THIERRY MATRAT
contact@sqltemp.com | Linkedin | sqltemp.github.io/portfolio

CONSEILLER EN CYBERSÉCURITÉ

Support technique | Analyse & résolution d'incidents | Gestion d'Identités et d'Accès

Professionnel orienté résultats, expérience dans l'implémentation et la gestion de systèmes informatiques sensibles. Capacité à identifier, résoudre et prévenir des problématiques complexes, en vue d'assurer la confidentialité, l'intégrité et la disponibilité des systèmes TI. Mise en place de standards et procédures adaptés aux enjeux de sécurité des clients. Formations de sensibilisation des usagers. **Champs d'expertise**:

☒Diagnostic et résolution d'incidents	☒Analyses d'incidents post-mortem	☒Gestion des opérations
☒Sessions sensibilisation des usagers	☒Renforcement posture défensive	☒Audits de sécurité

COMPÉTENCES TECHNOLOGIQUES

SIEM & IPS: Splunk, MS Sentinel, Wazuh, Snort
Pénétration & Scanner Vulnérabilités: Metasploit, BurpSuite, mimikatz, Nessus
Réseaux (Logiciels et protocoles): Wireshark, TCP/IP, protocoles OT (Modbus, DNP3, OPC)
Languages & Scripting: C#, C++, Python, T-SQL, Powershell, Bash, Java Script
Systèmes d'Exploitation : Windows, MacOS, iOS, Linux, Android
EDR : Bitdefender, Microsoft Defender for Endpoint
Autres outils: Active Directory, Office365, MSSQLServer, OCS Inventory
Normes et Standards : NIST CSF2.0, OSSTMM, ISO27001, IEC 62443

EXPÉRIENCES FONCTIONNELLES

- Tests de pénétration d'environnements vulnérables (Metasploitable, OWASP)
- Threat Intelligence : MITRE ATT&CK (Att&ck Navigator)
- CTF : HackTheBox, TryHackMe, Montrehack, Hackropole, picoCTF
- Bénévolat: animation village soudure au NorthSec 2025

EXPÉRIENCE PROFESSIONNELLE

vCISO

Recommandations et accompagnement de PME dans le développement et le maintien de leurs programmes cyber défensifs (identification sur demande) – 07/2023 – en cours

- Inventaire des mesures de sécurité en place, analyse d'écarts et recommandations
- Configuration & sécurisation d'environnements virtuels (VMWare Workstation, Oracle VBox)
- Installation et exploitation outils surveillance réseau : IPS (Snort), SIEM (Splunk), Wireshark
- Installation, configuration et exploitation d'outils de protection (EDR)
- Segmentation réseau & Inventaire d'équipements (OCS Inventory, Powershell)
- Scans de vulnérabilités (Nessus, Wazuh) et mise en œuvre d'activités de remédiation.
- Tests de robustesse de l'infrastucture (basés sur les méthodologies OSSTMM & NIST CSF)
- Production de tableaux de bord assurant le suivi des actions et leur documentation
- Animation de sessions de sensibilisation des employés aux techniques d'hameçonnage et d'ingénierie sociale les plus courantes.

Analyste Gestion d'Identités et d'Accès (CDPQ) – 11/2017 – 01/2022

- Définition, mise en œuvre et maintien des stratégies d'accès aux environnements de données sensibles en collaboration avec leurs propriétaires, conformément aux principes de moindre privilège (SQL Server, Active Directory)

Administrateur de bases de données MSSQL Server (Consultant/permanent) 06/1998 – 01/2022
Clients: CDPQ, CCQ, WSP, Tetra Tech, CGI, Bell Canada, Artprice.com, Alstom, CCI Lyon

---

ÉDUCATION & CERTIFICATIONS

Certificat Professionnel en Cybersécurité (Massachussetts Institute of Technology, USA, 09/2022)

CompTIA Security+ (08/2025)

En cours de préparation (12/2025) : **CCNA**

Diplôme Universitaire

Maitrise en Informatique (Conservatoire National des Arts et Métiers, Lyon, France, 2004)