**🔍 STELLA BARBARELLA**

**SOC Analyst | Threat Intelligence Specialist | Incident Responder**

📍 Paris, France | ✉️ [stiliana.stoyanova@orange.fr](https://d.docs.live.net/ed3ec81dc9dc70b2/Documents/chatGPT/stella_portfolio_final_clean_gofile/stiliana.stoyanova@orange.fr) | 🔗 <https://www.linkedin.com/in/stella-s-95ba5683/>

**🛡️ CORE EXPERTISE**

* **Threat Detection**: SIEM (Splunk, Elastic Stack), IDS/IPS (Suricata)
* **Incident Response**: Forensic Analysis (Velociraptor, FTK Imager), MITRE ATT&CK Mapping
* **Threat Hunting**: Proactive IOC Searches, Behavioral Analysis
* **Automation**: Python (Pandas), PowerShell, Sigma Rules

**📌 CASE STUDY: "Patissier Intrusion" Simulation**

**Scenario**: Detected & remediated GPO-based attack in Windows AD environment   
**Key Actions**:

1. **Detection**: Identified suspicious gpt.ini modifications via Splunk alert
2. **Investigation**:
   * Memory dump analysis → Malicious powershell.exe injection
   * Network traffic → C2 Beaconing to Bulgaria (IP: 185.143.223.41)
3. **Response**:
   * Isolated host → Reset credentials
   * Created Sigma rule for future detection   
     **Metrics**:

* Time to Contain: **47 minutes**
* IOCs Added to MISP: **12**

**🛠️ TECHNICAL STACK**

|  |  |
| --- | --- |
| **Category** | **Tools/Technologies** |
| **SIEM** | **Splunk, Wazuh, Elastic Security** |
| **EDR/Forensic** | **CrowdStrike, Velociraptor, Autopsy** |
| **Threat Intel** | **MISP, AlienVault OTX, MITRE ATT&CK** |
| **Automation** | **Python (Pandas, Requests), Sigma, PowerShell** |

**📈 KEY ACHIEVEMENTS**

* **+30%** detection rate after SIEM rule optimization
* **-25%** incident response time via playbook automation
* **100%** of critical IOCs integrated into MISP within 1 hour

**📚 EDUCATION & CERTIFICATIONS**

* **SOC Analyst Certification** | Sorbonne University (2024)
* **eJPT** (In Progress) | Expected Q3 2024
* **Network Security Diploma** | GRETA Paris (2014)

**📬 CONTACT**

* **Email**: [barbarella@mail.fr](https://mail.fr)
* **LinkedIn**: <https://www.linkedin.com/in/stella-s-95ba5683/>
* **GitHub**: [stellababy2004 - Overview](https://github.com/stellababy2004)



**"Ready to transform alerts into actionable defense strategies."**