AKSHAY GALGALI

Dallas, TX | +1 469-922-8892 | agalgali@cougarnet.uh.edu | GitHub | LinkedIn | Portfolio

PROFESSIONAL EXPERIENCE

Wireless Security Engineer, Simnovus Corporation - Cary, North Carolina **Jan 2023 - Jan 2024**

- Deployed Sophos XGS firewall within company's IT framework, fortifying the network's security by configuring and enforcing sophisticated firewall rules, this measure aimed to the safeguard sensitive information ensuring a resilient defense against potential cyber threats.
- Enhanced Security Operations through proactive threat detection, incident response, and vulnerability management; reduced average incident response time by 40% and increased threat detection rate by 25%.
- Collaborated with cross-functional teams to implement and optimize cloud-based solutions, contributing to increased operational efficiency and
- scalability. Proficiently utilized cloud service providers, including AWS and Azure, to architect and deploy robust infrastructures.
- Orchestrated seamless end-to-end project management, utilizing JIRA and Confluence, to enhance workflow efficiency; skillfully managed ticket workflows and delivered comprehensive technical insights, resulting in a 30% reduction in project execution time.

Wi-Fi Engineer (Instructional Assistant), University Information Technology - Houston, Texas **Sep 2022 - Jan 2023**

- Conducted a network and security audit by leveraging Ekahau data capture files seamlessly integrated with Aruba Central tools. This comprehensive audit successfully identified and remediated 40 rogue access points, thereby optimizing both the performance and security parameters of the network infrastructure.
- Revitalized campus-wide wireless infrastructure through strategic evaluation, redesign, and installation, optimizing performance, security, and seamless integration with existing networks.
- Performed an in-depth examination and analysis of the campus network, spanning across two data centers and 6500 access points. This strategic assessment facilitated the effective collection of crucial evidence and played a pivotal role in the successful implementation of the NIST (SP) 800-207 Zero-Trust Architecture framework.
- Contributed to the migration to cutting-edge 802.11ax Wi-Fi technology across diverse campus facilities, including a large-scale basketball arena, over 6,000 dormitory rooms, 500-person auditoriums, and high-density library and study areas.

KEYSKILLS

Programming Languages and Scripting: Golang, Python, C, Shell / Bash Scripting, JavaScript, JSON, HTML5, CSS, PHP.
Networking and Routing: TCP/IP, UDP, SSH, OSPF, FTP, HTTP/HTTPS, ARP, ICMP, TLS, VLAN, VPN, DNS, DHCP, ICMP, VoIP, TUN/TAP, Network Namespace, IP Subnetting, Network Slicing, IDS, Firewall (Cisco, Azure, Sophos).
Networking Devices: Routers, Switches, Access Points.
Information Security Techniques: CIA Triad, Intrusion Prevention System, Zero Trust, Cloud Security, Risk Management, Secure coding, SOC, IAM.
Tools: Wireshark, Nmap, Burp Suite, Metasploit, Snort, Kibana, Docker, MobaXterm, VMWare, VirtualBox, Putty, PyCharm, Git, EDR, Fiddler.
Standards, Frameworks: NIST Cybersecurity Framework, SOC2, ISO 27001/2, PCI DSS, HIPAA, CIS.
Cloud Computing: AWS, Microsoft Azure, IaaS, PaaS, SaaS.
Interpersonal Skills: Teamwork, Active Listening, Critical thinking, Leadership, Conflict Management, Problem solving, Communication.
Professional Certification: CISSP Aspirant, ISC2 Certified in Cybersecurity, Google Cybersecurity Professional.

EDUCATION

Master of Science in Cybersecurity | GPA: 3.93/4 **Aug 2021 - May 2023**
University of Houston, Texas
Relevant Coursework: Network Security, Security Operations Center, Applied Cryptography, Cybersecurity Risk Management, Project Management, Secure Enterprise Computing, Industrial Control Systems Security, Critical Thinking in Info-Sec.

Bachelor of Engineering in Information Technology | CGPA: 8.76/10 **May 2018 - Jun 2021**
Mumbai University, India
Relevant Coursework: Digital Forensics, Python Programming, Wireless Networking, Artificial Intelligence, Cryptography, Network Security, Security Labs, Data Structures and Analysis, Database Management System, Cloud Computing.

PUBLICATIONS

- SOC - Setup, Responsibilities and Accomplishments | Read
- Mitigating Cybersecurity threats to Industrial Control Systems: SCADA | Read
- Cybersecurity Risk Management - Risk Management Plan for an IT Firm | Read
- Analysis of APT [Advance Persistence Threat Group] And its Impact on the Organization | Read

ACADEMIC PROJECTS

Implementing Incident Prevention Plan | Kibana, VMs, IRP **|** GitHub, Report
Devised and executed an incident prevention plan for HR-operated system exhibiting suspicious behavior, leveraging Kibana for in-depth analysis of alerts, windows logs, and network traffic. Presented comprehensive mitigation strategies and preventive measures.

Packet Injection in Industrial Control System | Modsak Simulator, VMs, Shell Scripting **|** GitHub, Report
Simulated a MODBUS attack & Packet Injection attack in Industrial Control System in a Master-Slave environment using Modsak Simulator to assess the vulnerabilities and risks in Industrial Control System and how to mitigate and prevent the attack.

Advanced Keystroke Logger | Python Scripts, VMs, Python Libraries **|** GitHub
Developed a keystroke logger in an active browser using python scripting and libraries, to retrieve sensitive information, and credentials of a user like a username, passwords, card details, these credentials and URL information is sent via email to the attacker.