ARJUN ARUMUGHAN

SOC Analyst | CyberSecurity Engineer | Threat Detection Specialist | Network Security

Phone: +91 89434 57503 | E-mail: arjunarumughan02@gmail.com
LinkedIn: linkedin.com/in/arjun-a-454b85256 | TryHackMe: https://tryhackme.com/p/ppkunjumon
GitHub: github.com/arjunarju123 | Portfolio: arjun-sec.in
Kerala, India | Immediate joiner | Open to Relocation

PROFESSIONAL SUMMARY

CEH-certified Cybersecurity professional with hands-on experience in SOC operations, SIEM monitoring, incident response, vulnerability assessment and threat detection through enterprise lab environments and internship experience. Skilled in Wazuh SIEM, Microsoft Sentinel, Sysmon, MITRE ATT&CK, OpenVAS and Windows Server administration. Seeking an entry-level SOC Analyst, Cybersecurity Specialist, Network Security, Server Administration or System Administrator role.

TECHNICAL SKILLS

SIEM & Security Monitoring
Wazuh SIEM, Microsoft Sentinel, Splunk, Log Monitoring & Correlation Security Alert Triage, Event Log Analysis

Incident Response & Threat Detection
Incident Escalation, Incident Response, Runbook Execution, MITRE ATT&CK, Threat Hunting, IOC Analysis, Security Event Monitoring, Root Cause Analysis.

Vulnerability Assessment
OpenVAS (GVM), Nessus, Nmap, CVSS Scoring, CVE Triage, Vulnerability Validation, Remediation Verification

Compliance & Governance
OpenSCAP, CIS Benchmarks, Security Posture Assessment, Incident Documentation, Compliance Reporting.

Endpoint Security
Sysmon, FIM, EDR/XDR Concepts, Active Response, Endpoint Agent Management, Windows Event Logs

System Administration
Windows Server 2016, Active Directory, Group Policy, User & Group Management, Ubuntu Linux, kali Linux.

Productivity & Documentation
Microsoft Office, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Technical Documentation, Report Writing.

Web Application Security
OWASP Top 10, SQL Injection, Cross-Site Scripting (XSS), Web Vulnerability Assessment, Authentication & Session Testing

Network Security
TCP/IP,DNS, DHCP, OSI Model, VPN, Network Traffic Analysis, IDS/IPS, Network Segmentation, Routing & Switching Fundamentals, Firewall Fundamentals

Penetration Testing
OWASP Top 10, Burp Suite, Metasploit, SQL Injection, XSS, VAPT

Scripting & Automation
Bash Scripting, Security Workflow Automation, SOAR Concepts, PowerShell.

Security Tools
Wireshark, Burp Suite, Metasploit, OpenSCAP, Snort OWASP ZAP, Atomic RedTeam.

Cloud Security
Microsoft Azure Fundamentals, Cloud Security Concepts, Microsoft Sentinel

Soft Skills
Problem Solving, Analytical Thinking, Team Collaboration Skills, Time Management, Communication Skills

PROFESSIONAL EXPERIENCE & PROJECTS

Security Admin Associate L1 (Internship)
Jan 2026 – Mar 2026

Infotact Solutions | Bangalore, India

- Deployed Wazuh SIEM across Windows Server and Ubuntu endpoints to centralize security monitoring.
- Developed custom detection rules mapped to MITRE ATT&CK techniques.
- Investigated security alerts and validated ransomware detection using Atomic Red Team.
- Conducted authenticated vulnerability assessments using OpenVAS and prioritized remediation based on CVSS.
- Configured Active Response to automatically block SSH brute-force attacks.

■ SOC Enterprise EDR and Threat Hunting Grid

Technologies Used: Wazuh, Sysmon, Windows Server, Ubuntu, MITRE ATT&CK, Automic RedTeam, Active Response, FIM

GitHub: github.com/arjunarju123/Security-Operations-SOC---Enterprise-EDR-Threat-Hunting-Grid

- Built an enterprise SOC lab with Wazuh SIEM monitoring Windows Server and Ubuntu endpoints.
- Integrated Sysmon to improve visibility into process creation, persistence, and privilege escalation events.
- Implemented FIM with real-time alerts and CVE-based vulnerability detection across monitored endpoints.
- Developed custom detection rules mapped to the MITRE ATT&CK framework
- Configured Active Response to automatically block SSH brute-force attacks.
- Simulated ransomware (MITRE T1490) using Atomic Red Team and validated detection through SIEM alerts.

■ VulnVision 360 — Continuous Compliance & Threat Exposure Engine

Technologies Used: OpenVAS, OpenSCAP, Nmap, CVSS, CIS Benchmarks, Bash

GitHub: github.com/arjunarju123/Vulnvision-360

- Automated network asset discovery using Nmap.
- Conducted authenticated and unauthenticated vulnerability assessments with OpenVAS
- Prioritized vulnerabilities using CVSS scores and verified remediation.
- Performed CIS Benchmark compliance assessments using OpenSCAP.
- Generated executive security reports summarizing risks and remediation recommendations.

■ Windows Server 2016 Domain Environment Lab

Technologies Used: Windows Server 2016, Active Directory, DNS, DHCP, Group Policy, VirtualBox

- Built a complete Active Directory domain environment in Oracle VirtualBox.
- Configured DNS, DHCP, and Active Directory Domain Services.
- Created users, groups, and organizational units.
- Implemented Group Policy Objects (GPOs) for centralized administration.
- Demonstrated enterprise user and network management practices.

CERTIFICATIONS

Certified Ethical Hacker (CEH) — EC-Council | Credential ID: ECC4075298163

Advanced Diploma in Cyber Defence — RedTeam Hacker Academy

EDUCATION

BA English Literature *2020 – 2023*

University of Calicut, Kerala, India

Transitioned into cybersecurity through structured industry training, professional certifications, and independent hands-on lab practice — demonstrating self-driven technical capability.

AWARDS & RECOGNITION

Rajya Puraskar — Awarded by the Governor of Kerala through the Bharat Scouts and Guides programme (2018) for excellence across multiple achievement areas.

ADDITIONAL INFORMATION

Nationality: Indian

Languages: English (Fluent), Malayalam (Native), Tamil (Speak), Hindi (Read,Write Speak)