu'expert pour Microsoft Defender pour Endpoint (Intune), déployé sur tous les PC et serveurs de l'organisation. Cela inclut l'évaluation de l'efficacité des détections et des réponses aux menaces.
  - **Optimisation de la couverture de sécurité** : Améliorer la détection des menaces en ajustant les paramètres de sécurité et en intégrant des scénarios de réponse adaptés aux besoins de l'organisation.

- **Déploiement et Configuration de Microsoft Defender**
  - **Déploiement sur appareils mobiles** : Tester et déployer Microsoft Defender pour Endpoint sur des appareils mobiles, garantissant ainsi une protection uniforme sur tous les points d'accès.
  - **Sécurisation du processus de support** : Collaborer avec les équipes de support L1/L2 pour établir des procédures de sécurité lors de l'assistance sur les points de terminaison.

- **Analyse des Alertes et Réponse aux Incidents**
  - **Enquête sur les alertes de sécurité** : Analyser les événements et alertes de sécurité générés par Microsoft Defender, en menant des enquêtes sur des indicateurs de compromission de haute complexité.
  - **Rapports de sécurité :** Élaborer des rapports détaillés sur les incidents de sécurité identifiés par les EDRs, incluant des recommandations pour renforcer la sécurité.

- **Automatisation des Activités de Sécurité**
  - **Scripts d'automatisation** : Développer des scripts pour automatiser en **SentinelOne** afin d'avoir une protection contre les **ransomwares** et avec les réponses aux alertes de sécurité détectées par Microsoft Defender et d'autres solutions **antivirus**, réduisant ainsi le temps de réponse aux incidents.

- **Formation et Sensibilisation**
  - **Formation des équipes opérationnelles** : Assurer la formation des équipes sur l'utilisation et la gestion efficace de Microsoft Defender et des solutions EDR, y compris les meilleures pratiques en matière de détection et de réponse aux menaces.

- **Veille Technologique**
  - **Suivi des évolutions des EDR** : Réaliser une veille technologique sur les nouvelles fonctionnalités et mises à jour des solutions EDR, en proposant des améliorations et en mettant en œuvre les meilleures pratiques pour renforcer la sécurité des systèmes.

- **Environnement Technique :**

Microsoft Defender, EDR, VMware, HyperV, SentinelOne, Snort, Kali et Nessus, Agile, Selenium, VPN, SOC, pare-feu, IAM, Splunk, Linux (Ubuntu, CentOS), Windows Server, OpenSSL Snort , AWS IAM, Azure Active Director, Register, Risk Management Software

De Mai 2021 à Avril 2022 GENIELAB Montréal

génielab.

Projet : Gestion de projet CRM HUBSPOT

Améliorer l'efficacité opérationnelle de Genilab en optimisant l'utilisation de HubSpot pour la gestion des relations clients et l'automatisation du marketing.

Fonction : Consultant support IT et CRM HubSpot

- **Configuration de HubSpot :**
  - Personnaliser les pipelines de vente et les workflows d'automatisation en fonction des besoins spécifiques de Genilab.
  - Configurer les paramètres de suivi des performances des campagnes.
- **Support et Formation :**
  - Organiser des sessions de formation pour les équipes de vente et de marketing sur l'utilisation de HubSpot.
  - Créer des documents de formation et des guides d'utilisation pour faciliter l'adoption de la plateforme.
- **Gestion des Données :**
  - Mettre en œuvre des processus pour nettoyer et enrichir les données clients dans HubSpot.
  - Créer des rapports automatisés pour suivre la qualité des données.
- **Analyse et Reporting :**
  - Analyser les résultats des campagnes marketing et des activités de vente à l'aide des outils d'analyse de HubSpot.
  - Préparer des présentations pour les équipes de direction sur les performances et les opportunités d'amélioration.
- **Optimisation des Processus :**
  - Collaborer avec les équipes pour identifier les goulots d'étranglement dans les processus métiers et proposer des solutions.
  - Mettre en œuvre des améliorations pour maximiser l'efficacité des équipes.
- **Veille Technologique :**
  - Rechercher et tester les nouvelles fonctionnalités de HubSpot et évaluer leur pertinence pour Genilab.
  - Présenter les nouvelles fonctionnalités aux équipes et former les utilisateurs sur leur utilisation.

Environnement Technique :

Jira, WordPress, Hotspot, ASANA, Confluence, HTML, CSS, JavaScript, slack, Power BI

De Juillet 2017 à Nov. 2021 McSport Paris

Projet : Pilotage et management projet

Créer une plateforme de billetterie sécurisée et performante pour les événements, tout en garantissant la conformité aux normes de sécurité et la protection des données.

Fonction : Chef de projet

- **Planification de Projet :**
  - Élaborer un calendrier de projet intégrant les exigences de sécurité et de conformité dès le début.
  - Définir des KPI spécifiques pour évaluer la sécurité de la plateforme et le respect des délais.
- **Sécurisation de la Plateforme :**
  - Collaborer avec les équipes de développement pour intégrer des mécanismes de sécurité (chiffrement, surveillance des accès) dans la plateforme.
  - Mettre en place des tests de sécurité réguliers pour identifier et corriger les vulnérabilités.
- **Gestion des Environnements Cloud :**
  - Superviser la sécurisation des environnements Azure et AWS, en assurant la configuration sécurisée des services et la gestion des accès.
  - Implémenter des solutions de sauvegarde et de récupération pour protéger les données en cas d'incident.
- **Audit et Conformité :**
  - Planifier et réaliser des audits réguliers pour garantir la conformité à la norme ISO 27001.
  - Rédiger des rapports d'audit et élaborer des plans d'action pour corriger les non-conformités.
- **Gestion des Relations avec les Prestataires :**
  - Travailler avec des prestataires de services pour s'assurer que les solutions mises en œuvre respectent les normes de sécurité et les délais.
  - Évaluer la qualité des services fournis par les prestataires en matière de sécurité.
- **Suivi et Reporting :**
  - Surveiller l'avancement du projet et des initiatives de sécurité, en rapportant les résultats à la direction.
  - Préparer des rapports sur l'état de la sécurité de la plateforme et des environnements cloud.
- **Optimisation des Processus :**
  - Analyser les processus de billetterie existants et proposer des améliorations pour optimiser l'efficacité tout en garantissant la sécurité.
  - Intégrer des pratiques agiles pour s'adapter rapidement aux changements et aux exigences de sécurité.

Environnement Technique :

Jira, Cloud Azure, AWS, KPI, JIRA, Confluence, GitHub, Microsoft 365, Agile/Scrum, Waterfall, PRINCE2

De Nov. 2013 à Mars 2017 PSA / ADP / SNCF / crédit Agricole via IBM

Projet : Gestion de projet fonctionnel

Implémenter un SIRH moderne qui répond aux besoins des utilisateurs tout en optimisant les coûts et en améliorant l'efficacité des processus RH.

Fonction : Consultant en mission conduite du changement Digital et SIRH

- **Collecte et analyse des besoins :**
  - Identifier et recueillir les besoins des parties prenantes
  - Analyser les budgets alloués aux projets
  - Rédiger des user stories et spécifications fonctionnelles claires.
  - Prioriser le backlog pour s'assurer que les projets répondent aux attentes sont alignés avec les objectifs stratégiques.

- **Veille technologique :**
  - Mettre en place une veille active sur les tendances technologiques du secteur.
  - Analyser ces opportunités pour renforcer la compétitivité de l'entreprise et assurer que les projets en cours répondent aux enjeux stratégiques identifiés.

- **Gestion et optimisation budgétaire :**
  - Élaborer un budget informatique rigoureux, surveiller les dépenses et optimiser les coûts tout en garantissant l'efficacité des ressources.
  - Assurer la conformité aux normes de qualité, de coût et de délai, tout en adaptant le budget aux besoins changeants des projets.

- **Pilotage de projets et communication :**
  - Prendre en charge la gestion globale des projets en tenant compte de toutes leurs dimensions.
  - Piloter les actions nécessaires à la réussite des projets, animer la communication entre les équipes et les parties prenantes
  - Préparer la conduite du changement pour faciliter l'adaptation et l'acceptation des nouvelles solutions.

- **Production des Livrables :**
  - Produire des documents de projet, y compris des rapports d'avancement et des présentations pour les comités de direction.
  - S'assurer que tous les livrables sont livrés dans les délais impartis et répondent aux attentes des parties prenantes.

-

- **Conduite du Changement :**
  - Développer un plan de communication et de formation pour accompagner les utilisateurs dans la transition vers le nouveau SIRH.
  - Organiser des sessions de formation pour garantir une adoption réussie du système.

Environnement Technique :

Trello, Asana, JIRA, ServiceNow, Confluence, Google Docs, Power BI, Tableau, SAP SuccessFactors, Workday, BambooHR, Windows, macOS, SQL Server, MySQL, Azure, AWS, Agile, ADKAR, Lean Six Sigma

SCOLARITÉ

2024 : **Diplôme Réseautique et Cybersécurité** | Collège Universitaire d'Ahuntsic Montréal

2023 : **Bachelor Support informatique**| École Leonardo da Vinci Montréal

2013 : **Master en management** | École de commerce EIMP Paris

FORMATIONS ET CERTIFICATIONS

- Certificat Software Tester -2024
- LambdaTest Certification -2024
- Certificat CCNA Réseau Cisco -2023
- PMP & IT Support by Google -2023
- Certificat HubSpot SEO Sales -2023
- Certificat Agile Scrum Master - Scrum institute de Suisse – 2020
- Analyste SOC Certifié (CSA) – ISSMI - 2019
- Formation en Professionnel Certifié en Sécurité des Systèmes d'Information (CISSP) – ISSMI
- Formation en Sécurité Certifiée AWS - ISSMI
- Formation en Microsoft Certifié : Ingénieur en Sécurité Azure Associé - ISSMI
- Formation en Ingénieur en Sécurité Cloud Professionnel Google - ISSMI
- Formation en CEH (Hacker Éthique Certifié) - ISSMI
- Formation en Certificat CompTIA Security+ - ISSMI
- Formation en Certificat ISO/IEC 27001 Lead Implementer - ISSMI
- Formation en ISTQB Certifié Niveau Fondamental - ISSMI