TECHNOLIMITS

01. SUMMARY

In today's digital age, cybersecurity has the highest importance. This document explores various methods and techniques for enhancing cybersecurity and conducting online investigations.
1. Data Recovery: Techniques for retrieving deleted posts from websites, providing valuable insights into recovering lost data.
2. OSINT (Open-Source Intelligence): An overview of OSINT, its application in cybersecurity, and methods for investigating websites and gathering public information from social media platforms. It emphasizes both technical and non-technical aspects, making OSINT accessible to a broader audience.
3. Breach Analysis: Investigating breach forums to identify hackers and analyse compromised data. This includes strategies for analysing databases to find critical information about breaches and threat actors.
4. Data Breach Awareness: Steps to determine if your data has been breached, using resources like https://breachdirectory.org. The document highlights that even hackers are not immune to data breaches, underscoring the universal vulnerability to such incidents.
5. OSINT in Cybersecurity: The vital role OSINT plays in strengthening cybersecurity measures, helping organizations and individuals protect against various threats.
This summary provides a comprehensive overview of the interconnected topics, illustrating the importance of cybersecurity practices and the practical application of OSINT in safe guarding digital information.

02. INTRODUCTION

In today's digital world, cybersecurity needs to be considered important. With everything online and attacks getting evolved, understanding how one protects and recover data becomes very crucial. This poster presents key aspects related to cybersecurity and online investigation techniques that will help keep all our information safe. Learn methods for recovering deleted posts from websites and understand how OSINT is used to gather and analyze public information. Even hackers are not safe to data breaches, proving vigilance is required across the board. Understand OSINT's role in enhancing cybersecurity and threat intelligence. Provide yourself with knowledge and tools necessary to protect your digital life as the world moves towards IT world. Stay informed, stay safe, and take control of your cybersecurity.

CONTENT

OSINT (Open-Source Intelligence): practice of collecting, evaluating, and analyzing publicly available information to answer specific intelligence questions

Technical Terms: Domain names, IP addresses, and other digital footprints.

Non-Technical Terms: Checking social media profiles, posts, and other publicly shared information. For example, exploring new friends' Instagram or TikTok profiles.

Hacker's Paradise - Breach Forum
Breach forums are online spaces where hackers discuss various hacking topics and share breached data. These forums are a hub for cybercriminal activity, but they are also monitored by threat intelligence professionals who aim to gather insights and mitigate potential threats

How to OSINT a Website
OSINT involves collecting and analyzing publicly available information. When investigating a website, the "identity" is typically represented by the domain name or IP address of the site. By gathering data on these elements, you can build a profile of the website's activities and affiliations

How to Retrieve Deleted Post from a Website
Through Wayback machine, users are able to access archived versios of websites from past. To retrieve deleted post, entering the words related to site's home page or copy the URL of home page of media social. The link of Wayback machine: https://web.archive.org/

OSINT in Cybersecurity
Tracking Cybercriminals: Identifying and monitoring cybercriminal groups or individuals.
Defensive Uses: Gathering threat intelligence by following security vulnerability discussions to stay ahead of potential threats.
Monitoring Stolen Data: Watching for stolen data being sold or shared, usually on the dark web.

03.

Data Breach Investigation
While data breaches commonly affect everyday users, it's important to remember that hackers themselves can also fall victim to these incidents. This dual vulnerability underscores the need for robust cybersecurity practices across the board

How to Find Out If Your Data Has Been Breached
To check if your data has been compromised, you can use resources like BreachDirectory.org. This platform allows you to search for your email address or other personal information to see if it has appeared in known data breaches

Sherlock Usage
Sherlock is a tool used for OSINT investigations, particularly for searching social media usernames across multiple platforms
For Searching One User: sherlock insert_username1
For Searching Multiple Users: sherlock insert_username1 insert_username2 insert_username3

REFLECTION

04.

Based on the OSINT Beginner's Guide on Computing Open Day & Exhibition 2025(CODE'25), we know that the need for continuous learning and awareness in cybersecurity. It is crucial to stay informed about the tools and techniques available for protecting digital assets as cyberattacks grow more complex. The digital world is both a space of opportunity and vulnerability depends on the way we use it. The use of OSINT and the ability to recover and analyse data empower individuals and organizations to take control of their cybersecurity. In a world increasingly reliant on technology, understanding and applying cybersecurity principles and OSINT techniques is essential.
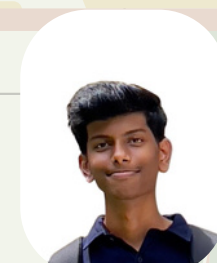
JOSHUA LING SHANG YANG
A24CS0089

FION TEE XIN YUE
A24CS5057

GAVENESH A/L BATUMALAI
A24CS0076

LIM ZOEY
A24CS5065