Dyapa Rajashekar Reddy

Linkedin | +91 8897406945 | Rajashekardyapa16@gamil.com

EDUCATION

GITAM University, Bengaluru, India **GPA 6.94**
Bachelor of Technology in Computer Science and Engineering **Jun 2020 – May 2024**

Coursework: *Programming with Python, DBMS, Java, Operating Systems, Design and Analysis of Algorithms, Data Structures & Algorithms, Computer Organization & Architecture, Cryptography and Network Security.*

TECHNICAL SKILLS

SIEM Tools:	Splunk Enterprise, Enterprise Security, FortySIEM.
EDR:	Falcon Crowd strike
Incident Analysis Tools:	CISCO Talos, Mx Toolbox, Virus Total, IBM-Xforce.
Vulnerability Management:	Nessus
Ticketing Tool:	Service Now
Web Technologies:	HTML, CSS
Databases:	MySQL

EXPERIENCE

Intern | WorldSecTech|

- Monitoring the customer network using Splunk SIEM
- Act as first level support for all Security Issues
- Analyzing Realtime security incidents and checking whether its true positive or false positive
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events.
- Raising true positive incidents to the respective team for further action
- Creating tickets on service now and assigning it to the respective team and taking the follow-up until closure

Splunk Hands-on

- Managed and maintained Splunk's distributed architecture, ensuring seamless integration of various devices into the platform.
- Developed and optimized searches, reports, and dashboards to deliver actionable insights.
- Possess knowledge of implementing correlation rules to enhance monitoring and improve security posture.

Falcon Hands-on

- Leveraged Falcon EDR to analyze security incidents, ensuring timely detection and response.
- Created and managed policies to align with organizational security requirements.
- Applied knowledge of static and dynamic groups to enhance system organization and functionality.

PROJECTS

Splunk Multi-Cluster Home Lab

- Set up a multi-cluster Splunk environment using 3 systems (2 VMs and 1 local PC) for log monitoring and analysis.
- Installed **Splunk Forwarders** on two PCs to send logs to the **Indexer**, which parsed and indexed the data. Used the **Search Head** for real-time log search and visualization.
- Gained hands-on experience with **Splunk Forwarders**, **Indexer**, and **Search Head** in a distributed architecture.
- Simulated a real-world log management and monitoring solution with centralized data collection.

Honeypot Deployment Using Modern Honey Network (MHN)(Ongoing)

- Setting up and managing a honeypot system using MHN on a virtual machine to monitor cyber threats.
- Deployed Cowrie (SSH/Telnet) and Dionaea (Malware) honeypots to log and analyze attack attempts.
- Configuring a web-based dashboard for real-time monitoring and threat intelligence.

Encryption and decryption of data using AES algorithm

- Successfully designed and developed a comprehensive project focused on securing data through encryption and decryption.
- Utilized the Advanced Encryption Standard (AES) algorithm to ensure robust data protection.
- Incorporated confidentiality, integrity, and availability (CIA) principles to enhance security practices.
- Delivered a solution that ensures efficient and secure data handling.

Certifications

- **Fortinet Certification**: Successfully completed the *Security Operations* certification from Fortinet.
- **SOC Expert Certification**: Earned the *Certified SOC Expert* credential from SIEM XEPERT,