Pitch

Hey, I'm Stella Barbarella - a SOC analyst who turns noisy alerts into actionable insights. I specialize in SIEM tuning, phishing incident response, and stealthy threat hunting. Recently, I cut alert fatigue and response time by 40% for a client through custom playbooks and smart rule engineering. If you need sharp eyes and fast action in your blue team - let's talk.

Key Services

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

Case Study - Patissier 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 mechanisms through autorun entries and tracked malware delivery via DNS spoofing. Delivered a full kill chain analysis and implemented detection and hardening recommendations.

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: https://www.linkedin.com/in/stella-s-95ba5683 Let's talk - I'm ready to deliver value from day one.

Kill Chain Overview - Patissier Attack

1. Reconnaissance - Attacker identifies the vulnerable internal resource.
2. Weaponization - Malicious file disguised as an internal report.
3. Delivery - File hosted via DNS-spoofed intranet page.
4. Exploitation - User executes the infected document.
5. Installation - Remote access established via GPO.
6. Command & Control - Persistent access achieved.
7. Actions on Objectives - GPO abuse and lateral movement.

Connect with me