OUAIL ALAMI

Ingénieur sécurité réseau

Firewall · Réseaux · Systèmes · Infrastructure as Code

ouailalami98@gmail.com · +41 78 860 98 55 · Cheseaux-sur-Lausanne, Suisse
ouail.com · linkedin.com/in/ouail-alami · github.com/spikelee000
Permis C · Mobilité Genève – Lausanne

EXPÉRIENCE PROFESSIONNELLE

PICTET GROUP

Ingénieur sécurité — 10.2025 · en poste · Genève

- Administration d'un parc d'une centaine d'équipements de sécurité, firewalls FortiGate et Check Point, VMware NSX et proxy, répartis sur les sites du groupe à l'international.
- Traitement de plus d'une centaine de règles de filtrage par semaine, majoritairement générées depuis les dépôts firewall as code en Terraform ; retrait de plusieurs dizaines de règles obsolètes sur la même période, et nettoyage complet du jeu de règles à la suite d'une migration d'infrastructure.
- Micro-segmentation sur NSX Distributed Firewall : cloisonnement des flux est-ouest dans une logique de moindre privilège et de Zero Trust.
- Proxy Broadcom ProxySG : plus d'une dizaine de demandes traitées par jour, politiques d'accès, filtrage d'URL et inspection SSL.
- Diagnostic réseau sur TCP/IP, DNS et routage par captures Wireshark ; investigation des incidents jusqu'à l'analyse de cause racine.
- Développement des scripts d'automatisation du firewall as code en Python et Terraform ; revue de code sur Git et Bitbucket, déploiements par pipelines Bamboo, avec plan de retour arrière systématique.
- Pilotage d'un projet de sécurité de bout en bout, et contribution à trois projets majeurs du périmètre.

ATOS

Ingénieur réseau et systèmes — 01.2022 · 09.2025 · Vevey

- Exploité les infrastructures réseau et systèmes de 26 sites clients majeurs et de plusieurs sites secondaires, sur Cisco, Check Point, Fortinet et Palo Alto : VPN IPsec, OSPF, VLANs, QoS, DHCP, DNS, NAT, load balancing, SNMP, ACLs et IDS/IPS.
- Conduit une migration d'infrastructure de la conception à la bascule en production.
- Déployé une infrastructure complète pour 5 clients : Active Directory, serveurs de stockage et serveurs de supervision.
- Mené la mise en place de la supervision et de l'alerting, avec la pile adaptée à chaque contexte client : Grafana, PRTG, Nagios ou Zabbix.
- Conçu et déployé des solutions sur mesure par client, dont l'intégration de systèmes de radiocommunication critiques aux systèmes d'information.
- Administré les environnements Windows et Active Directory, Red Hat et SUSE, la virtualisation VMware et Hyper-V, et Azure.
- Assuré la sauvegarde et la restauration des infrastructures et des machines virtuelles : politiques, supervision des travaux et vérification des restaurations.
- Industrialisé les déploiements avec Ansible et Puppet, automatisé l'exploitation en PowerShell et Python, et piloté les projets sous Jira et KIX en Agile et Kanban.
- Développé des outils et applications internes en Java, JavaScript, Python, PHP, C# et Angular, avec intégration d'API REST ; bases de données PostgreSQL, MariaDB, Oracle et MySQL.
- Assuré la récupération de données et les activités de forensique par file carving, et exploité l'infrastructure de visioconférence Polycom.

ALLIANCE FRANÇAISE DE GENÈVE

Référent informatique — 03.2020 · 01.2022 · Genève · temps partiel

- Interlocuteur informatique unique : parc Windows, LAN, Wi-Fi, DHCP et firewall ; diagnostic des pannes et optimisation des postes.
- Formation des équipes aux nouveaux outils et rédaction des manuels.

COMPÉTENCES TECHNIQUES

SÉCURITÉ RÉSEAU · CŒUR DE MÉTIER
FortiGate · Fortinet · Check Point · Palo Alto · VMware NSX / DFW · Broadcom ProxySG · Firewalls · IDS / IPS · VPN IPsec · Inspection SSL · Micro-segmentation · Zero Trust · ACLs · System Hardening

RÉSEAU
Cisco · Routing & Switching · TCP/IP · OSPF · VLANs · NAT · DNS · DHCP · QoS · WiFi · Load Balancing · SNMP · VPN · Wireshark

SÉCURITÉ OPÉRATIONNELLE
SOC · SIEM · Réponse à incident · Threat Hunting · Analyse de logs · Gestion des vulnérabilités · Analyse de CVE · MITRE ATT&CK · IAM · Forensics réseau · File Carving · Tests d'intrusion · Burp Suite · Kali Linux

SYSTÈMES, CLOUD & SUPERVISION
Windows · Active Directory · GPOs · Red Hat · Linux · SUSE · VMware · Hyper-V · ESXi · Azure · Sauvegarde et restauration · Apache · Nginx · Grafana · PRTG · Nagios · Zabbix

AUTOMATISATION & DEVOPS
Python · Terraform · Ansible · Puppet · PowerShell · Bash · Infrastructure as Code · Firewall as Code · Git · GitHub · GitLab · Bitbucket · CI/CD Bamboo · Docker · Kubernetes

DÉVELOPPEMENT & DONNÉES
Java · JavaScript · C# · PHP · Angular · ReactJS · REST APIs · SQL · PostgreSQL · MariaDB · Oracle · MySQL

GESTION DE PROJET & BUREAUTIQUE
Jira · KIX · Agile / Scrum · Kanban · Documentation technique · Microsoft 365 · Word · Excel · PowerPoint · Outlook · Visio · Teams · SharePoint

FORMATION

Bachelor en informatique de gestion
HEG · HES-SO, Genève
2018 · 2021

Projet : assistant conversationnel (RASA)
Université de Genève · traitement du langage naturel
2020 · 2021

Maturité professionnelle commerciale et CFC
ECG Aimée-Stitelmann, Genève
2014 · 2018

FORMATIONS SUIVIES

Attestation de cours CCNA
Implementing and Administering Cisco Networking Solutions · Digicomp · 2023

Formation TETRAPOL GPM9
Airbus · 2023

LANGUES

Français, langue maternelle · Arabe, langue maternelle · Anglais C1 · Italien B2

LABORATOIRE PERSONNEL

Pratiqué hors cadre professionnel, sur infrastructure de test.

- Infrastructure de test sous Proxmox : domaine Active Directory, GPOs et réseau segmenté derrière pfSense.
- SIEM Splunk : télémétrie Sysmon, collecte des journaux Windows et réseau, recherches SPL, tableaux de bord et alertes.
- Écriture de règles de détection Sigma cartographiées MITRE ATT&CK, validées en rejouant des scénarios d'attaque sur le domaine de test.
- Sécurité offensive sous Kali Linux : Nmap, Metasploit, Burp Suite, sqlmap, Hydra, John the Ripper, Hashcat, Nikto, Responder, BloodHound et Wireshark.