Informations personnelles

Tony ISKOW
Rueil-Malmaison
06 29 27 31 98
Tony.iskow@gmail.com

Portfolio :
https://www.tybbow.com/

https://www.linkedin.com/in/tybbow/
https://www.root-me.org/Tybbow-17659
https://github.com/tybbow

Diplôme

BTS Système électronique

Information complémentaires

Habilitation : TSC (Secret Otan)
Langue : Anglais professionnel

Recherche & Veille Sécurité

Découverte de Vulnérabilité (2025) : Identification d'une faille Kernel critique (DoS) affectant l'écosystème Apple. **CVE-2025-24224**.

Root-Me : Top 0,2 % mondial – Score : 5500 points. Spécialisation avancée en catégories Web et Système

Développement : Créateur de *frenchsweethome.com* et contributeur GitHub.

Certifications

Streamcore : STI & STE
Tanium : Essential & Administration 2.0

Performance & Reliability Engineer | RCA | Observability

J'interviens lors d'incidents complexes afin de comprendre le fonctionnement réel des applications, corréler métriques, logs et traces, puis identifier les causes racines impactant la performance et la stabilité des services critiques.
Mon expertise repose sur une compréhension approfondie des systèmes et des mécanismes applicatifs, développée au fil de l'évolution des pratiques de supervision : de la métrologie réseau (NPM) à l'observabilité applicative full-stack.
Approche renforcée par une pratique avancée en sécurité offensive, illustrée par un classement Top 0.2% mondial sur Root-Me et la découverte d'une vulnérabilité Kernel Apple (CVE-2025-24224).

Expérience professionnelle

Consultant Performance/Observabilité – QosGuard (Nov 2019 – Août 2025)

Ministère des Armées :

- Pilotage de l'observabilité et de la supervision de systèmes critiques nationaux multi-services
- Analyse d'incidents complexes applicatifs, systèmes et réseau afin d'identifier l'origine réelle des dégradations. (Proxy, Firewall, CAS, VPN, Services métiers)
- Corrélation des données d'observabilité, logs et métriques pour isoler les causes racines d'incidents.
  - Amélioration du score CQD (Microsoft Call Quality Dashboard) de 50% à 85, visio collaborative.
- Intervention sur incidents impactant des services critiques utilisés à l'échelle nationale.
- Développement d'outils d'ingestion et d'analyse de logs massifs pour faciliter le diagnostic d'incidents applicatifs (Nginx Access/Error, Stack Traces Java) utilisés par les équipes d'exploitation.
  - Algorithme de calcul statistiques automatiques pour isoler les temps de réponse par endPoint, la volumétrie et la typologie des erreurs (Codes http 4xx/5xx, Exceptions Java)
  - Réduction du temps d'analyse d'incidents de 50-70% passant de plusieurs jours à quelques heures.
- Downtime Manager – Solution de Pilotage de Disponibilité & Reporting SLA
  - Conception Full-Stack d'une plateforme complète (PHP OO, PDO, Jquery, Bootstrap, chartJS)
- Développement de sondes techniques bas niveau permettant la mesure fine des comportements systèmes lors d'incidents (C, C#, PowerShell, Python)

Intermarché/SNCF:

- Résolution d'incidents complexes impactant les environnements magasins et applications utilisées par plusieurs milliers d'utilisateurs. (Wi-Fi, Clients lourds, Applications métiers, Cloud)
  - Suppression des déconnexions utilisateurs récurrentes impactant les usages applicatifs quotidiens.
- Diagnostic des lenteurs applicatives via analyse des flux réseau, requêtes BDD et traitements serveurs
- Référent technique lors d'incidents majeurs, intervenant lorsque les analyses standards ne permettent plus d'identifier la cause racine.
- Mise en place et pilotage complet de Dynatrace pour l'analyse et la résolution d'incidents applicatifs.
- Capacité à corréler les données d'observabilité avec les comportements bas niveau système.
- Mise en place de mesures et alertes permettant d'objectiver les dégradations utilisateurs
  - Mise en place de mécanismes d'analyse de signaux faibles permettant d'anticiper des dégradations applicatives et de réduire les incidents.

Expert en Métrologie des Réseaux – ministère des Armées (Nov 2010 - Nov 2019)

- Arbitrage technique et troubleshooting N3 lors de crises multi-acteurs (Réseau/Appli/ops externes)
- Analyse des dégradations applicatives via mesures réseau et comportement des flux
- Pilotage de la performance (App, Réseau, VoIP) et monitoring multi-outils (Cacti, eHealth, Streamcore)
- Animation de formations sur les réseaux TCP/IP et protocoles (HTTPS, SNMP, LDAP, etc)
- QoS-Probe (C) : Développement d'un moteur de mesure de Qualité De Service Réseaux
  - Extension de la QoS opérateur couvrant 100% du parc en D1, D2 et D3, contre 40% initialement.
- TCPPing (C) : Développement d'un outil de mesure de latence basé sur le Handshake (TCP)
- CheckMSS (C) : Création d'une sonde d'analyse de la segmentation TCP (MTU/MSS)

Sécurité des systèmes d'information, Freelance (2018-2019)

- Responsable de la sécurité des systèmes d'information (RSSI) pour Serenitrip.
- Audits techniques et sécurisation d'infrastructures critiques
- Réalisation et pilotage d'audits techniques de sécurité.
- Découverte de vulnérabilités applicatives majeures.
- Rédaction de politiques de sécurité (PSSI, PCI) et suivi des plans d'action (correctifs et palliatifs).

Skills

Investigation & Observabilité : Dynatrace, Datadog, NewRelic, ELK, ManageEngine, Cacti, Zabbix, Ekara
Infrastructures : Cloud (AWS, Azure), Hybride (VmWare, Proxmox), Conteneurisation (K8s, Docker)
Analyse & Data : WireShark, Packet Analyser, Fiddler, PowerBi.
DevOps & Scripting : PowerShell, Python, C, C#, PHP, Javascript, Bash, Git, Ansible, Jenkins
Sécurité : Burp Suite, Sqlmap, Nessus, Hydra, ZAP, Dirb,