



Aurélien Marteau

33 ans

Expert technique cybersécurité/secops

aurelien@marteau.me – 06 51 92 24 96 – <https://aurelien.marteau.me>

Parcours professionnel

PMU – Paris

Depuis octobre 2018

Manager du pôle expertise technique/secops et référent cybersécurité technique

Pilotage du pôle de sécurité opérationnelle (3 personnes) :

- gestion des alertes de cybersécurité et accompagnement à la remédiation
- gestion de l'expertise de l'écosystème de solutions de cybersécurité (protection email, WAF, CASB, sondes de gestion de vulnérabilité et de conformité...)
- gestion du projet SOC : BUILD, RUN et amélioration continue

Référent technique cybersécurité :

- participation aux ateliers projets pour la définition de politiques de sécurité
- veille cybersécurité pour le PMU : surveillance des vulnérabilités, cyber threat intelligence
- expertise technique pour les appels d'offres (SOC, EDR, NAC...)
- tests d'intrusion et audits de sécurité sur l'ensemble du Système d'Information

Organisation de séances de sensibilisation : démonstrations techniques sur des outils internes, campagnes de phishing...

EXPERIENCES PRECEDENTES

Mars 2013 – octobre 2018

Pentesteur/consultant en sécurité informatique dans des équipes qualifiées PASSI

CGI Business Consulting (2 ans ½), Intrinsec (3 ans)

Test d'intrusion (Web, clients lourds, systèmes basés sur Windows/ActiveDirectory), Red Team/Purple Team, audit de configuration (système d'exploitation, serveur Web, SGBD, équipement réseau...), audit d'architecture, audit sans-fil

Dans tous secteurs (public, bancaire, hospitalier, assurance, transports, énergie...), en France et à l'étranger

Réalisation de sessions de sensibilisation cyber, usage de social engineering

Participation à la cellule CERT d'Intrinsec (réponse à incident), analyse forensique Linux

Chantiers internes : développement d'outils, administration réseau et système, gestion de la base de connaissance interne, participation aux avant-ventes, participation aux entretiens de recrutement, encadrement de stagiaire

Diplômes, certifications, formations

Hacking and securing cloud infrastructure (2021) de NotSoSecure lors de Hack in Paris

SANS SEC642 (2020) www.sans.org/cyber-security-courses/advanced-web-app-penetration-testing-ethical-hacking/

Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

Windows Post-Exploitation: Subverting the Core (2019) par Ruben Boonen lors de Hack in Paris

OSCP (2016) www.offensive-security.com/pwk-oscp/

Offensive Security Certified Professional



Ingénieur en informatique (2012) www.ensiie.fr

École Nationale Supérieure d'Informatique pour l'Industrie et l'Entreprise – Évry



Langues : Français (langue maternelle), **Anglais** (professionnel courant, TOEIC 910)

Autres centres d'intérêt

Musicien et associatif : euphonium dans plusieurs ensembles et orchestres (harmonie, ensemble de cuivres, banda, big band...), membre du Bureau dans plusieurs de ces associations

Administration réseau et système : gestion de serveurs Linux (serveur Web, bases de données, email, DNS, FTP, VPN, applications Web), gestion de masters Windows et de GPO