V S TEJANANDA

Mobile: +91 – 9113613388 **Email:** tejananda2048@gmail.com **LinkedIn**: teja-nanda-v-s

Achievement – oriented professional with expertise to utilize a wealth of knowledge in cybersecurity, particularly in Incident Response and Risk Management, to contribute effectively to the technology sector in Bangalore, enhancing Security Measures and Protocols.

Profile Summary

- **Security Analyst with nearly 2 years**, skilled at quickly identifying, investigating, and mitigating security incidents to safeguard organizational assets and ensure operational continuity in a dynamic threat landscape.
- Expertise in utilizing cutting-edge SIEM platforms like **IBM QRadar** and **Microsoft Sentinel** to analyze security event data, identify anomalies, and respond effectively to potential cyber threats.
- **Successfully preventing** and resolving phishing attacks and malware incidents through comprehensive analysis, sandboxing, and real-time response, ensuring minimal risk to business operations.
- Proficient in leveraging **Digital Risk Monitoring (DRM)** platforms such as **Cyble** and **iZOOlabs** to proactively block Indicators of Compromise (IOCs) and enhance threat intelligence capabilities.
- **Skilled in triaging complex** security events, prioritizing escalation pathways, and collaborating with the **CISO office** to execute high-priority risk mitigation directives.
- Expert in deploying **Attivo Deception Technology** to create advanced traps for threat actors, improving early detection and reducing false positives across security layers.
- **Comprehensive Cybersecurity Reporting**: Strong background in preparing detailed security incident reports, analysis findings, and executive summaries for senior management, aiding informed decision-making and incident resolution.
- **Regulatory Compliance & Risk Assessment**: Proficient at aligning security operations with **industry regulations** and **compliance standards**, while performing rigorous risk assessments to maintain organizational integrity.
- **Security Protocol Optimization**: Proven track record of fine-tuning and optimizing alert systems, reducing false positives, and ensuring effective detection mechanisms are in place to maintain a resilient cybersecurity posture.
- **Advanced Malware Analysis**: Highly skilled in leveraging sandboxing tools like **Securnex** to isolate and analyze suspicious executables, mitigating potential security threats and ensuring secure deployment of new applications.

Core Competencies

- Incident Response
- Security Monitoring
- Threat Analysis
- Threat Intelligence
- Risk Mitigation
- Cybersecurity Protocols
- Security Event Analysis
- Cybersecurity Incident Reporting
- Security Compliance
- Vulnerability Assessment
- Network Security Architecture
- Cybersecurity Best Practices

Work Experience

Security Analyst| Deloitte India, Navi Mumbai | Mar'2023 – Jan'25

Key Result Areas:

- Engaging in proactive monitoring and thorough investigation of security incidents, ensuring the integrity and resilience of organizational systems against potential threats.
- Conducting comprehensive analyses of security event data to swiftly identify and respond to emerging threats, thereby maintaining a robust security posture.
- Prioritizing & triaging escalated security events that necessitate in-depth review & analysis, ensuring timely resolution of critical incidents.
- Collaborating directly with the Chief Information Security Officer (CISO) office to execute high-priority risk mitigation directives, enhancing the overall security framework.
- Optimizing alert systems through thorough analysis and fine-tuning processes to considerably reduce false positives and improve incident response efficiency.
- Utilizing data from Digital Risk Monitoring partners, including Cyble and iZOOlabs, to proactively identify and neutralize Indicators of Compromise (IOCs) before they can impact the organization.
- Performing daily monitoring and analysis of various security tools, including DNS Security tools, deception technology (Attivo), EDR tools, and IBM QRadar, to ensure comprehensive threat detection.
- Executing sandboxing procedures for suspicious executables, taking decisive actions based on detailed analyses to mitigate potential risks.
- **Network Monitoring**: Conducted real-time monitoring and analysis of the organization's network using SIEM tools to detect and respond to anomalous activities and potential threats.
- **Phishing Email Analysis**: Investigated and analyzed suspected phishing emails using email headers, sandbox environments, and threat intelligence tools to identify malicious payloads, URLs, or social engineering tactics.
- **EDR Alerts Analysis**: Managed and analyzed Endpoint Detection and Response (EDR) alerts generated by tools like CrowdStrike, Microsoft Defender, or Carbon Black to identify malware infections, lateral movement, and unauthorized access. Escalated critical incidents for immediate remediation.
- **User-Reported Case Validation**: Validated and prioritized user-reported cybersecurity incidents, leveraging incident response playbooks to ensure timely resolution and communication with end-users for awareness and preventive actions.

- **Copilot:** Used copilot in SIEM for analyzing the incidents and writing queries and many more to make easier the task to understand the complicated task with in no time.

Education

- Bachelor of Engineering, Channabasaveshwara Institute of Technology, Sep'2020

Achievements

- Automated security tasks with XSOAR, improving efficiency and response time.
- Achieved 0 cybersecurity incidents in 2 years by mitigating alerts promptly.
- Resolved 90%+ SOC alerts within SLA, ensuring compliance and risk mitigation.

Certifications

- CCNA (Pursuing)
- Security Plus (Pursuing)
- Certified in Cybersecurity (CC), ISC2
- IBM QRadar SIEM Foundation

IT Skills

- IBM QRadar SIEM
- Microsoft Defender (EDR)
- O365 Defender
- Splunk Enterprise Security
- Digital Risk Monitoring (DRM) Tools
- Copilot
- Attivo Deception Technology
- Infoblox DNS Security
- Securnex Sandbox Tool
- ServiceNow (Ticketing Tool)
- MS Office Suite
- Microsoft Sentinel and ELK

Soft Skills

- Leadership
- Problem-Solving
- Critical Thinking
- Conflict Resolution
- Decision Making
- Adaptability
- Team Work
- Resilience
- Time Management

Personal Details

Date of Birth: 28th May 1999
Languages Known: English, Kannada, Telugu and Hindi
Current Address: Navi Mumbai, Maharashtra, India
Permanent Address: Bangalore, Karnataka, India