UMESHCHANDRA SAGAR

9407584943 | aravindsagar4510@gmail.com | www.linkedin.com/in/sugur-umeshchandra-sagar

PROFESSIONAL SUMMARY

- **CEH-certified cybersecurity professional** with expertise in **threat detection, incident response, vulnerability management, and security operations.**
- Proficient in analyzing security events using **SIEM tools**, conducting penetration testing, and strengthening system defenses through **secure configurations and risk assessments**.
- Adept at developing **security policies**, automating **threat intelligence** processes, and conducting **forensic investigations** to minimize security risks
- Strong background in **cloud security, blockchain security, and compliance auditing**, with a proven ability to collaborate with cross-functional teams to implement effective cybersecurity solutions.

EDUCATION

- **Masters in Cybersecurity** **Aug 2023 - present**
- *University of North Texas*
- GPA: 4.0
- Relevant Coursework: Cybersecurity Essentials, Computer Forensics, Secure Electronic Commerce, Secure Software Development, Introduction to Computer Security, Blockchain and Applications, and Wireless Networks and Protocols.

- **Bachelor of Technology in Computer Science & Engineering** **July 2018 – May 2022**
- *Malla Reddy College of Engineering and Technolog*y
- CGPA: 8.48
- Relevant Coursework: Cybersecurity, Data Structures, Artificial Intelligence, Big data, C, C++, Java, Python, and so on.

WORK EXPERIENCE

Security Analyst Intern Nov 2024 –Present

Johnson & Johnson, New Brunswick, New Jersey, US

- Analyzed 250+ security alerts weekly using SIEM tools, identifying and mitigating threats with a 95% accuracy rate.
- Assisted in conducting vulnerability scans across 100+ endpoints, reducing critical security risks by 40%.
- Investigated and responded to 20+ phishing attacks monthly, improving incident resolution time by 30%.
- Contributed to security awareness training, increasing employee phishing detection rates by 35%.

Computer Lab Assistant – Team Lead Aug 2023 – Nov 2024

Academic Technologies, University of North Texas

- Managed a team of 40+ lab employees, overseeing daily operations and ensuring the security of systems and infrastructure.
- Resolved over 50+ technical issues monthly, achieving a 95% resolution rate within a 2-day SLA.
- Developed and implemented efficient troubleshooting procedures, reducing system downtime by 20%.
- Trained 40+ team members on cybersecurity best practices and secure IT operations.

SOC Analyst May 2022 – July 2023

Synechron Technologies, Hyderabad, Telangana, India

- **Monitored and analyzed 500+ security alerts daily** using **SIEM tools like Splunk**, identifying and mitigating potential threats with a **98% accuracy rate.**
- Conducted **vulnerability assessments** using **Nessus** and **NMAP**, uncovering and mitigating critical vulnerabilities across organizational systems, reducing potential exploit risks by **40%.**
- Investigated and responded to **100+ phishing email** incidents monthly, utilizing **Open Source Intelligence (OSINT)** tools to block malicious domains, IPs, and URLs.
- Performed **log analysis** to identify suspicious activities and code anomalies, **resolving 75% of security events** during initial investigation without escalation.
- Collaborated with cross-functional teams to develop incident response plans, reducing **mean time to detect (MTTD)** and **mean time to respond (MTTR) by 20%.**
- Enhanced endpoint security by implementing detection rules and configuring **Intrusion Detection Systems (IDS)** and **Intrusion Prevention Systems (IPS)**, **reducing false positives by 30%.**

- Assisted in the development and delivery of security awareness training programs, improving employee phishing awareness rates by 25%.
- Led post-incident analysis and reporting, ensuring continuous improvement of SOC processes and policies, resulting in a 15% increase in threat containment efficiency.

Cybersecurity Intern Dec 2021 – May 2022

Synechron Technologies, Hyderabad, Telangana, India

- Assisted in security policy implementation, ensuring compliance with organizational standards.
- Conducted malware analysis on suspicious files, identifying and neutralizing 50+ potential threats.
- Researched emerging cyber threats and contributed to threat intelligence reports for the security team.
- Responded to security tickets, troubleshooting access control issues, data security concerns, and network vulnerabilities.

PROJECTS

Blockchain Smart Contract Development and Testing Aug 2024 – Dec 2024

- Configured and deployed 5+ smart contracts locally using Foundry, Anvil, and Ganache.
- Created a Vite-based interface for token operations and ownership controls, facilitating over 100 secure blockchain interactions weekly through seamless MetaMask integration.
- Conducted 10+ functional tests to ensure reliable contract performance, increasing deployment efficiency by 30%.

Tools & Technologies: Foundry, Anvil, Ganache, Metamask, Solidity, TypeScript, Vite

Simulated Ransomware Attack Using Phishing Emails Jan 2024- May 2024

- Designed a ransomware simulation using phishing emails, executing 100+ email campaigns to understand detection, mitigation, and recovery processes.
- Analyzed the attack's impact, identifying vulnerabilities, and proposed preventive measures that reduced future attack risk by 40%.
- Implemented Watchdog, Pyinotify, and Scapy to monitor 500+ file changes and analyze 1,000+ network packets, successfully identifying and mitigating 95% of simulated ransomware threats in real-time.
- Automated ransomware simulation by creating encryption and decryption scripts, reducing manual execution time by 50%.

Tools & Technologies: Watchdog, pyinotify, Scapy, psutil, Python, Email Phishing Techniques

Secure E-commerce Store for Sneakers (CyberSneak) Aug 2023 – Dec 2023

- Implemented Multi-Factor Authentication (MFA), achieving a 30% reduction in unauthorized access incidents.
- Integrated a Stripe payment gateway for encrypted payment transactions, enhancing payment security by 40%.
- Used end-to-end encryption to protect private information throughout more than 100 transactions, resulting in zero data breaches and a 25% increase in consumer trust.

Tools & Technologies: Multi-Factor Authentication (MFA), Stripe Payment Gateway, Encryption Protocols, Web Security Practices

SKILLS

Security Operations: SIEM (Splunk), IDS/IPS, Endpoint Security, Incident Response
Threat Intelligence & Monitoring: Log Analysis, Threat Hunting, Malware Analysis, Phishing Mitigation
Vulnerability Management: Nessus, Nmap, Penetration Testing, Risk Assessments
Security Engineering: Secure Configurations, Firewalls, IAM, Cloud Security (AWS, Azure)
Compliance & Documentation: Security Policies, Incident Reports, Security Awareness Training
Development & Automation: Python, Bash, PowerShell, Scripting for Security Automation
Blockchain Security: Smart Contracts, Cryptography, Web3 Security

ADDITIONAL SKILLS

- 3D Modelling
- Game Development

CERTIFICATIONS

- Certified Ethical Hacker (CEH) v13
- CompTIA Security+
- Splunk Core Certified Power User
- AWS Cloud Practitioner