**🔍 STELLA BARBARELLA**

***SOC Analyst | Threat Hunter | Incident Responder***

📍 Paris, France | ✉️ stiliana.stoyanova@orange.fr| 🔗 https://www.linkedin.com/in/stella-s-95ba5683/

**🚀 VALUE PROPOSITION**

*"Je transforme le bruit des alertes en actions concrètes pour protéger les infrastructures critiques, en combinant méthodologie SOC et expérience terrain."*

**🛡️ EXPERTISE CLÉ**

| **Détection** | **Réponse** | **Optimisation** |
| --- | --- | --- |
| Tuning de règles SIEM | Investigation forensic | Design de playbooks |
| Threat Hunting proactif | Containement malware | Mise en place MDR/XDR |
| Analyse MITRE ATT&CK | Coordination d'incidents | Intégration Threat Intel |

**📌 CASE STUDY : ATTQUE GPO SUR RÉSEAU WINDOWS**

**Contexte** : Simulation d'intrusion avancée (formation SOC)  
**Démarche** :

1. **Détection** : Alerte sur modification suspecte de GPO (gpt.ini)
2. **Investigation** :
   * Capture mémoire avec **Velociraptor** → Processus powershell.exe injectant du code
   * Analyse réseau **Wireshark** → Beaconing vers IP bulgare (AS 57169)
3. **Réponse** :
   * Création de règles **Sigma** pour détection future
   * Playbook documenté pour l'équipe

**Outils**: Velociraptor, Sysinternals, Sigma, Wireshark, Splunk

**🛠️ TECHNICAL STACK**

**SIEM/Logs**:

Splunk (ES) | Wazuh | Microsoft Sentinel

**EDR/Forensic**:

CrowdStrike | Microsoft Defender ATP | Velociraptor | FTK Imager

**Threat Intel**:

MISP | AlienVault OTX | MITRE ATT&CK Navigator

**Automatisation** :

Python (Pandas pour l'analyse de logs) | PowerShell | Sigma CLI

**📈 MÉTRIQUES D'IMPACT**

* **+30%** de détection précoce grâce au tuning de règles
* **-25%** de temps de réponse via playbooks standardisés
* **100%** des IOCs intégrés dans MISP en <1h

**📝 CONTACT PROFESSIONNEL**

* **Email** : [email pro]
* **LinkedIn**: <https://www.linkedin.com/in/stella-s-95ba5683/>
* **Portfolio** : <https://github.com/stellababy2004>
* **Disponibilité** : Immédiate pour missions SOC/IR

*"Prête à renforcer votre SOC avec une approche data-driven et terrain."*