HACK2LEAP22
October 28 – 29, 2022
PLAN OF ACTION

1. Abstract (Maximum 500 Words):

CYBOT-A Smart Cyber Security Bot System will offer high-quality IT and data protection and Data Visualization for businesses and provides an in-depth and customizable collection of managed cybersecurity services. With a team of security experts, it provides Wi-Fi monitoring and forensics ,Security information and Event management system (SIEM), End-Point Detection and response (EDR), Log Processing ,Automated Threat surveillance ,Remote manageable system with live monitoring, mobile threat defence, comprehensive vulnerability management, and application security among other services ,it not only supports endpoint protection but also threat investigation across firewalls, servers, and more data sources and help organizations and security practitioners through the complexities of cybersecurity to ensure their security posture is future-ready.

This is a hardware based smart security bot system especially for the Security Operation Centre (SOC) Teams in Companies, this monitor and detects various cyber-attacks. This bot analyses file's binaries and assembly code and Compare/Analysis those with various hashing algorithm for malicious signatures & examine code for suspicious properties through antivirus API. It also MITRE attack, Heuristics & Behaviour based detection.

The Admin panel of Cybot will access to Cyber Security Operation Centre Dashboard built with the help BI Tool, the dashboard will consist of multiple pages like Homepage showcasing the high level KPIs and redirection to other subpages, Department Analysis will provide insight of the department where breaches occurs, Breach Analysis will provide insight of type of breaches which occurs more often, A Summary page will provide basic understanding of analysis of the Cybersecurity breaches occurred in the past and how many breaches are currently open and closed, Average time for breach closure, Number of employees are affected by it, Employee ranking will provide ranking of the employee who solved the most breaches and all other details and the User Panel will have a report option to flag a breach or threat through a form which will be data source for the Admin Cyber Security Operation Centre Dashboard.

2. Roles Assigned to Members of a Team:

S. No	Student Name	Register Number (University Register Number)	Institution Name	Mail ID	Contact Number	Role in the project (Front end developer, Backend designer, Model developer, Implementation, Tester, etc…)	GitHub Link of the student (GitHub Profile title page)
1	Sadain Abdullah N	511919104014	Priyadarshini Engineering College	nsasadain@gmail.com	8778073334	Full Stack Developer, Model Developer, Implementation	https://github.com/sadain
2	Md Adnan K	511919106005	Priyadarshini Engineering College	md.adnan1901@gmail.com	7010639736	Data Analytics, Model Developer, Tester	https://github.com/adnan1901
3	Earnest Wesley S	511919104005	Priyadarshini Engineering College	mailtoearnestwesley77@gmail.com	9360996409	Backend Developer, Network Security,	https://github.com/Wesley-blackops
4	Zaheeb Afnan A	511919104026	Priyadarshini Engineering College	zaheebafnan11@gmail.com	8220479488	Front End Developer	https://github.com/Zaheebafnan22
5	Mohammed Rayan K	20MIS0098	Vellore Institute of Technology	mohamedrayanklt@gmail.com	7904696118	Front End Developer, Tester	https://github.com/rayan002

3. Plan of Action (to complete the project step by step):

1. Building EDR (End point Detection and Response.
2. Building SIEM (Security Information and Event Management).
3. Configuring all the programs into raspberry pi connected to Alpha card
4. Building CYBOT Landing Page.
5. CYBOT User Dashboard Having Report Form.
6. Security Operation Centre Dashboard Using Data analytics.

4. Tech stack (to be used during Hackathon):

1. Raspberry pi
2. Alpha Card
3. File Beat, Elastic Search, SQLite DB
4. Python, Bash Scripting
5. HTML, CSS, JavaScript, PHP, MySQL
6. Power BI

5. Model description (to be developed and deployed during Hackathon):

1. **EDR (Endpoint Detection and Response):**

   Centralized access to continuously recorded endpoint data means that security professionals have the information they need to hunt threats in real time as well as conduct in-depth investigations after a breach has occurred. So, this leverages AV API for Thread detection and Active response

2. **SIEM (Security information and Event management):**

   Utilizing advanced analytics to identify and understand intricate data patterns, event correlation provides insights to quickly locate and mitigate potential threats to business security. This is done using deep log processing method.

3. **Wi-Fi Scanning & Forensics:**

   A wireless monitoring system which results in better organized, searchable, sortable manner with visualization support. This also leverages SQLITE.DB for wireless forensics purposes.

4. **Security Operation Centre Dashboard Using Data analytics:**

   The Cyber Security Operation Centre Dashboard built with the help BI Tool like Power BI, the dashboard will consist of multiple pages like Homepage showcasing the high level KPIs and redirection to other subpages, Department Analysis will provide insight of the department where breaches occurs, Breach Analysis will provide insight of type of breaches which occurs more often, A Summary page will provide basic understanding of analysis of the Cybersecurity breaches occurred in the past and how many breaches are currently open and closed, Average time for breach closure, Number of employees are affected by it, Employee ranking will provide ranking of the employee who solved the most breaches and all other details and the User Panel will a report option to report a breach or threat through a form which will be data source for the Admin Cyber Security Operation Centre Dashboard.