MANOJSAI BANGARU

+1 (940)-843-3869 | manojsaibangaru@gmail.com | linkedin.com/in/manojsaibangaru-a65474189/

SUMMARY

Security Analyst with 2 years of experience in Security Operations, SIEM/SOAR, and growing expertise in Governance, Risk, and Compliance (GRC). Proficient in Splunk, Sentinel, and automation through Python and SOAR platforms. Demonstrated experience supporting security audits, performing access reviews, developing SOPs, and aligning controls with frameworks such as NIST and ISO 27001. Strong communicator and collaborator, capable of translating technical concepts for cross-functional teams in fast-paced environments.

EDUCATION

Master of Science in Computer Science August 2023 - May 2025
University of North Texas, Denton, TX

SKILLS

Scripting & Querying: Python, Bash, Regex, Kusto Query Language (KQL), SPL

Security Operations: Threat Hunting, Malware Analysis, Vulnerability Management, Digital Forensics, Log Analysis.

Cloud Security: AWS, Azure Security, Microsoft Defender for Endpoint security (EDR), Security Monitoring, System Logs.

Security Technologies: Splunk, Microsoft Sentinel, Splunk SOAR, Firewalls, Intrusion detection/prevention systems.

Governance, Risk & Compliance: Control Mapping, SOC2 Readiness, Security Policies, Process Documentation.

Cybersecurity Focus: Network Security, Threat Detection, Incident Response, IT Infrastructure, Ethical Hacking.

Soft Skills: Written and verbal communication, analytical, highly motivated, problem-solving, attention to detail.

Availability: Willing to relocate, Open to working 24/7 SOC rotations, including nights, weekends, and holidays.

PROFESSIONAL CERTIFICATIONS

1. **CompTIA Security+** 2. **Qualys VMDR** 3. **Cortex XSOAR 6.2: Automation and Orchestration**

WORK EXPERIENCE

Accenture – Bengaluru, India August 2021 – July 2023
Security Delivery Associate

- Assisted in deploying and managing security solutions across client environments, integrating them into broader security management systems for real-time monitoring and automated response.
- Monitored and triaged security alerts using Splunk (Security Information and Event Management) and Splunk SOAR (Phantom); escalated actionable incidents per defined runbooks. Analyzed logs to identify potential threats, reducing false positives by 15%.
- Designed and implemented **10+ SOAR (Phantom) automation playbooks** for **malware analysis, exploit detection**, increasing **incident resolution efficiency by 30%**.
- **Enhanced** SOAR (Phantom) functionalities by designing custom Python functions, reducing incident response time by 20% and optimizing Splunk queries to meet client-specific needs.
- Created and maintained **security documentation**, including **Standard Operating Procedure**s (**SOPs), playbooks and runbooks**, ensuring compliance with **NIST, ISO 27001** and streamlining **security automation workflows**.
- Provided **operational support and technical support** for client implementations.
- **Trained** and **mentored** 5 team members, boosting team performance by 15% and accelerating response times.
- **Collaborated** with SOC and ServiceNow teams to automate incident responses, improving client visibility and operational efficiency by 25%.

ACADEMIC PROJECTS

Red Team Simulation & Blue Team Response using Atomic Red Team + Splunk March 2025

- Simulated credential dumping **(T1003)** and lateral movement **(TA0008)** attacks using Atomic Red Team, enhancing Splunk detection rules to reduce MTTD by 20%.
- Created and fine-tuned Splunk correlation rules and detections to identify ATT&CK techniques like **T1003** (OS Credential Dumping), **T1059** (Command and Scripting Interpreter), and **T1071** (Application Layer Protocol).
- Simulated SOAR playbooks in Python to automate threat enrichment (IP reputation), analyst alerting, and host quarantine actions, based on Splunk detections.
- Documented playbooks aligned to Phantom SOAR structure, with modular enrichment and response actions triggered by MITRE-mapped alerts.