TARUN SHARMA

CEH™ CERTIFIED ETHICAL HACKER

tarunmps4496@gmail.com
Contact: +91-9680398779

OBJECTIVE: *To use my creative and technical skills that I am familiar with which will benefit the organization in the long run and also help me in building my professional career. I want to convert my innovative ideas into fruitful results and to work in cutting-edge competitive industry.*

SOFTWARES/TOOLS KNOWN:

- **SIEM:** ArcSight (Active Channels/Rules/Reports/Dashboard creation), QRadar
- **SOAR:** Resilient (Incident Response, Rules, Workflows)
- **ESA:** Cisco Ironport (Spam/Phishing mail analysis)
- **NBAD:** Cisco Stealthwatch (Network Traffic analysis, Rule creation, Policy creation)
- **FireEye APT** (C&C/Botnet Identification, Malware Analysis, APT detection)
- **Symantec Forensics** (Deep Packet Analysis, Malware Analysis)
- **Imperva WAF** (Log monitoring & analysis)
- **Infoblox DNS**
- **Protocols:** TCP/IP, UDP, DNS, DHCP, FTP, SFTP, SNMP, SMTP, SSH, SSL, VPN, RDP, HTTP and HTTPS
- **Programming Languages:** SQL, Core Java
- **Other Security Tools/Skills:** IDS/IPS, EDR , Virus Total, IPVoid, IBM X-force, Cisco Talos, MX Toolbox, PEiD, cyber kill chain, MITRE ATT&CK

CERTIFICATIONS: CEH (ECC4580632971)

WORK EXPERIENCE (3 Years):

- **SOC Analyst, Wipro Limited** **(06/2018 – Present)**

Responsibilities:

- Responsible for 24*7 SOC monitoring of security events and Logs of security devices like Firewall, IPS, WAF, Forensics, etc. using SIEM and various security devices.
- Following the **Incident Management Process using SOAR (IBM resilient)** and performing deep-dive incident analysis with advanced tools and techniques, including open-source tools like threat feeds.
- Take ownership of issues detected and drive them to closure until mitigation occurs.
- Follow-up with respective teams on raised incidents and give necessary **inputs on remediation actions to be taken.**
- Collecting IoCs, analyzing and preserving the evidence related to incidents.
- **Log monitoring and analysis** using ARcSight SIEM(active channels, filters, dashboards).
- Working on fine tuning of SIEM rules, SOAR rules and workflows, NBAD rules and policies.
- **Email Security Analysis** (Phishing mail analysis).
- Report generation on a daily, weekly, and monthly basis as well as analyzing automated reports.
- Analyzing security breaches and **preparing RCAs.**
- Performing deep-dive analysis using Symantec Forensics.

STRENGTHS:

- Zealous and committed towards the work assigned.
- Good at Analysis and Incident handling & response
- Proficient in communicating my thoughts and my ideas.
- Client Handling

ACADEMIC QUALIFICATION:

NATIONAL INSTITUTE OF TECHNOLOGY AGARTALA

B.Tech. Chemical Engineering (2018) CGPA: 8/10

MODERN PUBLIC SCHOOL, BHIWADI

- All India Senior School Certificate Examination (2013)
  87.80% (CBSE)