Mr. Gaurav

gauravsharma8516@gmail.com
+91-8839444260
Sushant Lok-1, Block C, Gurgaon, Haryana

Career Objective

To work enthusiastically & dynamically in a reputed organization, where with my knowledge and proficiency, I can contribute to individual as well as organizational goals with a strong commitment to diversity.

Working Experience:

- September 2024 – Present

  Working as Senior Consultant – Tech Consulting in Ernst & Young, Gurgaon.

  Job Responsibilities:

  - Threat Modelling :
    - Created threat models based on STRIDE framework for insurance and reassurance products being developed in-house by the client, by understanding end-to-end workflow of the products with product owners. Also, updated existing threat models versions and made relevant changes wherever applicable based on the scope of changes for each release type (major / minor releases).
    - Review and triaged issued countermeasures with application owners to ensure identified security controls are implemented. Created different user stories for each counter measure for better traceability and implementation.
    - Assisted in the development of threat modeling governance documentation, defining the requirements for threat model updates based on different release types and scope of changes.
    - Conducted security risk assessments of applications with respect to design and implementation of system and application.

  - VAPT : Performed Infra VAPT Co-ordinating with Application team, Server Team & Network Team to fix security issues with mitigation plan within timeline defined with retesting required.
  - SCD : Performed Secure Configuration review for middleware, OS and Network Devices.

- October 2022 – September 2024

  Worked as Manager, Information Security in Care Health Insurance, Gurgaon.

  Job Responsibilities:

  (Technical)

  - VAPT : SPOC for VAPT including DAST, SAST,MAST as Blackbox & Greybox Testing.

- Threat Modelling : Created & Reviewed the Risks associated in Application Architecture based on STRIDE Framework.
- Red Teaming : Performed Red-Team Activities from Internal & External Red Teamer approach.
- Configuration Review : SPOC for Network Config, Review including Firewalls, Routers, Switches, SDWAN, LB and for Database Config Review including MySql, MSSql, and Oracle Databases.
- EDR/XDR(MS Sentinel/Crowdstrike) : Managed Administration of EDR/XDR deployed.
- PIM/PAM : Managed PIM/PAM review and enhancement.
- Symantec PGP : Responsible for Disk Encryption deployment and migration.
- Security Tools Integration : Responsible for Additional Security Tools Integration with SIEM.
- Cloudsek : Managed Brand Monitoring tool with resolution of the incidents, vulnerability scanners, takedown of phishing and malicious websites.
- Cloud Security : Worked as add-on support for Cloud Configuration Security Review.
- Advisories : Advisory Release and confirmation of the blocked IOCs and took action on IOAs required from the respective teams.

(Management)

- Review Change Management for Applications : Reviewed change management approval in regards to VAPT issues on any applications
- Project planning and management : Developed and executed a project plan, including setting clear goals, timelines, and budgets.
- Team management: Lead and motivated a cross-functional team to achieve project objectives.
- Risk management: Ability to identify, assess, and mitigate organizational risks including compliance check, third-party software & website risk analysis to be allowed in organization.
- Communication and stakeholder management: Ability to effectively communicate with project team members, stakeholders, and clients.
- Budget management: Ability to manage project expenses and stay within budget.

- October 2021 – October 2022

  Worked as Security Analyst in Intelliroot Technologies, Bangalore deployed at Care Health Insurance, Gurgaon.

  Job Responsibilities:

  - VAPT : SPOC for VAPT including DAST, SAST,MAST as Blackbox & Greybox Testing. Responsible for VAPT security checks before production & on production. Managed and Reported VAPT & Source Code Review of all the Web & Mobile Applications and Infra devices including Windows/Linux servers and network devices.
  - Red Teaming : Responsible for performing Red-Team Activities from Internal & External Blackbox approach.

- Advisories : Release and confirmation of the blocked IOCs and took action on IOAs required from the respective teams.

- April 2019 – Sept 2021

  Worked as Vulnerability Assessment & Penetration Testing Associate in Tephratec Solutions, Noida

  Job Responsibilities:

  - Performed VAPT of Web Applications with Information Gathering, Reconnaissance, Attacking and Patching of Vulnerabilities.
  - Tested for OWASP Top 10, Metasploit and created proper reportaccording to the impact level and vulnerable parameters, etc.
  - Read Code of open-source security tools to update and use for desired network.

- Jul 2018 - Feb 2019

  Worked as Executive Penetration Tester in Web Secure Technologies, New Delhi

  Job Responsibilites:

  - Performed VAPT of Web Applications and IPs with Information Gathering, Reconnaissance, Attacking and Patching of Vulnerabilities.
  - Performed Automated and Manual Testing through different tools like Nmap, Wireshark, Burpsuite, Maltego, Sqlmap, Nikto, and vulnerabilityscanner tools like Acunetix, Netsparker, ZAP, Nessus etc.
  - Tested for OWASP Top 10, Metasploit and created proper reportaccording to the impact level and vulnerable parameters, etc.
  - Configured SMB and different servers for company testing.
  - Network Troubleshoot (Internal Branch Network Subnetting)

Academic Qualification's

Currently pursuing Masters of Business Administration (M.B.A.) in Information Technology from Amity University, Noida.

S. No	Degree	Institution	University / Board	Year of Passing	Division
1.	B.E.	Oriental College of Technology (OCT), Bhopal.	R.G.P.V.	2018	1st

Technical Exposure : Projects/ Industrial Visit / Workshops

- Completed EC-Council's Certified Ethical Hacker (CEH) certification and training.

- IT Proficiency: Platforms like Web/ Mobile Applications/ API VAPT, Red Teaming, Blue Teaming, EDR/ XDR, PIM/ PAM, Cloudsek, Symantec PGP, SIEM

- Hands on experience on Redhat Linux 6/7/8/9 OS or equivalent CentOS Management and Administration along with Debian Based OS Like Ubuntu, Kali Linux, Parrot OS.

- Hands on experience on following security administrative tasks:
    - Strong Information Security matter knowledge on Threat Modelling with tools such as Microsoft Threat Modelling Tool, OWASP Threat Dragon.
    - Knowledge incorporating Red Teaming including network, operating systems, and application security, AD Bypass, Password Spray, Data Exfiltration, External C2 server connection, Abusive Trusted Directory, etc.
    - Knowledge and experience on different VAPT tools such as Nessus, Nexpose, Acunetix, Netsparker, Qualys, Nikto, Nmap, Sqlmap, Burpsuite etc. as well as different SOC tools such as SentinelOne EDR, CrowdStrike XDR, Indusface WAF, Symantec Disk Encryption, Xvigil Brand Monitoring, Arcon PIM/ PAM etc.
    - Vulnerability scanning, remediation, auditing and reporting on Applications as well as Infra(Servers & End-Points)
    - Responding to tickets related to security events & Incident Response.

-Gaurav