SARANYA GADIPARTHI

saranyagadiparthi.25@gmail.com | www.linkedin.com/in/saranya-gadiparthi25 | +1 9132020335

Professional Summary

- Cybersecurity professional with 3+ years of experience in Security Operations Center (SOC) environments.
- Specialize in SIEM content development, alert tuning, and incident lifecycle management.
- Hands-on with Google Chronicle, Splunk, and QRadar for security event monitoring and detection engineering.
- Skilled in MITRE ATT&CK mapping, proactive threat hunting, and response automation using Python and PowerShell.
- Adept in cloud security (GCP, AWS, Azure), vulnerability management (Nessus, Qualys), and IAM controls.
- Experienced in managing Google Cloud IAM policies and integrating Chronicle SecOps into enterprise SOC workflows.
- Familiar with authentication protocols including SAML, OAuth2.0, and multi-factor authentication (MFA).
- Supported ISO 27001, NIST 800-61, and HIPAA audit readiness with strong documentation and procedural controls.
- Demonstrated success by reducing false positives by 30% and decreasing response time via scripting and workflow optimization.
- Adept at cross-functional collaboration with SOC, IR, DevOps, and compliance teams for full-spectrum security operations.
- CompTIA Security+ (Expected August 2025); certified in Google Cybersecurity Foundations, Networks, and Linux/SQL.
- Active member of Women in Cybersecurity (WiCyS) with strong communication and mentorship experience.

Experience

SOC Analyst I | Ally Bank **Jan 2024 – Present**

Tools & Technologies: Splunk, Suricata, Google Chronicle, Python, Powershell, MITRE ATT&CK, NIST 800-61

- Developed and optimized SIEM content and use cases in Google Chronicle and Splunk, reducing false positives by 30% and improving alert accuracy.
- Automated IOC triage and alert enrichment workflows using Python and PowerShell, enhancing detection speed and lowering MTTD by 25%.
- Managed full incident lifecycle, from triage and containment to RCA and post-incident reporting, in accordance with NIST 800-61 standards.
- Collaborated with DevOps, IR, and compliance teams to implement alerting rules for cloud-native workloads and improve SOC workflows.
- Built and maintained Chronicle dashboards, integrated MITRE ATT&CK tags into detection logic, and implemented threat intel feeds for proactive threat hunting.
- Mentored Tier I analysts in detection engineering, case handling, and SIEM tuning best practices.

SECURITY ANALYST | WILDAPPZ **Jan 2022 – Jul 2023**

Tools & Technologies: Nessus, QRadar, SentinelOne, Qualys, Suricata, Snort, Bash, ISO 27001, HIPAA

- Monitored and analyzed events from QRadar and SentinelOne across endpoint, network, and cloud environments within a 24/7 SOC.
- Conducted proactive MITRE-based threat hunting and hypothesis testing to uncover privilege escalation and lateral movement.
- Tuned SIEM detection rules and normalized log ingestion to reduce false positives and improve signal-to-noise ratio.
- Performed full vulnerability management lifecycle using Nessus and Qualys; worked with application owners to prioritize remediation.
- Created and updated incident response SOPs and supported audit readiness for HIPAA, ISO 27001, and PCI DSS by preparing documentation and evidence artifacts.

Education

University of Central Missouri, Lee's Summit, MO, USA

Master Of Science in Cybersecurity and Information Assurance (3.6/4.0)

Technical Skills

SIEM Tools	**:**	Splunk, Suricata, Google Chronicle, QRadar
Endpoint	**:**	SentinelOne, IDS/IPS(Snort, Suricata)
Firewalls & Network Security:		VPNs, TCP/IP, NAT, SSL/TLS
Scripting & Automation Tools:		Python, PowerShell, Bash, SQL, C
Vulnerability Management	**:**	Nessus, Qualys, OpenVAS
Security Tools	**:**	Metasploit, Burp Suite, Nmap, Hydra, SQLmap, Wireshark, Scapy, Netcat
Compliance & Frameworks	**:**	MITRE ATT&CK, NIST 800-61/53, ISO 27001, GDPR, HIPAA
Forensic & Analysis	**:**	Autopsy, Volatility, Packet Analysis, Root Cause Analysis
Cloud & Virtualization	**:**	Google Cloud IAM, AWS IAM, Azure Defender, VirtualBox, VMware
Security Concepts	**:**	SOAR, Alert Tuning, Log Normalization, Detection Engineering, IAM

ACADEMIC PROJECTS:

Vulnerability Assessment & Exploitation Automation (Nessus, Metasploit, PostgreSQL, Bash, Netcat)
Automated vulnerability scans with Nessus, imported results into Metasploit, and executed SMB exploitation via Bash. Configured reverse Meterpreter shells and persistent Netcat backdoors; managed exploit sessions using PostgreSQL.

Password Cracking & Network Credential Sniffing (Hydra, xHydra, John the Ripper, Tcpdump, Wireshark)
Performed brute-force attacks on SSH and SMB using Hydra with custom wordlists. Captured and analyzed network traffic with Wireshark for packet-level credential extraction, filtered weak passwords with pw-inspector.

Incident Response Plan Development for Startup (NIST 800-61, ISO 27001, MITRE ATT&CK)
Developed a complete incident response lifecycle plan based on NIST 800-61 and ISO 27001. Used MITRE ATT&CK mapping and Used Draw.io to visualize detection, escalation, and containment workflows, escalation, and containment workflows—boosting IR efficiency by 35%.

IoT-Based Environmental Alert System (Arduino, Embedded C, DHT11, LCD, Buzzer)
Designed and deployed a sensor-based alert system to detect temperature/humidity anomalies. Used Embedded C on Arduino to trigger buzzer and LCD-based alerts for asset protection and physical security monitoring.

Certifications

- **CompTIA Security+** *(Expected: August 2025)*
- **Google Cybersecurity Certificate** (Foundations, Networks, Tools of the Trade)

Professional Membership

Active Member, Women in Cybersecurity (WiCyS)