Logeshwaran M

Cybersecurity Analyst

Location: Ramanathapuram, Tamilnadu, India.

Email: waranlogesh834@gmail.com

Phone: +91 9021534947

LinkedIn: https://www.linkedin.com/in/logeshwaran-m-a843bb1b4/

Objective

Cybersecurity analyst with 2 years of hands-on experience in security monitoring, threat detection, and incident response. Proficient in analysing security logs, performing vulnerability management, and implementing proactive measures to safeguard networks and applications. Seeking to leverage my expertise in advanced security tools and frameworks to strengthen organizational defences and support continuous improvement in cybersecurity operation.

Skills

- Networking: TCP/IP, Network Security, Firewalls, IDS/IPS.
- Cybersecurity: Security Operations Center (SOC), OWASP Top 10, Web Application Security, Penetration Testing, Vulnerability Assessment and Management, Threat Hunting, Log analysis, Incident management, Endpoint Security.
- Programming Language: Python Scripting, JavaScript.
- Tools and Technologies: Splunk, NMAP, Nessus, Burp suite, Wireshark, AWS, GCP, Microsoft Defender.
- Operating Systems: Windows, Linux.
- Language: English, Tamil.

Professional Experience

Associate Cybersecurity Engineer — June 2023 -Present
Siemens Technology and Services Pvt Ltd, Pune

- Monitored and analysed security event logs from diverse systems and applications, ensuring proactive detection and mitigation of potential threats.
- Investigated and responded to complex incidents, including advanced persistent threats, phishing attacks, and denial-of-service events.
- Performed regular vulnerability assessments to identify and mitigate system and application weaknesses, enhancing the overall security posture.

- Specialized in operations using tools like SIEM, EDR, IDS/IPS, VPN, Antivirus, Firewall and cloud security solutions (AWS, GCP), ensuring efficient detection and response to threats.
- Conducted threat hunting and in-depth analysis of security events to determine scope, impact, and countermeasures.
- Investigated and implemented incident response plans, containing and eradicating security threats while documenting timelines, findings, and remediation actions per regulatory requirements.
- Documented and reported comprehensive investigation findings, including root cause analyses, while contributing to knowledge-sharing and operational improvements.

Internship

Cybersecurity Internship — January 2023-June 2023

Siemens Technology and Services Pvt Ltd, Pune

- Developed foundational knowledge of networking concepts, including protocols (TCP/IP, HTTP, Etc).
- Gained hands-on experience in web application security by identifying and assessing vulnerabilities using OWASP guidelines and security tools.
- Performed network security analysis by reviewing firewall configurations, analyzing network traffic, and identifying potential vulnerabilities or misconfigurations.
- Assisted in vulnerability management by scanning systems, analyzing results, and recommending remediation strategies to mitigate risks.
- Applied foundational knowledge of ISO 27001, the NIST framework, and the MITRE ATT&CK framework to enhance security protocols and align with industry standards, contributing to a more robust security posture

Education

SRM Institute of Science and Technology, Chennai. — June 2019-May 2023

Bachelor of Technology in Electronics and Communication Engineering (ECE).

Certification

- CAP (Certified Appsec Practitioner) By The Secops
- CNSP (Certified Network Security Practitioner) By The Secops