PRASANTH K

SECURITY ANALYST

Mobile : +91 9495778177
Mobile : +91 9895701119
Email : prasanthkgd@gmail.com

Linkedin : in.linkedin.com/in/prasanthc41m
Github : github.com/prasanthc41m
Blog : prasanthc41m.medium.com

A seasoned and accomplished cybersecurity professional with over a decade of experience in the IT industry. With 3 years of dedicated experience in cybersecurity and a proven track record of identifying and reporting vulnerabilities, I have the skills, knowledge, and drive to tackle complex security challenges. My expertise in systems, networks, and security combined with my certifications and volunteer work demonstrates my commitment to staying current in the ever-evolving field of cybersecurity.

EXPERIENCE

Freelance - JAN 2022 to Present
Designation: Security Analyst

- Configuring and monitoring Security Information and Event Management (SIEM) platform for security alerts.
- Ongoing review of SIEM dashboards, system, application logs, and custom monitoring tools.
- Monitor the organization's networks for security breaches and investigate a violation when one occurs.
- Investigate, document, and report on information security issues and emerging trends.

EHACKIFY CYBERSECURITY RESEARCH AND TRAININGS, TIRUR, KERALA - JAN 2020 to JAN 2022
Designation: Security Researcher

- Adept at designing customized training programs and courseware to meet the needs of students and organizations and ensure courses and skills are up to date with current standards.
- Develop and deliver security awareness and training programs.
- Build, install and maintain LMS, Labs, etc for training.
- Designed Security CTF competitions.

REDTEAM CYBERSECURITY LABS LLP, CALICUT, KERALA - JAN 2018 to MAR 2019
Designation: Security Analyst

- Scan and monitor system vulnerabilities on servers and infrastructure devices using a Threat and Vulnerability security solution.
- Expertise in SAST and DAST web application security testing.
- Doing Vulnerability Assessment and Penetration testing.
- Skilled in pentesting and remediating to patch vulnerabilities.
- Capable of internal and external pentesting.
- Skilled in vulnerability assessment and detailed report writing.
- Be a part of building secure IT infrastructure for ISO 27001 audit.

ANUPAMA GROUP OF INSTITUTIONS, BANGALORE, KARNATAKA - JUN 2016 to OCT 2017
Designation: System Administrator

- Managed Endpoint securities, Firewalls, etc
- Maintained computers, printers, scanners, and network for the entire institute.
- PC maintenance, including, setting up accounts and establishing network and peripheral connections.
- Taught computers skills to staff at the institute.
- Helped set up and maintain routers. Built and maintained mobile labs and desktop labs.
- Maintained all Windows Servers in the institute.
- Researched new programs to be introduced into the institute.

MALANAD CO-OPERATIVE SOCIETY, KASARAGOD, KERALA - DEC 2013 to APR 2016

Designation: System Administrator

- Secure the endpoints from viruses and ransomware with antivirus solutions and backups.
- PC maintenance, including, setting up and establishing network and peripheral connections.
- Coordination with vendors for IT Components purchasing.
- Providing solutions to technical service issues from users to ensure the highest possible user satisfaction.
- Troubleshooting and Coordinating with ISP of broadband connections.
- Researched new programs to secure the entire IT infrastructure.

ACHARYA INSTITUTE OF MANAGEMENT & SCIENCE, BANGALORE - SEP 2012 to NOV 2013
Designation: Assistant System Admin

- Managed all Firewalls, wireless, network routers/switches.
- Maintained Macintosh computers, printers, scanners, and network for the entire institute.
- PC maintenance, including, setting up accounts and establishing network and peripheral connections.
- Managed student repair groups, overseeing repairs, updates, and maintenance of computers.
- Managed technical help desk, responding to help requests from the institute.
- Trained all new computer technicians for the institute.
- Maintained all Windows Servers and Mac Servers in the institute.
- Researched new programs to be introduced into the institute.

MAGNUS TELECOMMUNICATIONS PVT LTD, COCHIN - MAR 2009 to JAN 2012
Designation: Network Engineer

- Monitoring of the lease lines connectivity, E1 lines, dial-up circuits, wireless connectivity and maintaining interoffice LAN/WAN connectivity and troubleshooting.
- Coordination with vendors for IT Components purchasing. Providing solutions to technical service issues from users to ensure the highest possible user satisfaction.
- Providing solutions to technical service issues from users to ensure the highest possible user satisfaction.
- Providing solutions to technical service issues from users to ensure the highest possible user satisfaction.
- Knowledge of LAN, MAN, WAN network infrastructure and Ethernet as well as Serial technology. Knowledge of OSI Layers.
- Troubleshooting of Leased line and ISDN.
- Knowledge of routers, switches & hubs.

ENIAC SYSTEMS, **KASARAGOD, KERALA** – APR 2007 to SEP 2008
Designation: Maintenance Engineer

- Removing spyware, ad-ware, key- loggers and other malware manually.
- Troubleshooting critical system and network problems.
- Installation and maintenance of OS like Windows XP and Ubuntu etc.
- Coordinating daily sales and service to customers.
- Creating a day-to-day customer service report.
- Visiting client places for troubleshooting critical/escalated issues.
- Maintenance of all the desktops, printers and other hardware.
- To handle all IT functions such as installation, networking, and Desktop support and LAN management.
- Assembling, Troubleshooting and Rectifying the Systems and Network Problems at Customer Site.
- Securing desktops and Denying launch of unauthorized or prohibited applications.
- Hardware and Software troubleshooting.

TECHNICAL/JOB SKILLS

- Good understanding and experience in SIEM tools (Splunk, QRadar, Sentinel), which includes log analysis, Flow analysis, incident investigation, reporting and experience in managing rules.
- Experienced in creating runbook/ Incident response plans according to the use case and customer infra/policies.
- Incident Handling - Carries out in-depth analysis (Like Analyzes running processes and configs on affected systems) to find the perpetrator, the type of attack, and the data or systems impacted. Creates and implements a strategy for containment and recovery.
- Experienced in Microsoft Azure/Cloud Security(E5) solutions- Includes Sentinel, Defender for O365, Defender for endpoints, MCAS- All were Addresses real security incidents. Evaluates incidents identified by Level- 1 analysts.
- Experienced in analysis of O365/Exchange logs, which includes- spam event thread logs, Internal email protect logs, URL protect logs, attachment protect logs.
- Experienced and closely worked with Identity & Access management team for ensuring the improvement of identity and access management processes, controls and communications related to Policies across the organization.
- Better Understanding of network security tools and the security functionality of these tools, such as Firewalls, web application firewalls, intrusion detection/prevention systems, and web proxies-Oversee the functionality of network security systems to ensure security policies are being withheld including internet browsing restrictions and software downloads, Responsible for maintenance and monitoring of security systems and change management process on security systems.
- Excellent coordination skill- Ensure collaboration of all supporting/responsible teams to mitigate threats
- Managed to send daily, weekly and monthly reports to clients in all format according the requirements
- Better understanding of all security products - FW, AV/EDR, IPS/IDS, Proxy, WAF, Exchange, VM tools.
- Experienced to manage all deliverables on time
- Able to learn and handle special requirements from customers.

SECURITY TOOLS

- Splunk, QRadar and Sentinel - Enterprise SIEM
- Microsoft Defender, Symantec, Sophos - Monitoring of virus/malware alerts using Antivirus/EDR
- FortiGate - Enterprise Perimeter/FW system
- Microsoft Cloud App Security - Real time monitoring of Cloud Apps
- Nessus, OpenVAS - Vulnerability scanning solution
- MHN - Centralized server for management and data collection of honeypots
- Kali Linux - Pentesting softwares.

EDUCATION

- Bachelor of Computer Application, 2014 from Dr. C. V. Raman University with 80% marks.
- Plus Two (Science Group), Board of Public examination Kerala 2004 from GHSS Balanthode with 61% marks.
- SSLC (10th) Kerala State Board 2002 from Government Higher Secondary School Balanthode with 59% marks.

TRAINING AND CERTIFICATIONS

- EC-Council Certified Security Analyst (ECSA V9) - Feb 2019 - Feb 2025
- Certified Security Analyst (CSA) - 2018
- Apple Certified Support Professional 10.7 (ACSP) - Jul 2012
- Certified Arcos PAM Implementor (CAPI)
- Cisco Certified Network Associate (CCNA)
- Microsoft Certified Systems Engineer (MCSE)

VOLUNTEER EXPERIENCE

Volunteer
Kerala Police Cyberdome, 2020 - Present

Chapter Leader
OWASP Kannur Chapter, 2021 - 2023

ACHIEVEMENTS

CVE-2020-5842 - *Codoforum 4.8.3 allows XSS in the user registration page*
Exploit Database GHDB - GHDB-ID: 5689
Exploit Database Exploit - EDB-ID: 47876

CONFERENCES

OWASP Kannur Chapter hosted multiple events in 2022
OWASP Kannur Chapter - *Organized*

Cyber Security Summit 2021 “Real Time Real Attack”
Kerala Police Cyberdome Kozhikode - *Technical support*

Retrain-2021, Adversary Emulation - A Practical Approach
eHackify Cybersecurity Research & Trainings - *Organized*

Redteam Security Summit-2018, Cyber Security & Hacking Conference
Redteam Hacker Academy - *Technical support*

INTERESTS

Reading blogs and articles, bug-hunting, creating CTFs, supporting and contributing to the cybersecurity community and more.