Siddartha Darisi

Cyber Security Analyst

CONTACT

Phone: +1 (209) 222-3177
Email: siddarthajobs1@gmail.com
Location: New York, NY

EDUCATION

Master of Science in Cyber Security & Privacy
New Jersey Institute of Technology, NJ

Bachelor of Technology in Computer Science & Engineering
Koneru Lakshmaiah Education Foundation, India

SKILLS

Networking Protocols:
TCP/IP, HTTP, DNS, SMTP, FTP, SSH, SNMP, RDP, IPsec, WPA/WPA2/WPA3, NetFlow and IPFIX

Security Tools:
SIEM, Splunk, LogRhythm, MISP, OpenVAS, Cisco ASA, FTK, BitLocker, VeraCrypt, Metasploit, Nmap, Nessus, Wireshark, Qualys

Cloud Technologies:
AWS Lambda, Amazon VPC, AWS GuardDuty, Azure sentinel

Other Skills:
Network Protocol Security, Cryptography and Security, Internet and Higher-Level Protocols, Computer Security Auditing, Threat & Vulnerability Management, Risk management, Firewalls, Border Gateway Protocol, Switches, Information Assurance, Penetration Testing & Countermeasures, Cloud Deployment

CERTIFICATION

- AWS Certified Solutions Architect Associate
- CompTIA Security+
- Certified Ethical Hacker(V12) from Ec-Council
- Brainnest Cyber Security Industry Training

Summary

- Accomplished Cybersecurity Analyst with over 3, in threat mitigation, network security protocols, and cloud infrastructure, consistently delivering results in fast-paced environments and strengthening organizational cybersecurity postures.
- Proficient in networking protocols such as TCP/IP, HTTP, DNS, SMTP, FTP, SSH, SNMP, RDP, IPsec.
- Skilled in utilizing SIEM tools including Splunk and LogRhythm for real-time anomaly detection.
- Conducted exhaustive threat analysis, unearthing latent malware instances for enhanced security.
- Proven track record of curbing lateral threat movement through Cisco ISE network segmentation.
- Proficient in vulnerability assessment tools such as OpenVAS, Nmap, and Nessus.
- Skilled in cloud security, deploying AWS Lambda, Amazon VPC, and GuardDuty and also Azure sentinel.
- Committed to compliance and risk management, achieving a 15% increase in audit scores.
- Strong documentation and communication skills, improving policy adherence.

Experience

Cognizant, NJ **Sept 2022 - Current**

Cyber Security Analyst

- Spearheaded strategic initiative to enhance global manufacturing sector's incident response capabilities for rapid threat containment and mitigation.
- Customized Splunk correlation rules for real-time anomaly detection across data streams.
- Leveraged Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) configurations to proactively identify and mitigate potential threats, enhancing security resilience by 40%.
- Implemented AWS GuardDuty for real-time threat detection, contributing to a 25% reduction in potential cloud security breaches.
- Conducted exhaustive analysis of historical data using specialized threat intelligence feeds, discovering latent malware instances that had previously evaded detection.
- Successfully neutralized a remarkable 80% of identified threats through prompt incident response and well-coordinated mitigation measures, significantly bolstering security posture.
- Collaborated closely with cross-functional teams to design and enforce robust Identity and Access Management (IAM) policies, ensuring stringent control over system access.

Wipro, India **Oct 2019 - Dec 2021**

Cyber Security Analyst

- Strengthened e-commerce cybersecurity, cutting successful phishing attacks by 20%.
- Utilized Proofpoint email security for advanced anti-phishing defenses.
- Reduced user-reported suspicious emails by 25% through awareness campaigns.
- Employed Cisco ISE for network segmentation, curbing lateral threat movement by 30%.
- Identified and resolved 40% of critical vulnerabilities with OpenVAS and Rapid7.
- Implemented comprehensive Endpoint Security measures, deploying tools like CrowdStrike to reduce malware incidents by 40%.
- Achieved 15% compliance score increase through comprehensive audits.
- Improved policy understanding and adherence by 20% through clear documentation.
- Demonstrated expertise in advanced email security, network segmentation, and compliance measures for robust e-commerce cybersecurity.