Godson Chittilapilly

Grzybowska 9, Warszaw, Mazovian • 729686565 • info@godsonchittilapilly.tech • linkedin.com/in/godson-chittilapilly-473894212 • godsonchittilapilly.tech

Cyber Security Engineer

Experienced and dedicated Cyber Security Specialist with a diverse background in SOC operations, incident response, and technical support. With a strong foundation in monitoring, detecting, and mitigating cyber threats, I excel at utilizing advanced security tools and technologies to safeguard organizational assets. My technical expertise is complemented by a hands-on approach to troubleshooting and support, developed through roles at Foundever, BNY Mellon, Brainotech IT Solutions, and Cybersoft Infosys. Proficient in a wide range of programming languages and security practices, I am committed to continuous improvement and staying abreast of emerging cyber threats. Visit my website at godsonchittilapilly.tech for more information.

WORK EXPERIENCE

CYBEROO • 03/2023 - Present
Cyber Security Engineer (SOC L2)

- Monitoring and Detection: Actively monitor logs, traffic, and alerts to spot potential breaches. Analyze and investigate incidents for severity and impact.

- Incident Response: Promptly respond to incidents, initiate procedures, and contain, eradicate, and recover. Conduct forensic analysis for root cause.

- Threat Intelligence: Stay updated on threats, use feeds and forums, identify emerging risks, and adjust controls accordingly.

- Security Tools and Technologies: Utilize SIEM, IDS/IPS, firewalls, and vulnerability scanning tools. Maintain for optimal performance and accurate threat detection.

- Security Incident Analysis: Analyze incidents deeply, examining logs, traffic, and data for anomalies. Identify compromise indicators and assess breach extent.

- Vulnerability Management: Conduct assessments and tests, prioritize and remediate weaknesses based on severity.

- Hands-on experience with implementation of Microsoft DLP technology across a large enterprise

- Continuous Improvement: Proactively identify areas for enhancement, make recommendations, optimize procedures, and increase operational efficiency.

- Expertise in Cloud Data Protection using MCAS

- Administration of the DLP tools to include configuration of policies, upgrading, patching etc.

- Implementation of proactive measures to enhance accuracy and effectiveness of Data Security tools.

- Experience to troubleshoot Microsoft DLP, AIP and MCAS issues

Foundever · 08/2022 - 02/2023
Support Specialist

- Update customer data and produce activity reports.
- Perform remote troubleshooting through diagnostic techniques and pertinent questions.
- Determine the best solution based on the issue and details provided by customers.
- Walk customers through the problem-solving process.

BNY Mellon · 07/2022 - 12/2022
Cyber Security Specialist (TRM)

- Detect insecure features and malicious activities within our networks and infrastructure. Implement customized application security assessments for client-based asset risk, corporate policy compliance as well as conduct vulnerability assessment. advanced understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, OSI model, defense-in-depth and common security elements.

Brainotech IT Solutions GmbH · 02/2022 - 03/2022
Technical Support Engineer

- Set up hardware
- Install software
- Maintain and repair technological equipment
- Manage software in computers and networks
- Ensure privacy and data protection
- Perform regular upgrades
- Perform troubleshoot activities
- Install well-functioning LAN/WAN and other networks
- Manage network components (servers, IPs, etc.)
- Manage and implement security solutions
- Create records of repairs and fixes
- Provide technical support
- Train and collaborate with other team members

MR technologies · 06/2020 - 10/2021
Full-stack Developer

- Focused on Android application development with flutter.
- Modifying software to fix errors, adapt it to new hardware, improve its performance, or upgrade interfaces.

- Directing system testing and validation procedures.
- Directing software programming and documentation development.
- Consulting with departments or customers on project status and proposals.
- Working with customers or departments on technical issues including software system design and maintenance.
- Analyzing information to recommend and plan the installation of new systems or modifications of an existing system.
- Consulting with engineering staff to evaluate software hardware interfaces and develop specifications and performance requirements.
- Designing and developing software systems using scientific analysis and mathematical models to predict and measure outcomes and design consequences.
- Preparing reports on programming project specifications, activities, or status.
- Conferring with project managers to obtain information on limitations or capabilities.
- Successfully led a project that developed a high-performance Android application using Flutter, resulting in a 30% increase in user engagement and a 25% improvement in app performance metrics.

Cybersoft infosys · 03/2017 - 03/2020
On-site
Technical Support Engineer

- Research and identify solutions to software and hardware issues
- Diagnose and troubleshoot technical issues, including account setup and network configuration
- Ask customers targeted questions to quickly understand the root of the problem
- Track computer system issues through to resolution, within agreed time limits
- Talk clients through a series of actions, either via phone, email or chat, until they've solved a technical issue
- Properly escalate unresolved issues to appropriate internal teams (e.g. software developers)
- Provide prompt and accurate feedback to customers
- Refer to internal database or external resources to provide accurate tech solutions
- Ensure all issues are properly logged
- Prioritize and manage several open issues at one time
- Follow up with clients to ensure their IT systems are fully functional after troubleshooting
- Prepare accurate and timely reports
- Document technical knowledge in the form of notes and manuals
- Maintain jovial relationships with clients

EDUCATION

Masters in Business Management
WSPIA • Warsaw

Bachelor of Science - BS in Computer Science
Anna University Chennai

CERTIFICATIONS

AZ-900 • 06/2024 - Present
Microsoft

Ethical Hacking with Javascript • 05/2024 - Present
LinkedIn

Network Security Support Engineer • 05/2024 - Present
Fortinet

OSINT : Content Discovery • 03/2024 - Present
LinkedIn

Reverse Engineering : Frida • 02/2024 - Present
EC-Council

Certified In Cyber Security • 02/2024 - Present
ISC2

Java : Data Structures • 05/2023 - Present
LinkedIn

Full Stack Web development • 01/2022 - Present
Udemy

PROJECTS

DLP (Insider Threat)
Self Project

The **Insider Threat Detection System** is a Data Loss Prevention (DLP) solution designed to detect unauthorized attempts to photograph a computer screen. The system uses algorithms embedded within the user's work laptop or PC to monitor for camera activity or changes in screen brightness that indicate a potential screen capture. If a camera or phone is detected attempting to take a picture, the system immediately triggers an alert, sending real-time notifications to the company's security monitoring team. The system can also log the event for further investigation and integrate with existing security tools.

SKILLS

Active Directory, Adaptability, Collaboration, Communication, Continuous Learning, CSS, Customer Service, Cybersecurity, Cyber Security, Cybersecurity Trends, Cyber Threat Intelligence, Data Protection, Documentation, Domains, English, Ethical Hacking, Firewalls, Flutter, Frida Toolkit, Full-stack Development, HTML, IDS/IPS, Incident Response, Information Technology, Java, JavaScript, JSON, Languages, Leadership, Malayalam, Metasploit, Microsoft Products, Networking, Networking Protocols, Network Scanning, Network Security, Other, Participation in Cybersecurity Forums, Penetration Testing, Problem-solving, Professional Development, Programming Languages, Project Management, Python, Python-nmap, REST APIs, Reverse Engineering, Scapy, SIEM, SOC Operations, Software Development, Software Installation, Splunk, SQL, TCP/IP, Teamwork, Technical Support, Time Management, Tools, Troubleshooting, VirtualBox, VMware, Vulnerability Management, Vulnerability Scanning Tools, Windows Server, XML