Mahanatarajan TV

Email: mahanatarajan1005@gmail.com
Mobile: +91 9591863500

SUMMARY:

Cybersecurity professional with 4 years of experience in threat detection, incident response, and security operations. Skilled in security analysis, risk management, and security tool implementation. Experienced in managing Firewalls, IDS/IPS systems, Proxy, DNS, NAC, VAPT, 2FA, DLP, PAM, EDR and SIEM tools. Strong analytical and problem-solving skills with the ability to work independently or as part of a team. Proven track record of managing and leading technical teams in fast-paced and dynamic environments. Seeking a challenging cybersecurity role to continue developing technical and leadership skills.

SKILLS:

Security incident response: Respond to security incidents and conduct forensic investigations to determine the root cause. Strong knowledge of incident response procedures and tools.
Vulnerability assessment and management: Conduct vulnerability assessments and penetration testing to identify and mitigate security risks. Experience using vulnerability scanners such as Nessus.
Security Audit: Having a good understanding of security audits and implementation with industry regulations and standards (ISO 27001)
Penetration testing: Conduct penetration testing to identify vulnerabilities in systems and applications. Experience with tools such as Cymulate.
Firewall and IDS/IPS management: Manage firewalls, IDS/IPS systems, and other network security devices. Experience working on Check Point and Palo Alto firewalls.
SIEM tools : Use SIEM tools to monitor network traffic and detect security incidents. Experience with Arcsight, Logrhythm, Splunk and other SIEM tools.
Endpoint security management: Manage endpoint security systems such as antivirus , HIPS/HIDS, DLP and EDR.

PROFESSIONAL EXPERIENCE:

Cybersecurity Engineer - Wipro Ltd. Bangalore.

July 2021 – Present

- Manage a team of 6 cyber security analysts and engineers responsible for threat detection, incident response, and security operations.
- Develop and implement incident response plans to ensure the organization is prepared to handle security incidents and breaches.
- Conduct vulnerability assessments and penetration testing to identify and mitigate security risks.
- Implemented and maintained security controls such as IDS/IPS, SIEM, EDR, Secure connector- NAC to protect company assets and ensure compliance with regulatory and industry standards.
- Lead incident response teams during security incidents and provide guidance to technical teams during remediation activities.
- Adding and removing DNS zones in InfoBlox, Troubleshooting issues related to Infoblox with vendor and support team.
- Develop and maintain security documentation, such as security policies, standards, and procedures.
- Manage relationships with third-party vendors and service providers to ensure their security controls meet the organization's requirements.
- Server Management with SIEM, Sever Hardening with internal SIEM Khika
- Help the security audit team to ensure compliance with regulatory and industry standards.
- Conduct security assessments of third-party vendors and service providers to ensure their security controls meet the organization's requirements.

- Provide technical guidance and mentorship to other security engineers and analysts.
- Participate in incident response efforts and provide technical expertise during remediation activities.
- Stay up-to-date with the latest security trends, threats, and technologies to ensure the organization's security posture is always improving.
- Conduct security awareness training programs for technical teams to ensure they are knowledgeable about security best practices.
- Analyze security logs and alerts to identify and respond to security incidents.
- Conduct a weekly call with IT teams to ensure that security measures were integrated into all systems and applications and compliance.

Security Analyst – Fidelis Pvt, Ltd. Bangalore.

September 2019 – February 2021

- 24/7 SIEM monitoring (Arc sight , LogRhythm), IDS, IPS, Malware Analysis, Log and Phishing Analysis, Managing the Security Operations Center.
- Investigate the security logs, mitigation strategies and Responsible for preparing generic.
- Investigated and responded to security incidents, ensuring that they were resolved in a timely and effective manner.
- Analyzed security logs and alerts to identify and respond to security incidents.
- Collecting the logs of all the network devices and analyze the logs to find the suspicious activities.
- Blocking of Malicious IP's, URL's and Domains in Firewall and Proxy
- Do a daily Health check and also check for log stoppage issues
- Blocking of Hashes that are proven malicious in Symantec.
- Follow-up the ticket raised with Point of contact till closure.
- Providing tuning recommendations for rules sets for policies based on findings during investigations or threat information reviews.
- Working on Windows/Unix Security Logs as well as logs form IDS/IPS,HIDS,DLP, Next Generation Firewalls, Anti-Virus/Malware, Vulnerability Assessment.
- Analyzing daily, weekly and monthly reports.
- Security incident report.
- Preparing SOPs required for client.
- Filling the Daily health checklist.
- Creating the tickets in ticketing tool.
- Conducted security awareness training programs for technical teams to ensure they are knowledgeable about security best practices.
- Conducted vulnerability assessments to identify and prioritize security risks.

TOOLS:

- Firewall : CheckPoint, PaloAlto Firewall.
- VAPT : - Nessus, Cymulate BAS .
- SIEM Tool : Arcsight, Logrhythm, Splunk, Khika.
- EDR : Falcon CrowdStrike, Fire Eye.
- AV : Symantec.
- DLP : Symantec.
- IDS/IPS : TrendMicro, Ossec.
- Proxy : Forcepoint, ZScalar.
- DNS : InfoBlox.
- 2FA : OneSpan, Vasco 2FA.
- NAC : Forescout.
- IAM : Iraje PAM.

EDUCATION:

Bachelor of Computer Applications [2016 – 2019] – CMRIMS, Bangalore.

Declaration :

I hereby declare that the above furnished details are true and correct to best of my knowledge and belief.

Thank you.

Yours faithfully,
Mahantarajan

Date: 05/07/2023
Place: Bangalore