Gérard BIGOT
Tél : + 33 6 50 41 52 55
Email : gerard.bigot@gmail.com
Chevilly-Larue (94) – Île-de-France, mobile et ouvert à relocalisation

MAJ : 28/07/2026

PROFIL

RSSI / Responsable de la sécurité des SI – ETI et PME

30 ans de systèmes d'information dont 15 en cybersécurité. Conception, déploiement et pilotage de SOC à trois reprises. Mise en conformité ISO 27001, analyses de risques EBIOS RM, définition de PCA/PRA. Expérience spécifique des structures sans équipe sécurité dédiée : cinq ans à concevoir et opérer un SOC mutualisé pour des PME industrielles, médicales, transport et distribution.

Interventions en temps partagé, en transition ou en création de dispositif.

DOMAINES DE COMPÉTENCES

Direction de la sécurité	● Définition et pilotage de la stratégie sécurité – PSSI, SMSI ● Comitologie, reporting de direction, tableaux de bord, budget ● Management d'équipes et pilotage de prestataires (MSSP, SLA) ● Sensibilisation et acculturation des métiers
Conformité et gestion des risques	● ISO 27001, 27002, 27005, 27035 – ISO 22301 – ITIL ● Analyses de risques EBIOS RM ● PCA/PRA – gestion et communication de crise ● Cartographie applicative, fonctionnelle, de processus et de flux
Détection et réponse	● Conception, déploiement et pilotage de SOC – trois réalisations ● SIEM, EDR/XDR/MDR, SOAR – collecte et normalisation des logs ● Supervision, gestion des incidents et des vulnérabilités
Sécurisation des projets et des infrastructures	● Architecture de sécurité périphérique et en profondeur ● DevSecOps – CI/CD, IaC, AppSec ● Sécurité logicielle et matérielle sur tout le cycle de vie ● Pilotage d'équipes externes de pentesting – boîtes noires, grises, blanches
Environnements techniques	Linux (Red Hat/CentOS, Debian/Ubuntu), Windows Server – Virtualisation : KVM, VMware, Xen, Hyper-V – Cloud : AWS, Azure – Kubernetes – Firewall : Cisco, Juniper, Linux – SIEM : Grafana, Kibana, Wazuh, Suricata – IAM : Keycloak, LemonLDAP::NG, Active Directory – WAF, MFA, DLP, PAM – Oracle, PostgreSQL, MySQL, MongoDB, InfluxDB
IA	Gouvernance et sécurisation des usages en entreprise – Agents et orchestration (MCP) – Modèles hébergés et locaux – Application à l'analyse et à l'enrichissement de logs

FORMATION

Maîtrise d'informatique – IUP Informatique, Université de Lille I (1993)

Programme Erasmus – Landau, Allemagne (1992)

LANGUES

- **Anglais :** Bilingue (C1+)
- **Allemand :** Courant

EXPÉRIENCES PROFESSIONNELLES

Consultant indépendant en cybersécurité

- Mai 2025 à Maintenant

Contexte : En tant qu'indépendant, je donne des formations pour adultes autour des thèmes de la cybersécurité. Je peux aussi être amené à réaliser des prestations ponctuelles de conseil sur des points précis.

Missions :

- Le groupement de formation pour adultes M2i de SKOLAE Formation me propose régulièrement de donner des formations comme :

  - SEC–RSSI - RSSI (Responsable de la Sécurité des SI) - Rôles et attentes organisationnelles
  - SEC-IAM - Gestion des identités et sécurité des accès
  - URB-SI - Urbanismes du SI et architectures des systèmes
  - SEC-LEC - Durcissement sécurité Linux
  - et d'autres

SOC Manager - Comutitres

- Septembre 2024 à Avril 2025

Contexte : Société gérant les titres de transport de l'île de France.

Forte contrainte réglementaire dans une société en cours de changement du mode de gestion de son SI.

Missions :

- Gestion d'une équipe de trois personnes
- Pilotage de l'activité opérationnelle du SOC. Relation avec les prestataires
- Amélioration et professionnalisation du reporting interne et externe
- Sensibilisation au Secure By Design du CI/CD de l'équipe DevOps
- Intégration de la cybersécurité dans le processus de l'entreprise

Environnement Technique et Fonctionnel :

Bureautique : Windows365 - EDR : Tehtris EPP/XDR, CrowdStrike - ITIL : Stack Atlassian - MBM : Lookout - Transfert de fichiers : Bluefiles

SOC : Bastion Wallix - XSOAR Palo Alto Network - SIEM : Sekoia/Google Devops/Datadog - Supervision : Qualys - Firewall : Forcepoint VPN + Proxy, Fortinet NGFW, Inwebo TrustBuilder Authenticator MFA

Prod : Cloud : AWS : EKS, WAF - Virtualisation : VMware ESXi

DSI / Expert SSI - EGERSEC

- Septembre 2019 à août 2024

Contexte : Co-création de la société EGERSEC dans le but de créer un SOC partagé à destination des TPE et PME.

Types de clients qui ont adopté la solution : Industrie, Médical, Transport, Distribution …

Missions :

- Pilotage de l'activité opérationnelle de la société
- Mise en place du SI de la société respectant la PSSI dans le cadre de ISO27001, et ITIL
- Création et management d'un SOC partagé. Utilisation de Wazuh
- Gestion des logs. Syslog pour linux et SysMon pour windows. Centralisation, et intégration dans le SIEM après parsing IA
- Audit et conseil
- Formateur cybersécurité (DevSecOps, AAA, CTI, SOC et gestion de crise), parfois en environnement sensible
- Rédaction et implémentation de la PSSI
- Amélioration continue du SI et de son système de management en vue de certification ISO27001
- Définitions de PCA/PRA en utilisant la méthodologie EBIOS RM dans le cadre des analyses de risques . Entre autres, pour la BSPP

Environnement Technique et Fonctionnel : Serveurs physiques loués en Datacenter • VM dans un cloud souverain • Utilisation IA • Serveurs sur site (Dell, Centos et Debian)…

CHEF DE PROJET SECURITE I DIGIPLUG (Filiale ACCENTURE)

- Septembre 2011 à juin 2019

Contexte : Société distribuant les MP3 d'Universal Music Group au niveau mondial.

Forte contrainte concernant le SI et sa sécurisation au regard des risques liés au piratage de ces données

Missions :

- Mise en place et respect des procédures ITIL
- Mise en place d'un SI respectant ISO27001
- Création d'un SOC avec Grafana. Utilisation de Logstash et Graylog pour formater les logs
- DevOps : Déploiement d'un environnement de dev en CI/CD
- Remontée des données et implémentation des demandes Accenture

Environnement Technique : ITIL : Atlassian, GLPI - Systèmes d'exploitation : Linux Red Hat/CentOS, Debian/Ubuntu, Windows Server - Hyperviseur : VMware ESXi Vcenter - IaC : Ansible, Terraform – Stockage : Isilon, XtremIO – Cloud : AWS, GRC - BdD : Oracle, PostgreSQL, MySQL et NoSQL – IAM : Microsoft AD…

INCIDENT MANAGER - CGG VÉRITAS

- Mai 2010 à Août 2011

Missions :

- Analyse des différents cas de mise en place du système d'information embarqué sur les bateaux
- Analyse des différents cas de construction des clusters NVidia embarqués utilisés pour prémâcher les datas recueillies
- Documentation des opérations standards de MCO et MCS du SI

Environnement Technique : Réseaux Windows, Linux Redhat, MySQL …

Responsable Réseaux - ESERVGLOBAL (Ex FERMA SA)

- De 1998 à 2010

Missions :

- Gestion de crises avec des clients Telco
- Création de VPN avec les clients Telco sur tous les continents pour accéder simplement aux serveurs de la société
- Déploiement de firewall et de VPN entre les 16 sites de la société
- Implémentation d'un datacenter interne pour sécuriser les serveurs de dev
- Management de 14 personnes

Environnement Technique : UNIX, Windows, Firewall, base de données …

Divers Postes

- De 1993 à 1998

Postes :

- Développeur C, bash et python – Responsable réseaux – Chef de projet à l'international