

Pitch

Hey, I'm Stella Barbarella - a SOC analyst who turns noisy alerts into actionable insights. I s

Key Services

- SIEM Rule Tuning
- Phishing & Incident Response
- Threat Hunting
- Playbook Development
- SOC Process Optimization

Case Study - Patisserie Intrusion

Client: Simulated enterprise case (SOC Analyst program)

Scope: Post-compromise investigation on a Windows domain admin workstation

Tools: Velociraptor, Sysinternals, Sigma, Wireshark

Summary:

Investigated a GPO-based attack originating from a compromised machine. Identified persistence

Toolstack

- SIEM: Splunk, Wazuh, Microsoft Sentinel
- EDR/XDR: CrowdStrike, Microsoft Defender, Elastic Agent
- Analysis: Wireshark, Sysinternals, Velociraptor
- Threat Intel: VirusTotal, AbuseIPDB, AlienVault OTX, Shodan
- Automation: Python, PowerShell, Sigma
- IR Tools: TheHive, MISP, CyberChef
- OSINT: Maltego, SpiderFoot, URLscan.io

Contact

Name: Stella Barbarella

Email: [your-email@domain.com]

Discord: [your-handle]

LinkedIn: [your-linkedin-profile]

Let's talk - I'm ready to deliver value from day one.