DIVYA PARUCHURI

Phone: +91 8008556401
Email: divyaparuchuri1999@gmail.com

OBJECTIVE

To work efficiently and effectively both as individual and as a member of a team using innovative ideas and a creative approach to the task assigned. To have challenging position within an organization where my technical, analytical skills knowledge and experience in can be shared and enhanced.

PROFILE SYNOPSIS

A cyber security professional with 4 plus years of experience as a security analyst specializing in real-time threat monitoring, threat detection, security incident management, threat intelligence, Email security, Malware Analysis, handling customer tickets, Threat and incident handling.

PROFESSIONAL EXPERIENCE

WPP IT (Wire & Plastic Product) April 2023 – Present
Designation : Cyber Security Operation Analyst

- For the Inhouse SOC Operation of the WPP Global tenants, my responsibilities as part of the SOC team includes Security Incident Monitoring, Analysis, Reporting, and Mitigation of the security alerts and events triggered from SIEM, Endpoint security, and Email security products.
- To maintain the organization's security and integrity, an incident response strategy that incorporates both proactive and reactive steps must be created.
- Developing new custom detection criteria and using Microsoft's advance hunting platform to identify suspicious files and good hands-on experience managing MS Defender alerts, identifying malware, and mitigating threats by isolating impacted computers to stop lateral movement.
- Coordinating response effects together with IT and other security teams. delivering event updates and communicating with management or the client OPCOs in situations of urgency.
- Performing in-depth analysis on the escalated security incidents in the environments by coordinating with the Countercept MDR team (Managed Detection & Response).
- Adding IOCs and starting blocks in Microsoft Defender to start remedial actions on our environment and verifying IOCs from vendor inputs, security blogs, and threat intelligence reports.
- Monitoring and looking into MS Azure Sentinel alarms, such as unwanted access (impossible traveling, risky sign-ins), using Azure identity protection and Azure active directory logs
- In addition to the requirements of my daily job, there are a few important areas, such as the requirements for internal auditing, engineering improvements, use case refinement, scope of work (SOW), and advanced analysis of critical issues that have been highlighted with supporting artifacts for process changes.
- Transferred knowledge to trainee security engineers, kept an eye on their progress, and served as the point of contact for any questions about alert handling and ongoing processes.

HCL Technologies

Designation: Cyber Security Analyst Oct 2020 – Apr 2023

The Project is about to Endpoint security & SOC were working on various technologies & Monitoring and Analyzing Security Events. Using various security devices i.e. SIEM tool, IPS, Email Gateway, EDR, apart that works on Threat monitoring, Phishing Mail analysis.

- Being part of the Security Operation Centre (SOC) team primarily focuses on daily Tracking and Monitoring the alerts tracking and follow up for incident closure with concerned teams, stake holders.
- Troubleshooting, Log Analysis and deep analysis of Security alerts.
- Handling the security incidents which we receive from the SOC team
- Working & analysing the phishing mails using Different threat intel feeds.
- Maintaining High level of Confidentiality and Integrity
- Troubleshooting the definition, out-of-date and other AV related issues on the Server.
- Daily health check and doing Daily reports and act for outdated assets
- Creating Exceptions for the Clients that need to be excluded.

TECHNICAL EXPERTISE

- Email Security : Proofpoint
- SIEM Tools : Microsoft Sentinel, Splunk
- XDR : Microsoft Defender
- MDR : Countercept
- ANTIVIRUS : SOPHOS AV, McAfee
- Malware Analysis : Cisco Threat Grid
- Ticketing Tools : Service Now

CERTIFICATIONS

- Trained and certified NSE level 1 and 2
- Completed Splunk 7.x Fundamentals Part 1

EDUCATION

- Completed an undergraduate Degree in Electrical and Communication Engineering from Narayana Engineering College Gudur in 2020
- Intermediate in Mathematics from Narayan Junior College Gudur in 2016
- SSC from Ratnam High school in 2014
- Active Cyber Security Defense Certification from SOC Experts.

PERSONAL PARTICULARS

Permanent Address : 12/162, Gamalapalem street, Gudur, Andhra Pradesh, 524101.
Gender : Female
Date of Birth : 20/02/1999
Languages Known : English, Telugu, Hindi

DECLARATION

I hereby solemnly affirm that all details provided above are true to the best of my knowledge and belief.