JOHN JEBAS

Cyber Security Analyst (Tier 1 & 2) | Microsoft Sentinel | VAPT | EDR | CEH®
Chennai, Tamil Nadu • +91 8939890285 • johnjebas02@gmail.com • linkedin.com/in/john-jebas-a24659275

PROFESSIONAL SUMMARY

Cyber Security Analyst with 1.6 years of Security Operations Center (SOC) experience at TVS Electronics, specializing in threat detection, incident investigation, and vulnerability management. Experienced in Microsoft Sentinel and Kusto Query Language (KQL) for SIEM monitoring, log analysis, threat hunting, and incident response. Investigated phishing, brute-force, malware, and suspicious authentication incidents while performing alert triage and endpoint investigations using Bitdefender EDR. Hands-on experience in creating and tuning Microsoft Sentinel analytics rules and conducting Vulnerability Assessment and Penetration Testing (VAPT) on web applications using Burp Suite Professional, Nessus, and OWASP ZAP. Strong understanding of the MITRE ATT&CK framework, OWASP Top 10, and CVE/CVSS. EC-Council Certified Ethical Hacker (CEH) and Splunk-certified.

PROFESSIONAL EXPERIENCE

Cyber Security Analyst — SOC Tier 1 & 2 — TVS Electronics*March 2025 – Present*

- Monitored and investigated security alerts using Microsoft Sentinel and Kusto Query Language (KQL), performing alert triage, log analysis, and threat hunting across enterprise environments.
- Created and tuned Microsoft Sentinel analytics rules, automation playbooks, and incident workflows to enhance threat detection and improve SOC operations.
- Investigated phishing, brute-force, malware, and suspicious authentication incidents, documenting findings and supporting containment and remediation activities.
- Conducted Vulnerability Assessment and Penetration Testing (VAPT) on web applications and internal systems using Burp Suite Professional, Nessus, and OWASP ZAP, identifying SQL Injection, Cross-Site Scripting (XSS), authentication flaws, and security misconfigurations.
- Performed vulnerability assessments across enterprise endpoints using SecPod SanerNow and Nessus, prioritizing remediation based on CVE/CVSS severity ratings.
- Managed endpoint security using Bitdefender EDR, performing malware investigation, threat containment, and endpoint analysis across Windows and Linux systems.
- Developed and executed KQL queries to investigate security events, correlate logs, and support proactive threat hunting activities.
- Prepared security incident reports and VAPT assessment reports with remediation recommendations for IT and application teams.
- Validated malicious IPs, domains, and file hashes using VirusTotal and threat intelligence sources to support incident investigation and containment.

TECHNICAL SKILLS

SIEM & Threat Detection: Microsoft Sentinel, KQL, Log Analysis, Threat Hunting, Alert Tuning & Triage, Playbook Development

VAPT & Security Testing: Burp Suite Professional, Nessus, Nmap, OWASP ZAP, SecPod SanerNow, Vulnerability Assessment, CVE/CVSS Scoring, Exploit Validation, Reconnaissance

EDR & Incident Response: Bitdefender EDR, Incident Response, Malware Analysis, Threat Containment, IOC, IOA, VirusTotal, Threat Intelligence, SOAR Concepts

Networking & Platforms: TCP/IP, DNS, HTTP/HTTPS, Windows, Linux (Kali), Firewall Fundamentals, Network Traffic Analysis

Scripting & Tools: KQL, SQL, Python (Basic), Bash

CERTIFICATIONS

★ **Certified Ethical Hacker (CEH) — EC-Council ✓ CERTIFIED**

- Security Operations and Defense Analyst — Splunk
- Understanding Threats and Attacks — Splunk
- Cybersecurity Essentials — Cisco Networking Academy
- SanerNow Cyber Hygiene Platform Training — SecPod

EDUCATION

Dr. M.G.R. Educational and Research Institute, Chennai *2020 – 2024*

Bachelor of Technology — Computer Science and Engineering **| CGPA: 7.91**

PROJECTS

IFLEX TRAX 1.7 — Facebook-Style User Registration System

Technologies: *Python, Django, MySQL, HTML, CSS, JavaScript, Visual Studio Code*

- Collaboratively developed a Facebook-style user registration system using Django and MySQL, implementing secure user signup, form validation, database integration, and a responsive user interface.

ADDITIONAL INFORMATION

- Active on TryHackMe and Hack The Box, practicing hands-on cybersecurity labs and Capture The Flag (CTF) challenges.
- Passionate about continuous learning in SOC operations, threat hunting, incident response, vulnerability assessment, and cloud security.
- Strong analytical, documentation, and communication skills with the ability to investigate security incidents and collaborate effectively with cross-functional teams.