**Summary of 2024**

Over the past year, I have made significant contributions to Brillio’s security posture while continuously developing my skills. This includes in-house VAPT for **four Brillio internal applications** by increasing my knowledge on various payloads and calendared activities form next year and have coordinated with various stake holders for **four external VAPT scans** and its closure. have actively monitored **external attack path** vulnerabilities from various tools on a daily basis, reporting around **55** vulnerabilities, with **80% closure rate.** Additionally, have contributed in **BESF** with security best practices from various sources across **six technologies** and coordinated with teams which led to successful **closure rate of 84%** of recommendations and have also developed a **KQL query** to tracked around **230 non-delivery location logins**, reporting them to the business unit on a daily basis.

Have collaborated closely with the **SOC Team on a daily basis** and worked to enhance the initial investigation process, thereby improving user experience and providing updates to management about secure incidents and posture. have supported around **eight P1 and P2 security incidents** and contributed to ISO 27001 audits, presented to **external auditors in Hyderabad** and coordinated with various stake holders, and **contributed to CSS initiatives** policy & Procedures and awareness mailers etc. also educated participants in a **cybersecurity seminar for NGOs** on key cyber security best practicesduring CSR annual partners' event.

This year, I earned the **ISC2 CC certification** and am currently upskilling in CEH, cloud security, advanced VAPT and communication skills. Through these efforts, I have significantly enhanced my expertise and communication skills and contributed to the Brillio’s ongoing security growth.

**1)Endpoint Security & BESF**

Successfully tracked and reported around 230 non-delivery locations till date, which involved creating a new process with a KQL query for daily monitoring. Contributed in MDE vulnerability dashboards (by sharing a weekly tracker till it is automated with a powerbi).

Automated infrastructure vulnerability assessments to run on 1st and 3rd of every month for network and servers with an automated mail trigger to team.

played a key role in Enhanced security posture through the Brillio Enterprise Security Framework by creation of a checklist, by referring various sources and coordination with multiple stakeholders for review and closure on daily basics across 6 technologies, which helps us in achieving an 84% overall closure rate, with over 95% for three technologies and above 80% for two.

**2)VAPT (Vulnerability Assessment & Penetration Testing)**

Performed internal VAPT assessments on 4 Brillio's internal applications by using Burp suite till date and regular communication with the DO and CTO teams throughout the assessment process and sharing of vulnerability trend reports and collaborated closely with the SISA team and internal team members for successful remediation of external vapt assessments for 4 Brillio applications. along with a detailed trend report.

Contributed to identifying and monitoring external attack path vulnerabilities using tools such as Secure Scorecard, Bitsight, and ImmuniWeb. Successfully reported approximately 55 vulnerabilities to application owners and tracked them through to resolution, with 80% Successful closure

**3)Security Incident Management - SOC Interaction Coordination**

Engaged with the SOC team through daily calls to review and analyse security incidents, providing updates on security incidents and the organization's overall security posture to management

Collaborated with the SOC team to enhance initial investigations and by reducing the need to involve end users for every case, to improve user experience.

Actively contributed in approximately 8 P1 and P2 security incidents (including client-reported cases) by collecting and analysing logs from various sources and assisting in report creation, assisting in report creation, and providing overnight and weekend support as needed.

**4)Audit and BAU Support**

Played a crucial role in 6 internal, 2 Client and external ISO 27001 audits facing external auditor at the Hyderabad location and coordinating with multiple teams to provide essential records.

Contributed to Power BI for CSS governance and assisted in risk governance.

Managed and updated various Microsoft Lists, assisted in creating policies and procedures, and delivered security awareness mailers to Brillio teams.

Also monitored daily alerts and provided on-call support until midnight on a shift basis with zero escalations from BU.

**5)MBO: Self-Learning / Upskilling, Demonstrating Brillio Values**

Demonstrated Brillio values by supporting the CSR team and leading a cybersecurity seminar for annual NGO partners meet and Educated participants on critical topics such as password security, phishing, data storage, and data protection, reinforcing Brillio's commitment to fostering a secure online environment. Participated in the Brillio organized Kanyathon 5km marathon, showcasing a dedication to Brillio Initiatives.

Achieved the ISC2 CC in cyber security certification, enhanced skills in cybersecurity and VAPT, and am currently upskilling in CEH, cloud security, advanced VAPT methodologies and communication skills.