LOUIS M. GALLEGOS III

louismgallegos@gmail.com | 720-297-4080 | linkedin.com/in/louis-g-cyber

OBJECTIVE

Cybersecurity professional and military veteran with hands-on experience in incident response, threat detection, and endpoint forensics. Skilled in triaging alerts, performing containment and forensic analysis, creating SOC playbooks, and mentoring junior analysts to improve security posture, seeking a Level 2 SOC Analyst or entry-level DFIR role. I also possess:

- Experience with Microsoft Defender XDR for alert triage, endpoint containment, and threat hunting across Windows and cloud environments.
- Proficient with Avanan for email security, phishing detection, and DLP monitoring in cloud-hosted applications.
- Utilized Jira for incident tracking, SOC workflow management, and documentation of runbooks, and remediation tasks.
- Experience with live investigations in SentialOne, Defender XDR, & Avanan

EDUCATION

SANS Technology Institute. (In-Progress)

- Bachelor of Applied Cybersecurity. (90 Credits)

CERTIFICATIONS

- GIAC - Security Essentials. (GSEC)
- GIAC - Information Security Fundamentals. (GISF)
- GIAC - Foundational Cybersecurity Technologies. (GFACT)

EXPERIENCE

JRPC InfoSec (MDR & Incident Response) October 2023 - Present
Level 2 Security Analyst (Remote)

- Triaged and investigated approximately 250 - 800 security alerts per week across EDR, email, and cloud platforms, identifying threats, reducing false positives, and escalating high-priority incidents for rapid containment.
- Conducted attack surface assessments to identify exposed assets and potential vulnerabilities for 8 clients. With an estimated total of 624 remediations in my 2+ years as an analyst. providing remediation recommendations that improved clients' overall security posture.
- Led containment and remediation for approximately 11 escalated incidents, including endpoint isolation, credential resets, session revocations, and delivering detailed client-facing incident reports
- Authored and maintained 5+ runbooks for Microsoft Defender XDR and Avanan, tailoring response procedures based on alert type to improve SOC efficiency and incident handling consistency.
- Trained and mentored two Level 1 analysts, improving alert triage accuracy, onboarding efficiency, and overall, SOC performance.
- Designed and implemented 10+ custom detection rules, including IOC integration into Microsoft Defender XDR and alert logic in EDR, SIEM, and cloud platforms, covering MITRE ATT&CK techniques: T1566.002 (Spear phishing), T1078.003 (Cloud Accounts) -Token theft, T1203.002 - Endpoint malware investigations, T1086.001 (PowerShell) - Suspicious script triage. Reducing false positives by 15% and improved incident response efficiency through tuning and playbook integration.