Eswar Vadapalli

Cyber Security Analyst

91 7794015755 vadapallieswar353@gmail.com https://www.linkedin.com/in/vadapalli-eswar/

Summary

Cybersecurity Analyst with **4+ years of experience** in **threat detection, incident response, and security automation**. Expertise in **SIEM solutions (Splunk, Microsoft Sentinel), EDR tools (CrowdStrike, SentinelOne, Trend Micro apex), and cloud security (AWS, Azure)**. Successfully **reduced false positives by 30% in SIEM deployment**, improving efficiency and response times. Proficient in **forensic analysis, log correlation, and vulnerability management**.

Experience

AMAZON — **2023 April 17th**

SOC Analyst — Hyderabad

- Investigate and respond to **malware alerts, phishing attempts, and suspicious login activities** using **MS Defender, CrowdStrike, and SentinelOne**.
- Manage and optimize **SIEM solutions** (Splunk, Microsoft Sentinel) to enhance threat detection and incident response.
- **Reduced false positives by 30%** in SIEM, streamlining security alert management and improving analyst efficiency.
- Conduct **threat hunting and forensic investigations** to identify advanced attack patterns and mitigate risks.
- Develop and automate **security playbooks** to improve response workflows and incident handling.
- Perform **vulnerability assessments** and recommend security improvements to minimize risks.

Amazon — **2021 June 7th**

SOC Analyst L1 — Hyderabad

- Monitored **security events and analyzed logs** using SIEM tools like **IBM QRadar .**
- Investigated and contained **endpoint threats** using **Carbon Black and Cybereason**, identifying **high-risk attack vectors**.
- Assisted in **cloud security assessments** for **AWS and Azure environments**, ensuring compliance with security best practices.
- Created **custom detection rules** to improve threat intelligence and visibility across security tools.
- Configured and managed **firewalls and email security solutions** (Palo Alto, Zscaler, Proofpoint, Mimecast).

Quess Corp LTD , Client (AMAZON) — **February 2020 - July 2020**

Intern — Hyderabad

Perform log analysis & event by using SIEM Solution. Research, Documentation and Presentation on network security. Prepared Client Machines for users with Operating Systems, Software, antivirus and required utilities and mailing clients etc. Maintained records of hardware and software used in network. Conducted internal vulnerability assessments scan using Tenable & Nessus, NMAP for OS. Analyzed the scan results to determine potential vulnerabilities. Prepared Weekly, Bi-Weekly & Monthly reports.

Technical Skills

IBM QRadar, Splunk, Microsoft Sentinel ,CrowdStrike, SentinelOne, Carbon Black, Cybereason ,Palo Alto, Zscaler ,Proofpoint, Mimecast, Symantec ,Threat Hunting & Forensic Analysis , Incident Response & Log Analysis , Vulnerability Management & Risk Assessment

Education

Jawaharlal Nehru Technological University **2011 - 2015**
Mechanical Engineering B.Tech

Adikavi Nannaya University **2017 - 2019**
Bachelors in Physical Education B.P.Ed

Projects

SIEM Rule Optimization & False Positive Reduction

- Analyzed, refined, and optimized **SIEM correlation rules** in **Splunk & Microsoft Sentinel**, leading to a **30% reduction in false positives**.
- Developed **custom detection rules** and **use-case enhancements**, improving **detection accuracy** and reducing **analyst workload**.
- Integrated **log sources from AWS and Azure**, increasing **visibility into cloud security events** and enhancing **threat hunting** capabilities.

Automated Threat Hunting with EDR & SIEM

- Designed an **automated threat-hunting workflow** integrating **CrowdStrike EDR and IBM QRadar** for advanced **malware detection**.
- Implemented **automated alert triage**, reducing **incident response time by 40%**.
- Developed **playbooks** to automate investigation and **containment of endpoint threats**, improving **SOC efficiency**.

Certifications

AWS Certified Security – Trained

Microsoft Azure AZ-900 – Trained

Soft Skills

Soft Skills
Problem-Solving & Critical Thinking, Team Collaboration & Communication, Incident Handling & Decision-Making, Process Optimization & Automation