Gopi Unnam

(469)-428-6476 |gopichowdaryu16@gmail.com | Celina, TX 75009
https://www.linkedin.com/in/gopi-chowdary-02640737b/

SUMMARY

Information Security Analyst with 3+ years of experience in securing enterprise systems through incident response, digital forensics, and penetration testing. Expertise in Splunk, CrowdStrike, and Tenable.io for identifying and mitigating advanced threats. Led SOC 2 compliance initiatives and cloud security hardening on AWS and Azure, achieving a 40% reduction in remediation time via automation. Skilled in translating complex security findings into actionable strategies that enhance enterprise resilience.

TECHNICAL SKILLS

- **Operating Systems:** Windows Server, Linux (Ubuntu, Kali, CentOS)
- **Programming & Scripting:** Python, Bash, PowerShell, JavaScript, SQL
- **Security Tools & Platforms:** Splunk Enterprise Security (ES), CrowdStrike Falcon, Tenable.io, Qualys, Nessus, Wireshark, Metasploit, Security Onion, Snort, Suricata
- **Cloud & Identity Security:** AWS Security Hub, Azure Security Center, Microsoft Entra ID (Azure AD), Okta, AWS IAM, Conditional Access, MFA, SSO Configuration, CloudTrail, Azure Sentinel
- **Vulnerability Management & Compliance:** Tenable.io, Qualys Guard, Rapid7, CIS Benchmarks, NIST 800-53, SOC 2 Type II, HIPAA, GDPR
- **Network & Endpoint Security:** FortiGate, Forti Web, Cisco ASA, Palo Alto, VLAN Segmentation, VPN Configuration, IDS/IPS Management, Endpoint Detection & Response (EDR), Web Proxy & WAF Tuning
- **Threat Detection & SIEM:** Splunk ES, QRadar, LogRhythm, ELK Stack, Syslog Analysis, Threat Hunting, Alert Correlation, MITRE ATT&CK
- **Automation & Patch Management:** PDQ Deploy, Ansible, SCCM, WSUS, Jira Integration, Python Scripting
- **Access Management:** Active Directory, LDAP, GPO Management, SAML, OAuth 2.0, PKI, Certificate Lifecycle Management
- **Email & Web Security:** Proofpoint, Mimecast, Zscaler, Barracuda, DKIM/DMARC/SPF Policies, URL Filtering
- **Frameworks & Standards:** NIST CSF, NIST 800-61 (Incident Handling), ISO 27001, SOC 2, OWASP Top 10, CIS Controls

PROFESSIONAL EXPERIENCE

Information Security Analyst, Bank of America, January 2025 - Present

- Reduced remediation cycle time by 40% by designing and implementing automated patching workflows and end-to-end vulnerability tracking integrations across enterprise systems.
- Investigated, contained, and remediated phishing, malware, and lateral movement incidents using Splunk ES and CrowdStrike Falcon to prevent business disruption and data exposure.
- Strengthened organizational phishing resilience by 60% through targeted security awareness programs, simulated phishing campaigns, and continuous user behavior monitoring.
- Improved organizational compliance posture by supporting a successful SOC 2 Type II audit, ensuring control effectiveness and sustained regulatory readiness with zero critical findings.
- Managed the complete vulnerability lifecycle for 1,000+ assets using Tenable.io and Jira dashboards to prioritize remediation and reduce enterprise risk exposure.
- Administered and secured Microsoft Entra ID and Azure environments, implementing MFA and conditional access and conducting internal penetration testing to reduce identity and infrastructure security risks.

Security Engineer, United Healthcare, August 2021 – July 2023

- Decreased mean time to detect (MTTD) by 35% through SIEM log automation, enhanced detection rules, and Python-based alert triage, improving SOC efficiency.
- Strengthened organizational security posture by supporting GDPR and HIPAA audits, authoring compliant security policies, and maintaining zero compliance deviations.

- Led security awareness initiatives and monitored network traffic using Splunk, Wireshark, and Snort to improve threat detection and increase phishing incident reporting by 45%.
- Conducted vulnerability assessments and penetration testing using Nessus and Metasploit, collaborating with IT teams to remediate risks and optimize security and endpoint controls.

System Administrator, eBay, January 2021 – July 2021

- Increased infrastructure uptime reliability by 20% by automating proactive monitoring, developing health-check scripts, and enabling early detection of system issues.
- Reduced manual maintenance effort by 30% through custom Python automation while standardizing SOPs and patch validation checklists to improve patch compliance from 82% to 97%.
- Managed Windows Server environments with least-privilege access and patching controls across dev, test, and production to improve system security, stability, and rollback reliability.
- Supported critical incident management and root-cause analysis for high-priority outages while collaborating with network and security teams on VLAN segmentation and firewall and security rule optimization.

EDUCATION

Master of Science

Cybersecurity, Southern Arkansas University, Magnolia, AR May 2025

- Relevant Coursework: Network Security and Cyber Risk Management
- GPA: 3.5

Bachelor of Technology

- Computer Science and Engineering, Presidency University, Bengaluru, India June 2022
- Relevant Coursework: Operating Systems and Computer Networks
- GPA: 3.2

CERTIFICATIONS

- CompTIA Security Plus
- Microsoft Certified: Azure Developer Associate (AZ-204)
- Certified CCNA

PROJECTS

Malware Analysis and Home Lab Projects Ongoing

- Built and analyzed malware samples in a fully isolated lab environment to study behavioral patterns, attack techniques, and mitigation strategies.
- Designed and maintained a malware analysis lab using Wireshark, Security Onion, and Splunk to safely detect, monitor, and analyze malicious activity.
- Performed static and dynamic malware analysis on executable samples to identify indicators of compromise and improve detection accuracy.
- Documented findings and analysis results to support threat detection, incident response, and security research initiatives.