Manojsai Bangaru

Security Analyst – SIEM, SOAR & SOC Operations

manojsaibangaru@gmail.com | +1 940-597-9780 | LinkedIn

PROFESSIONAL SUMMARY

- CompTIA Security+ certified Cybersecurity Analyst with 4+ years of experience across SOC operations, threat detection, incident response, vulnerability management, and digital forensics in healthcare and global consulting environments.
- Hands-on experience **leading implementation and operation** of SIEM/SOAR platforms, including Palo Alto Cortex XSOAR and Splunk SIEM, to deliver automated incident response and SOC workflow optimization.
- Strong background in designing, tuning, and optimizing detection rules, correlation searches, and IDS/IPS signatures mapped to **MITRE ATT&CK**, reducing false positives, and improving detection accuracy.
- Proficient in developing and maintaining SOAR playbooks and Python-based automation to enrich alerts, collect evidence, and orchestrate remediation, achieving measurable reductions in mean time to respond (**MTTR**).
- Skilled in vulnerability management and risk assessment using tools such as **Nessus**, **Tenable**, **Rapid7**, and **Nmap**, with a track record of driving remediation for high-severity findings.
- Familiar with cloud and endpoint security controls across **AWS** and **Azure**, including **IAM policies**, **MFA/SSO**, **EDR**, endpoint hardening, and alignment with **CIS Benchmarks**.
- Experience supporting cloud security tooling implementation and ongoing operations across Microsoft 365, Azure, and hybrid environments, including SIEM, EDR, email security, MFA, and vulnerability management platforms.
- Knowledgeable in security governance and compliance practices aligned with **ISO 27001**, **HIPAA**, **PCI-DSS**, and **NIST CSF**, supporting audits, documentation, and process standardization.

TECHNICAL SKILLS

Security Operations & Monitoring:
SIEM: Splunk, Wazuh, Kibana, SQL-style log analytics and SPL-based searches.
SOAR: Palo Alto Cortex XSOAR (playbook design, automation, integrations), Splunk SOAR (Phantom).
Threat Detection: IDS/IPS (Snort), TCPDump, Wireshark, email threat analysis, OSINT, MITRE ATT&CK–based use case creation.

Vulnerability, Risk & Forensics:
Vulnerability Management: Nessus, Tenable, Rapid7, Nmap, CVSS-based prioritization, remediation tracking.
Risk & Governance: Threat modeling, risk assessments, ISO 27001 control validation.
Forensics & DFIR: Chain of custody, phishing response, malware analysis support.

Cloud, Endpoint & Platform Security:
Cloud: AWS, Azure, cloud security monitoring, cloud-native logs, and alerts.
Identity & Access: IAM, MFA, SSO, OAuth/SAML, policy review and refinement.
Endpoint & Network: EDR (e.g., Microsoft Defender) endpoint hardening, CIS Benchmarks, firewall and VPN basics.

Scripting, Automation & Tooling:
Languages: Python, Bash, PowerShell.
Automation: SOAR playbooks, REST API integrations, log parsing scripts, CI/CD-integrated security monitoring.
Tooling: ServiceNow, Git, GitHub, basic CI/CD environments.

Networking & Systems:
Networking: TCP/IP, DNS, VPN, LAN/WAN concepts, basic firewall configuration.
Systems: Windows, Linux (including Kali), macOS; system and audit log analysis.

EDUCATION

Master of Science in Computer Science, *University of North Texas* **August 2023 – May 2025**

Bachelor of Technology in Electronics and Communication, *GITAM University* **July 2017 – May 2021**

CERTIFICATIONS

- CompTIA Security+
- Cortex XSOAR 6.2 Automation and Orchestration.
- Google Cybersecurity Professional Certificate
- Qualys VMDR.

WORK EXPERIENCE

Cortex XSOAR Engineer – Johnson & Johnson
New Brunswick, New Jersey, USA. **October 2024 – Present**

- Designed, tuned, and operationalized threat detection rules in SIEM and IDS/IPS platforms using MITRE ATT&CK–mapped hypotheses, improving detection accuracy and reducing false positives across enterprise and cloud workloads.
- Designed and optimized Cortex XSOAR playbooks for alert triage, enrichment, and response, aligning workflows with SOC operational requirements and **reducing manual analyst effort and response time**.
- Performed end-to-end incident response including alert triage, scoping, containment, eradication, and closure, coordinating with infrastructure, IAM, and application teams for high-severity incidents.
- Conducted threat research and hypothesis-driven threat hunting by correlating telemetry from Linux/Windows systems, AWS services, network sensors, and endpoint tools to uncover malicious activity not fully prevented by existing controls.
- Developed and maintained **Python-based automations in Cortex XSOAR** to accelerate alert enrichment, evidence collection, and standardized incident response workflows.
- Partnered with engineering and platform teams to identify logging and visibility gaps, driving improvements in telemetry coverage, and ensuring incident responders had reliable, actionable data.
- Utilized SQL-style log analytics and SPL searches to validate detections, evaluate rule performance, and support post-incident reviews and reporting.
- Supported on-call SOC rotations, documenting detection logic, runbooks, and lessons learned to continuously improve SOC processes and playbook quality.

SOAR Implementation Engineer – Accenture
Bengaluru, Karnataka, India. **August 2021 – July 2023**

- Assisted in implementing and operating **SOAR platforms including Palo Alto Cortex XSOAR and Splunk SOAR**, integrating them with Splunk SIEM for centralized alert ingestion and automated response.
- Monitored, triaged, and investigated security alerts using Splunk SIEM and SOAR, escalating validated incidents in accordance with defined SOC runbooks and incident response procedures.
- Analyzed and correlated security logs to identify suspicious activity and threat patterns, contributing to a reduction in false positives through alert tuning and refinement of detection use cases.
- Designed and implemented **10+ SOAR playbooks in Cortex XSOAR and Splunk SOAR** for malware analysis, phishing, and endpoint alerts, improving incident resolution efficiency by approximately 30%.
- Enhanced **Cortex XSOAR automation capabilities** by developing custom Python scripts and optimizing Splunk-integrated workflows, reducing mean time to respond (MTTR) by approximately 20%.
- Created and maintained **XSOAR playbook documentation, SOC runbooks, and automation workflows**, supporting operational readiness and knowledge transfer.
- Collaborated with ServiceNow and SOC teams to integrate SOAR workflows with incident case management, improving visibility, ticket quality, and operational efficiency.
- Mentored junior team members on SOC processes, Splunk search best practices, and SOAR playbook usage, providing operational support for client implementations and onboarding.
- Participated in change and release activities for SIEM/SOAR enhancements, validating new detections and automation flows in test environments before production rollout.

Security Intern – Sonata Software
Bengaluru, Karnataka, India. **October 2020 – June 2021**

- Assisted SOC engineers in integrating SIEM alerts with **SOAR platforms**, configuring basic playbooks for automated alert enrichment and notifications.
- Supported the development and validation of Splunk SPL queries and Wazuh/Kibana searches to correlate events from endpoint, network, and cloud logs and highlight suspicious activity.
- Helped build and test SOAR workflows for routine incidents such as phishing alerts, malware detections, and user access anomalies under guidance from senior analysts.
- Contributed to Python scripts and REST API integrations used to pull additional context from security tools and external services during investigations.
- Monitored SOC dashboards, reviewed security alerts, and escalated potential incidents following defined triage checklists and severity criteria.
- Investigated advanced security incidents across Microsoft 365 and hybrid Azure environments using Microsoft Defender for Endpoint and Azure Sentinel.
- Assisted with maintaining SOC documentation, including updating runbooks, playbook references, and detection rule catalogs.
- Participated in incident post-mortems and tuning sessions to refine alert thresholds, improve correlation logic, and reduce false positives.
- Helped track remediation status using ticketing tools, ensuring follow-up and closure of security findings in coordination with IT teams.