Gopichand Marri

Cyber Security Analyst

Long Beach, CA | +1 (562) 732 6104
gopichand@jobitwork.com

SUMMARY

- Cyber Security Analyst with 3+ years of expertise in SOC operations, threat intelligence, and cloud security, ensuring enterprise networks, cloud infrastructures, and financial systems remain protected against evolving cyber threats.
- Specialized in penetration testing, vulnerability management, and compliance enforcement, securing high-value financial transactions and ensuring regulatory adherence to NIST, PCI DSS, ISO 27001, and SOC 2 standards.
- Hands-on experience with SIEM tools (Splunk), IDS/IPS, and forensic analysis, improving security event monitoring, breach detection, and incident response time by implementing automation and proactive threat mitigation strategies.
- Strong knowledge of AWS security best practices, identity access management, and cloud threat intelligence, reducing misconfigurations and unauthorized access attempts by strengthening multi-cloud security controls.
- Expertise in financial cybersecurity, reducing fraud, securing sensitive financial data, and mitigating risks associated with DDoS attacks, insider threats, phishing attempts, and advanced persistent threats (APT) campaigns.

SKILLS

Security Operations & Threat Intelligence: SIEM (Splunk), IDS/IPS, HIDS/HIPS, Threat Hunting, Malware Analysis, Security Incident Handling

Network & Cloud Security: AWS Security (IAM, VPC, Security Hub), CSPM, TCP/IP, OSPF, BGP, VPN, DNS, LAN/WAN

Vulnerability Management & Penetration Testing: Nmap, Nessus, OpenVAS, Burp Suite, Metasploit, OWASP Testing, Exploit Development

Financial Sector Compliance & Risk Management: NIST, ISO 27001, SOC 2, PCI DSS, GDPR, CIS Controls, Risk Assessment

Operating Systems & Tools: Windows, Linux (Kali, Parrot OS, Ubuntu), macOS, Wireshark, Core Impact, TCPDump

EXPERIENCE

Morgan Stanley, USA | Cyber Security Analyst **Jul 2024 - Present**

- Monitored security incidents across financial transactions exceeding $500M daily, ensuring rapid incident response, threat mitigation, and zero major breaches impacting critical banking and investment operations.
- Analyzed threats using SIEM tools, identifying APTs and reducing financial fraud exposure by 40%.
- Strengthened network security controls, firewall configurations, and zero-trust security architecture, reducing unauthorized access attempts and minimizing risks associated with insider threats and privilege escalation.
- Automated vulnerability scanning, patch management, and security compliance tracking, reducing critical vulnerabilities and ensuring adherence to industry regulations such as NIST, ISO 27001, PCI DSS, and SOC 2.
- Developed cloud security policies for AWS environments, implementing IAM best practices, role-based access controls, and continuous monitoring to mitigate risks associated with cloud misconfigurations and external threats.
- Investigated phishing attacks, malware infections, and ransomware incidents, applying forensic techniques to identify malicious actors, contain breaches, and prevent future exploitation of financial data.
- Performed penetration testing, identified high-risk vulnerabilities, and ensured customer data protection and system resilience.
- Collaborated with cyber risk, fraud detection, and compliance teams, preventing fraudulent transactions and mitigating cyber threats, reducing financial losses and strengthening overall enterprise security.

Groovy Web, India | Cyber Security Analyst **Jun 2020 - Dec 2022**

- Secured networks with OSPF, BGP, and firewalls, reducing unauthorized access and enhancing cybersecurity resilience.
- Conducted penetration testing using Nessus, OpenVAS, and Metasploit, identifying and remediating high-risk vulnerabilities, ensuring critical IT assets remained protected against evolving cyber threats and security exploits.
- Created incident response playbooks, automated threat detection, and SOC procedures, reducing cyber attack response time 45%.
- Strengthened security compliance adherence to NIST, ISO 27001, and PCI DSS, implementing best practices and enforcing security policies that safeguarded sensitive data and reduced compliance-related risks.
- Monitored network traffic using Wireshark and TCPDump, identifying anomalies, detecting malicious activities, and mitigating cybersecurity risks associated with unauthorized data exfiltration and suspicious network behavior.
- Implemented AWS security, IAM least-privilege policies, and monitoring, reducing misconfigurations to enhance cloud security.
- Provided cybersecurity awareness training to employees, mitigating social engineering risks, phishing attacks, and human error-related security breaches that could compromise organizational security.

EDUCATION & CERTIFICATIONS

Master of Science in Cybersecurity **Dec 2024**

California State University Dominguez Hills Carson, California

- **CompTIA Security Analytics Plus (CompTIA SA+)**
- **Cisco Certified Network Associate (CCNA)**