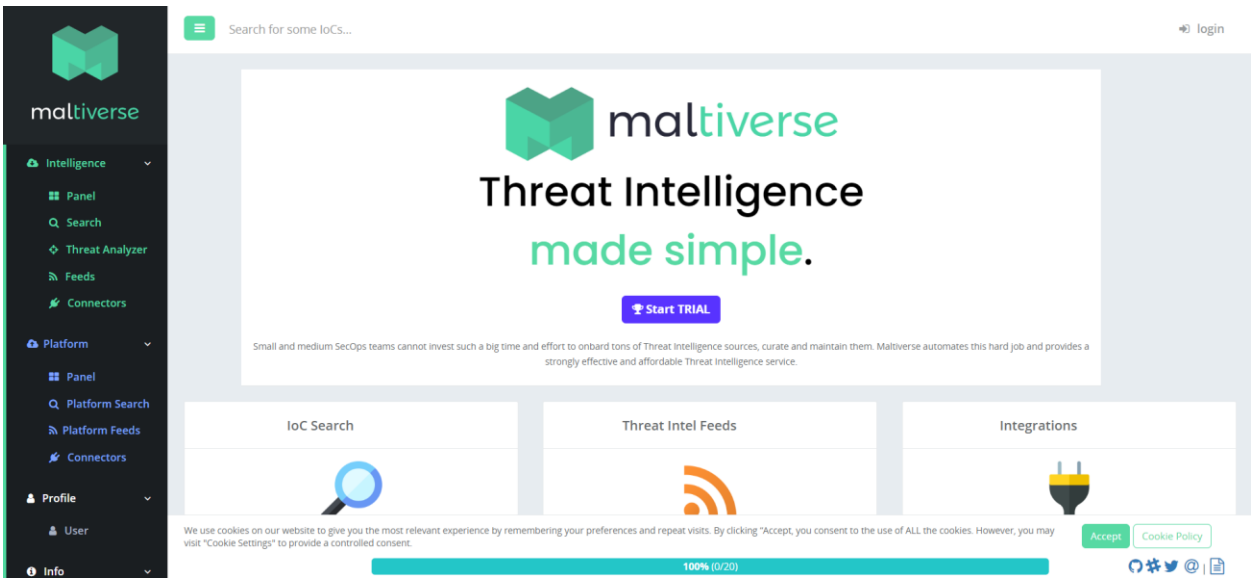
Cyber Security-Edge Program

Name: Afrin Faria ID: 2111270 Batch: B11

OSINT Framework: Threat Intelligence

1. Maltiverse:

Maltiverse is an open-source threat intelligence platform that collects and provides information on indicators of compromise (IOCs) such as domains, IP addresses, file hashes, and URLs. The platform aggregates threat data from various open sources and presents it in a centralized format for cybersecurity analysts to investigate and act on.



Key Features:

- IOC Lookup: Users can search for various IOCs (IP addresses, domains, file hashes) to see if they are associated with malicious activities.

- Threat Feeds: Maltiverse integrates multiple threat intelligence feeds, allowing security teams to identify known threats in real time.

- Crowdsourced Intelligence: It supports community contributions, allowing users to submit their own findings or corroborate threat reports.

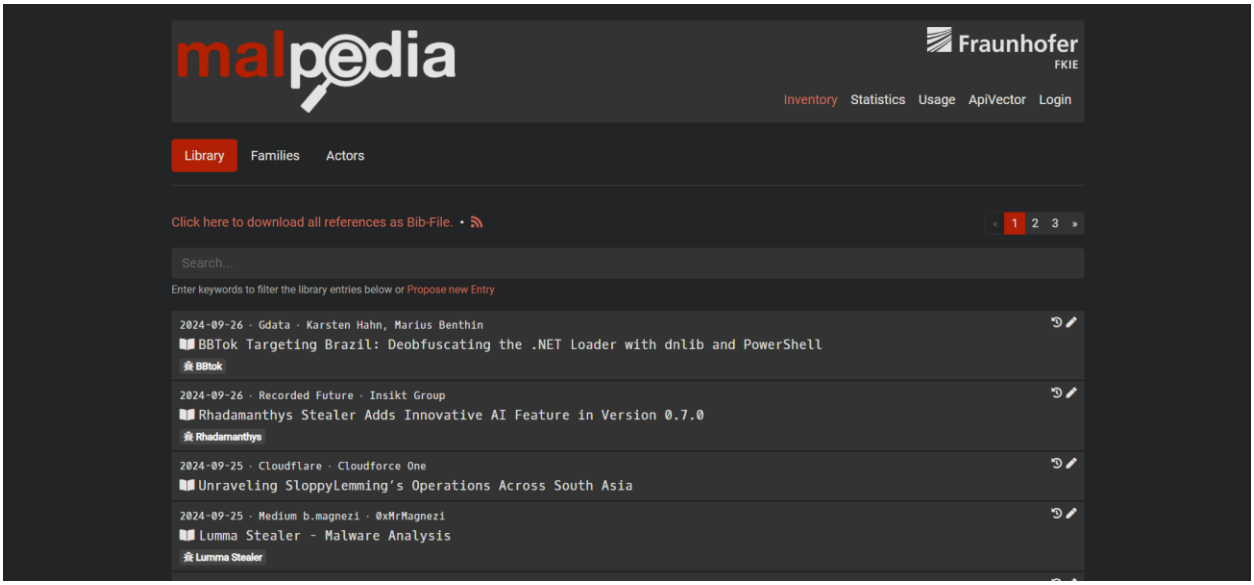
- API Access: Maltiverse offers APIs for easy integration into security operations and systems, enabling automated threat detection workflows.

Usage in Cybersecurity:

Security teams use Maltiverse to cross-check suspicious entities (IPs, domains, file hashes) and assess if they have been reported as involved in malicious activities. It provides contextual information to help decide whether to block or investigate further.

2. Malpedia:

Malpedia is a collaborative platform and wiki focused on the collection and classification of malware families. It provides extensive documentation on malware samples, their behavior, and associated threat actors. Security researchers and analysts contribute to Malpedia to help identify new strains of malware and update its repository with the latest information on existing malware.



Key Features:

-Malware Family Descriptions: Malpedia contains detailed information on hundreds of malware families, including their functionality, behavior, and techniques.

- YARA Rules: The platform provides YARA rules (pattern-matching rules used in malware detection) for many malware families, enabling analysts to integrate them into their detection tools.

- Collaborative Platform: It is a community-driven project, where malware researchers share their findings and updates on newly discovered malware or changes in known ones.

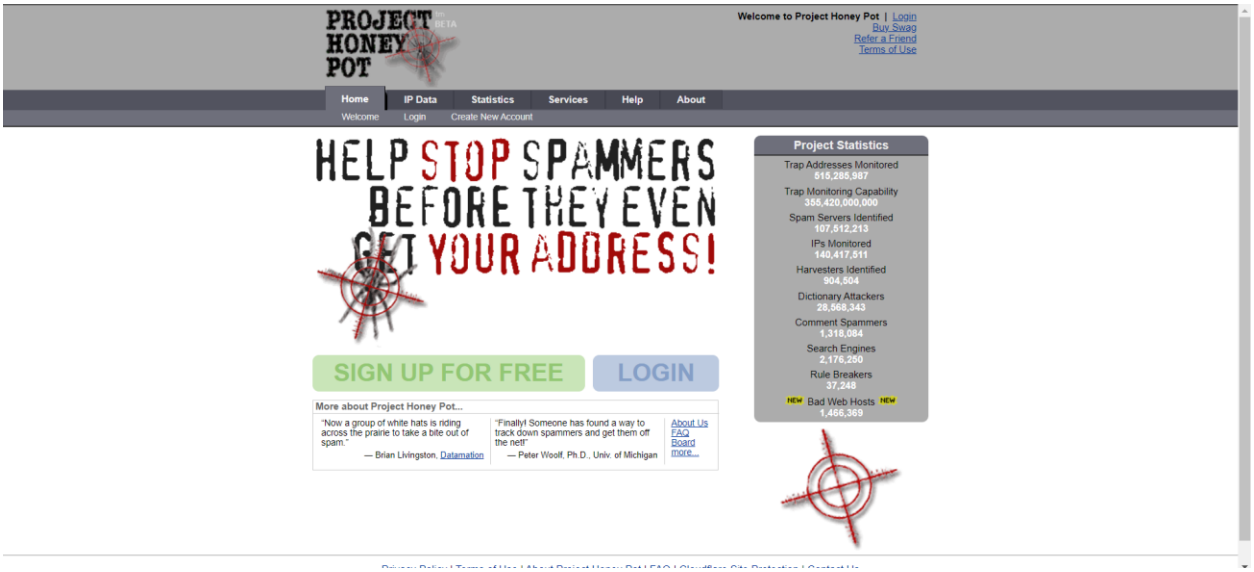
- Open Access: The platform is publicly accessible, which makes it a valuable resource for the cybersecurity community.

Usage in Cybersecurity:

Malpedia is used by malware analysts and security operations centers (SOCs) to investigate malware samples, understand their behavior, and create more accurate detection signatures. The YARA rules provided by Malpedia can also be used for hunting specific malware in an organization's environment.

3. Project Honey Pot:

Project Honey Pot is a community-driven initiative that tracks email harvesters, spambots, and other malicious actors by using honeypots (decoy servers or systems that attract malicious activity). It collects intelligence on spammers and bad bots that attempt to scrape email addresses or distribute spam.



Key Features:

- Email Harvester Tracking: Project Honey Pot deploys honeypots across the web to identify and track email harvesters, who collect email addresses for spam campaigns.

- Malicious IP Blacklisting: It maintains a database of IP addresses linked to spammers and malicious bots. Security professionals can use this data to block or monitor suspicious IPs.

- Spam Trap: Project Honey Pot uses spam trap addresses (fake email addresses created solely to attract spam) to collect intelligence on spamming activities and phishing campaigns.

- Collaborative Contribution: Website owners can participate by setting up honeypots on their sites to help track malicious actors.

Usage in Cybersecurity:

Security teams use Project Honey Pot's data to block known malicious IPs and detect potential phishing or spam attacks. The information is valuable for email service providers and security companies trying to filter out spam or prevent email-based attacks.