**USE CASES OF GITHUB IN CYBERSECURITY**

GitHub is extensively utilized in cybersecurity for a variety of purposes. Organizations and cybersecurity professionals use GitHub to collaborate on incident response strategies, share indicators of compromise (IOCs), and publish threat intelligence reports. Repositories like (Malware Information Sharing Platform) are used for threat intelligence sharing. GitHub serves as a platform for sharing vulnerability reports, exploits, and mitigation techniques. It is also used as a platform to manage and track the disclosure process of vulnerabilities, providing a transparent and organized way to reward security researchers. Companies often host bug bounty programs, where security researchers can submit vulnerabilities found in their codebase hosted on GitHub.

It helps researchers collaborate on identifying and fixing security issues. Security professionals use GitHub to manage infrastructure configurations, ensuring that security best practices are followed and changes are tracked. Cybersecurity is a constantly evolving field, and hands-on practice is essential for staying up-to-date. GitHub is a repository of knowledge where cybersecurity enthusiasts, students, and professionals can find educational resources. Many institutions and online platforms share labs, exercises, and CTF (Capture The Flag) challenges on GitHub. These resources allow learners to practice skills like penetration testing, reverse engineering, and network security in a controlled environment. For beginners, this hands-on experience is invaluable for understanding real-world cybersecurity concepts. Cybersecurity learning platforms and universities often publish labs and exercises on GitHub. Organizations often use GitHub to store and manage their security policies and best practices. By keeping these documents in a GitHub repository, they benefit from version control, meaning that every change is tracked, and it's easy to see who made a change and why. Teams can also collaborate on these documents, proposing changes and reviewing them through pull requests. This ensures that security policies are consistently updated and easily accessible to everyone in the organization.