Bastien Pourcine

› +33 6 73 96 00 30
› bastien.pourcine@gmail.com
› @bastien___

31400, Toulouse, **France | Remote**
31 ans | **8 ans** d'expérience

Permis A, déplacements ponctuels possibles en France et à l'international

« Avec plus de 15 ans d'expérience en cyberdéfense au travers de divers rôles technico-fonctionnels ou opérationnels, je suis à la recherche d'un environnement pour partager et perfectionner mes compétences, »

Environnements

DEFENSIFS <

Environnements SOC ELK, Graylog, Splunk

ATT&CK, Sysmon, WEL, OSQuery, auditd

Sigma, TheHive, MISP, OpenCTI

Tendances des malwares, menaces, TTP, évaluations MITRE Engenuity

OFFENSIFS <

Pentests web occasionnels (OWASP), rejeu de TTP IT & OT

Purple Team*: Caldera, scenarios, CI/CD capacités de détection

Audits techniques : scans, suivi des remédiations, comités, synthèse

GOUVERNANCE, RISQUES & CONFORMITE <

Analyses de risques: EBIOSv2, EBIOS-RM, GDPR, ISO 27001, 27002, 27005, TPN/TPN+, TPE/PME, support à la rédaction de PRA/PCA.

Audits SOC : suivi de projet, analyse du contexte et des objectifs, recommandations relatives à la collecte de données, la mise en place de moyens de détection ou de construction d'équipes ou de service SOC managé.

Notions : PCI-DSS, PDIS/PRIS, ii901 (FR)

Expériences professionnelles

> CONSULTANT INDEPENDANT › CORALIUM & AUTRES › 04/2023 – AUJOURD'HUI

#AUDIT ; #ESN ; #MALT ; #MISSIONS COURTES ; #AUDIT ; #GRC

Missions d'audit **GRC** à 60-80% (3-4j / semaine) pour une startup pure-player en cybersécurité. Audits et accompagnement pour l'obtention de labels de cybersécurité du domaine multimédia (**TPN**). Pilotage d'un consultant junior et restitution des éléments de suivi avec la co-CEO et responsable du pôle GRC.

Missions en tant que consultant **indépendant** micro-entrepreneur en 1er rang : audits flash, analyse de risque, recommandations de sécurité. **EBIOS-RM**, entretiens et production de livrables de synthèse.

> ENTRENARIAT › PURPLE SCOUT › 04/2023

#ENTREPRENARIAT ; #DETECTION ; #EVALUATION ; #MITRE ATT&CK ; #IA

« Purple Scout est une startup d'audit et de label qualité pour les solutions et services de cybersécurité. » - Suivi de programmes d'incubation pour **pitch** et tentative de levée de fonds sur pitch deck auprès de **business angels** et fonds d'investissement. (Pitch, business model, plan, etc.)

> SECKIOT › PRODUCT OWNER - ANALYSTE N3/CTI › 2021 – 2023 – 2 ANS

#ICS ; #EDITEUR SOLUTION ; #CARTOGRAPHIE ; #DETECTION ; #DPI ; #NIDS ; #THREAT INTELLIGENCE

Activités partagées entre le fonctionnel (**PO**/PM) pour la création, le recrutement, le développement et la vente d'une solution de cyberdéfense (**NIDS**) pour les milieux industriels (**ICS/OT**). Analyse de solutions concurrentes (Claroty, Dragos, CyberX, etc.) et expression des besoins. Mise en place de processus **Agile**, d'un Jira et accompagnement des team-leads dans la coordination des objectifs.

Et d'un autre coté, recherche, analyse et restitution en interne des objectifs éléments de threat intelligence (**CTI**) spécifiques aux environnements **SCADA**. Partage des éléments et stratégies a établir, contribution sur les éléments de rejeu sur des protocoles industriels (**OPC**-*, **Modbus**, S7, etc.). Présentations et organisation technique sur des scénarios et groupes offensifs majeurs connus (Triton, **Incontroller**, **APT28**, etc.). Responsable du projet de certification sécurité du produit (**CSPN**).

> LA POSTE – DSI BANQUE & RESEAU › EXPERT SOC › 06/2020 - 02/2021 – 9 MOIS

#DETECTION ; #CERT ; #SOC ; #COORDINATION ; #ALERTES ; #SPLUNK

Rôle technico-fonctionnel et expertise **SOC** : conduite de projet de détection de comportements malveillants sur les comptes particuliers de banque en ligne. **Coordination** DSI, centre d'expertise **CERT/N3**, développeurs **Splunk**, responsables métiers et cellule lutte anti-fraude.

Modélisation des comportements offensifs, mise en place de mesures de **détection** en collaboration avec les experts concernés. Sollicitation de services forensiques externes et de services spécialisés dans le cadre des activités de remédiation.

PROJETS PERSONNELS <

Entreprenariat – *2023*

Evil Twin & scenarios offensifs smartphones – *2010 - 2014*

Bypass anti-virus, malwares, RATs – *2005 - 2010*

SOFT SKILLS, FORMATIONS & CERTIFICATIONS <

Communication, intelligence émotionnelle, coordination, management

Splunk BOTS (2018), ELK Engineering and hands-on (2017)

MITRE MAD, challenges DFIR

SANS CTI, ICS/OT threats

AUTRES <

TOEIC 850 Langue natale

Langages : Niveau débutant Python & Go, C, ASM, niveau intermédiaire Bash, SPL, Graylog Lucene

Veille technologique : Twitter, MISC, CERTs, write-ups de bug bounty

Pilotage d'activité, construction de synthèses et maintien des **KPI** de suivi avec le support de ressources pour le **suivi** des actions, ainsi que l'appui du RSSI et DSI Banque & Réseau et du centre d'expertise

---

> CS GROUP › INGENIEUR CYBERSECURITE › 09/2019 - 05/2020 – 9 MOIS

#EMBARQUE ; #SCADA ; #IDS; #R&D; PROJECT MANAGEMENT; SIEM; SOC

Recrutement initial pour une mission de projet **SOC** & **IA** ; travail interne en régie au sein de la BU cybersécurité dans un contexte **embarqué** & **industriel**. Analyse de **protocoles industriels**, d'un projet de sonde **IDS** embarqué. Revue critique projet & technique, présentations, partages de connaissances **ATT&CK** & **purple-team**. Support sur les activités du directeur de BU sur des activités transverses **technico-fonctionnelles**.

> ITRUST › INGÉNIEUR CYBERSÉCURITÉ › 2017 - **2019** - 2 ANS

#RUN & BUILD SOC ; SIEM; DETECTION; TTP MITRE ATT&CK; CTI; ML; AI; KILL CHAIN; PURPLE TEAM; VULNERABILITÉS

- **RUN SOC : N2** et chef de projet **SOC** : installation, déploiement, intégration des sources de données. Mise en place d'alertes, dashboards, procédures de réponse à incident. Suivi des vulnérabilités et remédiation en coordination avec les clients. Formations & conduite de projets multi-clients (Contextes **PCI-DSS**, industriels, défense, etc.) **B2B** et **B2C**, en France et à l'étranger.
- **BUILD SOC : Coordination** avec les développeurs des solutions, avec les équipes red-team pour le rejeu d'éléments offensifs et les activités purple team, partage des connaissances MITRE **ATT&CK /** TTP.
- Autres : Missions forensique - déplacements sur site et coordination des actions face à des attaques avérées en cours (3). **Support transversal –** support avant-vente, recrutement, activités juniors.

> ENSEIGNEMENT UNIX & CYBER › INDEPENDANT › 2016 - 2020 – 20 jours / an

- **Mise à jour programme & supports, préparation TP** Linux & Cybersécurité pour SUPINFO Toulouse en 2016 en étudiant et 2019/2020 en tant qu'enseignant externe indépendant.

Diplômes

2015 – 2017 › **M.SC.2 - MASTER 2** › *SUPINFO TOULOUSE*

2011 – 2013 › **DUT INFO.** › *PAUL SABATIER, TOULOUSE*

Hobbies

- ✓ Outdoor : ski, plongée, montagne
- ✓ E-Sport
- ✓ Scripting, veille technologique

> CGI › R&D BLUE TEAM › APRIL **2017** - ***STAGE DE FIN D'ÉTUDES*** – 6 MOIS

#SONDE RESEAU; ELK; DOCKER; GRAYLOG; D3.JS; FULL PACKET CAPTURE; DFIR; NETWORK VISUALIZATION; MDM; CASB

> ATOS › *ANALYSE DE RISQUE PROJET DGA* › JUILLET **2016** - ***STAGE BAC+4*** – 3 MOIS

#ANALYSE DE RISQUE ; MOBILITE ; CHIFFREMENT ; RECOMMENDATIONS DE SECURITE ; END TO END ; AUXYLIUM

> SOPRA STERIA › *R&D RED TEAM* › AVRIL **2014** - ***STAGE DUT*** – 3 MOIS

#KILL CHAIN POC; R&D; SPOOF; EXPLOIT; PAYLOAD CUSTOMISATION; PRIVILEGE ESCALATION; MSF; MALWARE; SPYPHONE

Bastien Pourcine

› +33 6 73 96 00 30
› bastien.pourcine@gmail.com