Julien BIERME

Ingénieur Systèmes et Réseaux • *4 années d'expérience*

Ingénieur Système et Réseaux de formation (BUT Réseaux et Télécommunications spécialité Cybersécurité), j'évolue sur des environnements de production critiques (secteur bancaire, industrie). Mon profil est hybride : je combine une vision bas niveau des systèmes et réseaux avec une forte rigueur issue de mes missions en cybersécurité (SecOps, conformité, gestion des incidents). Je suis convaincu qu'une infrastructure fiable passe par une industrialisation poussée.
Ayant une forte appétence pour la continuité de service, je cible aujourd'hui des missions d'ingénierie système (Linux/Windows) axées sur la fiabilisation des infrastructures, la virtualisation et la mise en place d'architectures sécurisés.

contrôles de sécurité

cybersécurité

gestion de la gouvernance, des risques et de la conformité

Microsoft Active Directory

sécurité réseau

scripting

Compétences

TECHNIQUES : cybersécurité, sécurité réseau, scripting, commutation de paquets, conception de systèmes, configuration, configuration pare-feu, informatique, phishing, programmation, protocole réseau, scripts UNIX, switch, sécurité informatique, équipements réseau, administration d'infrastructures, administration de système, algorithmique, analyse de vulnérabilité, audit de sécurité informatique, automatisation, autorisation utilisateur, CERT, Cisco, cryptographie, détection d'intrusion, flux de trafic, gestion de la sauvegarde du système, gestion des accès privilégiés, gestion des identités et des accès, gestion des vulnérabilités, infrastructure informatique, ingénierie des systèmes, Linux HA, network DLP, opérations de sécurité, performance informatique, planification et conception de réseaux, protocoles de routage, routage, sauvegarde de données, serveur Microsoft Windows, support informatique, surveillance d'infrastructures, surveillance de réseaux, surveillance de systèmes, systèmes d'information, systèmes de communication, sécurité de l'information, sécurité des applications, sécurité des données, télécommunications, virtualisation, audit informatique, base de données, point d'accès sans fil, security operations center, tests d'intrusion

FONCTIONNELLES : contrôles de sécurité, gestion de la gouvernance, des risques et de la conformité, analyse des flux, analyse des incidents, application des procédures, formation des utilisateurs, gestion des incidents, poste de travail, suivi des incidents, support utilisateur, sécurité, travail en équipe, veille technologique, vulnérabilité, amélioration de la performance, analyse des menaces, analyse des risques, audit, collaboration inter-organisationnelle, efficacité opérationnelle, gestion de projet, gestion des escalades, gestion du temps, industrie, mathématiques, méthodes d'analyse, politique de groupe, politique de sécurité, procédures internes, résolution de problème, science et recherche, traitement des déchets, communication interne, formation du personnel, gestion des risques

TRANSVERSES : documentation, documentation technique, pensée abstraite, synthèse

COMPORTEMENTALES : adaptabilité, autonomie, pensée logique, rigueur

LOGICIELS MÉTIER : Microsoft Active Directory

MÉTHODES : méthodologies agiles, ITIL Service desk

OUTILS : Bash, pare-feu, Proxmox Virtual Environment, Algosec, GitLab, Kali Linux, KVM, LibreOffice, Microsoft PowerShell, script batch, Dynatrace, IBM Security Identity Manager, ServiceNow OTM

LANGAGES DE DÉVELOPPEMENT : HTML, Java, JavaScript, Microsoft Visual Basic, PHP

BASES DE DONNÉES : Progress

SYSTÈMES D'EXPLOITATION : Linux, PfSense, Ubuntu, Debian, SUSE

PLATEFORMES : SentinelOne Singularity

PROTOCOLES : Preboot Execution Environment

LANGUES : Français (Langue Maternelle), Anglais (Intermédiaire), Allemand (Débutant)

Certifications

Cisco CCNA • CISCO Networking Academy • 04/2024

Linguaskill • Cambridge Assessment • 06/2022

Compétences pratiquées : Anglais

Formations

Institut universitaire de technologie du Nord-Franche-Comté, France • BUT Réseaux et Télécommunications - Parcours Cybersécurité • 09/2023 • 06/2025

Compétences pratiquées : administration de système, serveur Microsoft Windows, Linux, configuration, sécurité réseau, sécurité des données, autorisation utilisateur, surveillance de réseaux, surveillance de systèmes, surveillance d'infrastructures, scripting, protocoles de routage, protocole réseau, routage, switch, point d'accès sans fil, audit de sécurité informatique, virtualisation, pare-feu, politique de groupe, gestion des identités et des accès, base de données, gestion des incidents, détection d'intrusion, analyse de vulnérabilité, tests d'intrusion

Université de technologie de Belfort-Montbéliard • Cycle Préparatoire Ingénieur • 09/2020 • 06/2023

Compétences pratiquées : informatique, mathématiques, résolution de problème, synthèse, méthodes d'analyse, gestion de projet, Anglais, algorithmique, programmation, pensée logique

Lycée Jean Michel • **Baccalauréat Scientifique spécialité Mathématique** 06/2020

Compétences pratiquées : science et recherche, mathématiques

Synthèse des missions

CAPFM • **Référent Sécurité** • 10/2025 à 06/2026 (9 mois)

Détail des missions

CAPFM • **Référent Sécurité** • 10/2025 à 06/2026 (9 mois) • Roubaix

Crédit agricole Personal Finance & Mobility est une entité du groupe Crédit Agricole S.A. opérant dans 17 pays européens ainsi qu'en Chine et au Maroc dans différents secteurs tels que les réseaux bancaires, l'automobile ou la distribution spécialisée.
Le pôle Sécurité du SI dont la mission est intégrée, est en charge de définir, faire appliquer et contrôler la politique de sécurité de l'entreprise. Son rôle est d'anticiper les risques, de sécuriser les environnements de production et de coordonner les actions de remédiation avec les équipes d'exploitation (CAGIP) en cas de crise.
Intégré au sein du pôle Sécurité du SI de l'entité France de CAPFM, le Centre de Compétences opère selon un modèle d'Assistance Technique Globale (ATG).
L'équipe assure la coordination critique entre les équipes d'infrastructure (CAGIP), les cellules de cyberdéfense (SOC, CERT, SOC Métier) et la direction de la sécurité avec pôle Sécurité du SI de l'entité France, mais également en lien avec l'entité CORP.
La mission repose sur trois périmètres :
La Sécurité Réseau (VSE) : L'équipe a pour rôle de contrôler et valider toutes les évolutions d'architecture réseaux, les whitelistings et les ouvertures de flux.
Le périmètre des Opérations de Sécurité (SecOps) : L'équipe centralise la gestion opérationnelle de niveau 1 et 2 des incidents et alertes cyber.
Le périmètre Gouvernance et Délégation CISO : le centre instruit l'ensemble des demandes d'accès à privilèges et des dérogations de sécurité.

Au sein du Centre de Compétences, mon activité s'articule autour de deux axes : la gestion opérationnelle quotidienne (Run) et l'industrialisation de nos processus (Build).
Au quotidien, j'assure le traitement technique des demandes et des incidents sur trois périmètres distincts :
Coté sécurité Réseau (VSE), l'objectif et l'audit et validation technique des demandes d'ouvertures de flux. Je contrôle la cohérence des schémas réseaux, vérifie l'absence de protocoles vulnérables et valide la conformité avec les analyses de risques préalables (Covalar) avant d'autoriser l'implémentation par les équipes d'infrastructure.
Coté SecOps, l'objectif est le traitement des alertes de sécurité remontées par le SOC, le CERT ou via les outils d'observabilité (Dynatrace). J'effectue l'analyse technique des incidents/alertes, puis je coordonne les investigations et l'escalade vers les équipes d'exploitation (CAGIP) et les entités métiers en cas de besoin.
Coté gouvernance et Identités, j'instruits les dérogations de sécurité et gestion des accès à privilèges, comptes techniques et whitelisting (proxy, tenant de restrictions M365, domaine mail...). J'effectue les investigations techniques nécessaires pour monter les dossiers d'arbitrage, propose des alternatives en fonctions des possibilités offertes par la PSSI, et en assure la revue entre la réalité et les dérogations.

En parallèle du Run, j'ai piloté et réalisé plusieurs projets visant à automatiser nos actions manuelles, fiabiliser nos données et réduire notre dette technique :
J'ai mis en place plusieurs scripts PowerShell pour automatiser le contrôle des dérogations CISO, en croisant massivement toutes les extractions brutes du SI avec nos bases d'accords existants et les données utilisateurs.
J'ai créé un script d'analyse ciblant les noms de domaine liés à des services d'IA en backend, afin d'identifier les URL non bloqués par le proxy et de forcer leur mise en liste noire (blacklistage) après validation de nos résultats par le CISO et le responsable IA.
J'ai également proposé et mis en exécution d'un plan d'assainissement technique ciblant les règles de whitelisting USB sur l'EDR ainsi que la gestion des comptes génériques.
Coté intégration ServiceNow / Conformité PSSI j'ai mis en place un outil en PowerShell permettant de formater les données brutes des logiciels non-conformes détectés sur le parc et de générer en suivant les cas d'usages, les tickets de remédiation dans ServiceNow.

Compétences pratiquées : gestion de la gouvernance, des risques et de la conformité, cybersécurité, sécurité réseau, suivi des incidents, opérations de sécurité, IBM Security Identity Manager, gestion des accès privilégiés, gestion des escalades, analyse des incidents, ITIL Service desk, analyse des flux, analyse de vulnérabilité, procédures internes, documentation, ServiceNow OTM, Microsoft Active Directory, Microsoft PowerShell, Algosec, Dynatrace, sécurité de l'information, network DLP, rigueur, adaptabilité, autonomie, travail en équipe, protocole réseau

Synthèse des postes

Consort Group • **Ingénieur Systèmes et Réseaux** • depuis 10/2025 (10 mois)

Space Informatique • **Apprenti Systèmes et Méthodes - Cybersécurité** • 09/2023 à 08/2025 (2 ans)

ESDI • **Technicien Informatique** • 06/2023 à 07/2023 (2 mois)

Chimirec • **Manutentionnaire saisonnier** • 07/2022 à 08/2022 (2 mois)

Détail des postes

Consort Group • **Ingénieur Systèmes et Réseaux** • depuis 10/2025 (10 mois) • Lille

En tant qu'Ingénieur Système et Réseaux, mon rôle est d'assurer la conception, le déploiement et la maintenance des infrastructures de l'entreprise. L'objectif est de garantir leur performance, leur disponibilité et leur sécurité globale, tout en participant activement aux projets d'évolution.
Mon activité s'articule autour de plusieurs axes :
Coté exploitation (Run), l'objectif est d'assurer la maintenance préventive et corrective des systèmes et réseaux. Je gère la prise en charge et la résolution des incidents au quotidien. Je surveille en permanence les performances des infrastructures dans le but de les optimiser, tout en collaborant régulièrement avec les équipes applicatives et télécoms.
Coté projets (Build), l'objectif est d'accompagner l'évolution du SI. Je participe à la conception et au déploiement technique des nouvelles architectures systèmes et réseaux pour répondre aux besoins de l'entreprise.
Coté sécurité et conformité, l'objectif est de protéger les réseaux. Je mets en place les mesures de sécurité techniques nécessaires et je participe aux différents audits de sécurité et de conformité sur le parc.

Coté documentaire, l'objectif est d'assurer le suivi et la traçabilité. Je documente l'ensemble des configurations mises en place ainsi que les interventions techniques réalisées.

Compétences pratiquées : sécurité informatique, gestion des incidents, documentation technique, surveillance d'infrastructures, audit informatique, collaboration inter-organisationnelle, planification et conception de réseaux, amélioration de la performance, performance informatique, administration d'infrastructures, conception de systèmes

Space Informatique • **Apprenti Systèmes et Méthodes - Cybersécurité** • 09/2023 à 08/2025 (2 ans) • Belfort

SPACE Informatique est une moyenne entreprise (50 salariés) spécialisée dans l'édition de logiciels et la gestion infrastructure associée. Elle développe notamment Aladin, un utilitaire global de back-office (gestion des stocks, commandes, statistiques) destiné à trois centrales d'achat Leclerc, et à leurs magasins, ainsi que la gestion de l'infrastructure serveurs pour cette application dans les 138 magasins.
Dans cet écosystème, j'ai intégré le département Système et Méthodes. Le service fournit l'infrastructure nécessaire aux environnements de développement, intervient en escalade sur les incidents complexes remontés par la hotline (N3), et a pour mission la stabilité, la sécurité et les méthodes sur l'ensemble du parc matériel et serveur.
Dans ce cadre, et avec une priorité sur la tension entre modernisation des infrastructures (sécurité, durcissement) et continuité de service, j'ai mené mes missions de refonte et d'administration des systèmes Linux/Windows, réseaux et de sécurité infra/utilisateurs.
L'un de mes chantiers majeurs a été la refonte complète du cœur de réseau de l'entreprise avec la modernisation du système de pare-feu Netgate avec de la HA, des liens VPN, IPsec, de l'autorité de certification, de la gestion des logs, du failover multi-WAN, la mise en place d'un proxy automatique...
L'exécution de cette migration a fait l'objet d'une feuille de route détaillée de 43 étapes avec un proof of concept complet en 3 phases. Cette planification intégrait les créneaux d'intervention en heures non ouvrées, les procédures de sauvegarde systématiques, les tests de validation à chaque palier, ainsi que les procédures de rollback.
Au-delà du réseau, j'ai administré en profondeur l'environnement hétérogène mélangeant systèmes Linux (OpenSUSE) et Windows Server :
Côté administration Linux, au-delà de la gestion des incidents (supervision, bases de données...), j'ai architecturé et déployé une solution de double authentification (MFA) complète et auto-hébergée pour sécuriser les accès VPN.
J'ai mis en place une solution (Bash) de restauration de sauvegarde planifiée des sauvegardes sur bandes magnétiques, afin d'en assurer la fiabilité sur les serveurs.
J'ai également scripté (Bash) un système de vigie automatisé qui télécharge, filtre intelligemment et envoie un rapport par mail à partir de flux RSS de sécurité pour anticiper les vulnérabilités et avoir un panorama des actualités en fonction des systèmes utilisés.
J'ai de plus participé à une évaluation de la prochaine génération du parc serveur, en évaluant le passage de la gestion des VM de KVM vers Proxmox et de la solution de stockage DRBD vers Ceph ou NAS centralisé avec l'architecte.
Côté administration Windows, à la suite d'audits de sécurité que j'ai menés (via Purple Knight, PingCastle et échange avec Orange Cyberdéfense), j'ai piloté le durcissement de l'Active Directory avec un plan distribué en fonction des risques cyber, des risques de continuité de service et des procédures de mise en place.
À la suite de contraintes qui bloquaient les anciens processus de création de sauvegardes de postes de travail, j'ai développé une solution complète d'automatisation des sauvegardes via des scripts (Batch) exécutés par tâches planifiées sous un compte de service avec un système de supervision centralisé (Bash).
Enfin, la pérennisation des architectures est passée par la formalisation des processus via des « fiches réflexes » techniques destinées au service Système et Méthodes. Ces procédures détaillent l'investigation, le diagnostic et la résolution pour chaque type d'incident de sécurité, en intégrant les

mesures de sécurisation immédiates, les outils d'analyse à mobiliser et les éléments de traçabilité post-incident.

Compétences pratiquées : Microsoft Active Directory, Linux, infrastructure informatique, SUSE, PfSense, efficacité opérationnelle, configuration pare-feu, formation des utilisateurs, veille technologique, audit, sécurité, SentinelOne Singularity, commutation de paquets, phishing, Progress, scripting, script batch, scripts UNIX, rigueur, travail en équipe, résolution de problème, autonomie, adaptabilité, gestion du temps, serveur Microsoft Windows, administration d'infrastructures, protocole réseau, virtualisation, KVM, équipements réseau, Proxmox Virtual Environment, automatisation, sécurité réseau, sécurité des applications, gestion de la sauvegarde du système, sauvegarde de données, gestion des vulnérabilités, vulnérabilité, analyse des menaces, communication interne, formation du personnel, Linux HA, méthodologies agiles

ESDI • **Technicien Informatique** • 06/2023 à 07/2023 (2 mois) • Belfort

Installation et intégration de nouveaux postes de travail dans une usine cliente, avec configuration via un serveur PXE. Mise en place et déploiement des équipements, assurant leur bon fonctionnement et intégration dans l'environnement réseau existant.

Compétences pratiquées : support informatique, Preboot Execution Environment, poste de travail

Chimirec • **Manutentionnaire saisonnier** • 07/2022 à 08/2022 (2 mois) • Montmorot

Participation aux opérations en équipe de traitement de déchets industriels, comprenant la surveillance et l'entretien des équipements, le respect des procédures de sécurité, dans le cadre d'une conformité environnementale.

Compétences pratiquées : traitement des déchets, industrie, application des procédures, travail en équipe